

Håndhævelse af ophavsrettigheder ved krænkelse begået på internettet

Copyright enforcement directed against infringements on the Internet

Indholdsfortegnelse

1	Indledning.....	1
1.1	Emne og baggrund.....	1
1.2	Problemformulering.....	2
1.3	Metode.....	2
1.4	Fremgangsmåde.....	3
1.5	Afgrænsning.....	4
1.6	Terminologi.....	5
2	Beskrivelse af tjenester og teknologier	6
2.1	Hjemmesider.....	6
2.2	Linking.....	6
2.3	Download og upload	8
2.4	Fildeling.....	8
2.5	Streaming og stream ripping	9
3	Håndhævelsesmuligheder	11
3.1	Fremskaffelse af beviser	12
3.1.1	<i>Udenretlig bevissikring</i>	<i>12</i>
3.1.2	<i>Indenretlig bevissikring</i>	<i>13</i>
3.2	Midlertidige afgørelser om forbud og påbud	19
3.3	Civile sager.....	21
3.3.1	<i>Økonomiske sanktioner</i>	<i>21</i>
3.3.2	<i>Forbud</i>	<i>23</i>
3.3.3	<i>Straf.....</i>	<i>23</i>
3.3.4	<i>Offentliggørelse af dom</i>	<i>23</i>
3.4	Straffesager.....	23
3.5	Breve til formodede krænkeres.....	24
3.6	Rettighedshaverorganisationer.....	25
4	E-handelsdirektivets og e-handelslovens ansvarsregler for formidlere.....	25
4.1	Ren videreformidling – EHD artikel 12 og EHL § 14.....	26
4.2	Caching – EHD artikel 13 og EHL § 15	27
4.3	Oplagring – EHD artikel 14 og EHL § 16.....	27
4.4	Foreløbige retsmidler over for formidlere.....	28
4.5	Overvågningsforbuddet	29
5	Aktører, som håndhævelsen kan rettes imod.....	29
5.1	Brugere	29
5.1.1	<i>Sporing og identifikation</i>	<i>30</i>
5.1.2	<i>Breve til formodede krænkeres.....</i>	<i>42</i>

5.1.3	<i>Civil retssag mod brugere</i>	45
5.2	Indholdsudbydere	51
5.2.1	<i>Civil retssag mod indholdsudbydere</i>	52
5.2.2	<i>Spærring eller lukning af ulovlige tjenester og hjemmesider</i>	54
5.3	Formidlere og mellemænd	56
5.3.1	<i>Internetudbydere</i>	57
5.3.2	<i>Tjenesteudbydere</i>	62
5.3.3	<i>Forbud eller påbud mod internet- eller tjenesteudbydere</i>	67
6	Konklusion	73
7	Engelsk resumé	76
8	Litteratur	78

Håndhævelse af ophavsrettigheder ved krænkelse begået på internettet

1 Indledning

1.1 Emne og baggrund

En af gevinsterne ved de seneste par årtiers udvikling i den digitale teknologi er de mange nye muligheder for at lytte til musik og se film på internettet, som er skabt, og som fortsat skabes. Er et værk ikke allerede født digitalt, kan det efterfølgende digitaliseres og spredes på internettet. Dermed kan den ophavsretlige eksemplar-fremstilling og tilgængeliggørelse af værker i dag ske uden et fysisk medium i form af f.eks. et bånd eller en disk. Bagsiden af medaljen er imidlertid, at også mulighederne for uretmæssig udnyttelse af ophavsretligt beskyttede værker er blevet større. Omfanget af krænkelse kan næppe dokumenteres, men det er utvivlsomt stort, og det samme er derfor problemet for rettighedshaverne.

Den ophavsretlige eneret er uafhængig af mediet, og ophavsmanden kan naturligvis gøre sin ret gældende over for krænkelse, som sker på internettet. Imidlertid har internettet også skabt udfordringer for håndhævelsen af ophavsrettigheder, for det kan være svært at opdage krænkelse, det er ikke altid klart, hvem krænkelse er, hvilken krænkelse de egentlig har begået, og hvordan det kan bevise. Desuden kan der være mange aktører involveret med forskellige roller – der er personen, som udvikler et fildelingsprogram og lægger det ud på internettet, der er brugeren ved computerskærmen, som henter og ser en film ved hjælp af programmet, og der er selskabet, som gør det hele muligt ved at levere internetforbindelse. Håndhævelse kan ske over for en eller flere af disse, og alt efter hvilken aktør den rettes imod, rejser forskellige problemer.

I forbindelse med håndhævelse af ophavsretten er der også modstående hensyn, som skal afvejes mod hinanden. Den danske retsorden beskytter både ejendomsretten – som blandt andet er ophavsretten – retten til privatlivets fred og retten til beskyttelse af personoplysninger. Det samme gør – inden for EU-rettens anvendelsesområde – Den Europæiske Unions charter om grundlæggende rettigheder.¹ Foruden flere andre grundlæggende rettigheder og friheder beskyttes også adgangen til effektive retsmidler,

¹ EFT 2000 C 364, s. 1. Herefter "charteret". Der henvises til artikel 7, 8 og 17.

så de sikrede rettigheder kan håndhæves. Men ophavsretten er ikke absolut, og ved dens håndhævelse er den således i konkurrence med andre hensyn.

Håndhævelsen har været i fokus, og sanktionssystemet og de processuelle muligheder er også blevet styrket. Alligevel er spørgsmålet, om håndhævelsen kan følge med udviklingen, om det er blevet for nemt at slippe af sted med krænkelse, og om øvrige grundlæggende rettigheder har vundet over ophavsretten.

1.2 Problemformulering

Det leder til det spørgsmål, som er dette speciales problem:

Er håndhævelsen af ophavsrettigheder ved krænkelse på internettet illusorisk?

Med udgangspunkt i ovenstående er det formålet med specialet at undersøge, hvilke praktiske, juridiske og processuelle udfordringer rettighedshaverne møder, i forhold til relevante aktører, når de vil håndhæve ophavsrettigheder, som er blevet krænkede på internettet, og på grundlag heraf vurdere rettighedshavernes aktuelle stilling.

1.3 Metode

Specialets metode er overordnet retsdogmatisk, idet det ved anvendelse af relevante retskilder søger først at fremstille eller afklare gældende ret på de områder, som har betydning for besvarelsen af specialets spørgsmål, og dernæst analysere den gældende rets betydning for håndhævelsen af ophavsretten ved krænkelse på internettet.

Et islæt af retssociologi vil indgå i enkelte af de afsnit, hvor der tages stilling til rettighedshavernes reelle muligheder for at håndhæve deres rettigheder. Med udgangspunkt i de svagheder ved håndhævelsen, set fra rettighedshavernes side, som er identificeret undervejs, inddrages i specialets konklusion endvidere nogle få og helt kortfattede retspolitiske overvejelser, som er alt andet end udtømmende, men blot et forsøg på at spille bolden op til diskussion.

Ophavsretten er et EU-retligt reguleret område, og specialet vil derfor inddrage EU-ret, herunder praksis fra EU-Domstolen. I enkelte tilfælde vil retspraksis fra andre lande blive behandlet, ikke som bidrag til fastlæggelsen af den danske retstilstand på et

område, men som illustration af problemstillinger, der også er aktuelle i Danmark, og som antydning af en udvikling, der måske kan blive det.

På nogle af de områder, som specialet behandler, er dansk retspraksis sparsom. EU-Domstolens praksis kan her supplere med fortolkninger. Når der på denne baggrund udledes resultater i specialet, vil der skulle tages hensyn til, at fortolkningen måske endnu ikke er set anvendt i dansk ret. På andre områder må der formodes at være praksis, men denne er i vidt omfang ikke trykt. Specialet vil her anvende omtale af praksis i litteraturen med det forbehold, at der er en vis usikkerhed forbundet med at basere sig på referater af kilder i stedet for på kilden selv.

1.4 Fremgangsmåde

Som baggrund for den videre behandling af specialets emne – og som eksempler på, hvor mangfoldige og raffinerede krænkelsesmulighederne er – beskrives i afsnit 2 nogle af de vigtigste tjenester og teknologier, som i dag typisk benyttes ved krænkelse på internettet, og det angives, hvori krænkelsen kan bestå. Eksempler på nye teknologier medtages til illustration af, hvordan ophavsretten hele tiden udfordres af udviklingen.

I afsnit 3 gives en kort beskrivelse af de håndhævelsesmuligheder, som rettighedshaverne kan tage i brug. Det indebærer henvisning til adskillige bestemmelser i retsplejeloven (RPL),² der hver især kunne give stof til en afhandling. Da reglerne i dette speciales sammenhæng tjener som baggrund for analysen af de problemer, som rettighedshaverne kan møde ved håndhævelsen af krænkelse på internettet, forekommer det dog rimeligt – og nødvendigt – at nøjes med en opsummering af retsstillingen. Der tilstræbes således ikke en detaljeret gennemgang af reglerne, men en beskrivelse, som medtager forhold, der må antages at kunne få praktisk betydning i forbindelse med specialets emne, og undlader andre forhold. Detaljer er altså udeladt ud fra et relevanskriterium, som til dels er subjektivt, men som dog bygger på specialets emne.

² Lovbkb. nr. 1257 af 13. oktober 2016.

For rettighedshaverne kan det være relevant at rette håndhævelsen mod internetudbydere. Da disse i mange tilfælde er fritaget for ansvar efter regler i e-handelsloven (EHL),³ beskrives – i afsnit 4 – de pågældende ansvarsfrihedsregler.

Endelig analyseres i afsnit 5 de konkrete problemer, som kan opstå i forbindelse med rettighedshavernes håndhævelse af deres ophavsrettigheder over for de enkelte aktører, hvorefter der rundes af med en konklusion i afsnit 6.

1.5 Afgrænsning

Ovenfor spørges til *håndhævelsen* – ikke *retshåndhævelsen*. Heri ligger blot, at specialet fokuserer på rettighedshavernes muligheder for at håndhæve deres rettigheder med eller uden de retshåndhævende myndigheders medvirken. Udgangspunktet ved besvarelsen af dette spørgsmål er dernæst, at en krænkelse har fundet sted, og det er derfor de bagudrettede og genoprettende foranstaltninger, som er i centrum. Derimod er det ikke hensigten at behandle mere fremadrettede tiltag, som rettighedshavere kan iværksætte for at forhindre krænkelse, f.eks. gennem oplysningskampagner eller anvendelse af tekniske foranstaltninger, der gør kopiering besværlig eller umulig.

Specialets udgangspunkt er, at der foreligger en krænkelse af en ophavsret, og derfor gennemgås de materielle ophavsretlige regler ikke, men det vil undervejs i fornødent omfang fremgå, hvilke krænkelse der begås af de forskellige aktører, som håndhævelsen kan rettes imod.

Internettet bruges ved mange forskellige ophavsretskrænkelser, men i dette speciale vedrører eksemplerne navnlig ulovlig udnyttelse af musik- og filmværker.

Da specialets fokus er rettighedshavernes håndhævelsesmuligheder, og udgangspunktet i ophavsretsloven (OHL)⁴ er, at krænkelse skal påtåles af den forurettede selv, jf. lovens § 81, stk. 1, er det fundet rimeligt ud fra et afgrænsningshensyn kun at behandle muligheden for betinget offentlig påtale kort og alene i det indledende afsnit om håndhævelsesmulighederne. Det betyder ikke, at mulighederne for at få krænkere idømt straf ved betinget offentlig påtale, eller det strafferetlige værn af immaterialrettigheder i

³ Lov nr. 227 af 22. april 2002 om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel.

⁴ Lovbkg. nr. 1144 af 23. oktober 2014 om ophavsret.

det hele taget, ikke er vigtige for rettighedshaverne i håndhævelsesmæssig henseende, men når først den private begæring om påtale er fremsat, er sagen så at sige ude af rettighedshavernes hænder og overladt til politi og anklagemyndighed. Med samme begrundelse er muligheden for offentlig omtale også kun omtalt kort.

Spørgsmål om jurisdiktion og lovvalg er af betydning for rettighedshavernes reelle muligheder for håndhævelse. Ved krænkelser på internettet – der jo kan siges at foregå overalt – er det f.eks. relevant, hvordan den specielle kompetenceregulering om stedet, hvor skadetilføjelsen er foregået,⁵ skal fortolkes. Kan sag efter denne regel kun anlægges i de lande, som en hjemmeside med ulovligt indhold er specifikt rettet imod, eller er det tilstrækkeligt, at hjemmesiden er tilgængelig? Og når sag er anlagt, kan erstatning så tilkendes for tab, som rettighedshaveren har lidt i flere lande, eller kun for tab, som han har lidt i det land, hvor sagen er anlagt? Inden for EU, og specifikt for ophavsret, er det korte svar på det første spørgsmål, at det er tilstrækkeligt, at hjemmesiden er tilgængelig, fordi der så vil kunne indtræde skade i det pågældende land, og på det andet spørgsmål, at der til gengæld kun kan tilkendes erstatning for den skade, der er lidt i dette land.⁶ Emnet rejser i øvrigt mange detailspørgsmål, men ud over disse hovedlinjer behandles jurisdiktion og lovvalg ikke i dette speciale.

1.6 Terminologi

I specialet anvendes ofte den specifikke betegnelse ophavsretskrænkelser, men også udtrykket pirateri vil blive brugt. Det anvendes i dag bredt om mange forskellige typer krænkelser, men navnlig om alle ophavsretlige krænkelser.⁷

Udtrykket rettighedshaver anvendes generelt om den, der er indehaver af en ophavsret. Det kan være ophavsmanden selv eller den, som har fået rettigheden overdraget, og det kan være en rettighedshaverorganisation.

⁵ Artikel 7, nr. 2, i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 af 12. december 2012 om retternes kompetence og om anerkendelse og fuldbyrdelse af retsafgørelser på det civil- og handelsretlige område (Bruxelles I-forordningen (2015)) (EUT 2012 L 351/1).

⁶ EU-Domstolens dom af 3. oktober 2013 i sag C-170/12, Pinckney, præmis 43-45. Senest bekræftet ved Domstolens dom af 21. december 2016 i sag C-618/15, Concurrence mod Samsung, præmis 30-31.

⁷ Jf. Andersen m.fl., *Retshåndhævelse af immaterialrettigheder*, 2006, s. 15-17.

I omtale af retspraksis er processuelle betegnelser for parterne for læsevenlighedens skyld ofte erstattet af betegnelser som ”den formodede krænker” og ”rettighedshaverne”.

2 Beskrivelse af tjenester og teknologier

Krænkelser af ophavsrettigheder på internettet kan begås ved hjælp af forskellige tjenester og teknologier, hvorved ophavsretligt beskyttet materiale kan downloades, deles eller distribueres. Nedenfor præsenteres de vigtigste sammen med en kort beskrivelse af, hvilke ophavsretlige enerettigheder der kan krænkes ved deres benyttelse.

2.1 Hjemmesider

Ophavsretligt beskyttede værker kan stilles til rådighed på en helt almindelig hjemmeside. Det blev allerede med Infosoc-direktivet ⁸ slået fast, at en sådan tilgængeliggørelse af værker på hjemmesider og i det hele taget via internettet er en offentlig fremførelse, som er omfattet af ophavsmandens eneret til tilgængeliggørelse,⁹ jf. OHL § 2, stk. 4, nr. 1. Hvis en anden end ophavsmanden eller rettighedshaveren, uden dennes samtykke, tilgængeliggør ophavsretligt beskyttet materiale på en hjemmeside, sker der derfor en krænkelse af denne eneret.

Hjemmesider, som tilgængeliggør ophavsretligt beskyttet materiale uden rettighedshaverens samtykke, rejser flere håndhævelsesproblemer. Kan udbyderen af hjemmesiden gøres ansvarlig? Kan hjemmesiden lukkes, og er det i givet fald effektivt? Disse spørgsmål behandles nedenfor i afsnit 5.2.1 og 5.2.2.

2.2 Linking

Der findes flere linktyper, og de adskiller sig fra hinanden ved at føre til forskellige steder på en hjemmeside og præsentere materialet, der linkes til, forskelligt. *Surface links* eller referencelinks fører til en hjemmesides forside eller hovedside. *Deep links* – også kaldet dybe links eller direkte links – fører til en underside eller filer, som befinder

⁸ Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (EFT 2001 L 167, s. 10).

⁹ OHL § 2, stk. 4, nr. 1, gennemfører artikel 3, stk. 1 i Infosoc-direktivet. Dette var muligvis retsstillingen allerede før direktivet, jf. Udsen: *IT-ret*, 2016, s. 73.

sig længere ned i hjemmesidehierarkiet. Ved både *surface links* og *deep links* føres den, der klikker på linket, over på den hjemmeside, der linkes *til*. Ved såkaldt *framing* trækkes materialet derimod over på den side, der linkes *fra*, hvor det fremstår som en integreret del af denne.¹⁰

Der har hersket tvivl om lovligheden af links i forhold til ophavsretten, men EU-Domstolen har opstillet en række kriterier. Af dommen i Svensson-sagen¹¹ følger det, at linking er en overføring til almenheden,¹² hvis overføringen retter sig mod et ”nyt publikum”, hvilket vil sige ”et publikum, som indehaverne af ophavsrettigheden ikke havde taget i betragtning, da de tillod den første overføring til almenheden”.¹³ Hvis materiale på en hjemmeside er frit tilgængeligt for alle, kan der derfor lovligt linkes til det, fordi publikum i denne situation ikke kan være nyt. Hvis materialet *ikke* er frit tilgængeligt, men f.eks. passwordbeskyttet og kun til rådighed for abonnenter, og linket omgår en sådan – eller en anden – ”restriktiv foranstaltning”,¹⁴ vil alle andre end abonnenterne være et nyt publikum. Linkingen vil her udgøre en ophavsretskrænkelse i form af overføring til almenheden uden rettighedshaverens samtykke.

Det har været antaget i litteraturen, at det samme må gælde, hvis der linkes til materiale, som er tilgængeliggjort på internettet *uden* rettighedshaverens samtykke, altså piratkopieret materiale, idet *ethvert* publikum her er nyt.¹⁵ Svensson-sagen omhandlede imidlertid ikke denne situation, og EU-Domstolen har i sin senere dom i GS Media-sagen¹⁶ bekræftet, at Svensson-kriteriet om ”nyt publikum” kun gælder i forhold til værker, der er blevet gjort frit tilgængelige *med* indehaverens samtykke.¹⁷ Hvad angår linking til værker, der er tilgængeliggjort på internettet *uden* indehaverens samtykke, udtaler Domstolen herefter, at der skal foretages en individualiseret vurdering af, om der foreligger en overføring til almenheden¹⁸. I denne vurdering indgår det, om linket er oprettet med vinding for øje. Almindelige internetbrugere, som ikke har vinding for øje, må formodes ikke at have viden eller burde viden om det ulovlige i

¹⁰ Se for flere detaljer f.eks. Udsen: *IT-ret*, 2016, s. 75-76, Jakobsen og Schaumburg-Müller, *Medieretten*, 2013, s. 808-809, og Trzaskowski (red.): *Internetretten*, 2012, s. 476-477.

¹¹ Domstolens dom af 13. februar 2014 i sag C-466/12.

¹² Som omhandlet i OHL § 2, stk. 4, nr. 1.

¹³ Op.cit., fodnote 11, præmis 24.

¹⁴ Op.cit., fodnote 11, præmis 31.

¹⁵ Udsen: *IT-ret*, 2016, s. 79.

¹⁶ Domstolens dom af 8. september 2016 i sag C-160/15.

¹⁷ Ibid., præmis 41 og 43.

¹⁸ Præmis 33 og 47.

tilgængeliggørelsen.¹⁹ Derimod må en person, som har vinding for øje, forventes at foretage den nødvendige kontrol af lovligheden af materialet, før der linkes til det, og ved linking til ulovligt materiale gælder der derfor her en formodning om viden.²⁰ Udgangspunktet er herefter, at almindelige, private internetbrugere ikke krænker ophavsrettigheder ved at linke til piratkopieret materiale, mens brugere med vinding for øje gør det.

2.3 Download og upload

Ved download henter en bruger med en internetforbindelse et værk i form af en digital fil på internettet, typisk tekst, musik eller film. Når værket er downloadet i traditionel, permanent forstand, findes en kopi på brugerens computer, så værket også kan benyttes, når brugeren er offline. Der sker derfor en eksemplarfremsstilling, jf. OHL § 2, stk. 2. Værker kan downloades lovligt fra en lang række tjenester, f.eks. iTunes, og ulovligt fra mindst lige så mange.

Ved upload kopieres den digitale fil fra brugerens computer til en anden computer eller server, så andre får adgang til den. Upload er derfor som udgangspunkt en grovere krænkelse end download, fordi der både sker en eksemplarfremsstilling og en tilgængeliggørelse for almenheden i form af offentlig fremførelse, jf. OHL § 2, stk. 4, nr. 1.

Download kan betragtes som et overbegreb til forskellige teknologier, som kan benyttes til at hente filer fra internettet, f.eks. fildeling og streaming, jf. straks nedenfor.

2.4 Fildeling

Ved fildeling tænkes her på den deling af digitalt indhold, som kan ske via internettet.²¹ Brugeren har installeret et program på sin computer, hvorigennem der kan udveksles filer med andre brugere, der også har installeret programmet. Brugerne foretager tilgængeliggørelse for almenheden i form af offentlig fremførelse. Når materialet downloades, sker der desuden en eksemplarfremsstilling.

¹⁹ Præmis 47.

²⁰ Præmis 51.

²¹ For en kort beskrivelse af fildeling, se Udsen: *IT-ret*, 2016, s. 251-252, og en lidt længere Jakobsen og Schaumburg-Müller, *Medieretten*, 2013, s. 806-808.

Delingen kan involvere en mellemmand, som udvikler og udbyder fildelingsprogrammet, opretter søgbare lister over de tilgængelige filer, etablerer kontakten mellem brugerne og lader delingen af de ønskede filer ske gennem sit system, således at der herved lagres en midlertidig kopi i dette. Den midlertidige lagring vil være en eksemplarfremsstilling, men der sker også en tilgængeliggørelse for almenheden.

Den teknologiske udvikling har dog gjort fildeling mulig uden lagring af en midlertidig kopi i udbyderens system og nu endda helt uden direkte at involvere en mellemmand. For rettighedshaverne gør det ikke håndhævelsen nemmere, hvis udbyderen eller mellemmanden er så perifert involveret, at han ikke pådrager sig et ansvar. Dette behandles nedenfor i afsnit 5.2.1 i forbindelse med medvirkensansvar for systemudviklere. Dog vil der naturligvis fortsat være en internetudbyder involveret. Denne er næppe selv ansvarlig, men har muligheden for at stoppe krænkelsen ved at spærre for adgangen til fildelingstjenesten. Muligheden for at få nedlagt et foreløbigt forbud og problemerne i forbindelse hermed behandles i afsnit 5.3.3.

Ved fildeling benyttes i dag ofte en teknologi, som kaldes *bittorrent*. Den indebærer, at en bruger downloader og deler filer fra og på et netværk ved hjælp af et program, som henter mange små *bits* af filen fra forskellige andre brugere af programmet og samler dem til én hel fil, f.eks. en film, på den første brugers computer, uden at en central server er involveret. Brugere kaldes *peers*, og man taler derfor om *peer-to-peer*-netværk eller P2P-netværk.²²

2.5 Streaming og stream ripping

Ved streaming af f.eks. musik og film sker overføringen fra udbyder til bruger ved, at små pakker af data svarende til små dele af værket overføres i en kontinuerlig strøm – deraf navnet streaming – uden at der lagres en permanent kopi af det streamede værk på brugerens computer. De enkelte små dele af værket lagres kun kortvarigt i computerens cache eller ram, hvor de efterfølgende slettes automatisk. Ved streaming *on demand* vælger brugeren selv, hvornår værket skal afspilles, hvorimod der ved live streaming – som navnet antyder – sendes direkte, f.eks. fra en fodboldkamp.

²² Jf. Nielsen og Jakobsen: *E-handelsret*, 2011, s. 436. Generaladvokat Szpunar beskriver mere detaljeret, hvordan et *peer-to-peer*-netværk fungerer, i sit forslag til afgørelse af 8. februar 2017 i sag C-610/15, Stichting Brein, punkt 19-27.

Ved streaming *on demand* sker der hos *udbyderen* en eksemplarfremsstilling. Ved begge former for streaming sker der desuden en overføring til almenheden, som hvad angår live streaming nærmere bestemt er omfattet af OHL § 2, stk. 4, nr. 1, første led, og hvad angår streaming *on demand* er omfattet af samme bestemmelses andet led om tilrådighedsstillelse.²³

Hos *brugeren* sker der ved streaming en midlertidig lagring af værket i computerens ram eller cache.²⁴ Denne midlertidige eksemplarfremsstilling vil som udgangspunkt være tilladt efter undtagelsen i OHL § 11 a, stk. 1, men hvis der er tale om streaming af ulovligt tilgængeliggjort materiale, vil der ikke være tale om ”lovlig brug af et værk” som omhandlet i bestemmelsen. Dog må det bemærkes, at nogle ulovlige streamingtjenester i dag benytter den ovenfor nævnte *bittorrent*-teknologi. Det betyder, at brugeren automatisk også *deler* små *bits* af f.eks. en film fra sin egen computer, og at han derfor – selv om han ikke aktivt uploader – foretager tilgængeliggørelse i form af overføring til almenheden.

EU-Domstolen har for nylig fastslået, at det også er overføring til almenheden at sælge en medieafspiller med præinstallerede add-ons indeholdende links, der henviser til både lovlige og ulovlige streamingtjenester, og som ved et enkelt klik henter det ønskede indhold og afspiller det på en forbundet tv-skærm.²⁵

Ved en særlig form for streaming er det nu også muligt at streame ulovligt fra lovlige musik- og filmstreamingtjenester som Spotify og Netflix. Teknologien kaldes *stream ripping*.²⁶ Den kræver et værktøj, som også findes i form af apps, og som kan hentes på *stream ripping*-platforme. I modsætning til traditionel streaming fra lovlige eller ulovlige tjenester foretages der her download af en permanent kopi af værket. Brugeren foretager derfor en eksemplarfremsstilling. På *stream ripping*-platformen sker der ikke hverken eksemplarfremsstilling eller tilgængeliggørelse, eftersom værkerne ikke findes eller deles på selve platformen – den udbyder blot et værktøj. Dermed opstår også her

²³ Jf. Schønning: *Ophavsretsloven med kommentarer*, 2016, s. 193-194, og Schovsbo m.fl.: *Immaterialret*, 2015, s. 164.

²⁴ Jf. Schønning: *Ophavsretsloven med kommentarer*, 2016, s. 267.

²⁵ Dom af 26. april 2017, sag C-527/17, Stichting Brein, præmis 17 og domskonklusionen.

²⁶ For en beskrivelse se Terrica Carrington: ”*Stream-Ripping*” *A Growing Threat to the Music Industry*, copyrightalliance.org, 10. november 2016.

spørgsmål vedrørende medvirkensansvar som foreløbigt omtalt ovenfor vedrørende fildeling.

3 Håndhævelsesmuligheder

I takt med at den teknologiske udvikling har åbnet nye døre til ulovlig udnyttelse af ophavsretligt beskyttede værker, er der naturligvis også opstået ønsker om og behov for at lukke dem igen. På ophavsrettens område er håndhævelsesmulighederne da også blevet styrket. Allerede i WTO's TRIPS-aftale²⁷ del III er der opstillet minimumskrav til retshåndhævelsen af immaterialrettigheder, og de kommer i EU blandt andet til udtryk i Infosoc-direktivet og retshåndhævelsesdirektivet.²⁸

Infosoc-direktivets artikel 8 om sanktioner og retsmidler indeholder således i stk. 1 det generelle princip for retshåndhævelsen, at sanktionerne skal være effektive, stå i et rimeligt forhold til krænkelsen og være afskrækkende. Retshåndhævelsesdirektivet indeholder i artikel 3 et tilsvarende princip og bestemmer yderligere, at foranstaltninger, procedurer og retsmidler til håndhævelse af rettighederne skal være fair og rimelige, og at de ikke må være unødigt komplicerede eller udgiftskrævende, indebære urimelige frister eller medføre ugrundede forsinkelser.

Ved håndhævelsen er der imidlertid også andre hensyn at tage, og i denne forbindelse henviser retshåndhævelsesdirektivet i betragtning 32 til de grundlæggende rettigheder, som charteret beskytter, og i artikel 2, stk. 3, litra a), specifikt til beskyttelsen af personoplysninger.²⁹

I det følgende gennemgås de vigtigste håndhævelsesmuligheder, som kan bringes i anvendelse over for ophavsretskrænkelser. Afsnittet er struktureret således, at det først beskriver nogle indledende skridt, som rettighedshaveren kan tage for at konstatere krænkelsen, herefter gennemgås de retligt definerede beføjelser, som kan hjælpe rettighedshaveren videre fra selve konstateringen af krænkelsen, og endelig medtages

²⁷ Trade Related Aspects of Intellectual Property Rights, tilgængelig på www.wto.org.

²⁸ Europa-Parlamentets og Rådets direktiv 2004/48/EF af 29. april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder (EUT 2004 nr. L 157, s. 45).

²⁹ Det bemærkes, at EU-Domstolen vægter persondataskyddelsen særdeles højt, jf. f.eks. dommen af 21. december 2016 i de forenede sager C-203/15 og C-698/15, Tele2 Sverige, hvori Domstolen udtaler, at undtagelser og begrænsninger vedrørende personoplysninger skal "holdes inden for det strengt nødvendige" (præmis 96).

nogle fremgangsmåder, som rettighedshaverne i praksis kan benytte ved håndhævelsen.

3.1 Fremskaffelse af beviser

Når ophavsrettigheder skal håndhæves, er det naturligvis afgørende at kunne dokumentere de formodede krænkelse, deres omfang, og hvem der har foretaget dem. Ved krænkelse begået via internettet kan det blive et praktisk problem, at teknologien giver gode muligheder for at skjule krænkelse og slette spor via værktøjer, som især mere professionelle krænkere udnytter. Da de fleste sager om ophavsretskrænkelser formentlig føres som civile sager, er det i første omgang rettighedshaveren selv, der må sørge for at fremskaffe beviserne.

Ved selve konstateringen af krænkelsen kan der tages indledende skridt, som ikke involverer retten – såkaldt udenretlig bevissikring. I afsnittet nedenfor følger ikke en udtømmende opregning af mulighederne, men alene en omtale af nogle bevissikringsskridt, som er særligt relevante i relation til ophavsretskrænkelser på internettet. I afsnittet om indenretlig bevissikring redegøres der dernæst kort for en række relevante bestemmelser i retsplejeloven, som kan lette rettighedshaverens fremskaffelse af beviser med rettens hjælp.

3.1.1 Udenretlig bevissikring

Den udenretlige bevissikring kan tilvejebringe grundlaget for den videre retsforfølgning. Afhængigt af hvilke retsskridt der senere ønskes iværksat, kan der være behov for et egentligt bevis eller blot en sandsynliggørelse af, at en krænkelse har fundet sted. Under alle omstændigheder vil bevissikringen skulle respektere lovgivningens grænser, og i relation til krænkelse på internettet kan f.eks. beskyttelsen af personoplysninger komme i spil.

3.1.1.1 IP-adresser

Et første skridt i retning af at konstatere en ophavsretskrænkelser på internettet kan være at identificere de IP-adresser, som har været anvendt ved en krænkelse. Der findes specialudviklet software, som kan spore sådanne IP-adresser og generere lister over IP-adresser, som har været benyttet ved f.eks. ulovlig deling og download af

ophavsretskrænkende materiale.³⁰ Dette afslører dog ikke navnet bag IP-adressen – i hvert fald ikke direkte. IP-adresser kan ganske vist slås op i databaser, men disse angiver blot den internetudbyder, som har adressen i sin pulje. Som det er beskrevet nærmere nedenfor i afsnit 5.1.1.1, er IP-adresser personoplysninger, og internetudbyderen vil derfor ikke umiddelbart udlevere oplysningerne. Herfra vil rettighedshaveren derfor have brug for rettens bistand i form af en dommerkendelse, og listen over IP-adresser kan i denne forbindelse formentlig tjene til opfyldelse af et krav om sandsynliggørelse af, at en krænkelse er begået.

3.1.1.2 Skærmpoint

En rettighedshaver, som observerer en hjemmeside med ophavsretskrænkende materiale, kan dokumentere sin observation med et simpelt skærmpoint. Dette giver et øjebliksbillede, men der findes også tjenester, som kan gengive, hvordan en hjemmeside tidligere har set ud.³¹ Der er taget stilling til bevisværdien af skærmpoints i retspraksis, som kan sammenfattes således, at skærmpoints – naturligvis – kan påberåbes som bevis og kan tjene som bevis, men at omstændighederne, hvorunder de er lavet, har betydning for vurderingen.³² Skærmpoints bør derfor om muligt understøttes af andre beviser, men til opfyldelse af et krav om sandsynliggørelse må de antages at være tilstrækkelige i sig selv.³³

3.1.2 Indenretlig bevissikring

I det følgende redegøres der kort for retsplejelovens regler om bevissikring, oplysningspligt, editionspligt og isoleret bevisoptagelse.

3.1.2.1 Bevissikring

De ovenfor nævnte bevisproblemer – og lignende bevisproblemer i andre grene af immaterialretten – er baggrunden for bestemmelserne i RPL kapitel 57 a om

³⁰ F.eks. programmet DCAGENT, som var blevet anvendt i U 2011.1736 H, omtalt nedenfor i afsnit 5.1.3.

³¹ F.eks. <https://archive.org>.

³² Jf. sammenfatning af retspraksis i Andersen m.fl.: *Retshåndhævelse af immaterialrettigheder*, 2006, s. 174-176.

³³ Ibid., s. 175-176.

bevissikring.³⁴ Efter reglerne i dette kapitel kan fogedretten efter anmodning fra rekvirenten, som kan være en rettighedshaver eller en anden påtalebeføjjet, foretage en undersøgelse hos en anden (rekvisitus) for at sikre bevis for kränkelsen og dens omfang, jf. lovens § 653, stk. 1. I RPL § 653, stk. 2, opregnes udtømmende de rettigheder, som er omfattet af bevissikringsreglerne. Det er blandt andet både de egentlige ophavsrettigheder og de nærtstående rettigheder.³⁵

Efter bestemmelsen skal rekvirenten *sandsynliggøre*, at rekvisitus har begået eller vil begå en relevant krænkelse, og der skal være grund til at antage, at bevis herfor kan findes i de lokaler, der ønskes undersøgt.

En bevisundersøgelse er en indgribende foranstaltning, som krænker privatlivets fred. Derfor opfyldes sandsynliggørelseskravet ifølge den bagvedliggende betænkning ved ”en væsentligt underbygget formodning”.³⁶ Heri ligger ifølge betænkningen et strengere krav end det, at noget ”med rimelighed kan antages”. På den anden side kræves naturligvis ikke et egentligt bevis for en krænkelse. Kravet er i øvrigt det samme som ved midlertidige afgørelser om forbud og påbud efter RPL kapitel 40, jf. afsnit 3.2 nedenfor.

Det er tilstrækkeligt, at der er tale om en krænkelse i objektiv forstand, dvs. at det ikke skal sandsynliggøres, at der er grundlag for at pålægge krænkeren strafansvar eller erstatningsansvar.³⁷

Undersøgelsen kan ifølge RPL § 653, stk. 3, omfatte alt materiale af betydning for at konstatere kränkelsen og dens omfang, herunder ”oplysninger på edb-anlæg, edb-programmer og elektroniske lagringsmidler”.

RPL § 653, stk. 4, indeholder en proportionalitetsbestemmelse, hvorefter fogedretten skal foretage en vurdering af, om en undersøgelse ”under hensyn til privatlivets fred, erhvervshemmeligheder eller i øvrigt [...] vil påføre rekvisitus skade eller ulempe, som står i misforhold til rettighedshaverens interesse i undersøgelsens gennemførelse”. I

³⁴ Kapitlet er indsat i retsplejeloven ved lov nr. 216 af 28. marts 2001 på baggrund af betænkning nr. 1385/2000. De nye regler skulle bl.a. ”fjerne enhver tvivl om, hvorvidt Danmark på dette punkt [levede] op til TRIPS-aftalens krav”, jf. s. 8 i betænkningen.

³⁵ Jf. for en nærmere gennemgang Andersen m.fl.: *Retshåndhævelse af immaterialrettigheder*, 2006, s. 346-347.

³⁶ Betænkning nr. 1385/2000, s. 65.

³⁷ Ibid., s. 65.

modsætning til det proportionalitetsprincip, som gælder i forbindelse med nedlæggelse af midlertidige afgørelser om forbud og påbud, behøver misforholdet ikke at være åbenbart.³⁸

Ud fra ikke mindst en ophavsretlig synsvinkel har det interesse, at der i bestemmelsen tidligere var formuleret et udtrykkeligt krav om, at den pågældende krænkelse skulle være begået ”som led i erhvervsvirksomhed eller i øvrigt i ikke ubetydeligt omfang”. Dette krav udgik dog af RPL § 653 ved implementeringen af retshåndhævelsesdirektivet i 2005, men det betyder ikke, at der nu kan foretages undersøgelser i private hjem uanset omfanget af krænkelsen. I bemærkningerne til lovforslaget anføres, at en bevissikringsundersøgelse ved krænkelse af ubetydeligt omfang ”efter omstændighederne [vil] kunne nægtes efter en konkret interesseafvejning”, at dette ikke mindst gælder, ”når undersøgelsen begæres foretaget i et privat hjem”, og at ”integritetshensyn i reglen vil veje tungere, når der begæres undersøgelse i et privat hjem”.³⁹ Den obligatoriske interesseafvejning – som foretages efter proportionalitetsbestemmelsen i RPL § 653, stk. 4, og som omfatter hensyn til privatlivets fred – indebærer således i realiteten, at adgangen til at gennemføre bevissikringsundersøgelser i private hjem ikke er blevet udvidet, hvilket heller ikke har været hensigten.⁴⁰

Ved indsættelse af ordene ”eller vil begå en sådan krænkelse” i § 653, stk. 1, medførte gennemførelsen af retshåndhævelsesdirektivet også den ændring, at reglerne blev gjort anvendelige på fremtidige krænkelse.

Lovens udgangspunkt for forløbet af bevissikringsundersøgelsen er forudgående underretning, men denne kan undlades, hvis der må antages at være risiko for, at det materiale, som er genstand for undersøgelsen, ”fjernes, tilintetgøres eller ændres”, jf. RPL § 653 a, stk. 2, 2. pkt. Ved f.eks. ulovlig download fra internettet af ophavsretligt beskyttet materiale vil en sådan risiko oftest kunne antages at foreligge, og i sådanne og mange lignende tilfælde vedrørende krænkelse på internettet vil det derfor være muligt

³⁸ Ibid., s. 67.

³⁹ Jf. lovforslag L 67: Forslag til lov om ændring af retsplejeloven (Gennemførelse af EU-regler om håndhævelse af immaterialrettigheder mv.), fremsat den 16. november 2005, bemærkningerne til § 653, stk. 1. Forslaget blev vedtaget ved lov nr. 279 af 5. april 2006 om ændring af retsplejeloven, der trådte i kraft den 15. april 2006.

⁴⁰ Jf. de almindelige bemærkninger til lovforslaget, punkt 4.2.2.

at gennemføre undersøgelsen uden forudgående underretning. Det fremgår i øvrigt af forarbejderne, at betingelsen ofte vil være opfyldt.⁴¹

Fogedretten kan i forbindelse med undersøgelsen beslaglægge genstande eller dokumenter, og materiale kan fotograferes og kopieres, jf. RPL § 653 b, stk. 1, 2. pkt. Undersøgelsen kan også gennemføres tvangsmæssigt, jf. § 653 b, stk. 6.

3.1.2.2 Oplysningspligt

Ved implementeringen af retshåndhævelsesdirektivet blev der også indsat et kapitel 29 a i retsplejeloven om oplysningspligt i *verserende sager* om krænkelse af immaterialrettigheder,⁴² hvor det må lægges til grund, at der forligger en krænkelse.⁴³ Reglerne i kapitlet gennemfører retshåndhævelsesdirektivets artikel 8 og supplerer bevissikringsreglerne ved at give rettighedshaveren eller en anden påtalebeføjet part mulighed for at få retten til at pålægge en modpart eller tredjemand at give visse oplysninger om de krænkende varer eller tjenesteydelser, jf. RPL § 306, stk. 1 og 2.

Informationspålægget kan gennemtvinges ved tvang efter RPL § 178, både over for en modpart og en tredjemand, jf. RPL § 306, stk. 5.

Den modpart eller tredjemand, som informationspålægget rettes imod, skal naturligvis råde over de pågældende oplysninger, jf. § 306, stk. 1. Der skal være tale om en person, der *som led i erhvervsvirksomhed* er fundet i besiddelse af, i færd med at anvende eller i færd med at yde de krænkende varer eller ydelser, jf. RPL § 306, stk. 1, nr. 1-3, eller en person, som ifølge personer omfattet af nr. 1-3, har medvirket til produktion, fremstilling, distribution eller levering af de krænkende varer eller ydelser, jf. RPL § 306, stk. 1, nr. 4. I lovforslaget anføres det, at foranstaltningerne ifølge betragtning 14 til retshåndhævelsesdirektivet ”kun skal være obligatoriske i forbindelse med handlinger, der udføres i kommerciel målestok”, hvorved forstås ”handling, der udføres med henblik på direkte eller indirekte økonomisk eller kommerciel gevinst”.⁴⁴ Lovgiver synes således ikke at have udnyttet adgangen efter direktivet til også at anvende foranstaltningerne i forbindelse med andre handlinger. Dermed kan en

⁴¹ Jf. svar fra justitsministeren på spørgsmål 20 til lovforslaget.

⁴² Vedtaget ved lov nr. 279 af 5. april 2006, jf. fodnote 39 ovenfor.

⁴³ Jf. bemærkningerne til § 306 i L 67, op.cit., fodnote 39. Krænkelsesspørgsmålet kan eventuelt afgøres forlods efter RPL § 253.

⁴⁴ Jf. L 67, op.cit. fodnote 39, de almindelige bemærkninger til lovforslaget, punkt 4.3.1.

forbruger, som i god tro har streamet et ophavsretligt beskyttet filmværk uden rettighedshaverens samtykke, *ikke* pålægges en oplysningspligt, fordi han hverken besidder produktet som led i erhvervsvirksomhed eller har medvirket til dets produktion, fremstilling eller distribution.

Reglerne giver heller ikke hjemmel til at pålægge internetudbydere at oplyse navne og adresser på private indehavere af IP-adresser, idet sådanne oplysninger ikke er omfattet af opregningen i RPL § 306, stk. 2.

Muligheden for at pålægge oplysningspligt er begrænset af en almindelig proportionalitetsgrundsætning i RPL § 306, stk. 3, der bestemmer, at retten skal afslå en anmodning om informationspålæg, hvis dets gennemførelse vil medføre ”skade eller ulempe, som står i misforhold til den anmodende parts interesse i oplysningerne”.

Derudover gælder et forbud mod selvinkriminering, idet der i RPL § 306, stk. 4, henvises til blandt andet § 171. Det betyder konkret, at en part, som er indehaver af en internetforbindelse, som har været brugt til f.eks. ulovlig deling af musikfiler, ikke kan pålægges oplysningspligt, hvis opfyldelsen heraf vil kunne udsætte den pågældende selv eller hans nærmeste for straf mv. Endelig skal reglerne i persondataloven (PDL)⁴⁵ naturligvis overholdes.

3.1.2.3 Editionspligt og isoleret bevisoptagelse

De almindelige regler om parts- eller tredjemandsedition i RPL kapitel 28 finder også anvendelse i immaterialretlige sager.⁴⁶ Efter disse regler kan retten efter begæring fra en part pålægge modparten eller en tredjemand at fremlægge eller udlevere dokumenter, der er undergivet deres rådighed, og som har betydning for sagen, jf. RPL §§ 298 og 299. Også her gælder et forbud mod selvinkriminering mv., jf. § 298, stk. 1, og § 299, stk. 1. Til forskel fra reglerne om oplysningspligt kan det – hvis en *modpart* ikke efterkommer et editionspålæg – dog kun medføre processuel skadevirkning, jf. § 298, stk. 2. I forhold til tredjemand kan et editionspålæg godt gennemføres ved tvang, jf. § 299, stk. 2, idet editionsreglerne her svarer til tredjemands vidnepligt.

⁴⁵ Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.

⁴⁶ I forbindelse med gennemførelsen af retshåndhævelsesdirektivet fandtes retsplejelovens editionsregler at opfylde forpligtelserne i direktivet vedrørende edition, jf. de almindelige bemærkninger til lovforslaget, punkt 4.1., og retsplejeloven blev derfor ikke ændret på dette punkt.

Tredjemandseditionsreglen indebærer, at en part i en *verserende retssag* kan få retten til at pålægge f.eks. en internetudbyder – som ikke selv har begået eller medvirket til en ophavsretskrænkelser, men blot har stillet en internetforbindelse til rådighed – at give oplysninger om indehaverne af IP-adresser, som har været anvendt til krænkelser på internettet. Efter RPL § 343 om isoleret bevisoptagelse kan der også ”optages bevis, selv om dette ikke sker til brug for en verserende retssag”. I bestemmelsens stk. 1, 2. pkt. om stedlig kompetence nævnes dog kun vidner samt syn og skøn, men det er anerkendt i retspraksis, at bestemmelsen også omfatter edition, og at tredjemand således kan pålægges editionspligt med henblik på at undersøge, hvem der kan sagsøges.⁴⁷ Det sker da normalt ved en kombination af tredjemandseditionsreglen i § 299 og reglen om isoleret bevisoptagelse i § 343. Modparten er i situationen her ukendt på tidspunktet for bevisoptagelsen. I denne forbindelse er det af betydning, at det følger af henvisningen i RPL § 343, stk. 4, til bestemmelsen i § 340, stk. 2, 1. og 2. pkt., at modparten skal underrettes om bevisførelsen på forhånd, men at retten i ”påtrængende tilfælde” kan gøre undtagelse herfra og evt. beskikke en advokat til at varetage modpartens interesser. I afsnit 5.1.1 nedenfor analyseres anvendelsen af ovennævnte bestemmelser konkret i forhold til internetudbydere og IP-adresser.

Ifølge forarbejderne kan isoleret bevisoptagelse efter retsplejelovens bestemmelser foretages, ”når retten finder det hensigtsmæssigt”.⁴⁸ Denne formulering lægger op til et betydeligt skøn og en bred adgang, og editionsreglen og reglen om isoleret bevisoptagelse kræver heller ikke udtrykkeligt hensyntagen til hverken grundlæggende rettigheder eller proportionalitetsprincippet. Det følger dog af EU-Domstolens praksis, at der i relation til ophavsretskrænkelser på internettet, hvor navne bag IP-adresser ønskes oplyst, vil skulle tages hensyn til proportionalitetsprincippet og foretages en passende afvejning af hensynet til en effektiv håndhævelse og hensynet til navnlig persondatabeskyttelsen og privatlivets fred for indehaveren af IP-adressen.

EU-Domstolens praksis og afvejningen behandles nærmere nedenfor i afsnit 5.1.1.

⁴⁷ Jf. Bang-Pedersen og Højlund Christensen: *Den civile retspleje*, 2015, s. 486, og Schovsbo m.fl.: *Immaterialret*, 2015, s. 751, der begge henviser til U 2003.2264 Ø og U 2005.1410 V.

⁴⁸ Betænkning nr. 698/1973 om behandling af borgerlige sager, s. 127.

3.2 Midlertidige afgørelser om forbud og påbud

Et vigtigt foreløbigt retsmiddel til håndhævelse ophavsrettigheder er reglerne om midlertidige afgørelser om forbud og påbud i RPL kapitel 40.⁴⁹

I ophavsretlige krænkelssager kan det netop være et problem, at en påstået krænkelse kan fortsætte under en civil retssags behandling, men gennem forbudsinstituttet kan den hurtigt, omend på et foreløbigt grundlag, bringes til ophør. Det kan navnlig ske ved, at en internetudbyder pålægges at spærre for adgangen til en hjemmeside, som krænker ophavsretsloven.

Adgangen til bevisførelse i sager om midlertidige afgørelser er bred, og parterne kan som udgangspunkt føre de beviser, de ønsker.⁵⁰ Der kan f.eks. indhentes syn og skøn og fremlægges ensidigt indhentede sagkyndige erklæringer.

Retsplejeloven opstiller i § 413, nr. 1-3, tre positive betingelser for meddelelse af forbud og påbud. Rekvirenten skal således godtgøre eller sandsynliggøre, 1) at parten har den ret, der søges beskyttet ved forbuddet eller påbuddet, 2) at modpartens adfærd nødvendiggør, at der meddeles forbud eller påbud, og 3) at partens mulighed for at opnå sin ret vil forspildes, hvis han henvises til at afvente en retlig afgørelse på tvisten.

Kravet om sandsynliggørelse indebærer en bevislettelse eller lempet bevisbyrde og tillader retten at foretage et konkret skøn af, om kravet er opfyldt.⁵¹ Det antages for det første, at der skal være såkaldt sandsynlighedsovervægt, forstået således at det skal være mere sandsynligt end det modsatte, at betingelserne er opfyldt, og for det andet, at der slet ikke bør indrømmes bevislettelse, hvis det kan lægges til grund, at der ikke vil

⁴⁹ Forbudsreglerne fandtes tidligere i kapitel 57 om fagedforbud, men blev ved en reform i 2013 flyttet fra fagedreglerne til de almindelige retssagsregler, jf. lovforslag L 47: Forslag til lov om ændring af retsplejeloven, lov om retsafgifter, designloven, varemærkeloven, markedsføringsloven og lov om forbud til beskyttelse af forbrugernes interesser, fremsat den 1. november 2012. Lovforslaget blev vedtaget ved lov nr. 1387 af 23. december 2012 om ændring af retsplejeloven, der trådte i kraft den 1. juli 2013. Forbudsreglerne er i vidt omfang de samme, jf. Schovsbo m.fl.: *Immaterialret*, 2015, s. 755, men omfatter nu også påbud (handlepligter).

⁵⁰ Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 156-159.

⁵¹ Hvad der nærmere ligger i sandsynliggørelse har været genstand for diskussion i litteraturen. Se f.eks. Petersen: *Immaterialrettigheder og foreløbige forbud*, 2008, s. 334-359, og Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 163-164, hvis konklusioner ovenstående afsnit bygger på.

kunne ske yderligere bevisførelse omkring et bevistema i en efterfølgende hovedsag.⁵² Retten kan inden for disse rammer lade bevislettelsens omfang afhænge af rekvirentens behov for det foreløbige forbud eller påbud og dets betydning for rekvisitus.⁵³

I de første to af ovennævnte tre forhold, som rekvirenten skal godtgøre eller sandsynliggøre, ligger det retsstridighedskrav, som tidligere var udtrykt ved, at forbud kunne nedlægges mod handlinger, der stred mod rekvirentens ret.⁵⁴ Retsstridighedskravet er videreført ved reformen i 2013 og indebærer, at der ikke kan nedlægges forbud, hvis rekvisiti handlinger ikke krænker rekvirentens ret. Spørgsmålet har været aktuelt i forbindelse med forbudssager mod internetudbydere, som har gjort gældende, at de ikke har handlet retsstridigt, men blot stillet en internetforbindelse til rådighed, jf. nærmere afsnit 5.3.3. nedenfor.

Den tredje betingelse – at rekvirentens formål vil forspildes, hvis han henvises til at afvente en retlig afgørelse på tvisten – vil ofte kunne opfyldes i sager om ophavsretskrænkelser. Hvis ikke adgangen til f.eks. en ulovligt tilgængeliggjort film hurtigt afskæres ved hjælp af et påbud herom til internetoperatøren, risikerer rettighedshaveren et stort tab. Enhver internetbruger kan potentielt downloade filmen, og det kan blive vanskeligt eller umuligt at få dækket tabet efterfølgende ved at rette kravet mod de enkelte brugere.

Herudover indeholder RPL § 414 to betingelser. For det første kan der ikke meddeles forbud eller påbud, hvis ”lovens almindelige regler om straf og erstatning og eventuelt en af modparten tilbudt sikkerhed yder parten tilstrækkeligt værn”, jf. bestemmelsens stk. 1. Det synes at være konklusionen i forarbejder og litteraturen, at muligheden for forbud og påbud kan være den primære retsbeskyttelse ved krænkelser af immaterialrettigheder, og at straf, erstatning og tilbudt sikkerhed ikke er et tilstrækkeligt værn i sådanne sager.⁵⁵ Betingelsen vil således oftest være opfyldt ved forbudsbegæring rettet mod ophavsretlige krænkelser. For det andet gælder efter bestemmelsens stk. 2 et almindeligt proportionalitetsprincip, idet forbud eller påbud kan nægtes, ”hvis det vil påføre modparten skade eller ulempe, der står i åbenbart

⁵² Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 163.

⁵³ *Ibid.*, s. 163.

⁵⁴ Jf. den tidligere § 642, nr. 1, som affattet ved lovbekendtgørelse nr. 1008 af 24. oktober 2012, og jf. betænkning nr. 1530/2012, s. 108.

⁵⁵ Jf. Justitsministeriets overvejelser i punkt 2.4.3. i lovforslag L 47, op.cit., fodnote 49, Schovsbo m.fl.: *Immaterialret*, 2015, s. 758, og Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 180-182.

misforhold til partens interesse i meddelelse af forbuddet eller påbuddet”. Der er tale om en undtagelsesregel, som ifølge forarbejderne ”kun forudsættes anvendt i de få tilfælde, hvor der består en betydelig forskel mellem rekvirentens interesse i nedlæggelse af forbud og de mulige skadevirkninger for rekvisitus”.⁵⁶

Endelig indgår hensynet til grundlæggende rettigheder også i vurderingen af, om forbud eller påbud kan meddeles, og i forbindelse hermed skal der foretages en passende afvejning mellem de relevante rettigheder, jf. charterets artikel 52, stk. 1.

3.3 Civile sager

I civile sager om ophavsretskrænkelser kan sagsøgeren nedlægge en række forskellige påstande, hvoraf den vigtigste nok er økonomiske sanktioner. Nedenfor omtales denne samt påstand om forbud, straf og offentliggørelse af dom.

3.3.1 Økonomiske sanktioner

OHL § 83 indeholder en almindelig regel om erstatning. Der kan ifølge bestemmelsen kræves et rimeligt vederlag for udnyttelsen, egentlig erstatning og godtgørelse for ikke økonomisk skade. Bestemmelsen finder anvendelse på de overtrædelser, der er udtrykkeligt henvist til i §§ 76 og 77. For andre krænkelser kan erstatning kræves efter dansk rets almindelige erstatningsregler,⁵⁷ som i øvrigt udfylder og supplerer reglen i ophavsretsloven.⁵⁸ Det betyder blandt andet, at ansvar kan ifaldes af både fysiske og juridiske personer.

Bestemmelsen i OHL § 83, stk. 1, nr. 1, om et rimeligt vederlag er indført i ophavsretsloven ved 1995-loven.⁵⁹ Det beløb, som kan kræves i rimeligt vederlag, er ikke baseret på det lidte tab. Det skal snarere kompensere for, at dette tab kan være svært at dokumentere, og at domstolene derfor fastsætter erstatningen skønsmæssigt – og nogle gange til et lavere beløb, end rettighedshaveren finder rimeligt.⁶⁰ Vederlaget svarer til ophavsmandens sædvanlige honorar for retmæssige udnyttelser, men kan også

⁵⁶ Jf. bemærkningerne til § 414 i lovforslag L 47, op.cit., fodnote 49. Bestemmelsen viderefører det proportionalitetsprincip, som også var gældende før reformen i 2013.

⁵⁷ Schönning: *Ophavsretsloven med kommentarer*, 2016, s. 785.

⁵⁸ Schovsbo m.fl.: *Immaterialret*, 2015, s. 772.

⁵⁹ Jf. lovforslag L 119: Forslag til lov om ophavsret, fremsat den 18. januar 1995. Lovforslaget blev vedtaget ved lov nr. 395 af 14. juni 1995 om ophavsret, der trådte i kraft den 1. juli 1995.

⁶⁰ Jf. Schovsbo m.fl.: *Immaterialret*, 2015, s. 775-776.

– hvis der ikke findes et sædvanligt honorar på området – fastsættes skønsmæssigt af domstolene.⁶¹ Den erstatning, som kan kræves efter OHL § 83, stk. 1, nr. 2, er for ”den yderligere skade, som overtrædelsen har medført”, således at der samlet ydes en erstatning, der genopretter det lidte tab.⁶² I vurderingen kan indgå alle relevante elementer, herunder, foruden den forurettedes tabte fortjeneste, også krænkerens uberettigede fortjeneste, jf. § 83, stk. 2. Kriteriet om krænkerens uberettigede fortjeneste er kommet ind i bestemmelsen ved gennemførelsen af retshåndhævelsesdirektivet i 2005, der – som i øvrigt også TRIPS – forudsætter, at den krænkende part skal kunne pålægges at betale erstatning til rettighedshaveren.⁶³ Kriteriet er nyt i forhold til gældende erstatningsretlige principper i dansk ret og betyder ifølge lovmotiverne, ”at domstolene har mulighed for en friere vurdering af fastsættelsen af det lidte tab – og dermed erstatningens størrelse [...]”.⁶⁴ Det lidte tab vil navnlig være afsætningstab, tab som følge af markedsforstyrrelse og interne tab.

Godtgørelsen for ikke økonomisk skade er at sammenligne med en tortgodtgørelse, altså godtgørelse for en krænkelse, som ikke kan opgøres i et økonomisk tab, men som har medført en skade i ideel henseende. Tidligere var godtgørelse principielt obligatorisk, men efter gennemførelsen af retshåndhævelsesdirektivet har den forurettede nu ikke længere et ubetinget krav på godtgørelse. Betaling af godtgørelse er betinget af, at der foreligger et retsstridigt forhold og en skadevirkning.⁶⁵

Ansvarsgrundlaget er culpa, dvs. at overtrædelsen skal være begået forsætligt eller uagtsomt. Modsat strafansvaret er simpel uagtsomhed tilstrækkeligt, og testen er derfor, om den påståede krænker indså eller burde have indset, at han begik en krænkelse.

Det erstatningsretlige medvirkensansvar er ikke lovreguleret, men kan pålægges efter dansk rets almindelige regler om flere erstatningsansvarlige og har hjemmel i retspraksis.⁶⁶ Medvirkensansvaret omfatter både aktiv og passiv medvirken. Ansvarsgrundlaget er naturligvis det samme som for den hovedansvarlige.

⁶¹ Jf. Schønning: *Ophavsretsloven med kommentarer*, 2016, s. 787.

⁶² Jf. Schovsbo m.fl.: *Immaterialret*, 2015, s. 779.

⁶³ TRIPS i artikel 45 og retshåndhævelsesdirektivet i artikel 13.

⁶⁴ Jf. bemærkningerne til § 83 i lovforslag L 48: Lov om ændring af patentloven, ophavsretsloven m.v., fremsat den 9. november 2005. Lovforslaget blev vedtaget ved lov nr. 1430 af 21. december 2005 om ændring af patentloven, ophavsretsloven med flere love, der trådte i kraft den 1. januar 2006.

⁶⁵ Ibid., jf. bemærkningerne til § 83 i L 48, og jf. Schønning: *Ophavsretsloven med kommentarer*, 2016, s. 794.

⁶⁶ Som f.eks. beskrevet af Von Eyben og Isager: *Lærebog i erstatningsret*, 2015, s. 457.

3.3.2 Forbud

Ved en forbudsdom fastslås det, at modparten ikke må foretage de krænkende handlinger. Hvis rettighedshaveren får medhold i en anerkendelsespåstand, skal krænkeren anerkende at have krænket den pågældende rettighed. Normalt nedlægges også en fuldbyrdelsespåstand, som – hvis rettighedshaveren får medhold – fører til en fuldbyrdelsesdom, der har samme virkning som et forbud meddelt ved en midlertidig afgørelse.⁶⁷

3.3.3 Straf

Efter OHL § 81, stk. 1, kan rettighedshaveren, som forurettet, nedlægge påstand om straf i den civile retssag. Det fremgår af bestemmelsen, at det er overtrædelser, der kan straffes med bøde, som rettighedshaveren kan påtale, nemlig overtrædelser omfattet af OHL § 76, stk. 1, § 77, stk. 1, og § 79. Ved straf er tilregnelseskravet forsæt eller grov uagtsomhed.

3.3.4 Offentliggørelse af dom

Sagsøgeren i en civil sag kan også nedlægge påstand om offentliggørelse af dommen. Det følger af OHL § 84 a, som er indsat med henblik på at gennemføre artikel 15 i retshåndhævelsesdirektivet. Formålet med bestemmelsen er at ”afskrække en fremtidig krænkende part og fremme en øget bevidsthed hos den brede offentlighed”.⁶⁸

3.4 Straffesager

Ophavsretsloven indeholder i §§ 76-80 også bestemmelser om straf i form af bøde for grovere immaterialretskrænkelser, der er begået forsætligt eller groft uagtsomt, jf. OHL § 76, stk. 1, og – for forsætlige overtrædelser begået under skærpende omstændigheder – fængselsstraf i op til et år og seks måneder, jf. OHL § 76, stk. 2. For overtrædelser af særlig grov karakter begået under særligt skærpende omstændigheder har straffelovens § 299 b skærpet strafferammen, så der kan idømmes fængselsstraf i op

⁶⁷ Jf. Schovsbo m.fl.: *Immaterialret*, 2015, s. 766-767.

⁶⁸ Jf. betragtning 27 til direktivet.

til 6 år.⁶⁹ Juridiske personer kan idømmes bødestraf, jf. OHL § 80 med henvisning til straffelovens kap. 5.

Strafansvaret kan gøres gældende efter reglen i straffelovens § 23 om medvirken til gerningen ved ”tilskyndelse, råd eller dåd”. Der vil oftest være tale om aktiv medvirken, men der er også eksempler i dansk retspraksis på idømmelse af straf for passiv medvirken.⁷⁰ Det er naturligvis en betingelse, at tilregnelseskravet – forsæt eller grov uagtsomhed – er opfyldt.

De strafbare forhold, som er omfattet af OHL § 76, stk. 2, er undergivet betinget offentlig påtale eller – hvis almene hensyn kræver det – offentlig påtale, jf. § 82, og overtrædelse af bestemmelserne i straffelovens § 299 b er undergivet offentlig påtale.

I nogle tilfælde – f.eks. hvis et erstatningskrav ikke kan bære en civilretlig forfølgning – kan det have interesse for rettighedshaverne, at de efter bestemmelserne i RPL kapitel 89 har mulighed for at påtale civilretlige krav under straffesagen. Der er dog en del begrænsninger forbundet hermed, bl.a. at retten kan afvise at behandle kravet, hvis det ”ikke kan ske uden væsentlig ulempe”, jf. RPL § 991, stk. 4.

3.5 Breve til formodede kränkere

Rettighedshaverne kan vælge at gribe en krænkelse af deres ophavsrettigheder an ved at sende breve til de formodede kränkere, hvori de gør opmærksom på, at en krænkelse er konstateret, og opfordrer til, at et forlig indgås ved betaling af et nærmere bestemt beløb.

Et eksempel på et brev er offentligt tilgængeligt, fordi Advokatnævnet har haft lejlighed til at tage stilling til, om fremsendelse af det til en formodet krænker var i overensstemmelse med god advokatskik.⁷¹ Det var det i det pågældende tilfælde. I Advokatnævnets kendelse herom er dele af brevet gengivet. Brevet redegør for sagens faktuelle omstændigheder, herunder hvornår en IP-adresse har været aktiv til at downloade og tilgængeliggøre et angivet ophavsretligt beskyttet værk, og hvordan

⁶⁹ Lovforslag L 55: Forslag til lov om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet mv.), fremsat den 5. november 2003. Forslaget blev vedtaget ved lov nr. 352 af 19. maj 2004, og reglerne trådte i kraft den 1. juli 2004.

⁷⁰ U 1996.209/2 H. Jf. herom Nielsen og Jakobsen: *E-handelsret*, 2011, s. 267.

⁷¹ Advokatnævnets kendelse af 23. juni 2016.

advokaten ved editionskendelse har fået udleveret navn og adresse på den formodede krænker. Brevet angiver endvidere lovgrundlaget og betydningen af de relevante lovbestemmelser for krænkeren. Det lægger op til en forligsmæssig afslutning af sagen mod betaling af et forligsbeløb. For det tilfælde at forlig ikke ønskes indgået, forbeholder advokaten sig ret til på sin klients vegne at fortsætte inddrivelsen af kravet, undersøge, om der er sket yderligere krænkelser fra IP-adressen, og opføre det fulde krav, eventuelt i forbindelse med en retssag med påstand om erstatning. Endelig opfordres den formodede krænker til at søge juridisk bistand hos egen advokat.

Styrker og svagheder ved dette håndhævelsesskridt er behandlet nedenfor i afsnit 5.1.2.

3.6 Rettighedshaverorganisationer

Rettighedshavere til musik og film er ofte medlemmer af organisationer, som forvalter deres rettigheder. Mange af disse er sammensluttet i interesseorganisationen RettighedsAlliancen,⁷² som driver oplysende og politisk arbejde for at skabe bedre vilkår for medlemmerne, og som anlægger og fører mange af retssagerne på området på vegne af medlemmerne.

4 E-handelsdirektivets og e-handelslovens ansvarsregler for formidlere

For alle de aktører, som håndhævelsen kan rettes imod, kan der blive tale om både et strafansvar og et erstatningsansvar, begge dele eventuelt som et medvirkensansvar, efter de ansvarsregler, som er skitseret ovenfor. Dog kan en tjenesteyder, der kan pålægges straf- eller erstatningsansvar efter disse regler, i nogle tilfælde være ansvarsfri efter reglerne i e-handelsdirektivet (EHD)⁷³ og dets danske implementering – e-handelsloven.⁷⁴ Ansvarsfritagelsesreglerne gælder for tjenesteydere, der optræder som formidlere af ”informationssamfundstjenester”. Informationssamfundstjenester er ifølge forarbejderne tjenester med et kommercielt sigte, der normalt leveres mod betaling.⁷⁵

⁷² RettighedsAlliancen har afløst det tidligere Antipiratgruppen. Medlemmer er blandt andre IFPI Danmark, KODA og Nordisk Film A/S.

⁷³ Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»Direktivet om elektronisk handel«), EUT 2000 L 178, s. 1.

⁷⁴ Lov nr. 227 af 22. april 2002, jf. fodnote 3 ovenfor. Direktivets og lovens ansvarsfritagelsesregler omfatter enhver form for ulovlig information, herunder også materiale, som krænker ophavsrettigheder.

⁷⁵ Punkt 2.1. i de almindelige bemærkninger til lovforslag L 61: Forslag til lov om tjenester i informationssamfundet, herunder visse aspekter af elektronisk handel, fremsat den 29. januar 2002.

Ydere af sådanne tjenester er ”alle fysiske og juridiske personer, som leverer tjenester, der er nødvendige for, at en modtager kan få adgang til f.eks. internettet og kan søge efter og give oplysninger på åbne netværk”, og sådanne personer kan f.eks. være ”internetleverandører, netværksoperatører, serverejere og erhvervsdrivende, der udbyder tjenesteydelser online”.⁷⁶

Hvis en formidler derimod *ikke* kan pålægges ansvar efter de almindelige ansvarsregler, bliver det ikke aktuelt at anvende ansvarsfritagelsesreglerne.⁷⁷ De skal således kun anvendes, hvis der så at sige er et ansvar at fritage for. Ansaret vil være et medvirkensansvar, idet formidleren ikke selv spreder eller er den oprindelige kilde til den retsstridige information, men blot optræder som mellemmand mellem afsenderen og modtageren af informationen.⁷⁸

Begrænsningen af ansaret gælder for tre typer aktiviteter, som er omfattet af lovens §§ 14-16, svarende til direktivets artikel 12-14, om henholdsvis ren videreformidling, *caching* og oplagring. Det er et fællestræk, at de pågældende aktiviteter har en teknisk, automatisk og passiv karakter, og at formidleren ikke har kendskab til eller kontrol over den information, som transmitteres eller oplagres.⁷⁹ I det følgende gennemgås kort ansvarsfritagelsesreglerne og to andre forhold, som også har betydning for håndhævelsen af ophavsrettigheder på internettet, nemlig reglerne om, at der skal være adgang til at nedlægge forbud over for formidlere, hvis tjenester anvendes af tredjemænd til at krænke immaterialrettigheder, og e-handelsdirektivets forbud mod at pålægge formidlerne en generel overvågningspligt.

4.1 Ren videreformidling – EHD artikel 12 og EHL § 14

Ved ren videreformidling – eller med direktivets ord *mere conduit* – sørger en tjenesteyder eller formidler for transmission på et kommunikationsnet af information, som en anden – tjenestemodtageren – stiller til rådighed, eller for levering af adgang til et kommunikationsnet, jf. EHL § 14, stk. 1 og stk. 3. Det handler konkret om netværksoperatører og internetudbydere. Bestemmelsen omfatter også såkaldt ”automatisk, mellemliggende og kortvarig oplagring af information, hvis denne oplagring udelukkende har til formål at gennemføre transmissionen, og hvis oplagringen

⁷⁶ Ibid., Almindelige bemærkninger, punkt 2.2.

⁷⁷ Se. f.eks. Udsen: *IT-ret*, 2016, s. 257.

⁷⁸ Jf. Mathiasen m.fl.: *E-Handelsloven med kommentarer*, 2004, s. 181.

⁷⁹ Jf. betragtning 42 til direktivet.

ikke varer længere, end hvad der med rimelighed kan antages at være nødvendigt for at gennemføre transmissionen”, jf. bestemmelsens stk. 2.

Ved denne rene videreformidling er formidleren ikke ansvarlig for den information, der transmitteres, hvis tre betingelser er opfyldt, nemlig at han ikke selv tager initiativ til transmissionen, ikke udvælger modtageren af transmissionen og hverken udvælger eller ændrer den transmitterede information, jf. lovens § 14, stk. 1, nr. 1-3.

4.2 Caching – EHD artikel 13 og EHL § 15

Ved *caching* lagrer en formidler i form af en internetoperatør kopier af hyppigt besøgte hjemmesider på sine egne servere. Det letter trafikken på internettet og gør transmissionen af information mere effektiv, at brugere, som ønsker at besøge sådanne hjemmesider, ledes til den cachede version på formidlerens server.

Formidleren er fritaget for ansvar for denne automatiske, mellemliggende og midlertidige oplagring af information og for dens indhold under de betingelser, som er oplistet i EHL § 15, 2. led, nr. 1-5. Ansvarsfriheden er også her baseret på formidlerens passive rolle og svage tilknytning til informationen, og formidleren må derfor for det første ikke ændre den cachede information. Formidleren skal for det andet overholde betingelserne for adgang til informationen. Hvis adgang til den oprindelige hjemmeside f.eks. kræver betaling eller kode, skal det samme således gælde for cache-kopien. For det tredje skal informationen holdes ajourført ifølge branchens regler. Det vil i praksis sige, at den cachede hjemmesidekopi ikke må være en gammel version af den originale side. Efter den fjerde betingelse må der ikke foretages indgreb i den teknologi, som genererer data om anvendelsen af hjemmesiden. Det kan f.eks. være teknologi, der bruges til at tælle besøg. Endelig skal formidleren for det femte straks fjerne eller hindre adgang til kopieret information, når han får kendskab til, at den er fjernet fra nettet, at adgang til den er hindret, eller at en domstol eller administrativ myndighed har krævet dette. Herved sikres, at formidleren f.eks. ikke fortsat lagrer og giver adgang til ophavsretskrænkende materiale, som hjemmesideindehaveren selv har fjernet.

4.3 Oplagring – EHD artikel 14 og EHL § 16

Ved oplagring – eller *hosting* – fungerer formidleren som vært for information leveret af andre, f.eks. ved at formidleren stiller plads på egne servere til rådighed for

hjemmesider. Betingelserne for ansvarsfriheden for denne information er strengere end ved ren videreformidling og *caching*, fordi formidlerens rolle er lidt mere aktiv og hans tilknytning til informationen lidt stærkere. Oplagringen skal således ifølge EHL § 16 ske på anmodning fra en anden – tjenestemodtageren – og formidleren må ikke have kendskab til den ulovlige information og, for så vidt angår *erstatningskrav*, ikke have ”kendskab til forhold eller omstændigheder, hvoraf den skadevoldende aktivitet eller information fremgår”, jf. EHL § 16, stk. 1, nr. 1. Det svarer til, at formidleren erstatningsretligt er underlagt den almindelige culparegel⁸⁰ og altså ikke må have burde viden. Hvis formidleren får et sådant kendskab, skal han – for at bevare ansvarsfriheden – straks tage skridt til at fjerne informationen eller hindre adgangen til den, jf. EHL § 16, stk. 1, nr. 2.

Der skelnes altså ved oplagring mellem strafansvaret og erstatningsansvaret. Fritagelse for strafansvaret forudsætter, at formidleren ikke har kendskab til – positiv viden om – den ulovlige information. Formidleren må med andre ord ikke have handlet forsætligt. Derimod bortfalder strafansvarsfriheden ikke ved burde viden, og formidleren kan derfor opnå ansvarsfrihed, selv om han har handlet groft uagtsomt.⁸¹ Dette forhold vil blive omtalt nedenfor i afsnit 5.3.1.

4.4 Foreløbige retsmidler over for formidlere

Uanset ansvarsfriheden skal det være muligt at få nedlagt forbud eller anvende andre foreløbige retsmidler over for formidleren for at forhindre eller bringe en krænkelse til ophør. Dette følger for de tre aktivitetstyper af henholdsvis EHD artikel 12, stk. 3, artikel 13, stk. 2, og artikel 14, stk. 3. Det er også forudsat i Infosoc-direktivets artikel 8, stk. 3, og i retshåndhævelsesdirektivets artikel 11, 3. pkt. De nærmere betingelser og procedurer herfor fastsætter medlemsstaterne selv i deres nationale lovgivning,⁸² og for dansk rets vedkommende drejer det sig navnlig om reglerne om midlertidige afgørelser om forbud og påbud i RPL kapitel 40, jf. afsnit 3.2 ovenfor.

⁸⁰ Jf. bemærkningerne til § 16 i lovforslag L 61, op.cit., fodnote 75.

⁸¹ Dette fremgår modsætningsvis af punkt 12.2.1.3.a i de almindelige bemærkninger til lovforslag L 61. Der synes også i litteraturen at være enighed om, at retsstillingen er, at strafansvaret bortfalder ved grov uagtsomhed, jf. i denne retning Udsen, *IT-ret*, 2016, s. 277, Jakobsen og Schaumburg-Müller, *Medieretten*, 2013, s. 336, Nielsen og Jakobsen: *E-handelsret*, 2011, s. 282-283, og Mathiasen m.fl.: *E-Handelsloven med kommentarer*, 2004, s. 219.

⁸² Jf. betragtning 59 til Infosoc-direktivet og betragtning 23 til retshåndhævelsesdirektivet.

4.5 Overvågningsforbuddet

Endelig indeholder e-handelsdirektivet i artikel 15 en bestemmelse om, at formidlere ikke må pålægges en generel forpligtelse til at overvåge den information, de fremsender eller oplagrer via deres net og servere, eller til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed. Derimod må formidlerne godt pålægges mere specifikke tilsynspligter i særlige tilfælde,⁸³ ligesom bestemmelsen ikke er til hinder for, at formidlere, som oplagrer oplysninger, pålægges ”pligt til en sådan agtpågivenhed, som med rimelighed kan forventes af dem, og som der er fastsat bestemmelser om i den nationale lovgivning, med henblik på at afsløre og forhindre visse former for ulovlige aktiviteter”.⁸⁴ Overvågningsforbuddet er ikke direkte implementeret i dansk ret, idet det er i overensstemmelse med, hvad der allerede før direktivet var retsstillingen i dansk ret, nemlig at der ikke gælder en generel overvågningspligt.⁸⁵

5 Aktører, som håndhævelsen kan rettes imod

Der synes – baseret på ovenstående – at være ganske mange håndhævelses- og sanktionsmuligheder, hvoraf nogle endda er blevet styrket. Strafferammen er blevet forhøjet, det erstatningsretlige værn er blevet stærkere, og mulighederne for at sikre beviset er blevet bedre. I de følgende afsnit sættes fokus imidlertid på de konkrete problemer, der kan opstå i forbindelse med håndhævelsen af rettighederne over for de enkelte aktører.

5.1 Brugere

Når der via download, upload, streaming eller fildeling udveksles ophavsretligt beskyttet materiale uden samtykke fra rettighedshaveren, er det primære ansvarssubjekt brugeren af en tjeneste eller hjemmeside, dvs. den, der downloader, uploader, streamer eller foretager fildelingen. Det er denne bruger, der umiddelbart kan ifalde et straffe- eller erstatningsretligt ansvar for den ulovlige tilgængeliggørelse og/eller eksemplar-fremstilling, og håndhævelsen vil da også ofte blive rettet mod brugeren. Et første

⁸³ Jf. betragtning 47 til e-handelsdirektivet.

⁸⁴ Jf. betragtning 48 til direktivet.

⁸⁵ Jf. punkt 12.2.3. i de almindelige bemærkning til lovforslag L 61, op.cit., fodnote 75.

problem, som kan opstå i denne forbindelse, er selve sporingen af krænkelsen og identifikationen af den, der har foretaget den.

5.1.1 Sporing og identifikation

I forbindelse med denne sporing og identifikation kan der opstå visse hindringer undervejs. IP-adresser kan spores, men der kan stilles spørgsmålstejn ved bevisværdien af resultaterne og lovligheden af sporingen og ved internetudbydernes pligt til – og mulighed for – at udlevere oplysninger om deres kunder til rettighedshaverne. Disse spørgsmål behandles i det følgende.

5.1.1.1 Første skridt – sporing af IP-adresser

Når der foretages f.eks. upload eller download af en fil til og fra internettet, kan denne aktivitet ofte spores til en bestemt IP-adresse, fordi IP-adressen er synlig de steder på internettet, som den digitale enhed bag IP-adressen, f.eks. en computer, besøger. IP-adressen tildeles af internetudbyderen fra en pulje og knyttes til den digitale enhed ved dennes tilslutning til internettet. Den angiver stedet, hvor data, som brugeren efterspørger, skal sendes hen.

Tidligere var IP-adresser statiske eller med andre ord altid tilknyttet den samme digitale enhed. Da der ikke længere er nok IP-adresser til rådighed til alle enheder, anvendes i dag også såkaldte dynamiske IP-adresser. En dynamisk IP-adresse tildeles midlertidigt for det tidsrum, hvor en brugers enhed er sluttet til internettet. Når forbindelsen til internettet afbrydes, kan den dynamiske IP-adresse anvendes til en anden enhed. I denne situation er det kun muligt at sætte f.eks. en ulovlig fildeling i forbindelse med en bestemt enhed, hvis både IP-adresse og tidspunkt for fildelingen kendes.

Som nævnt ovenfor i afsnit 3.1.1.1 findes der dog specialudviklet software, som gør det muligt at spore såvel de IP-adresser, som har været brugt til den ulovlige handling, som tidspunktet for den. Det vil sige, at rettighedshavere er i stand til at indsamle oplysninger om IP-adresser og piratkopier, som er delt eller downloadet af enheden bag IP-adressen.

Bevisværdien

Det vil være rimeligt at stille spørgsmålstejn ved pålideligheden af de resultater, som det specialudviklede sporingssoftware genererer. Det er et meget teknisk spørgsmål, men der synes ikke at være trykte domme, som anfægter sammenhængen mellem IP-adresse og sporede krænkelse. Derimod har sammenhængen mellem sporede krænkelse og det faktiske indhold på sagsøgt computer været anfægtet, jf. afsnit 5.1.3 nedenfor.

Persondataretten

En næste hindring for rettighedshaverne ved indsamling af IP-adresser kunne være de persondataretlige regler. Må rettighedshaverne overhovedet overvåge trafik på internettet og registrere privates IP-adresser, for er der ikke tale om personfølsomme oplysninger?

EU-Domstolen har allerede i dommen i *Scarlett Extended*-sagen fastslået, at internetbrugeres IP-adresser er beskyttede personoplysninger, fordi de gør det muligt præcist at identificere disse brugere.⁸⁶ Sagen vedrørte dog en *internetudbyders* indsamling og identificering af IP-adresser, og der var netop tale om en behandling af personoplysninger, fordi internetudbyderen ved hjælp af *andre* oplysninger, som denne selv lå inde med, kunne identificere personen bag IP-adressen. Domstolen har nu også i sin dom i *Breyer*-sagen⁸⁷ fastslået, at dynamiske IP-adresser, der som nævnt ikke uden videre kan knyttes til bestemte digitale enheder – og dermed personer, *kan* være personoplysninger. Det er de ifølge Domstolen, når den hjemmesideindehaver, som har registreret de dynamiske IP-adresser, ved lovlige midler kan få identificeret navnene bag dem gennem yderligere viden, som hjemmesideindehaverens internetudbyder råder over.⁸⁸

Domstolens konklusioner i sidstnævnte sag må antages at gælde også i forhold til både statiske IP-adresser og de rettighedshavere, som er i fokus her. De statiske IP-adresser fordi de lettere end de dynamiske kan henføres til bestemte personer, og rettighedshaverne fordi de er underlagt de samme persondataretlige regler som hjemmesideindehavere. Rettighedshavere foretager altså en behandling af personoplysninger, når de indsamler og registrerer statiske eller dynamiske IP-adresser

⁸⁶ Domstolens dom af 24. november 2011 i sag C-70/10, præmis 51.

⁸⁷ Domstolens dom af 19. oktober 2016 i sag C-582/14.

⁸⁸ Præmis 49.

og ved lovlige midler kan få internetudbydere til at udlevere oplysninger, som gør det muligt at identificere brugeren af IP-adressen. Som det vil fremgå nedenfor, er sådanne lovlige midler til rådighed for rettighedshaverne.

Forinden rettighedshaveren – nu i sin rolle som dataansvarlig i persondatalovens forstand – iværksætter en sådan behandling af personoplysninger, skal behandlingen anmeldes til Datatilsynet. Det fremgår af PDL § 48. I visse tilfælde skal Datatilsynet også give sin tilladelse til behandlingen, inden den kan foretages, jf. lovens § 50, stk. 1, og blandt de tilfælde, som opregnes i bestemmelsen, er behandling af oplysninger om strafbare forhold, jf. PDL § 50, stk. 1, nr. 1, med henvisningen til lovens § 8, stk. 4. Da rettighedshavere vil have behov for at sammenkøre oplysninger om IP-adresser med oplysninger om formodede ophavsretskrænkelser, der jo er strafbare, behandler de i denne forbindelse oplysninger om strafbare forhold og skal afvente Datatilsynets tilladelse. Datatilsynets tilstræbte sagsbehandlingstid er ifølge tilsynets hjemmeside ”ikke over 5 måneder”.⁸⁹ En anmeldelse – og den efterfølgende tilladelse – er dog generel og kan dække behandlinger, der foregår flere forskellige steder,⁹⁰ og der skal således ikke indhentes tilladelse i forhold til hver enkelt formodede krænkelse.

Datatilsynet har tidligere haft lejlighed til at tage stilling til Antipiratgruppens indsamling af IP-adresser efter en anmeldelse indgivet i 2001. Datatilsynet meddelte dengang organisationen tilladelse, men anmodede den efterfølgende om en redegørelse. Datatilsynet udtalte i sit svar⁹¹ på redegørelsen, at behandling af ”almindelige ikke-følsomme oplysninger, herunder f.eks. oplysninger om navn, adresse og IP-adresse, skal ske i overensstemmelse med persondatalovens § 6, stk. 1, nr. 1-7”, og henviste til, at behandling kan ske, hvis den ”er nødvendig for, at den dataansvarlige [...] kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse”, jf. PDL § 6, stk. 1, nr. 7. Når der behandles oplysninger om strafbare forhold ved at kæde IP-adresser sammen med formodede ophavsretskrænkelser – som jo er strafbare – er hjemmelen PDL § 8, stk. 4, og her kan behandling bl.a. ske, ”hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede”. Datatilsynet fandt, at nødvendighedskravet var opfyldt, fordi ophavsretskrænkelser som hovedregel er undergivet privat påtale, og hvis oplysningerne ikke kan behandles, kan ophavsrettighederne ikke håndhæves. Behandlingen var således

⁸⁹ Jf. <https://www.datatilsynet.dk/om-datatilsynet/sagsbehandlingstider/>.

⁹⁰ Jf. <https://www.datatilsynet.dk/blanketter/generelt-om-anmeldelse/>.

⁹¹ Datatilsynets brev af 23. april 2003, journalnummer 2002-219-0135.

efter Datatilsynets opfattelse nødvendig for, at ”et retskrav kan fastlægges, gøres gældende eller forsvares”.

Datatilsynet fandt også, at Antipiratgruppen overholdt god databehandlingsskik, idet oplysningerne var indsamlet via offentligt tilgængelige kilder eller modtaget ved en lovlig videregivelse efter retskendelse. Oplysningspligten var opfyldt, fordi gruppen sendte den registrerede et brev, så snart det var muligt, dvs. når den pågældende var identificeret. Endelig var det Datatilsynets opfattelse, at håndhævelse af ophavsrettigheder er et sagligt formål, og behandlingen gik ikke videre, end hvad der kræves til opfyldelse af dette formål.

Datatilsynets afgørelse er naturligvis konkret og vedrører blot ét eksempel på, hvordan indsamling af oplysninger om IP-adresser er blevet tilrettelagt. Antipiratgruppens formål med databehandlingen var at kunne fremsende breve til de formodede krænkere med tilbud om en forligsmæssig løsning eller med henblik på eventuel retsforfølgning. For de rettighedshavere eller advokatfirmaer, som i dag på vegne af rettighedshavere fremsender lignende breve, er opgaven den samme, og de viderefører formentlig på mange punkter den databehandlingspraksis, som Datatilsynet tidligere har godkendt.

Sammenfatning og diskussion – IP-adresser

Det er teknisk muligt at spore og registrere IP-adresser, som har været i brug ved udveksling af ophavsretligt beskyttet materiale uden rettighedshaverens samtykke, og bevisværdien af oplysningerne synes at være anerkendt. Allerede når rettighedshavere registrerer en IP-adresse, og så meget desto mere når de knytter denne til en strafbar handling og en person, der formodes at have foretaget denne, sker der imidlertid en behandling af personoplysninger, som skal anmeldes til Datatilsynet og – når der er tale om behandling af oplysninger om strafbare forhold – tillades af tilsynet. Persondataloven indeholder hjemmel til behandlingen, og det er muligt at opfylde kravene om blandt andet saglighed og nødvendighed.

Rettighedshaverne bliver altså ikke på dette indledende stadium bremset i deres eventuelle forsøg på at rette håndhævelsen af deres rettigheder mod det primære ansvarssubjekt, brugeren. Persondataretten opstiller nogle hindringer på vejen, men de synes praktisk overkommelige, og da der naturligvis også er et hensyn at tage til de registrerede, må det vurderes at være rimeligt, at rettighedshaverne – ligesom alle andre dataansvarlige – skal overholde persondatalovens regler. Når en praksis først er tilladt,

kan den fortsættes, og ventetiden på en tilladelse kan derfor højst udgøre et indledende problem.

At rettighedshaverne *kan* spore krænkelse, viser i øvrigt ikke noget om, i hvilket omfang det *sker* – eller med andre ord, hvor mange – små eller store – krænkelse der aldrig bliver sporet.

5.1.1.2 Næste skridt – udlevering af abonnentoplysninger

Oplysninger om IP-adresser og kommunikationstidspunkter fører ikke rettighedshaveren direkte til den formodede krænkelse, men de er i mange tilfælde nok til, at internetudbyderen kan identificere den bruger eller internetabonnent, som er tildelt IP-adressen. Denne oplysning skal rettighedshaveren naturligvis bruge for at kunne forfølge krænkelsen, f.eks. ved at anlægge retssag.

Kravet om retskendelse

Som det er fremgået ovenfor, er oplysninger om IP-adresser persondata, allerede inden de er koblet sammen med en identificerbar person, og de skal derfor behandles i overensstemmelse med persondatalovens regler. Spørgsmålet er, om internetudbyderen kan udlevere oplysningerne til rettighedshaverne uden retskendelse. Så længe der kun er tale om almindelige, ikke følsomme oplysninger, finder PDL § 6 anvendelse. Det betyder, at oplysningerne blandt andet kan udleveres, hvis den registrerede har givet sit udtrykkelige samtykke, jf. PDL § 6, stk. 1, nr. 1. Et sådant samtykke kan ikke forventes at foreligge i den her omhandlede situation. Så længe der ikke er udstedt en retskendelse, påhviler der ikke internetudbyderen en retlig forpligtelse til at udlevere oplysningerne, jf. PDL § 6, stk. 1, nr. 3. Derimod vil interesseafvejningsreglen i PDL § 6, stk. 1, nr. 7, eventuelt kunne danne hjemmel. Datatilsynet har i et yderligere brev til Antipiratgruppen i den ovenfor omtalte sag⁹² foretaget en sådan afvejning, og konkluderet, at udleveringen kræver retskendelse. På den ene side havde Antipiratgruppen en berettiget interesse i få oplysningerne udleveret, men på den anden side var der også meget væsentlige hensyn at tage til de registrerede, idet sammenkædningen af data kunne føre til oplysninger om formodede strafbare forhold vedrørende dem. Også teleselskabernes forhold til deres kunder og deres forventning

⁹² Journalnummer 2002-219-0135, jf. fodnote 91 ovenfor.

om fortrolighed blev vægtet. I det konkrete tilfælde var der altså ikke hjemmel til udleveringen i § 6, stk. 1, nr. 7, og den kunne ikke ske uden forudgående retskendelse.

Det næste spørgsmål bliver, om en sådan kendelse kan udstedes på et tidspunkt, hvor en retssag ikke verserer.

Udlevering af abonnentoplysninger uden for retssag

I dansk ret findes ikke bestemmelser, som generelt pålægger internetudbydere en pligt til at udlevere oplysninger om IP-adresser, men som anført ovenfor i afsnit 3.1.2.3 er det anerkendt i retspraksis, at reglerne om isoleret bevisoptagelse også omfatter tredjemandsedition. Det giver en adgang for rettighedshaverne til at få pålagt internetudbydere at udlevere oplysninger om indehaverne af IP-adresser, som har været anvendt til ophavsretskrænkelser, også uden at en retssag verserer. Netop i forhold til internetudbydere og oplysninger om IP-adresser er dette fastslået i to sager. I den ene, U 2003.2264 Ø, havde byretten – netop fordi en retssag *ikke* verserede – afvist en begæring om edition, som rettighedshaverne havde fremsat over for TDC og CyberCity vedrørende navne og adresser på indehavere af IP-adresser. Østre Landsret henviste til forarbejderne til den nugældende § 343 i retsplejeloven. Ifølge disse kræver bevisoptagelse, uden at der er anlagt retssag, sandsynliggørelse af en særlig interesse heri, og kravet hertil lempes, men falder ikke bort, blot fordi parterne er enige om at ønske beviset optaget. Desuden kan bevisoptagelsen ikke tillades, hvis den alene tjener ”til vejledning for, om sag overhovedet skal anlægges”, men efter omstændighederne godt, hvis den er ”nødvendig for, at ”parten” kan finde ud af, hvem han skal sagsøge”. Østre Landsret citerede også forarbejderne for, at bevisoptagelse kan finde sted, ”når retten finder det hensigtsmæssigt”, hvilket som nævnt ovenfor indebærer et betydeligt skøn og en bred adgang.

En dissentierende dommer mente ikke, at reglen om isoleret bevisoptagelse kunne anvendes sammen med tredjemandseditionsreglen, hverken efter bestemmelsens ordlyd eller forarbejder, men landsrettens flertal fandt, at RPL § 343 sammenholdt med forarbejderne ikke på forhånd udelukkede bevisoptagelsen. Da der i den konkrete sag var en høj grad af sandsynlighed for, at de oplyste IP-adresser var blevet brugt til krænkelse af ophavsrettigheder, og da rettighedshaverne kun kunne varetage deres interesser, hvis de fik udleveret oplysningerne, blev byrettens afgørelse ophævet og hjemvist til afgørelse af, om det i den konkrete sag var hensigtsmæssigt at pålægge editionspligt.

I den anden, meget lignende sag – U 2005.1410 V – citerede Vestre Landsret fra samme sted i forarbejderne og henviste som begrundelse for, at § 343 overhovedet hjemler editionspålæg – og ikke kun vidneførsel samt syn og skøn – for det første til, at bestemmelsen med ordlyden om, at retten kan tillade, ”at der optages bevis”, kan rumme edition, for det andet til, at tredjemandseditionspligten har nær sammenhæng med vidnepligten, og for det tredje til placeringen af tredjemandseditionsreglen i retsplejelovens tredje bog, første afsnit, om ”Almindelige bestemmelser”.

Med disse afgørelser har landsretterne således fastslået, at rettighedshavere gennem retskendelse kan få internetudbydere til at udlevere navne og adresser bag IP-adresser med hjemmel i reglerne om isoleret bevisoptagelse, sammenholdt med tredjemandseditionsreglen, for at finde ud af, hvem der kan sagsøges.

Pligt til at indlede retssag

Man kan spørge, hvilken betydning det skal tillægges, om formålet med udleveringen af oplysningerne faktisk er – efterfølgende – at indlede en retssag. På den ene side henviser landsretten i U 2003.2264 Ø til udtalelserne i forarbejderne om, at bevisoptagelse ikke kan tillades, hvis den alene tjener til vejledning for, om sag overhovedet skal anlægges, altså ikke ud fra en efterforskningsmæssig interesse, men godt hvis den er nødvendig for at finde ud af, hvem man skal sagsøge. Det fremgår ikke af sagen, om det var de kærendes hensigt at anlægge retssag, eller om de blot på anden vis ville varetage deres interesser, men retten tillod altså editionspålægget netop med den begrundelse, at det var deres eneste mulighed for at varetage deres interesser. Den fremhævede ikke nogen pligt for de kærrende til efterfølgende at anlægge en retssag.

Formålet med breve, som rettighedshavere sender til formodede krænker, når de har fået oplysningerne om deres navne og adresser, jf. nærmere nedenfor i afsnit 5.1.2, er i første omgang ikke nødvendigvis at indlede en retssag, men måske snarere at indgå et forlig. De udleverede oplysninger gør det imidlertid muligt for rettighedshaverne at finde ud af, ”hvem de skal sagsøge”, og efter den ovenfor omhandlede retspraksis har de ikke nogen pligt til at følge bevisoptagelsen op med en retssag.

Rettighedshaverne har således med disse regler som *udgangspunkt* gode muligheder for at få adgang til navne og adresser på de formodede krænker. Retten skal ifølge

forarbejderne til RPL § 343 blot finde det hensigtsmæssigt at pålægge internetudbydere editionsplæg om udlevering af de pågældende oplysninger.

Interesseafvejning

Som nævnt ovenfor i afsnit 3.1.2.3 følger der imidlertid af EU-Domstolens praksis nu også et krav om en interesseafvejning, idet der over for hensynet til en effektiv håndhævelse af ophavsretten også er et hensyn at tage til indehaverens ret til persondatabeskyttelse og privatlivets fred. Alle tre hensyn er i vidt omfang EU-retligt regulerede, og EU-Domstolen har da også haft lejlighed til at tage stilling til afvejningen af dem i relation til ophavsretten.

EU-Domstolens praksis

I Promusicae-sagen⁹³ skulle EU-Domstolen således besvare et præjudicielt spørgsmål, som netop vedrørte udlevering af navne og adresser på internetabonnenter. I sagen havde en spansk rettighedshaverorganisation, Promusicae, anlagt sag om foreløbige foranstaltninger mod teleselskabet Telefónica med henblik på at få udleveret navne bag IP-adresser, som var tildelt af Telefónica, og som angiveligt var blevet brugt til ulovlig fildeling via P2P-tjenesten KaZaA. Telefónica nægtede at udlevere disse oplysninger, idet selskabet gjorde gældende, at dette efter spansk lovgivning kun var tilladt under en strafferetlig undersøgelse eller med henblik på at beskytte den offentlige sikkerhed og det nationale forsvar, men ikke under en civil retssag eller som foreløbig foranstaltning. Spørgsmålet, som herefter blev forelagt Domstolen, var – lettere omformuleret – om medlemsstaterne efter EU-retten skal pålægge internetudbyderne pligt til at videregive personoplysninger under en *civil retssag* med det formål at sikre en effektiv beskyttelse af ophavsretten.⁹⁴

Domstolen måtte for at besvare spørgsmålet i sagen afveje hensynet til en effektiv håndhævelse af ophavsretten mod hensynet til navnlig persondatabeskyttelsen, kommunikationshemmeligheden og privatlivets fred. Alle hensyn er reguleret i forskellige EU-direktiver, nemlig e-databeskyttelsesdirektivet,⁹⁵ e-handelsdirektivet, Infosoc-direktivet og retshåndhævelsesdirektivet samt charteret. Domstolen lagde til

⁹³ Domstolens dom af 29. januar 2008 i sag C-275/06.

⁹⁴ Jf. præmis 41.

⁹⁵ Jf. præmis 45. E-databeskyttelsesdirektivet er Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT 2002 L 201, s. 37). Direktivet er revideret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EUT 2009 L 337, s. 11).

grund, at videregivelse af oplysninger om navne og adresser på brugere af KaZaA – dvs. på personer, som anvender en fildelingstjeneste – udgør en behandling af personoplysninger som omhandlet i e-databeskyttelsesdirektivet. Efter at have undersøgt og sammenholdt de relevante direktiver kunne Domstolen konkludere, at navnlig beskyttelsen af personoplysninger går forud for retshåndhævelsessyn,⁹⁶ og at direktivbestemmelserne ikke pålægger medlemsstaterne at fastsætte en *pligt* for internetudbydere til at videregive personoplysninger med henblik på at sikre den effektive beskyttelse af ophavsretten under en civil retssag.⁹⁷ På den anden side er direktiverne ikke til hinder for, at de gør det. Når medlemsstaterne og deres myndigheder gennemfører og fortolker direktiverne – og altså i denne forbindelse udsteder regler og afsiger domme og kendelser om internetudbyderes udlevering af personoplysninger – skal de imidlertid ”sikre den rette afvejning af de forskellige grundlæggende rettigheder, der er beskyttet af Fællesskabets retsorden” og samtidigt iagttage ”almindelige fællesskabsretlige principper, såsom proportionalitetsprincippet.”⁹⁸ Da den danske tredjepartseditionsregel i kombination med reglen om isoleret bevisoptagelse som nævnt giver adgang til at pålægge internetudbydere at udlevere oplysninger om IP-adresser, *uden* at en retssag verserer, må disse regler dog skulle fortolkes i overensstemmelse med Domstolens resultat.⁹⁹

EU-Domstolen har desuden i sin dom i Bonnier Audio-sagen¹⁰⁰ fastslået, at det senere annullerede logningsdirektiv¹⁰¹ ikke er til hinder for lovgivning om pligt til udlevering af oplysninger med henblik på at få fastslået en krænkelse af intellektuelle ejendomsrettigheder, idet formålet hermed er et andet end det, logningsdirektivet forfulgte.¹⁰²

Hvad der nærmere ligger i den ovenfor nævnte ”rette afvejning” må medlemsstaterne udlede af de direktiver, som beskytter rettighederne, og af de nationale gennemførelsesbestemmelser hertil.¹⁰³

⁹⁶ Jf. præmis 57.

⁹⁷ Jf. præmis 58-60.

⁹⁸ Præmis 70.

⁹⁹ Jf. Søren Sandfeld Jakobsen i Juristen 2008, nr. 10, s. 305-312, på s. 308.

¹⁰⁰ Dom af 19. april 2012 i sag C-461/10.

¹⁰¹ Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikations-tjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT 2006 L 105, s. 54). Logningsbekendtgørelsen er fortsat i kraft, men kravet om sessionslogging er taget ud.

¹⁰² Op.cit., fodnote 100, præmis 38-45, særligt præmis 45.

¹⁰³ Jf. dommens præmis 66.

Danmark

Som nævnt har internetudbydere i Danmark ikke en generel pligt til at udlevere oplysninger om IP-adresser, men de kan ved kendelse pålægges at gøre det gennem editionsreglerne. Da disse regler ikke udtrykkeligt kræver hensyntagen til hverken grundlæggende rettigheder eller proportionalitetsprincippet, men kan anvendes, når det skønnes hensigtsmæssigt, jf. afsnit 3.1.2.3 ovenfor, er spørgsmålet, om domstolene – efter Promusicae-dommens krav om en afvejning af de relevante grundlæggende rettigheder og hensyntagen til proportionalitetsprincippet – anvender reglen mere restriktivt end det, der ligger i den brede skønsbeføjelse.

Det bemærkes i den forbindelse, at landsretterne i de to ovennævnte kendelser kun tog stilling til, om tredjepartseditionsreglen i kombination med reglen om isoleret bevisoptagelse gav hjemmel til at kræve oplysningerne udleveret uden for retssag, mens det var byretterne – der efter at sagerne var blevet hjemvist – skulle afgøre, om det i den konkrete sag var hensigtsmæssigt at pålægge editionspligt. Hvad afgørelserne blev, vides ikke, men de ligger under alle omstændigheder før dommen i Promusicae-sagen, og allerede af den grund, er det mindre interessant, hvad byretterne dengang lod indgå i hensigtsmæssighedsvurderingen.

Editionskendelser afsiges i første instans af byretterne og er ikke umiddelbart tilgængelige. Så vidt vides har landsretterne heller ikke afsagt flere kendelser i kæresager om tredjemandseditionspålæg til internetudbydere uden for retssag siden de to ovenfor omtalte kendelser. Det kan derfor ikke uden videre undersøges, om vurderingen er ændret, så det nu på grund af den krævede interesseafvejning og proportionalitetsvurdering er blevet sværere for rettighedshaverne at få adgang til internetudbydernes oplysninger om navne bag IP-adresser.

Norge

I Norge er en sag om spørgsmålet netop blevet afgjort af Høyesterett.¹⁰⁴ Sagen vedrørte den norske ophavsretslov § 56 b, der fastsætter betingelserne for, at blandt andre internetudbydere må udlevere oplysninger, som identificerer navne bag IP-adresser. For det første gælder et krav om retskendelse og et sandsynliggørelseskrav vedrørende den formodede krænkelse, for det andet skal den norske myndighed svarende til Datatilsynet forud anmodes om at fritage internetudbyderen for den tavshedspligt, som efter den

¹⁰⁴ Norsk Høyesterets kendelse af 26. april 2017, HR-2017-833-A, sag nr. 2016/2216.

norske e-handelslovs §§ 2-9 påhviler blandt andre internetudbydere om indholdet af elektronisk kommunikation, og for det tredje skal der foretages en afvejning af hensynet til abonnenten mod rettighedshavernes interesse, henset til krænkelsens grovhed, omfang og skadevirkninger. Når disse krav er opfyldt – og altså kun, hvis interesseafvejningen falder ud til rettighedshaverens fordel – kan der gøres undtagelse fra tavshedspligten.

Baggrunden for sagen var den, at det danske Scanbox Entertainment havde konstateret krænkelse af ophavsretten til en film begået fra otte computere ved hjælp af *bittorrent*-teknologien. De anvendte IP-adresser tilhørte Telenor Norge. Borgarting lagmannsrett bestemte, at oplysningerne ikke skulle udleveres, fordi krænkelseerne ikke havde et tilstrækkeligt omfang. Scanbox Entertainment appellerede afgørelsen til den norske Høyesterett, som dog også gav Telenor Norge medhold.

Den norske højesteret lagde til grund som uomtvistet, at sandsynliggørelseskravet var opfyldt. Den henviste herefter til forarbejderne til ophavsretsloven og fremhævede hensynet til rettighedshavernes muligheder for i praksis at håndhæve deres rettigheder ved krænkelse på internettet, idet internettet netop har vanskeliggjort den civilretlige håndhævelse på grund af teknologier, som gør det svært at vurdere omfanget af fildelingen.¹⁰⁵ Retten fandt, at det ikke kan være udslagsgivende i sig selv, at det er umuligt at føre bevis for krænkelsens omfang.¹⁰⁶ Derimod skal der foretages en konkret afvejning i hver enkelt sag af hensynet til beskyttelsen af personoplysninger over for rettighedshavernes interesser, hvori også indgår elementer som krænkelsens omfang, grovhed, skadevirkninger og værkstype.¹⁰⁷

Sammenfatning og perspektiver – udlevering af abonnentoplysninger

Det er klart, at den norske kendelse ikke umiddelbart har betydning for retsstillingen i Danmark. Det er imidlertid bemærkelsesværdigt, at den interesseafvejning og hensyntagen til krænkelsens grovhed, omfang og skadevirkninger, som den norske højesteret – og norsk lovgivning – kræver, er meget lig den interesseafvejning og proportionalitetsvurdering, som EU-Domstolen har beskrevet i dommen i *Promusicae*-sagen. Baggrunden for den norske sag er meget aktuel i forhold til ophavsretskrænkelser på internettet, hvor rettighedshaverne har brug for oplysninger fra internetudbydere for

¹⁰⁵ Præmis 31.

¹⁰⁶ Præmis 35.

¹⁰⁷ Præmis 37.

at kunne forfølge krænkelseerne. Efter den hidtidige danske retsstilling har de som beskrevet kunnet få det, hvis blot det var hensigtsmæssigt, og i vurderingen heraf har det haft en vis vægt, at de kun derved kunne varetage deres interesser. Hvordan byretterne konkret har foretaget hensigtsmæssighedsvurderingen, samt om og hvordan proportionalitetsprincippet og hensynet til beskyttelsen af personoplysninger er blevet vægtet, fremgår ikke af den trykte praksis.

For så vidt som der tilsyneladende ikke foreligger nyere, trykte danske domme med en konkret interesseafvejning og proportionalitetsvurdering, er det uklart, om en sådan faktisk foretages, eller om hensigtsmæssighedsvurderingen står alene. For rettighedshaverne vil det være interessant at få nogle vejledende angivelser af, hvordan f.eks. krænkelsens omfang og grovhed bedømmes. I den norske sag var det under bagatelgrænsen, at otte brugere hver havde downloadet én film. Men er det antallet af formodede krænkere eller antallet af værker, eller kombinationen, der skal være afgørende? Har det betydning for vægtningen af hensynet til internetudbyderens interesser og hensynet til beskyttelsen af personoplysninger, at internetudbyderen – som tredjemand – ikke *ønsker* at møde i retten,¹⁰⁸ og at den formodede krænker – der endnu ikke er identificeret – ikke *kan* møde i retten og varetage sine interesser? Og er vægtningen af sidstnævnte hensyn den samme i en sag med ti formodede krænkere, som hver har downloadet én film, som i en sag, der omfatter tusinde krænkere, der hver især også kun har downloadet én film? Fra den enkelte brugers synsvinkel er hensynet lige vægtigt.

Som retspraksis viser, har det i hvert fald i nogle tilfælde hidtil været muligt for rettighedshaverne at få oplysningerne udleveret, men det er jo tænkeligt, at det i andre tilfælde, måske mange, ikke har været det. Oprindeligt var det som nævnt hensigten, at der skulle være en bred adgang til at anvende reglen om isoleret bevisoptagelse, og reglen synes også anvendt i overensstemmelse hermed i forhold til internetudbyderes udlevering af abonnementsoplysninger. Denne adgang er indsnævret af EU-Domstolen. Hvis dette fører til en skærpelse af praksis ved de danske domstole, vil det begrænse rettighedshavernes muligheder for at håndhæve deres ophavsrettigheder i alle de tilfælde, hvor de er afhængige af internetudbyderne for at kunne identificere de formodede krænkere.

¹⁰⁸ TDC udtalte i oktober 2015 til Information, at "[d]et er en helt sædvanlig fremgangsmåde for TDC og andre bredbåndsudbydere [ikke at deltage i retsmødet]", jf. www.information.dk.

Ny teknologi – nyt problem

Et er, at rettighedshaverne kan få pålagt internetudbydere at oplyse, hvem IP-adressen er knyttet til på krænkelsetidspunktet. Noget andet er, om det faktisk er muligt for internetudbydere. Nogle internetudbydere anvender nemlig nu en teknologi,¹⁰⁹ som tillader, at flere brugere deles om den samme IP-adresse på samme tid. Fra rettighedshavernes synspunkt gør denne teknologi sporingen mere besværlig, for selv med kendskab til både IP-adressen og kommunikationstidspunktet er det ikke muligt at henhøre en krænkende handling til en bestemt enhed. Enheden skal findes blandt måske hundredvis af brugere af den samme IP-adresse. Også dette er muligt, men det kræver, at internetudbydere foretager en såkaldt sessionslogning af trafikken, som – foruden IP-adresser og kommunikationstidspunkter – også registrerer portnumre. En sådan logning er dyr, ikke sædvanlig i telebranchen og heller ikke lovpligtig.

Der findes så vidt vides ikke oplysninger om problemets omfang set fra rettighedshavernes synsvinkel, men det kan vel antages at vokse i takt med udbredelsen af teknologien. Og udviklingen stopper nok ikke her, men vil – med nye teknikker – give rettighedshaverne nye udfordringer ved sporingen og identifikationen af brugerne.

I det følgende er udgangspunktet dog den nuværende tekniske situation og retstilstand, nemlig at rettighedshaverne ved hjælp af deres egne oplysninger om IP-adresser kombineret med oplysninger udleveret af internetudbydere faktisk kan identificere de formodede direkte krænkere og tage håndhævelsesskridt på grundlag heraf.

Et muligt næste skridt er de ovenfor i afsnit 3.5 omtalte breve til de formodede krænkere. I afsnittet nedenfor peges på fordele og ulemper ved dette håndhævelsesskridt set fra rettighedshavernes synsvinkel.

5.1.2 Breve til formodede krænkere

Baggrund og udbredelse

Fremgangsmåden blev i en årrække i 00'erne brugt af Antipiratgruppen, der sendte brevene som led i en større kampagne mod navnlig musikpirateri. De blev i den forbindelse kendt for slogans som "Parkeringsbøder bliver din mindste bekymring", og "Vi sagsøger dig ind i helvede". Om det var fordi, dette gav en del modvind i medierne, eller fordi lovlige musikstreamingtjenester mindskede pirateriproblemet, at strømmen af

¹⁰⁹ Carrier-grade NAT eller bare NAT-teknologi (Network Address Translation).

breve aftog, er ikke til at sige. Måske har det været medvirkende, at rettighedshaverne i senere retssager ikke har kunnet løfte bevisbyrden for, at det er internetabonnenten selv, der har begået den ophavsretskrænkelser, som hans IP-adresse er blevet forbundet med, jf. nærmere herom nedenfor i afsnit 5.1.3.

Tiltag fra officiel side

Det skal bemærkes, at det tidligere også fra officiel side har været overvejet at indføre en såkaldt ”brevmodel”. I en rapport fra Kulturministeriet fra 2011¹¹⁰ lød anbefalingen på en model, hvor rettighedshaverorganisationer skulle have til opgave at spore anvendte IP-adresser og videregive oplysningerne til internetudbydere sammen med et informationsbrev på eget brevpapir. Internetudbydere skulle så, uden retskendelse, identificere abonnenterne og sende informationsbrevet til disse. Når en abonnent havde modtaget brevet to gange, skulle internetudbyderen i stedet for at sende et tredje brev informere rettighedshaverorganisationen. Der skulle ikke være knyttet sanktioner til informationsbrevet, idet hensigten navnlig var at gøre internetabonnenten opmærksom på problemet, få stoppet eventuelle ulovlige aktiviteter og opfordre til sikring af internetforbindelsen. Modellen blev kritiseret for at vægte rettighedshavernes interesser for højt i forhold til internetabonnenternes retssikkerhed og for at øge overvågningen på internettet. Den blev ikke vedtaget.

I de seneste par år er den ”private metode” imidlertid blevet taget i brug igen af rettighedshaverne – at dømme efter nyhedsstrømmen på både analoge og digitale medier i ikke ubetydeligt omfang. Der er denne gang tilsyneladende typisk tale om streaming af en enkelt film fra en ulovlig tjeneste.

Fordele

For rettighedshaverne er der da også flere fordele forbundet med denne form for håndhævelse, og som det er fremgået ovenfor, er det muligt at formulere brevet på en måde, som opfylder Advokatnævnets krav til god advokatskik.

En helt indlysende fordel er, at det er billigt. Der er uden tvivl tale om standardbreve, der hurtigt kan flettes med de navne og adresser, som internetudbydere har udleveret. Også set i forhold til udgifterne til retssager – og risikoen for at tabe dem – forekommer metoden særdeles attraktiv. Desuden er mange af adressaterne formentlig kun ”småkrænker”, hvorfor det vil være ineffektivt at føre sagerne ved domstolene.

¹¹⁰ Rapport fra udvalget om ophavsrettigheder på internettet, Kulturministeriet, 2011.

Der ligger en yderligere fordel i den forebyggende eller opdragende effekt, som brevene må formodes at have. For en internetabonnent, som slet ikke har foretaget en ulovlig handling, vil brevet måske give anledning til en snak i husstanden om ophavsret og lovlig adfærd på internettet. Og for en forsætlig bruger af en ulovlig tjeneste kan det føre til overvejelser om konsekvenserne.

Det er selvfølgelig ikke alle brevmodtagere, som ønsker at indgå det tilbudte forlig, og det er umuligt at vurdere, hvor meget rettighedshaverne økonomisk får ud af denne form for håndhævelse. Under alle omstændigheder kan brevet have ført til en korrespondance og oplysninger fra brevmodtagerne, som kan indgå i rettighedshaverens grundlag for at afgøre, om en retssag i givet fald skal indledes.

I den forbindelse kan breve som disse have en betydning i forhold til ansvarsgrundlaget. Som nævnt ovenfor er simpel uagtsomhed tilstrækkeligt til at ifalde erstatningsansvar for ophavsretskrænkelser. En internetbruger, som streamer film ulovligt, kan naturligvis ikke undskylde sig med ikke at have kendt ophavsretslovens § 2, men derimod måske med ikke at have vidst, at han med sin aktivitet på internettet foretog en ulovlig midlertidig eksemplarfremsstilling. Højesteret har ganske vist fastslået,¹¹¹ at det er uagtsomt ikke at gøre sig bekendt med, hvad det indebærer at benytte et fildelingsprogram, og det samme vil formentlig gælde andre tjenester og teknologier til ulovlig distribution af ophavsretligt beskyttet materiale. Med internettets mange veje og vildveje kan det dog ikke udelukkes, at en bruger rent hændeligt har fået lagt en ulovlig kopi på sin computer eller delt den. Udgangspunktet er dog det modsatte – at det er brugerens eget ansvar at finde ud af, om en tjeneste eller teknologi er lovlig eller ulovlig. Under alle omstændigheder vil et brev til brugeren med ovennævnte indhold bringe ham i ond tro, formentlig også i forhold til et eventuelt medvirkensansvar for andres brug af hans internetforbindelse.

Ulemper

Heroverfor ligger der en ulempe i, at brevene ikke bliver lige vel modtaget hos alle adressater. Nogle føler sig overvågede og er fortørnede over, at deres aktiviteter på internettet er blevet sporet. Brevene opfattes ikke som forligstilbud, men omtales som advarselsbreve, trusselsbreve og endda afpresning, og internettet svømmer over med råd

¹¹¹ U 2011.1736 H. Omtalt nedenfor i afsnit 5.1.3.

om, hvordan man skal forholde sig over for advokaterne, der opfattes som aggressive og griske.

Vreden over brevene hos nogle af modtagerne kan hænge sammen med, at de ikke opfatter det som forkert at downloade noget, som de har været i god tro om lovligheden af, eller at de mener, at ophavsretten beskytter for bredt. Til det kan man sige, at nok er ophavsrettens originalitetskrav måske ikke så strengt, og nok beskytter ophavsretten også værket i ændret skikkelse, men ved upload eller download til og fra f.eks. ulovlige fildelingstjenester, og ved de fleste ophavsretskrænkelser på internettet i øvrigt, er det en helt slavisk kopi, brugeren tilgængeliggør eller fremstiller. Brugeren kan dog også være af den opfattelse, at ophavsretten slet ikke har nogen berettigelse. I forhold til begge synspunkter må svaret ligge i sådanne forebyggende og oplysende tiltag, som det ligger uden for dette speciales rammer at behandle.

5.1.3 Civil retssag mod brugere

Bevisproblemet

Hvis en retssag er anlagt mod brugere, som er identificeret ved hjælp af IP-adresser kombineret med internetudbydernes oplysninger om disse, opstår et helt grundlæggende problem vedrørende beviset. Sagsøger skal – hvis han påstår erstatning – kunne bevise, at sagsøgte har handlet mindst simpelt uagtsomt, jf. ovenfor i afsnit 3.3.1, og – hvis han påstår bødestraf – mindst groft uagtsomt, jf. afsnit 3.3.3. Sagsøgeren er naturligvis – og i overensstemmelse med dansk rets altovervejende hovedregel – ikke objektivt ansvarlig for brugen af sin internetforbindelse. Internetforbindelsen kan have været brugt af andre medlemmer af eller gæster i hustanden og af andre udenfor, men i nærheden af hjemmet.

Vestre Landsrets dom i U 2009.280 V er illustrerende for det sidste. Rettighedshaverne havde ved hjælp af sporingsprogrammet DCAgent konstateret, at sagsøgtes internetforbindelse var blevet brugt til ulovlig tilgængeliggørelse af små to tusinde musiknumre via P2P-fildelingsprogrammet Direct Connect. Sagsøgte boede alene i en lejlighed, men med mange andre lejligheder både i ejendommen og i nærheden, og hans internetforbindelse var hverken sikret ved kryptering eller password. Han oplyste, at han ikke interesserede sig særligt for musik og ikke havde musik på sin computer, at han ikke kendte Direct Connect-programmet, og at computeren var spærret med en kode og kun brugt af ham.

Landsretten fandt det på grundlag af sagens oplysninger bevist, at sagsøgte var indehaver af IP-adressen, og at der gennem denne var blevet stillet det pågældende antal musiknumre til rådighed. Under hensyn til at forbindelsen ikke var sikret, og at der var mange andre lejligheder i området, kunne landsretten imidlertid ikke udelukke, at det var andre, der havde misbrugt IP-adressen.

Situationen kunne også have været den, at internetforbindelsen – sikret eller ej – var blevet anvendt af andre medlemmer af husstanden end sagsøgte til ophavsretskrænkelser, men sådanne krænkelser vil en sagsøgt naturligvis heller ikke være erstatningsansvarlig for.¹¹²

Landsretten fastslog desuden for det første, at sagsøgte ikke havde pligt til at sikre sin trådløse internetforbindelse, og for det andet, at det ikke påhvilede ham at bevise, at han ikke havde krænket sagsøgerens rettigheder. Landsretten ville altså ikke vende bevisbyrden om. Sagsøgte blev derfor – på grund af det manglende bevis – frifundet for rettighedshavernes påstand om erstatning og vederlag.

I sager, der er startet med et brev til en formodet krænker, jf. ovenfor, er der i en enkelt nyere sag afsagt en byretsdom, som har været omtalt i medierne.¹¹³ Den sagsøgte blev idømt erstatning, men det fremgår af omtalen, at vedkommende havde erkendt forholdet. Sagen er derfor ikke et eksempel på, at rettighedshaverne har kunnet løfte bevisbyrden for krænkelse alene baseret på brugerens IP-adresse.

Omvendt bevisbyrde

Det ovenfor omtalte bevisproblem kunne lede til overvejelser om at omlægge bevisbyrden, så skadevolderen skal bevise, at han ikke har handlet uagtsomt. En sådan skærpelse af ansvaret kan pålægges af domstolene i konkrete tilfælde, men det er en væsentlig skærpelse i forhold til det almindelige culpaansvar.¹¹⁴ I en sag som ovennævnte er det svært at se berettigelsen. Den kan ikke ligge i en betragtning om, at sagsøgte – der var en almindelig pc- og internetbruger – havde bedre mulighed for at

¹¹² Et eventuelt hæftelsesansvar for hjemmeboende børn kan der dog blive tale om efter Lov nr. 363 af 13. maj 2009 om hæftelse for børns erstatningsansvar mv.

¹¹³ Se Christian Hansen: *Nu er det afgjort: Så meget kan det koste at se én film ulovligt*, www.mx.dk, 29. november 2016, og Mads Elkær: *Flere pirat-stævninger på vej i 2017*, www.computerworld.dk, 9. december 2016.

¹¹⁴ Jf. herom Von Eyben og Isager: *Lærebog i erstatningsret*, 2015, s. 176.

bevise, at han ikke havde foretaget fildelingen, end sagsøgerne havde for at bevise det modsatte. Rettighedshaverne i sagen var heller ikke tæt på det fulde bevis for uagtsomhed, og en stærk formodning herfor var ikke skabt, således at det eventuelt kunne anses for rimeligt at pålægge sagsøgte at afkræfte denne.

Konklusionen kunne måske blive en anden i dag. Det er ikke længere sædvanligt for almindelige internetabonnenter at have usikrede trådløse internetforbindelser, og i mange opsætninger med trådløse routere indgår kryptering nu som standard, bl.a. som følge af stigende opmærksomhed på mulighederne for misbrug. Argumentet skulle være, at det dermed er uagtsomt ikke at have kode på sin internetforbindelse, ligesom det i forsikringsmæssig sammenhæng er det ikke at låse sin dør, og at det da må blive sagsøgte, der skal bevise, at han ikke har begået krænkelser via sin usikrede internetforbindelse. Et modargument er dog, at en kodet internetforbindelse kan hackes, uden at det efterlader synlige spor som på en opbrudt dør.

Der blev i 2008 afsagt yderligere tre landsretsdomme i lignende sager vedrørende brug af fildelingsprogrammet Direct Connect.¹¹⁵ I de to af dem blev resultatet det samme som i U 2009.280 V – de sagsøgte kunne ikke holdes ansvarlige for deres usikrede internetforbindelser. Der er så vidt vides ikke senere afsagt domme, hvor den sagsøgte er blevet dømt efter at have oplyst ikke at have sikret sin internetforbindelse.

Krav til beviset

I den tredje sag fra 2008¹¹⁶ var der ikke tale om en usikret trådløs internetforbindelse. Computeren havde trådløs komponent, men sagsøgte havde ingen trådløs router. Ifølge den udmeldte skønsmand var der derfor kun adgang til internetforbindelsen via computeren i hustanden, som kun omfattede sagsøgte. Sagsøgte erkendte at have brugt Direct Connect-programmet et par gange uden at gøre sig bekendt med, hvad dette indebar. Vestre Landsret fandt det på denne baggrund bevist, at sagsøgeren havde handlet uagtsomt og tilgængeliggjort det omhandlede antal musiknumre.

Denne sag blev imidlertid anket til Højesteret, sag U 2011.1736 H, hvor den fik et andet resultat. Højesteret lagde vægt på, at rettighedshaverne ikke havde redegjort for retningslinjerne for deres kontrolarbejde ved hjælp af DCAGENT, herunder hvordan

¹¹⁵ Østre Landsrets domme af 5. september 2008 i sagerne B-19-08 og B-52-08 og Vestre Landsrets dom af 20. oktober 2008 i sag B-0292-07, alle utrykte.

¹¹⁶ B-0292-07, jf. fodnoten ovenfor.

kontrollen af bilagene, som viste lister med de mange værker på den pågældende IP-adresse, var blevet udført. Det var således værdien af det digitale bevismateriale, som blev draget i tvivl. Rettighedshaverne havde derfor efter Højesterets opfattelse ikke godtgjort, at de mange musiktitler anført i bilagene dækkede over musikværker på sagsøgtes computer.

Bevissikring

Højesteret henviste i denne forbindelse til muligheden for bevissikring efter RPL kapitel 57 a, jf. afsnit 3.1.2 ovenfor. Denne mulighed havde rettighedshaverne ikke udnyttet, hvilket tilsyneladende kom dem til skade.

Mange krænkelse på internettet begås af private, og det er derfor interessant, hvor meget eller lidt der skal til, for at kravet om formodede krænkelse af ”ikke ubetydeligt omfang” er opfyldt, således at bevissikringsinstituttet kan anvendes med henblik på undersøgelse i private hjem.

I ovennævnte sag for Højesteret ville rettighedshaverne ved en sådan bevissikring kunne have fået undersøgt sagsøgtes computer og sikret sig det bevis for krænkelse, som de digitale bilag ikke udgjorde. Da Højesteret henviste til muligheden for bevissikring, må det antages, at den anså disse digitale bilag for at ville kunne opfylde kravene til sandsynliggørelse af, at sagsøgte havde begået krænkelse, og at der var grund til at antage, at bevis derfor kunne findes i hans hjem. I sagen var der tale om ca. 13.000 musiknumre, altså et ganske betydeligt omfang. I den krævede proportionalitetsvurdering ville dette omfang formentlig også have vejet tungere end hensynet til privatlivets fred. Sagsøgerne kunne uden tvivl også have fået foretaget undersøgelsen uden forudgående underretning, fordi der ville være risiko for, at genstanden for undersøgelsen ellers ville blive fjernet, tilintetgjort eller ændret, jf. RPL § 653 a, stk. 2, 2. pkt.

I det konkrete tilfælde er der i det hele taget næppe tvivl om, at rettighedshaverne ville have kunnet benytte dette foreløbige retsmiddel, som netop også er indført for at afhjælpe bevisproblemer inden for immaterialretten.

Der vil dog altid skulle foretages en konkret vurdering, og i andre tilfælde vil anmodningen blive afslået. I U 2013.2890 Ø fremgår det af referatet af fogedrettens afgørelse, at denne havde fundet, at undersøgelsen ikke ville være proportional i forhold

til rekvirentens interesse over for hensynet til privatlivets fred. Der var kun tale om en mistanke om, at der var tilgængeliggjort to film og to afsnit af en tv-serie i en kort periode, og det var ikke sandsynliggjort, at rekvisitus havde været den første til at dele materialet, inden dvd-release, eller at rekvisitus var bagmand inden for piratmiljøet. For landsretten blev der dog fremlagt yderligere bevismateriale, som sandsynliggjorde tilgængeliggørelse i en længere periode, for nogle værkers vedkommende også inden dvd-release, således at proportionalitetsprincippet var opfyldt.

Da det er fogedretterne, der foretager proportionalitetsvurderingen i første instans, er praksis for denne ikke umiddelbart tilgængelig, undtagen selvfølgelig i kæresager som ovenstående. En del fogedretskendelser er dog omtalt i litteraturen¹¹⁷. På baggrund af denne omtale og ovenstående sager synes der i sager om ophavsretskrænkelser på internettet blandt andet at blive lagt vægt på, om de formodede krænkelser er foretaget som led i erhvervsvirksomhed eller privat, og at der ved f.eks. ulovlig fildeling må foretages en helhedsvurdering, der omfatter antallet af delte filer og delingens omfang.¹¹⁸ Fogedretternes praksis viser tilsyneladende også, at der ved *tilgængeliggørelse* på internettet anlægges en streng bedømmelse, fordi omfanget da per definition er ”ikke ubetydeligt”.¹¹⁹

I de formentlig mange tilfælde, hvor ulovlig eksemplarfremsstilling og tilgængeliggørelse via internettet sker uden erhvervsmæssigt sigte, synes der således at være forholdsvis nem adgang til bevissikring efter reglerne i RPL kapitel 57 a, når den formodede krænkelse har et vist omfang. Til det bemærkes, at f.eks. ulovlig streaming ved hjælp af *bittorrent*-teknologi indebærer både eksemplarfremsstilling og tilgængeliggørelse, jf. afsnit 2.5, og derfor må blive ramt af den strenge bedømmelse nævnt ovenfor, mens ”almindelig” streaming kun indebærer eksemplarfremsstilling. Hvis der da kun er tale om streaming af en enkelt eller nogle få film, vil bevissikringsinstituttet næppe kunne anvendes, fordi hensynet til den formodede krænkers privatliv – rimeligt nok – vil vinde over rettighedshaverens interesser.

¹¹⁷ Se f.eks. Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 301-304, og Høyer og Mathiasen: *Bevissikringsinstituttet i praksis*, NIR 2005, s. 193.

¹¹⁸ Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 301-302.

¹¹⁹ Høyer og Mathiasen: *Bevissikringsinstituttet i praksis*, NIR 2005, på s. 195-196, med henvisning til FS 4-1798/2004, FS 20-9376/2003, FS 20-9377/2003, FS 20-4770/2002 og FS 5-868/2004.

Erstatningsudmålingen

Resultatet i U 2011.1736 H adskilte sig også fra landsrettens dom med hensyn til erstatningsudmålingen. Landsretten havde anvendt det såkaldte ”dobbelt-op”-princip, ifølge hvilket det rimelige vederlag for udnyttelsen af ophavsretten først beregnes, hvorefter erstatningen for det yderligere tab fastsættes til det samme beløb, således at den samlede erstatning bliver det dobbelte af vederlaget, uanset det yderligere tabs størrelse. Anvendelsen af denne metode havde landsretten tidligere begrundet i, at der er behov for generelt anvendelige principper, fordi krænkelserformerne til stadighed kan ændre sig, kontrolforanstaltninger kan være bekostelige, og markedsforstyrrelser særdeles vanskelige at gøre op.¹²⁰ Ved beregningen af vederlaget tog landsretten herefter udgangspunkt i principper, som rettighedshaverne havde anført, nemlig et skønnet vederlagskrav pr. værk ganget med det antal kopieringer, som krænkeren *som minimum skønnedes* at have foretaget. Et beløb af samme størrelse blev herefter lagt til som erstatning for markedsforstyrrelse, hvorefter det samlede beløb i vederlag og erstatning blev kr. 160.000.

Højesteret lagde vægt på, at rettighedshaverne hverken havde givet oplysninger, som kunne danne grundlag for fastsættelsen af det rimelige vederlag, dokumenteret det nærmere omfang af krænkelserne eller underbygget deres påstand om erstatning. Vederlaget og erstatningen måtte derfor fastsættes på grundlag af et skøn, som var forbundet med betydelig usikkerhed. Højesteret fastslog også – konkret i forhold til sager om retsstridig tilgængeliggørelse af musikværker og lignende over internettet – at der ikke er grundlag for at udmåle erstatningen i forhold til vederlagets størrelse, og afskaffede dermed ”dobbelt-op”-princippet i sådanne sager. Der er nok heller ikke grundlag for at anvende det i andre sager, idet det klare udgangspunkt jo er, at erstatning fastsættes på grundlag af det lidte tab.

Det bemærkes vedrørende erstatningsudmålingen, at der i sager mod brugeren af en ulovlig tjeneste eller hjemmeside, hvor der er tilgængeliggjort store mængder af ophavsretligt beskyttet materiale, og derfor idømt et stort samlet vederlags- og erstatningskrav, kan være grundlag for at nedsætte erstatningen efter erstatningsansvarslovens § 24, når ansvaret ”vil virke urimeligt tyngende for den erstatningsansvarlige” på grund af dennes økonomiske situation. Et eksempel på nedsættelse findes i U 2005.60 V. Sagen vedrørte en indehaver af en hjemmeside og er derfor omtalt nedenfor i afsnit 5.2.

¹²⁰ U 2005.60 V.

Der er som nævnt afsagt en enkelt nyere byretsdom i en sag baseret på den formodede krænkelsers IP-adresse.¹²¹ Der var tale om download af én film, og den sagsøgte blev idømt en erstatning på kr. 5.000.

Sammenfatning og perspektiver – civil retssag mod brugere

Det er et praktisk problem for rettighedshaverne, at en krænkelse ikke er bevist, blot fordi den kan henføres til en IP-adresse. Brugere har ikke pligt til at sikre deres internetforbindelse, og formodede krænkerne kan henvise til, at forbindelsen var usikret. At vende bevisbyrden om er betænkeligt og næppe effektivt, men kunne have en præventiv virkning.

Det digitale bevismateriale er ikke altid holdbart, men bevissikringsinstituttet kan – ved krænkelse af et vist omfang – afhjælpe dette. For så vidt som der ved tilgængeliggørelse anlægges en streng bedømmelse af proportionaliteten, således som der tilsyneladende har været praksis for ved fogedretterne, vil det være interessant for rettighedshaverne at få afklaret, om anvendelse af ny teknologi – som indebærer tilgængeliggørelse, uden at de formodede krænkerne nødvendigvis er klar over det – altid udløser en sådan streng bedømmelse.

Retspraksis viser, at rettighedshaverne ikke kan basere sig på faste principper ved beregningen af deres vederlags- og erstatningskrav. Omfanget af en krænkelse må dokumenteres, og sker det ikke, må retten foretage et skøn baseret på sagens oplysninger. Vanskelighederne ved at opgøre det yderligere tab fritager ikke rettighedshaverne for dokumentationskravet. I mindre krænkelsessager mod brugere af ulovlige tjenester kan erstatningen næppe bære omkostningerne ved sagen.

5.2 Indholdsudbydere

Ved indholdsudbydere forstås her den, der stiller selve det retsstridige indhold – det ophavsretskrænkende materiale – til rådighed.¹²² Der findes naturligvis også lovlige indholdsudbydere.

¹²¹ Jf. fodnote 113 ovenfor.

¹²² Trzaskowski (red.): *Internetretten*, 2012, s. 610.

Indholdsudbyderen kan være udvikleren af teknologien eller programmet bag f.eks. en ulovlig fildelings- eller streamingtjeneste eller enhver hjemmeside eller platform, der benytter teknologien eller stiller den til rådighed. Eksempler er The Pirate Bay og Popcorn Time. Indholdsudbyderen opnår ofte en indtægt eller omsætning fra reklamer på hjemmesiden.

5.2.1 Civil retssag mod indholdsudbydere

I stedet for at anlægge sag mod de primære ansvarssubjekter kan det overvejes, om udvikleren af systemet bag en ulovlig hjemmeside eller indehaveren af denne, typisk en fildelingstjeneste, kan gøres ansvarlig. Det er indlysende, at det vil være langt mere effektivt at gå mod selve tjenesten end mod de enkelte brugere af den.

Medvirkensansvar

Synspunktet er, at systemudvikleren medvirker til de ophavsretskrænkelser, som brugerne begår. Der skal dog lidt mere til end udvikling af en tjeneste eller teknologi for at statuere medvirken. Det illustreres i litteraturen ofte ved henvisning til den amerikanske Betamax-sag fra 1984.¹²³ Spørgsmålet var, om Sony kunne gøres medvirkensansvarlig for den ulovlige kopiering af film, som købere af Sonys videomaskiner eventuelt foretog, og svaret var selvfølgelig nej. Sony havde en svag forbindelse til brugerne, som alene lå i, at selskabet havde solgt maskinerne til dem. Den amerikanske højesteret lagde vægt på, at maskinerne i væsentligt omfang kunne bruges til lovlige formål, og at Sony ikke kunne være ansvarlig for brugernes ulovlige handlinger alene på grund af risikoen for misbrug.

Situationen var ganske anderledes i U 2005.60 V. Her havde systemudvikleren oprettet en ulovlig hjemmeside, som formidlede kontakt mellem brugere med henblik på ulovlig deling af film. Brugere oprettede filmlister og afgav kontaktoplysninger til hjemmesiden, således at udveksling af film direkte mellem brugerne kunne aftales. Indehaveren vedligeholdte hjemmesiden og vejledte brugerne. Der kunne ikke uploades eller downloades film til og fra hjemmesiden. Vestre Landsret udtalte, at det var ”ubetænkeligt at fastslå, at hjemmesiden havde til formål at opfordre til og medvirke til ulovlig kopiering og distribution af digitale filmværker [...]”.

¹²³ Se f.eks. Udsen: *IT-ret*, 2016, s. 289, Trzaskowski (red.): *Internetretten*, 2012, s. 470, og Mathiasen: *Fildeling*, NIR 2007, s. 51.

De primære krænkere var i denne sag brugerne af siden, som gjorde deres filmlister tilgængelige for andre brugere via siden, men indehaveren medvirkede altså ganske åbenbart til dette. Et erstatningsretligt medvirkensansvar kan som nævnt ovenfor pålægges efter de almindelige regler om flere erstatningsansvarlige og både for aktiv og passiv medvirken. I sagen her var der klart tale om aktiv medvirken, blandt andet fordi indehaveren opfordrede til de ulovlige handlinger. Indehaverens forbindelse til hjemmesiden og brugerne var åbenbar.

Der er så vidt vides ikke afsagt andre danske domme om medvirkensansvar for brugeres ulovlige fildeling,¹²⁴ men i litteraturen er udenlandsk retspraksis sammenfattet.¹²⁵ Af denne kan udledes nogle kriterier, som måske kan være anvendelige i mindre oplagte sager, hvor der er tale om en mere passiv medvirken. Først og fremmest forudsætter medvirkensansvar, at systemudvikleren eller hjemmesideindehaveren har en *konkret* viden om den ulovlige fildeling. En generel viden om, at misbrug er muligt, er ikke tilstrækkeligt. Hvis der derudover *opfordres* til den ulovlige handling, som i den danske sag, eller det ulovlige formål markedsføres, vil der formentlig kunne pålægges et medvirkensansvar. Den enkelte sag må imidlertid vurderes konkret, og i vurderingen vil desuden indgå omfanget af de ulovlige handlinger, forholdet mellem lovlige og ulovlige handlinger, en eventuel økonomisk interesse i ulovlighederne og systemudviklerens mere eller mindre aktive rolle.

Perspektiver

Det bemærkes vedrørende systemudviklerens rolle, at der i U 2005.60 V ikke lå nogen raffineret teknologi bag hjemmesiden, f.eks. *bittorrent*-teknologi, hvor udbyderen har en løs eller ingen direkte tilknytning til det ulovlige materiale og udvekslingen af det, således at han eventuelt kan undskylde sig med ikke at have været aktivt eller direkte involveret, fordi intet ophavsretligt beskyttet materiale passerer igennem hans system.

Under alle omstændigheder vil teknologien og f.eks. det forhold, at der ikke lagres ulovlige filer på en server, næppe være afgørende, og et medvirkensansvar vil formentlig også kunne gøres gældende mod tjenester, der anvender *bittorrent*-

¹²⁴ Jf. Udsen: *IT-ret*, 2016, s. 289.

¹²⁵ F.eks. Udsen: *IT-ret*, 2016, s. 292, hvis konklusioner ovenstående afsnit bygger på. Jf. også Mathiasen: *Fildeling*, NIR 2007, s. 46 ff.

teknologi,¹²⁶ mod de endnu knapt så kendte stream ripping-platforme, som er nævnt ovenfor, og i forhold til nye teknologier, som fremtiden vil bringe. I hvert fald kan de kriterier, som er skitseret ovenfor, godt tænkes at være opfyldt, nemlig en konkret viden om benyttelse til et ulovligt formål, opfordring til dette, udbredelse, forholdet mellem lovligt og ulovligt materiale og en økonomiske interesse i tjenesten.

Det vil sige, at håndhævelsen her ikke bremses af en teknikalitet, nemlig at der ikke lagres en midlertidig kopi hos systemudvikleren, idet dette ikke forhindrer et medvirkensansvar. Beskyttelsen af eneretten efter ophavsretsloven kan således rumme nye teknologier, omend det snarere skyldes medvirkensreglerne end lovens egne regler.

Når det således ser ud til at være muligt at opfylde kriterierne for at statuere et erstatningsretligt medvirkensansvar for krænkelse af ophavsretten på internettet, kan man undre sig over, at der ikke findes flere trykte domme, hvor det er sket. Måske er de på vej. Men en forklaring kan også være, at det simpelthen er svært at finde frem til folkene bag de moderne tjenester. Det oprindelige Popcorn Time er for længst lukket, og det er den danske udgave også,¹²⁷ men da programmet bag tjenesten var såkaldt *open source*, har det været nemt at kopiere det og herefter udbyde det under et nyt domænenavn. Derfor er tjenesten stadig tilgængelig under nye domæner,¹²⁸ og efterhånden som de lukkes ned, dukker nye formentlig op. Hvem der står bag sådanne og lignende platforme, kan ikke slås op i en IP-database – her vil der nok ofte være behov for politimæssig efterforskning.

5.2.2 Spærring eller lukning af ulovlige tjenester og hjemmesider

En måske mere fremkommelig vej kunne være at få gjort den ulovlige tjeneste eller hjemmeside utilgængelig for brugerne. Det giver ikke rettighedshaverne kompensation for den ulovlige udnyttelse af deres eneret, som allerede måtte være sket, men det kan forhindre yderligere tab.

¹²⁶ Det er blandt andet sket i Sverige i den meget omtalte sag mod hjemmesiden The Pirate Bay, jf. Stockholm Tingrätts dom af 17. april 2009 i sag B 13301-06, stadfæstet ved Svea hovrätts dom af 26. november 2010 i sag B 4041-09.

¹²⁷ Det skete ved, at Statsadvokaten for Særlig Økonomisk og International Kriminalitet i juni 2015 beslaglagde domænerne www.popcorn-time.dk og www.popcorn-time.dk og fik udleveret domænenavnene fra DK Hostmaster. Byrettens kendelse herom kan ses på domænerne.

¹²⁸ F.eks. <https://popcorn-time.to> og <https://popcorn-time-online.tv>.

Det relevante håndhævelsesinstrument i den forbindelse er de ovenfor omtalte regler om midlertidige forbud og påbud. Rettighedshaveren kan her ved en forbudskendelse mod den ulovlige tjeneste eller hjemmeside få bragt krænkelsen til ophør på et foreløbigt grundlag.

Rette rekvisitus

Østre Landsrets dom i U 2013.4 Ø viser dog, at det ikke altid er hensigtsmæssigt at rette dette håndhævelsesinstrument mod indholdsudbyderen. I denne sag havde fogedretten afsagt en kendelse om forbud mod rekvisiti brug af et krænkende varemærke, blandt andet på sin hjemmeside, og en kendelse om påbud om nedtagning af hjemmesiden. Rekvisitus var det selskab, som var den direkte krænkende part, dvs. hjemmesideindehaveren, men hverken denne eller hosteren af hjemmesiden ville rette sig efter påbuddet. Rekvisitus anførte, at indholdet på hjemmesiden efterfølgende var blevet ændret i forhold til rekvirentens indsigelser, og at det derfor var uproportionalt at kræve den nedtaget. Som bistand til gennemførelsen af påbuddet¹²⁹ pålagde fogedretten herefter et udenforstående domænenavnselskab at ophøre med at videresende trafik til hjemmesiden. Dette selskab kærede fogedrettens beslutning herom til Østre Landsret, der fastslog, at ordlyden af og forarbejderne til retsplejelovens regler om fogedrettens bistand til gennemførelse af et forbud eller påbud ”ikke indeholder hjemmel til at pålægge en udenforstående at bistå [hermed]”.

Perspektiver

Afgørelsen viser, at det er rekvisitus, som kan pålægges at gennemføre et forbud eller påbud, ikke andre. Det helt rimelige i dette følger af, at den udenforstående part jo slet ikke har været part i forbudssagen, og at der i forhold til ham blandt andet ikke er foretaget den proportionalitetsvurdering, som kræves efter RPL § 414, stk. 2. For rettighedshaveren giver det imidlertid anledning til at overveje, hvem et forbud eller påbud mest hensigtsmæssigt kan rettes imod. Det er ikke til megen nytte at have viden om, hvem indehaveren af en ulovlig hjemmeside er, og opnå en påbudskendelse om lukning af denne, hvis vedkommende ikke vil rette sig efter kendelsen. Fogedretten yder bistand til gennemførelsen af påbuddet, men naturligvis kun i det omfang, det er praktisk muligt. Den kan ikke selv lukke hjemmesider og altså heller ikke pålægge en udenforstående internetudbyder at gøre det.

¹²⁹ Fogedrettens bistand efter bestemmelsen i den daværende RPL § 645, stk. 1, i dag RPL § 424.

Hvis rettighedshaveren i stedet for at rette det midlertidige forbud eller påbud mod den egentlige krænker retter det imod internetudbyderen, kan dette valg formentlig få en betydning for proportionalitetsvurderingen, idet hensynet til en part, som kun objektivt har handlet retsstridigt, vil veje tungere end et tilsvarende hensyn til en egentlig krænker. Proportionalitetsvurderingen ved midlertidige forbud eller påbud mod internetudbydere behandles nedenfor i afsnit 5.3.3.

5.3 Formidlere og mellemmand

Som ovenstående analyse viser, kan rettighedshaverne støde på vanskeligheder ved håndhævelsen af deres rettigheder over for brugere og indholdsudbydere. Det er formentlig en af grundene til, at opmærksomheden i stigende grad også har været rettet mod andre end de direkte krænker, nemlig de formidlere, som stiller de ydelser og tjenester til rådighed, som gør det muligt at begå krænkelse. To af de ovenfor nævnte håndhævelsesproblemer – at de direkte krænker kan være svære at identificere, og at det kan være ineffektivt at gå imod enkelte krænker – vil måske netop *ikke* være aktuelle i forhold til formidlere. De er nemmere at identificere, og de har mulighed for at fjerne eller spærre for adgangen til ulovligt materiale eller hele hjemmesider for alle deres abonnenter eller brugere på én gang.

Formidlerne er mellemlid mellem de to hovedtyper af aktører, som har været genstand for behandlingen ovenfor – brugerne og indholdsudbydere. Der kan for det første være tale om formidlere, som giver *adgang* til internettet. Det gør egentlige netværksoperatører og internetudbydere i form af teleselskaber, men det gør også caféer, hoteller, lufthavne, universiteter og mange flere, når de stiller deres wi-fi-netværk til rådighed for brugerne. Samlet kaldes disse formidlere ofte blot internetudbydere. For det andet er der tale om formidlere, som udbyder forskellige *tjenester* på internettet, som – uanset om de har et lovligt formål – også kan benyttes til ulovlige formål som f.eks. ophavsretskrænkelser. Sådanne tjenester er blandt andet forskellige søgemaskiner som Google og Safari, det er sociale medier med brugergenereret indhold som Facebook og YouTube, og det er onlinemarkedspladser som eBay, Amazon og QXL. De kan samlet kaldes tjenesteudbydere.

Formidlerne varetager en samfundsgavnlig funktion ved at bidrage til et velfungerende internet med nem adgang til informationsudveksling. Denne rolle trues, hvis sådanne formidlere kan pålægges ansvar for udveksling af ulovlig information, som de ikke

kontrollerer eller har nogen egentlig forbindelse til. Også hensynet til erhvervsfriheden kommer her i spil. Og hvis formidlerne pålægges at overvåge informationsstrømmen på internettet, bringes hensynet til privatlivets fred og ytringsfriheden i fare.

Ovenstående er en del af baggrunden for de ansvarsfritagelsesregler, som er beskrevet i afsnit 4.1-4.3, og som nedenfor analyseres i forhold til internetudbydere og tjenesteudbydere. Hvis internetudbyderen eller tjenesteudbyderen er ansvarsfri, kan rettighedshaverne alternativt forsøge at få nedlagt forbud mod dem. Denne mulighed behandles i afsnit 5.3.3.

5.3.1 Internetudbydere

Ren videreformidling

En formidler – typisk en internetudbyder – som alene stiller midlerne til rådighed for, at andre kan sende f.eks. musikfiler over internettet, har normalt hverken viden eller burde viden om indholdet af disse filer og deres lovlighed eller ulovlighed. Hvis en piratkopieret film sendes over internettet, er transmissionen som udgangspunkt ikke udtryk for en uagtsom handling fra internetudbyderens side, og han kan derfor ikke blive straf- eller erstatningsansvarlig for krænkelsen.

Hvis formidleren bringes i ond tro, er situationen en anden. Et eksempel kunne være, at en rettighedshaver konstaterer, at en server anvendes til ulovlig distribution af ophavsretligt beskyttede værker ved hjælp af internetudbyderens netværk. Rettighedshaveren gør internetudbyderen opmærksom på dette og fremlægger dokumentation for krænkelse. Hvis internetudbyderen ikke herefter afbryder forbindelsen til serveren, vil han – med sit kendskab – være passivt medvirkende til krænkelse og kan ifalde straf- og erstatningsansvar efter dansk rets almindelige regler. E-handelsloven fritager ham dog for dette ansvar. Internetudbyderens aktivitet er her en ren videreformidling som omhandlet i EHL § 14, og da han ikke selv har taget initiativ til transmissionen, ikke har udvalgt modtageren og ikke har hverken udvalgt eller ændret den transmitterede information, jf. EHL § 14, stk. 1, nr. 1-3, er han ikke ansvarlig, selv om han altså havde kendskab og var i ond tro, fordi lovens § 14 – i overensstemmelse med EHD artikel 12 – ikke betinger ansvarsfriheden af ikke kendskab. I forhold til dansk rets almindelige regler har e-handelsloven dermed indskrænket formidlerens ansvar for ren videreformidling.

Det har været diskuteret i litteraturen, om dette har været tilsigtet.¹³⁰ Det fremgår af betragtning 42 til e-handelsdirektivet, at direktivets ansvarsfrihedsregler kun gælder, når formidleren ”hverken har kendskab til eller kontrol over” den transmitterede information, men kravet om ikke kendskab er ikke gentaget i reglen om ren videreformidling. I lovbemærkningerne er konflikten mellem direktivets ansvarsfrihedsregler og dansk rets almindelige regler nævnt generelt,¹³¹ og i litteraturen konkluderes det derfor, at det må have været hensigten at gøre formidleren ansvarsfri selv ved positivt kendskab.¹³²

Når en fil sendes via en internetforbindelse, kan det forekomme, at den undervejs lagres midlertidigt i systemet. Der fremstilles herved et midlertidigt transmissionseksemplar, jf. OHL § 11 a, som – hvis der ikke er lovligt forlæg som omhandlet i § 11, stk. 3 – udgør en selvstændig ophavsretskrænkelser, jf. den særlige danske implementering af Infosoc-direktivets artikel 5, stk. 1.¹³³ Det følger dog af EHL § 14, stk. 2, at formidleren heller ikke kan ifalde ansvar for en sådan ”automatisk, mellemliggende og kortvarig oplagring”, og det vil i overensstemmelse med ovenstående også gælde, selv om formidleren er i ond tro.

Internetudbydere kan også være erhvervsdrivende, der stiller et wi-fi-netværk til rådighed for deres kunder, besøgende eller andre. De vil ligeledes være ansvarsfri selv ved positivt kendskab, hvis de opfylder betingelserne i EHL § 14, stk. 1, nr. 1-3. Rettighedshaverne kan derfor ikke umiddelbart stille noget op over for ophavsretskrænkelser, som begås ved, at en person benytter et – måske ubeskyttet – wi-fi-netværk på f.eks. en café til at dele et ophavsretligt beskyttet værk uden rettighedshavernes tilladelse.

Situationen var omhandlet i Mc Fadden-sagen.¹³⁴ Her havde en erhvervsdrivende i Tyskland – Tobias Mc Fadden – stillet internetadgang til rådighed for enhver inden for sit usikrede trådløse netværks rækkevidde. Dette blev udnyttet – formentlig af en ukendt bruger – til at stille et musikværk til offentlighedens rådighed på internettet uden rettighedshavernes tilladelse. Efter tysk retspraksis kan der pålægges en person, der

¹³⁰ Jf. Mathiasen m.fl.: *E-Handelsloven med kommentarer*, 2004, s. 198-200.

¹³¹ Pkt. 12.2.1.3.a i lovforslag L 61, op.cit., fodnote 75.

¹³² Op.cit., fodnote 130.

¹³³ Nielsen og Jakobsen: *E-handelsret*, 2011, s. 420, anfører korrekt, at Infosoc-direktivets artikel 5, stk. 1, i modsætning til OHL § 11 a, som implementerer bestemmelsen, *ikke* betinger undtagelsen for flygtige og tilfældige kopier af lovligt forlæg.

¹³⁴ EU-Domstolens dom af 15. september 2016 i sag C-484/14.

driver et usikret wi-fi-netværk, indirekte ansvar (*Störerhaftung*) for tredjemands ophavsretskrænkelser.¹³⁵ Rettighedshaverne – Sony – fremsatte påkrav over for Mc Fadden om overholdelse af ophavsretten, og under en efterfølgende retssag om blandt andet erstatningsansvaret blev der forelagt EU-Domstolen en række spørgsmål vedrørende EHD artikel 12. Det fremgår af Domstolens svar, at bestemmelsen fritager for dette erstatningsansvar. En person, som stiller usikret wi-fi til rådighed, kan altså ikke gøres ansvarlig for de krænkelser, som brugerne måtte begå via netværket, hvis e-handelsdirektivets ansvarsfrihedsbetingelser er opfyldt. Herefter fastslog Domsstolen, at direktivet derimod ikke er til hinder for, at den pågældende forbydes at fortsætte krænkelserne efter en rets- eller myndighedsafgørelse herom.¹³⁶

Det kunne i sagen rent praktisk ske ved enten at overvåge al information, som blev transmitteret via netværket, lukke internetforbindelsen helt eller sikre den ved et password. De to første muligheder forkastede Domstolen. Den ene fordi den oplagt strider mod overvågningsforbuddet i direktivets artikel 15, og den anden fordi en fuldstændig lukning af internetforbindelsen vil være for indgribende i forhold til den pågældendes ret til at drive virksomhed og dermed ikke udtryk for en passende afvejning af grundrettigheder. Derimod ville en foranstaltning, som påbyder anvendelse af password, der kun udleveres, efter at brugerne har identificeret sig, efter Domstolens opfattelse ramme den rette balance mellem hensynene til retten til at drive virksomhed, informationsfriheden og beskyttelsen af ophavsretten.¹³⁷

Perspektiver

For rettighedshaverne indebærer det en indskrænkning af håndhævelsesmulighederne, at de ikke kan gøre et medvirkensansvar gældende over for tjenesteydere, der leverer ren videreformidling, hvad enten der er tale om teleselskaber eller operatører af wi-fi-netværk. Hvad angår de sidste er det tvivlsomt, om muligheden for at pålægge operatørerne at anvende password og kræve identifikation vil få nogen særlig praktisk betydning for rettighedshaverne. Gevinsten ved at få pålagt en wi-fi-operatør at passwordsikre sit netværk vil nok i de fleste tilfælde ikke kunne bære de betydelige processuelle omkostninger, der må være forbundet med at nå dertil. I forhold til wi-fi-operatøren har muligheden for at blive *pålagt* passwordpligt næppe en forebyggende

¹³⁵ Præmis 21.

¹³⁶ Præmis 79.

¹³⁷ Præmis 100.

virkning i den forstand, at han vil *vælge* selv at gøre det, for han løber som nævnt ikke nogen risiko for erstatningsansvar ved ikke at gøre det.

Caching

Når formidleren – igen typisk en internetudbyder – lagrer cache-kopier på sin server for at lette transmissionen af information, sker der også i denne forbindelse en eksemplarfremstilling, der er omfattet af OHL § 11 a, men som på grund af den danske implementering af den bagvedliggende direktivbestemmelse¹³⁸ er retsstridig, hvis der ikke er lovligt forlæg. Formidleren kan også blive medvirkende til de krænkelse, der f.eks. sker, når ulovlige eksemplarer downloades. I denne situation er det EHL § 15, som gør formidleren ansvarsfri, både for selve oplagringen og indholdet, hvis de fem betingelser heri er opfyldt. Disse betingelser er som nævnt ovenfor i afsnit 4.2, at formidleren for det første ikke ændrer den cachede information, for det andet overholder betingelserne for adgang til informationen, for det tredje holder informationen ajourført, for det fjerde ikke foretager indgreb i den teknologi, som genererer data om anvendelsen af hjemmesiden, og for det femte straks fjerner eller hindrer adgang til kopieret information, når han får kendskab til, at den ikke længere er tilgængelig på den originale side, eller at en domstol eller administrativ myndighed har krævet informationen fjernet.

Formidleren er altså også ved denne aktivitet ansvarsfri, selv om han har kendskab til, at han kopierer f.eks. ophavsretskrænkende materiale. En internetudbyder, som godt ved, at der i den cachede information på hans servere er piratkopierede film, kan ikke ifalde hverken straf- eller erstatningsansvar herfor, så længe de fem ansvarsfrihedsbetingelser er opfyldt. Det vil dog her få betydning, at formidleren efter den tredje betingelse skal ajourføre informationen med den frekvens, der er kutyme for i branchen – hvilket for velbesøgte hjemmesider er dagligt eller endnu hyppigere.¹³⁹ Hvis en hjemmeside har fjernet ophavsretskrænkende materiale, vil det derfor – ved overholdelse af den tredje betingelse – også hurtigt afspejle sig i den cachede kopi, idet formidleren i modsat fald risikerer ansvar. Det har endvidere betydning, at formidleren efter den femte betingelse skal fjerne information, når han får kendskab til, at den er fjernet fra nettet, eller at en domstol eller administrativ myndighed har krævet dette. Hvis en rettighedshaver således

¹³⁸ Jf. fodnote 133.

¹³⁹ Udsen: *IT-ret*, 2016, s. 275.

har fået en hjemmeside til at fjerne ophavsretskrænkende materiale, f.eks. via et forbud, og gjort formidleren bekendt hermed, er denne ikke længere ansvarsfri.

Perspektiver

I forhold til egentlige pirathjemmesider, som det ikke er lykkedes rettighedshaverne at få lukket, må det dog være et potentielt håndhævelsesproblem, at en internetudbyder, som lagrer en cache-kopi af siden, ikke kan gøres ansvarlig herfor. I praksis er det formentlig mængden af trafik til hjemmesider, der afgør, om de caches, og en populær ulovlig tjeneste vil i så fald blive det. Uanset at ansvarsfriheden vil ophøre ved kendskab til f.eks. et forbud mod siden, hjælper internetudbyderen trods alt indtil da med til at muliggøre flere besøg. Det ellers helt rimelige i, at formidleren ikke skal kunne ifalde ansvar for – ved *caching* – at bidrage til et velfungerende internet, synes her at kunne medføre det afledte problem, at adgangen til ulovlige sider også bliver mere effektiv.

Oplagring

En internetudbyder, som stiller lagerplads til rådighed for en hjemmeside, er en mere permanent vært for det eventuelt ulovlige materiale, som han lagrer, end den rene videreformidler og *caching*-videreformidleren. Derfor er muligheden for, at han får viden eller burde viden om det ulovlige indhold også større. Med en sådan viden kan han blive straf- eller erstatningsansvarlig for den eksemplarfremsstilling, som sker, når han f.eks. oplagrer en piratkopieret film. Efter de almindelige regler forudsætter strafansvaret som nævnt forsæt eller grov uagtsomhed, mens erstatningsansvaret forudsætter simpel uagtsomhed.

Efter e-handelslovens ansvarsfritagelsesregler vedrørende oplagring vil internetudbyderen *ikke* blive fritaget for erstatningsansvaret, hvis han har burde viden eller – med lovens ord – ”kendskab til forhold eller omstændigheder, hvoraf den skadevoldende aktivitet eller information fremgår”. Der er dermed overensstemmelse med den almindelige culparegel, jf. afsnit 4.3 ovenfor. Spørgsmålet er, hvor meget der skal til, for at internetudbyderen har burde viden. Han kan ikke pålægges en generel pligt til at overvåge indhold på de hjemmesider, han oplagrer på sin server. Det ville være i strid med overvågningsforbuddet i EHD artikel 15, jf. afsnit 4.5 ovenfor.

Mange ophavsretskrænkelser på internettet ville ellers kunne undgås, hvis formidlerne havde en generel pligt til at holde øje med al den information, der sendes via deres net

og lagres på deres servere. En sådan generel overvågning ville dog være, hvis ikke umulig, så i hvert fald meget omkostningstung for formidlerne, ligesom den ville udfordre nogle af de fundamentale rettigheder, som charteret beskytter, f.eks. erhvervsfrihed, informationsfrihed og persondatabeskyttelse. Overvågning er heller ikke en opgave, man normalt pålægger private parter.

Hvad angår strafansvaret har e-handelsloven reelt lempet ansvarsgrundlaget ved oplagring. Som nævnt ovenfor kan ophavsretskrænkelser begået forsætligt eller groft uagtsomt straffes med bøde, men e-handelsloven fritager efter ordlyden af § 16, stk. 1, nr. 1, for strafansvaret, når blot der ikke er handlet forsætligt. En bruger, som groft uagtsomt uploader piratkopierede film til internettet, kan således blive idømt bødestraf, mens den formidler, som lægger serverplads til hjemmesiden, og som burde have kendt til ulovligheden, skal fritages for strafansvaret efter EHL § 16, når de øvrige betingelser heri er opfyldt.

Det synes ikke at være almindeligt, at rettighedshavere påstår straf i civilretlige sager om krænkelse af ophavsrettigheder, og ansvarsfriheden for *hosting*-formidlere ved groft uagtsomme overtrædelser har derfor næppe større betydning i denne sammenhæng.

5.3.2 Tjenesteudbydere

På sociale medier som Facebook og YouTube har brugerne mulighed for at uploade ophavsretligt beskyttet materiale uden rettighedshaverens samtykke. Hvis udbyderen af tjenesten har viden om dette ulovlige brugergenererede indhold eller burde have det, kan han ifalde straffe- eller erstatningsretligt ansvar som medvirkende til den ulovlige eksemplarfremsstilling og tilgængeliggørelse.

E-handelsloven giver dog som nævnt mulighed for ansvarsfritagelse, hvis tjenesteudbyderens rolle er begrænset til den passive formidlers. Tjenesteudbyderen er vært for og oplagrer information på de sider, som stilles til rådighed, og det er derfor bestemmelsen i § 16 om *hosting*, der er relevant. Bag ansvarsfritagelsesreglerne i e-handelsdirektivet fra 2000 lå imidlertid ikke direkte et hensyn til de dengang stort set ukendte sociale medier, og reglen i direktivets artikel 14 tog snarere sigte på den mere tekniske oplagring af hjemmesider på internetudbyderes servere. Baggrunden var blandt

andet et ønske om at sikre fri bevægelighed for informationssamfundstjenester.¹⁴⁰ Det kræver et velfungerende internet, og derfor skulle formidlere, som leverer informationssamfundstjenester, være beskyttet af ensartede ansvarsfritagelsesregler.

Spørgsmålet er imidlertid, om grænsen mellem den ”tekniske, automatiske og passive” rolle uden kendskab til eller kontrol over den lagrede information og den mere aktive rolle overskrides af tjenester som f.eks. YouTube og Facebook, så de bliver indholdsudbydere snarere end tjenesteudbydere og dermed ikke opfylder ansvarsfrihedsbetingelserne. Alene udbuddet af tjenesten som sådan, med fastlæggelse af nogle rammer for dens anvendelse og brugernes adfærd og med mulighed for økonomisk gevinst for udbyderen, skaber måske den tilknytning, som kunne få tjenesten til at minde om en indholdsudbyder.

For overhovedet at være omfattet af ansvarsfrihedsreglerne er det en første forudsætning, at der leveres en informationssamfundstjeneste, dvs. en tjeneste med et kommercielt sigte, som normalt leveres mod betaling, jf. afsnit 4 ovenfor. Med hensyn til det kommercielle aspekt følger det af EU-Domstolens dom i Papassavas-sagen,¹⁴¹ at begrebet informationssamfundstjenester i direktivets forstand omfatter tjenester, hvor den – indirekte – betaling, som udbyderen modtager, stammer fra midler opnået gennem reklamer, der vises på internettet.¹⁴² Af samme dom fremgår det, i god overensstemmelse med betragtningerne til e-handelsdirektivet, at kendskab til og kontrol med den information, som offentliggøres, bringer tjenesten uden for anvendelsesområdet for ansvarsfrihedsreglerne, mens det ikke er afgørende, om adgang til siden er gratis eller sker mod betaling.¹⁴³

Spørgsmålet om, hvor grænsen går mellem den passive og den aktive rolle – eller mellem kendskab og ukendskab, kontrol og ikke-kontrol – har været behandlet af EU-Domstolen i den meget omtalte dom i Google France-sagen.¹⁴⁴ Sagen vedrørte Googles AdWords-tjeneste, som gør det muligt for annoncører at abonnere på søgeord – også andres varemærker – således at deres annoncer vises, når brugere søger på de

¹⁴⁰ Betragtning 8 til e-handelsdirektivet.

¹⁴¹ Dom af 11. september 2014 i sag C-291/13.

¹⁴² Præmis 30.

¹⁴³ Præmis 46.

¹⁴⁴ Dom af 23. marts 2010 i de forenede sager C-236/08 – C-238/08, AdWords-sagen. Sagen vedrørte ansvarsfrihed for formidlere i forbindelse med varemærkekrænkelser, men da direktivets regler jo som nævnt gælder generelt for alle ”formidlere af informationssamfundstjenester”, er dommen også relevant i relation til ophavsretskrænkelser.

pågældende ord. Google tilbød i den forbindelse også annoncørerne at kombinere tredjemands varemærke med et ord, som ledte tanken hen på en efterligning, f.eks. kombinationen af ”Louis Vuitton” og ”kopi”.¹⁴⁵

Domstolen fastslog, at den blotte omstændighed, at Google modtager betaling for tjenesten, fastsætter betalingsvilkårene og giver en række generelle oplysninger til sine kunder, ikke bringer den uden for anvendelsesområdet for direktivets ansvarsfritagelser.¹⁴⁶ I forbindelse med tjenesten behandler og inddrager Google endvidere det brugergenererede indhold ved hjælp af software, som virksomheden selv har udviklet. Søgeord, AdWords i systemet og klik på annoncer bliver sammenholdt, og Google bestemmer rækkefølgen af visningen, bl.a. på grundlag af det betalte vederlag. Alt dette forhindrer ifølge EU-Domstolen heller ikke, at Google fortsat kan være passiv formidler, men det var op til den nationale domstol at afgøre, om dette konkret var tilfældet.

Domstolen har i sin dom i eBay-sagen¹⁴⁷ uddybet, at hvis formidleren derimod yder bistand bestående i bl.a. at ”optimere eller fremme salgsudbud”, udøver han en aktiv rolle, som giver ham kendskab til eller kontrol over de lagrede informationer, hvorefter han ikke længere er ansvarsfri efter direktivets regler.¹⁴⁸

Ovennævnte vedrører bestemmelsen i EHL § 16, stk. 1, nr. 1, om, at formidleren ikke må have viden eller burde viden. Ansvarsfriheden efter *hosting*-reglen kræver som nævnt også, at formidleren fjerner information eller hindrer adgang til den, straks han får kendskab til, at den er ulovlig, jf. EHL § 16, stk. 1, nr. 2. Spørgsmålet er, hvornår formidleren har fået et sådant kendskab. En domstolskendelse om retsstridigheden vil selvfølgelig være tilstrækkelig. Men hvis formidleren reagerer på enhver anden henvendelse om ulovligt materiale uden selv at undersøge det, bringes hensynet til ytringsfriheden i fare, ligesom han i nogle tilfælde også kan risikere et erstatningsansvar, hvis han fjerner lovligt materiale. EU-Domstolen udtalte sig om spørgsmålet i eBay-sagen. Den fastslog, at en meddelelse om ulovlig aktivitet eller information ikke automatisk indebærer bortfald af ansvarsfriheden, idet oplysningerne kan være utilstrækkelige eller ubegrundede, men meddelelsen er dog en omstændighed,

¹⁴⁵ Præmis 29.

¹⁴⁶ Præmis 116.

¹⁴⁷ Dom af 12. juli 2011 i sag C-324/09.

¹⁴⁸ Præmis 116.

som der skal tages hensyn til ved den retlige efterprøvelse af, om formidleren havde burde viden.¹⁴⁹

Det skal understreges, at disse – måske lidt uklare – kriterier hvad angår begge betingelser i EHL § 16, stk. 1, blot indgår som elementer i den konkrete vurdering, som skal foretages i hver enkelt sag for at afgøre, om ansvarsfrihedsbetingelserne er opfyldt.¹⁵⁰

På en tjeneste som YouTube sker der utvivlsomt krænkelse af ophavsretten.¹⁵¹ Spørgsmålet er, om tjenesten – hvis man forsøger at anvende Domstolens vejledende kriterier sammen med den obligatoriske konkrete vurdering – må anses for at falde uden for det ansvarsfrie område.

For YouTube genereres der indtjening, når brugerne klikker på annoncer på siden, også når de er i gang med at afspille ulovligt uploadet materiale. Der er dermed næppe tvivl om, at YouTube er en kommerciel tjeneste. Som fastslået i dommen i Papassavas-sagen bringer det netop ikke en tjeneste uden for ansvarsfrie regleres anvendelsesområde, at der er tale om indirekte betaling i form af reklameindtægter.

YouTube deler indhold på siden op i kategorier, viser lister over højest rangerende videoer og gør det muligt for brugerne at generere spillelister. YouTube kan dermed siges at foretage en vis behandling af det brugergenererede, eventuelt ulovlige indhold ved at integrere dette i tjenestens funktioner. Som vi har set i Google France-sagen, kan den aktive inddragelse af det brugergenererede indhold – og det forhold, at der tjenes penge på dette – imidlertid ikke i sig selv bringe tjenesten uden for det ansvarsfrie område.

Kriteriet fra eBay-sagen om optimering eller fremme af salgsudbud synes ikke at være relevant i forhold til en tjeneste som YouTube, som ikke er en onlinemarkedsplads.

Ovennævnte må herefter suppleres af en konkret vurdering af, om der sker en rent teknisk og automatiseret behandling, eller om YouTube spiller en aktiv rolle.

¹⁴⁹ Præmis 122.

¹⁵⁰ EU-Domstolen henviser til en sådan konkret vurdering i præmis 119 i Google France-sagen og i præmis 117 i eBay-sagen.

¹⁵¹ YouTube har indgået aftaler med musikbranchen om distribution af musikvideoer, men der kunne være tale om filmklip eller hele film.

Det bemærkes, at YouTube – ligesom Facebook – synes at være i stand til at filtrere nogle former for uønsket indhold fra, f.eks. pornografisk materiale, og det kan derfor anføres, at sådanne tjenester ikke bør kunne holde sig i uvidenhed ved ikke at gøre det. Ansvarsfritagelsen ved *hosting* er som nævnt ovenfor i afsnit 4.3 betinget af, at formidleren ikke har kendskab til eller burde viden om den ulovlige information. I vurderingen må det dog også indgå, at YouTube – og andre sociale tjenester – har indført procedurer, som skal sikre, at ulovligt indhold kan anmeldes og fjernes så hurtigt som muligt.

De fleste almindelige mennesker ved, at der findes store mængder piratkopieret materiale på en tjeneste som YouTube. Ved tjenesten det så ikke også selv – eller burde den i det mindste ikke vide det? Det gør den selvfølgelig, men kun på et generelt plan og ikke som konkret viden om bestemte, ophavsretskrænkende videoer. Hvis tjenesten kunne ifalde ansvar på grund af denne generelle viden, ville den være nødt til at overvåge alt indhold, men at pålægge den dette ville være i strid med overvågningsforbuddet i EHD artikel 15. Henvendelser fra rettighedshavere om ulovligt indhold kan imidlertid – efter en konkret vurdering – få ansvarsfriheden til at falde bort, jf. dommen i eBay-sagen.

Perspektiver

Konklusionen må blive, at YouTube kan være ansvarsfritaget, men dens behandling af det eventuelt ulovlige materiale og inddragelsen af dette i tjenestens egne funktioner kan medføre ansvar, hvis tjenesten efter en konkret vurdering spiller en mere aktiv rolle i denne forbindelse. Tjenesten skal ved kendskab til ulovligt indhold straks fjerne dette for at bevare ansvarsfriheden, men hvornår kendskab er indtrådt, må vurderes konkret.

I forhold til andre sociale medier og tjenester med brugergenereret indhold generelt vil en konkret vurdering ligeledes blive afgørende. For rettighedshaverne ligger der altså her en håndhævelsesmulighed, hvis tjenesterne gennem en mere aktiv rolle har bragt sig uden for det ansvarsfrie område. Det er ikke en mulighed, som har været udnyttet i Danmark, måske fordi oplagringstjenester traditionelt anses som passive formidlere. Imidlertid sælger de ikke længere bare serverplads, og dermed står *hosting*-reglen måske til at blive udfordret.

5.3.3 Forbud eller påbud mod internet- eller tjenesteudbydere

Ansvarsfrihedsreglerne synes således i de fleste situationer at beskytte formidlerne mod at kunne ifalde ansvar. Imidlertid forudsætter Infosoc-direktivet som nævnt, at det skal være muligt at få nedlagt forbud mod internet- eller tjenesteudbydere. Dette er i direktivet netop begrundet i, at mellemmåendenes tjenester på det digitale område i stigende grad anvendes til krænkelse, og at de ofte er bedst i stand til at bringe dem til ophør.¹⁵²

I praksis rettes det midlertidige forbud eller påbud da også ofte mod internetudbyderen. Det kan f.eks. ske ved, at internetudbyderen påbydes at afbryde en abonnents internetforbindelse eller forbydes at formidle adgang til en ulovlig hjemmeside, således at siden blokeres. Derimod kan det ikke pålægges internetudbyderen at indføre et filtreringssystem, fordi dette ifølge EU-Domstolens faste praksis er i strid med overvågningsforbuddet i EHD artikel 15 og i øvrigt også med grundlæggende rettigheder som friheden til at oprette og drive egen virksomhed, beskyttelsen af personoplysninger og informationsfriheden.¹⁵³

Nedenfor behandles nogle særlige spørgsmål, som reglerne om midlertidige forbud og påbud rejser, når de anvendes på netop internetudbydere.

Retsstridighedskravet

Som allerede nævnt ovenfor i afsnit 3.2 har retsstridighedskravet været til prøvelse i forbudssager mod internetudbydere. Internetudbydere videreformidler blot passivt det ophavsretskrænkende materiale eller giver adgang til det via internetforbindelsen.

I retspraksis er det dog fastslået, at denne passive rolle kan bevirke, at retsstridighedskravet er opfyldt, enten som følge af en selvstændig krænkelse fra internetudbyderens side eller som følge af dennes medvirken til de egentlige krænkere retsstridige handlinger.

En selvstændig krænkelse foreligger i tilfælde, hvor selve de ophavsretligt beskyttede værker transmitteres gennem internetudbyderens net. Dette er en teknisk, midlertidig og

¹⁵² Jf. betragtning 59 til direktivet. Muligheden følger også af e-handelsdirektivet og retshåndhævelsesdirektivet. jf. afsnit 4.4 ovenfor.

¹⁵³ Jf. f.eks. EU-Domstolens dom af 16. februar 2012 i sag C-360/10, SABAM mod Netlog, præmis 38, 47 og 48.

tilfældig eksemplarfremsstilling, der som udgangspunkt er tilladt efter OHL § 11 a, men som er retsstridig, når der ikke er lovligt forlæg, jf. undtagelsen i § 11, stk. 3. Situationen forelå i U 2006.1474 H. I denne sag havde de egentlige krænkere foretaget omfattende ophavsretskrænkelser ved at gøre musikværker tilgængelige på nogle servere. Rettighedshaverne havde nedlagt påstand om, at det skulle forbydes netværksoperatøren, TDC, at transmittere de ophavsretligt beskyttede værker, men fik ikke medhold i fogedretten, blandt andet fordi den ikke fandt, at det var retsstridig medvirken at stille internetforbindelsen til rådighed for krænkere. Rettighedshaverne fik dog medhold i både Østre Landsret og Højesteret. TDC bestred ikke, at der blev transmitteret flygtige kopier uden lovligt forlæg via dets net, men anførte, at retsstridighedsbetingelsen ikke var opfyldt, fordi TDC ikke var bekendt med kopieringen. Højesteret fastslog imidlertid, at TDC *objektivt* krænkede ophavsrettigheder ved den midlertidige eksemplarfremsstilling, som skete ved transmissionen.

I den senere forbudssag U 2010.2221 H vedrørende The Pirate Bay transmitterede netværksoperatøren, Telenor, *ikke* midlertidige kopier via sit net. Den ulovlige hjemmeside benyttede *bittorrent*-teknologien, og torrentfiler indeholder som nævnt ikke ophavsretligt beskyttet materiale, men viser blot vej til filer, der gør det. Fogedretten havde faktisk lagt til grund, at transmissionen indebar midlertidig eksemplarfremsstilling uden lovligt forlæg, og i landsretten gjorde netværksoperatøren derfor blandt andet gældende, at fogedrettens kendelse om nedlæggelse af forbuddet var truffet ud fra en faktisk vildfarelse. Det kunne dog ikke forhindre Østre Landsret i at stadfæste forbuddet, idet retsstridighedskravet ansås for opfyldt ud fra et medvirkenssynspunkt. Østre Landsret fastslog således, at netværksoperatøren ved at give sine kunder adgang til hjemmesiden medvirkede til den ulovlige eksemplarfremsstilling og tilgængeliggørelse. Højesteret stadfæstede kendelsen, idet medvirkenssynspunktet dog ikke var blevet bestridt.

Det er blevet diskuteret i litteraturen, hvor langt ud i medvirkenskæden retsstridighedskravet kan opfyldes.¹⁵⁴ I Pirate Bay-sagen medvirkede Telenor til The Pirate Bays medvirken til brugernes ophavsretskrænkelser, idet hjemmesiden – som følge af den anvendte teknologi – jo ikke selv foretog eksemplarfremsstilling eller tilgængeliggørelse, men kun medvirkede til, at brugerne gjorde det. Spørgsmålet er, om

¹⁵⁴ Søren Sandfeld Jakobsen i Juristen 2010, nr. 8, s. 207-215, på s. 212.

retsstridighedskravet så også kan opfyldes ved medvirken i fjernere led. Det bør dog ikke være rekvisiti nummer i rækken af medvirkende, der er afgørende, men snarere omfanget og grovheden af den krænkelse, der medvirkes til. I sagen var der tale om omfattende krænkelse. En alt for fjern medvirken vil under alle omstændigheder falde på betingelsen om årsagsforbindelse og adækvans.

Retsstridighedskravet kan altså opfyldes ved en selvstændig krænkelse, uden noget subjektivt tilregnelsskrav, eller ud fra en medvirkensbetragtning, der formentlig vil være påvirket af krænkelseernes omfang og grovhed. Det sidste vil også indgå i proportionalitetsvurderingen, jf. nedenfor.

Proportionalitetsprincippet

Som nævnt ovenfor kan forbud eller påbud nægtes, hvis det vil påføre rekvisitus skade eller ulempe, der står i åbenbart misforhold til rekvisitens interesse i forbuddets nedlæggelse. I sager mod internetudbydere kan et sådant misforhold ligge i, at udbyderen må foretage en større investering for at kunne gennemføre forbuddet.

I ovennævnte to sager gjorde internetoperatørerne gældende, at et forbud ville være uproportionalt, men fik ikke medhold. I U 2006.1474 H gjorde TDC gældende, at selskabet – som følge af muligt lovligt indhold på serverne – kunne komme til at medvirke til lukning af en lovlig aktivitet og ifalde erstatningsansvar herfor, og at et forbud ville pålægge det en overvågnings- og censureringsforpligtelse, der ville være en ”uoverstigelig hæmsko for selskabets virke som netværksudbyder” og derfor i strid med proportionalitetsprincippet. Højesteret fastslog, at det måtte indgå i proportionalitetsvurderingen, at TDC kun kunne efterleve forbuddet ved at afbryde internetforbindelsen til serverne eller for de pågældende abonnenter generelt, men dette forhindrede ikke et forbud i sig selv. Det var ikke sandsynliggjort, at serverne også blev anvendt til lovlige formål, og der var derfor ikke en reel risiko for, at TDC ville pådrage sig et erstatningsansvar ved at lukke forbindelsen. Højesteret anerkendte, at forbuddet ville medføre et vist administrativt arbejde for TDC, men alt i alt var der ikke tale om skade eller ulempe, som stod i åbenbart misforhold til rettighedshavernes interesse i at få krænkelsen bragt til ophør.

I U 2010.2221 H blev der formentlig i et vist omfang også udøvet lovlige aktiviteter på hjemmesiden, og Telenor gjorde gældende, at usikkerheden herom skulle indgå i proportionalitetsvurderingen. Højesteret lagde imidlertid vægt på de meget omfattende

krænkelser, som fandt sted, og efter det oplyste om omkostninger og ulemper forbundet med en såkaldt DNS-spærring – som rettighedshaverne havde erklæret, var tilstrækkelig til at opfylde forbuddet – lod Højesteret herefter proportionalitetsvurderingen falde ud til rettighedshavernes fordel.

Det bemærkes, at i TDC-sagen var krænkerens identitet ikke rettighedshaverne bekendt, mens de svenske personer bag The Pirate Bay i Telenor-sagen var identificerede på tidspunktet for de faktiske omstændigheder i sagen. Det ville således i sidstnævnte sag have været muligt at rette forbuddet mod dem. Som nævnt ovenfor kan det have betydning for proportionalitetsafvejningen, om forbuddet er rettet mod den egentlige krænker eller formidleren, men Telenor-sagen viser således, at det ikke behøver at være afgørende. I den forbindelse kan det have haft betydning, at krænkerne var hjemmehørende i Sverige, og at der derfor kan have været visse vanskeligheder forbundet med at rette håndhævelsen direkte imod dem.

I sagen U 2013.2873 Ø fik det derimod betydning, at forbudskravet ikke var rettet mod den egentlige, påståede krænker. Rettighedshaverne havde nedlagt påstand om, at det skulle forbydes internetudbyderen – TDC – at formidle adgang til en britisk hjemmeside, www.voga.com, som solgte kopier af designermøbler. Østre Landsret nedlagde ikke forbuddet og begrundede dette med, at det var Voga, der var den reelle krænker og derfor den, som forbudskravet i første omgang burde rettes imod. Landsretten udtalte, at dette gælder undtagen i tilfælde, hvor en krænkelse er konstateret ved en retskraftig dom, eller hjemmesiden er åbenbart ulovlig. I sagen kunne der nok være tvivl om ulovligheden, for dels blev der også markedsført produkter, som ikke var omfattet af forbudskravet, dels var der uafklarede lovvalgsspørgsmål. På denne baggrund stod ulempen for TDC i åbenbart misforhold til rettighedshavernes interesse i forbuddets nedlæggelse. Det bemærkes, at der var dissens, idet én dommer fandt proportionalitetskravet opfyldt og stemte for at nedlægge forbuddet.

Betingelsen om retskraftig dom eller åbenbart ulovlig hjemmeside

Det videre forløb i Voga-sagen viser en komplikation. Rettighedshaverne anlagde, sådan som Østre Landsret nærmest havde anvist, en sag om midlertidigt forbud mod den egentlige krænker, Voga, og fik det meddelt.¹⁵⁵ Voga havde løbende foretaget tilpasninger af hjemmesiden og ændringer af sine aktiviteter, men efter Sø- og

¹⁵⁵ Jf. Sø- og Handelsrettens kendelse af 12. november 2014 i sag A-0025-14, stadfæstet af Østre Landsret ved kendelse af 3. juni 2015 i sag B-3147-14.

Handelsrettens og senere Østre Landsrets opfattelse uden at krænkelserne var ophørt. Efter det midlertidige forbud mod Voga anlagde rettighedshaverne igen forbudssag mod TDC, men fik i første omgang ikke medhold.¹⁵⁶ Da den hovedsag, som var anlagt efter forbudskendelsen mod Voga, endnu verserede, fastslog Sø- og Handelsretten i den nye forbudssag mod TDC, at der ikke forelå en retskraftig dom vedrørende krænkelserne. Voga havde desuden efter Østre Landsrets forbudskendelse mod Voga indført nogle nye ændringer på siden med hensyn til levering til danske kunder, som havde rejst et lovvalgsspørgsmål, og grundlaget for de aktuelle krænkelser fandtes ikke at være åbenbart. Sø- og Handelsrettens kendelse blev kæret, og Østre Landsret nedlagde forbuddet mod TDC med den begrundelse, at *indholdet* på hjemmesiden var uændret, og at ændringerne i leveringsbetingelserne ikke ændrede ved, at dansk lovgivning fandt anvendelse.¹⁵⁷

Forløbet viser, hvordan forbudsproceduren mod internetudbyderen i realiteten kan besværliggøres af, at den formodede egentlige krænker foretager ændringer, som ikke bringer krænkelserne til ophør, men som nødvendiggør en ny vurdering, før midlertidigt forbud kan nedlægges.

Grundlæggende rettigheder

Retten skal også tage hensyn til relevante grundlæggende rettigheder. I forbindelse med midlertidige afgørelser om forbud og påbud mod en internet- eller tjenesteudbyder skal den således afveje rettighedshavernes ret til beskyttelse og effektiv håndhævelse af deres ophavsret mod internetudbydernes ret til at drive virksomhed. Det er i et vist omfang afspejlet i ovennævnte danske domme, blandt andet ved at internetudbydernes omkostninger ved spærringen er blev inddraget i vurderingen. Hensynet til internetbrugerne synes derimod ikke udtrykkeligt at være vægtet. Det følger af EU-Domstolens dom i UPC Telekabel Wien-sagen¹⁵⁸, at netop internetbrugernes grundlæggende ret til informationsfrihed også skal respekteres i forbindelse med nedlæggelse af forbud mod internetudbydere. Dommen er blevet kritiseret for at give en grundlæggende ret horisontal virkning, idet den pålægger *internetudbyderne* at sørge for, at brugernes informationsfrihed respekteres,¹⁵⁹ og for at lægge en urimelig byrde på internetudbyderne ved at tillade en ”resultatforpligtelse” uden at præcisere, hvad internetudbyderen skal gøre for at efterleve forbuddet.

¹⁵⁶ Sø- og Handelsrettens kendelse af 17. november 2015 i sag A-19-15.

¹⁵⁷ Østre Landsrets kendelse af 8. februar 2016 i sag B-2633-15.

¹⁵⁸ Domstolens dom af 27. marts 2014 i sag C-314/12.

¹⁵⁹ Præmis 55. Jf. Petersen m.fl.: *Judicielle forbud/påbud og immaterialretsproces*, 2015, s. 201-203.

I Danmark er forbuddet normalt blevet pålagt som en forpligtelse til at blokere for adgangen på en bestemt måde, jf. nærmere nedenfor. Herved bliver det indirekte domstolene, som varetager hensynet til også brugerne, og sikrer, at internetudbydere kan gennemføre forbuddet i overensstemmelse med den afvejning af grundlæggende rettigheder, som domstolene må antages at have foretaget.

Spærring af adgang til hjemmesider

Rent praktisk foregår internetudbydernes spærring af adgangen til hjemmesider i dag typisk ved en såkaldt blokering på DNS-niveau (domain name system-blokering). Blokeringen bevirker, at man ikke kan tilgå den ønskede IP-adresse ved hjælp af dens domænenavn. Når internetudbyderen har gennemført en påbudt blokering af en hjemmeside, får en bruger, der klikker sig ind på den, i stedet for adgang til siden en besked om, at han har forsøgt at få adgang til materiale, der krænker ophavsretten, og en opfordring til at benytte lovlige tjenester.

Et første problem i den forbindelse er, at DNS-blokeringen kan brydes. I nogle kredse anses det for nemt at gøre, men for mere almindelige internetbrugere kræver det formentlig vejledning. Dette sammen med den advarende besked på siden må antages at afholde mange fra at forsøge.

Et andet problem har været, at et forbud eller påbud som nævnt skal gennemføres af rekvisitus, eventuelt med fogedrettens hjælp. Hvis et påbud skal være effektivt, skal rekvirenten derfor i princippet begære det meddelt over for alle internetudbydere i Danmark. Problemet synes nu at være løst ved, at medlemmerne af teleselskabernes branchesamarbejde, Teleindustrien (TI), har indgået en *Code of Conduct* med Rettighedsalliancen, som indebærer, at når ét teleselskab er påbudt at gennemføre en DNS-blokering af en hjemmeside, vil alle teleselskaber gennemføre den samme blokering.¹⁶⁰

Endelig er det et problem, hvis indhold fra en blokeret hjemmeside blot flyttes til en ny adresse, som giver brugeren mulighed for at tilgå den blokerede tjeneste. Måske kan dette også håndteres gennem ovennævnte *Code of Conduct*. I hvert fald angives det heri,

¹⁶⁰ *Code of Conduct* for håndtering af afgørelser om blokering af adgang til tjenester, der krænker immaterielle rettigheder, som senest revideret 12. december 2016.

at TI-medlemmer vil ”blokere for yderligere hjemmesideadresser, såfremt rettighedshaver, repræsenteret ved RettighedsAlliancen, indestår for, at disse hjemmesideadresser ligeledes giver adgang til den tjeneste, som er omfattet af den forudgående domstols-/myndighedsafgørelse”. RettighedsAlliancen overvåger altså, hvilke hjemmesideadresser der giver adgang til en tjeneste, hvorefter Teleindustrien inkluderer disse i sin blokeringsliste. Dette må antages at gøre en DNS-blokering mere effektiv.

Opsamling - forbud

Alt i alt synes der at være en forholdsvis nem adgang for rettighedshaverne til at få nedlagt et foreløbigt forbud, således at krænkelse kan forebygges eller standses, i hvert fald i grovere sager. Proportionalitetskravet synes ikke at være en alvorlig hindring for dette, især ikke når den egentlige krænkelse er ukendt. Kæresager kan kompliceres af, at der foretages ændringer på den hjemmeside, der er genstand for forbuddet, men det forhindrer naturligvis ikke endeligt et forbud. Den valgte spærring er ikke nødvendigvis effektiv, men samarbejde i branchen kan afhjælpe dette.

6 Konklusion

Håndhævelsen af ophavsrettigheder ved krænkelse på internettet er naturligvis ikke illusorisk, men den er trods styrkede håndhævelsesmuligheder på mange punkter heller ikke problemfri.

Nye og hele tiden mere avancerede teknologier rejser håndhævelsesmæssige og praktiske udfordringer, fordi krænkelse bliver lettere at foretage og sværere at opdage. Samtidig er hensynet til rettighedshaverne blot et af mange, der skal tages, når krænkelse spores, og rettigheder håndhæves. Det i mange sammenhænge højt vægtede hensyn til beskyttelse af personoplysninger stiller krav til rettighedshavernes sagsbehandling, som dog må anses for rimelige.

Når rettighedshaverne har overvundet de indledende vanskeligheder ved at identificere IP-adresser, har de hidtil tilsyneladende kunnet få udleveret abonnentoplysninger, idet dette har været anset for hensigtsmæssigt ud fra den betragtning, at de ellers ikke kan varetage deres interesser. Det er dog ikke utænkeligt, at hensynet til beskyttelse af personoplysninger her kan komme til at indgå i den krævede interesseafvejning og proportionalitetsvurdering med en sådan vægt, at det vil føre til en skærpelse af praksis i

sager om mindre krænkelse – en sagstype, som i forvejen er vanskelig at håndtere for rettighedshaverne. En konklusion herom er dog forbundet med den usikkerhed, at det ikke fremgår af trykt praksis, om – og i givet fald hvordan – den krævede interesseafvejning allerede foretages.

Udsendelse af breve til formodede krænker er et muligt næste skridt, som har visse fordele, især at det er billigt og derfor et alternativ til retssag om mindre krænkelse. Brevene kan rejse negativ omtale, men den mulige forebyggende virkning må dog nok antages at opveje dette.

I civile retssager mod de primære ansvarssubjekter kan rettighedshaverne få bevisproblemer på grund af den ligefremme bevisbyrde og bevisværdien af den digitale dokumentation. Her kan bevissikringsreglerne være til hjælp, især hvis tilgængeliggørelse altid vil udløse en streng proportionalitetsbedømmelse, men praksis herom fra fogedretterne ses ikke at være bekræftet. Rettighedshaverne har endvidere en svær opgave i at dokumentere deres tab ved krænkelse på internettet, og de kan ikke basere sig på faste principper for erstatningsudmåling.

I retssager mod systemudviklere eller indholdsudbydere kan rettighedshaverne gøre et medvirkensansvar gældende. Sagerne er dog få, hvilket ikke skyldes, at systemudviklerne kan forsvare sig med, at de – på grund af raffineret teknologi – slet ikke lagrer eller tilgængeliggør ulovligt materiale, men snarere at samme teknologi gør det svært at finde frem til folkene bag de ulovlige tjenester.

E-handelsdirektivet har på visse punkter indskrænket formidlernes ansvar, og rettighedshaverne vil – helt i overensstemmelse med direktivets intentioner – sjældent kunne gøre et formidleransvar gældende, omend det dog er muligt at få pålagt wi-fi-udbydere passwordpligt. Formidlernes ansvarsfrihed ved *caching* af hjemmesider har den utilsigtede virkning, at også adgangen til ulovlige sider gøres mere effektiv, til skade for rettighedshaverne. Sociale medier og andre tjenesteudbydere er som udgangspunkt også skærmet af ansvarsfriheden ved *hosting*, men med de mere avancerede funktioner og tjenester, de tilbyder, har de ikke nødvendigvis den samme passive rolle som de formidlere, *hosting*-reglen oprindeligt er tiltænkt at beskytte. Det er derfor ikke utænkeligt, at de – efter en konkret bedømmelse – kan blive anset for at være sejlet uden for reglens sikre havn, således at rettighedshaverne vil kunne gøre et erstatningskrav gældende mod dem.

Under alle omstændigheder giver forbudsinstituttet rettighedshaverne gode muligheder for i det mindste at få standset krænkelse i grovere sager. Proportionalitetsprincippet og grundlæggende rettigheder synes ikke at være en alvorlig hindring, og samarbejde i telebranchen gør forbud mere effektive.

Problemerne lægger op til nogle retspolitiske overvejelser. Indførelse af objektivt ansvar eller præsumptionsansvar for personers internetforbindelse er vidtgående og giver anledning til retssikkerhedsmæssige betænkeligheder. Det er næppe heller særligt effektivt. I dag leveres de fleste internetforbindelser som standard med kode, men en internetforbindelse, der oprindeligt er sikret, er det derfor ikke nødvendigvis på det relevante tidspunkt. Oplyser en formodet krænker, at en forbindelse *var* sikret, må det være rettighedshaver, der eventuelt skal bevise, at den *ikke* var det på det relevante tidspunkt. Det vil være vanskeligt. Omvendt bevisbyrde vil dog formentlig have en præventiv virkning.

En anden mulighed, som har været vendt, men endnu ikke udnyttet i Danmark, er at pålægge internetabonnenter en pligt til at sikre deres internetforbindelse mod krænkelse, og – hvis krænkelse alligevel sker – lukke deres forbindelse efter en nærmere bestemt advarselsprocedure, som involverer internetudbyderne.

Endnu et spørgsmål er, om tiden er løbet fra e-handelsdirektivet og dets – i forhold til navnlig sociale tjenester – meget lempelige regler, eller om man snarere skal lade tiden indhente sådanne tjenester med en mere restriktiv fortolkning af reglerne. I hvert fald kan det diskuteres, om ansvarsfriheden er for vidtgående på nogle områder.

7 Engelsk resumé

The Internet presents a particular challenge to copyright owners. With improved technology, works can – if not born-digitally – easily be converted into digital format and then spread on the Internet without the permission of the copyright holder.

This thesis seeks to analyse the practical, legal and procedural challenges to the copyright owners when they enforce their rights in connection with online infringements.

It does so by first introducing some important technologies used in file sharing and piracy and explaining in which ways they constitute copyright infringements. It then describes key enforcement measures available to the right holders, including central provisions of the Danish Administration of Justice Act. As intermediaries, the role of internet service providers is of obvious interest to the copyright owners. However, provisions in mainly the e-Commerce Directive ensure that, under certain conditions, they are free of liability for infringements in connection with certain types of activity. The thesis therefore includes an introduction to the relevant provisions, as implemented in the Danish e-Commerce Act.

Based on this, the thesis then analyses the challenges that meet copyright holders when they seek to enforce their rights against the direct online infringers and internet content providers. Evidence of the infringements must be produced, and at this and later stages the interests of internet users, internet service providers and right holders must be balanced. Letters to alleged infringers is a possible step that involves both advantages and disadvantages. In lawsuits against the direct infringers the burden of proof can be difficult to meet.

Modern technology not involving any direct infringement by the system developers and internet content providers, as e.g. *peer-to-peer* file sharing, does not prevent copyright holders from enforcing their rights against such parties, as they can assert contributory liability. It might, however, be difficult to identify the system developers.

Some duties may be imposed on the internet service providers, but they are to a wide extent exempt from liability when they perform mere conduit, caching and hosting activities. As regards caching, the exemption may be considered to involve an unintended facilitating of the access to illegal sites to the detriment of the copyright

holders. The liability regime also provides a safe harbour to social media which might, however, be open to challenge.

As an important – preliminary – alternative to lawsuits, copyright holders seem to have relatively easy access to injunctive relief, whereby infringements can be terminated.

Based on the analysis, the thesis concludes that copyright enforcement directed against infringements on the internet is not impossible but raises some important problems with respect to both direct infringers, system developers and internet content providers, intermediaries and social media.

8 Litteratur

Bøger:

Andersen, Niels M., Arly Carlquist og Anders Rubinstein: *Retshåndhævelse af immaterialrettigheder*, Jurist- og Økonomforbundets Forlag, 2006.

Bang-Pedersen, Ulrik Rammeskov og Lasse Højlund Christensen: *Den civile retspleje*, Pejus, 3. udgave, 1. oplag, 2015.

Christoffersen, Jonas: *EU's Charter om grundlæggende rettigheder med kommentarer*, Jurist- og Økonomforbundets Forlag, 1. udgave, 1. oplag, 2014.

Jakobsen, Søren Sandfeld og Sten Schaumburg-Müller: *Medieretten*, Jurist- og Økonomforbundets Forlag, 1. udgave, 1. oplag, 2013.

Jakobsen, Søren Sandfeld, Søren Johansen og Christian Bergqvist: *Teleretten*, Jurist- og Økonomforbundets Forlag, 1. udgave, 1. oplag, 2014.

Jochumsen, Bjarke G.: *Fogedforbud rettet mod netværksoperatørers videreformidling af ophavsretskrænkelser*, Boggruppen ApS, 1. udgave, 2011.

Mathiasen, Jacob Plesner, Niels Bo Jørgensen og Johan Schlüter: *E-handelsloven med kommentarer*, Jurist- og Økonomforbundets Forlag, 1. udgave, 1. oplag, 2004.

Nielsen, Ruth og Søren Sandfeld Jakobsen: *E-handelsret*, Jurist- og Økonomforbundets Forlag, 3. reviderede udgave, 1. oplag, 2011.

Petersen, Clement Salung: *Immaterialrettigheder og foreløbige forbud*, Jurist- og Økonomforbundets Forlag, 1. udgave, 1. oplag, 2008.

Petersen, Clement Salung, Peter Møgelvang-Hansen og Thomas Riis: *Judicielle forbud/påbud og immaterialretsproces*, Karnov Group Denmark, 1. udgave, 1. oplag, 2015.

Rasmussen, Thomas Munk og Peter Fogh Knudsen: *E-handel, Praktisk jura for erhvervsdrivende*, Forlaget Thomson, 1. udgave, 1. oplag, 2005.

Schovsbo, Jens, Morten Rosenmeier og Clement Salung Petersen: *Immaterialret*, Jurist- og Økonomforbundets Forlag, 4. udgave, 1. oplag, 2015.

Schønning, Peter: *Ophavsretsloven med kommentarer*, Karnov Group, 6. udgave, 2016.

Trzaskowski, Jan (red.), Hanne Kirk Deichmann, Søren Sandfeld Jakobsen, Susanne Karstoft, Lars Bo Langsted, Thomas Riis og Charlotte Bagger Tranberg: *Internetretten*, Ex Tuto Publishing, 2. udgave, 1. oplag, 2012.

Trzaskowski, Jan, Andrej Savin, Björn Lundqvist, Patrik Lindskoug: *Introduction to EU Internet Law*, Ex Tuto Publishing, 1. udgave, 1. oplag, 2015.

Udsen, Henrik: *IT-ret*, Ex Tuto Publishing, 3. udgave, 1. oplag, 2016

Von Eyben, Bo og Helle Isager: *Lærebog i erstatningsret*, Jurist- og Økonomforbundets Forlag, 8. udgave, 2015.

Tidsskrifter:

Jakobsen, Søren Sandfeld: *Formidleransvar på internettet – en kommentar til Højesterets kendelse i Pirate Bay-sagen*, Juristen 2010, nr. 8, s. 207-2015.

Johnsen, Anders Sevel: *Ophavsret på sociale medier*, NIR 2016, nr. 2, s. 147-171.

Marusic, Branka: *Gate Keeper or Trespasser? EU ISP Liability Regime and its Privacy Implications*, NIR 2016, nr. 1, s. 4-16.

Mathiasen, Jacob Plesner: *Fildeling*, NIR 2007, nr. 1, s. 46-55.

Petersen, Clement Salung: *Internet Service Providers and Copyright in the Nordic Countries*, NIR 2015, nr. 6, s. 642-651.

Petersen, Clement Salung: *Bemærkninger til Kulturministeriets »Rapport fra udvalget om ophavsrettigheder på internettet«*, U 2011 B 283.

Trzaskowski, Jan: *Direktivet om elektronisk handel*, U 2000 B 643.

Schønning, Peter: *Lovligheden af links på internettet efter Svensson/Retriever-dommen*, U 2014 B 417.

Angelopoulos, Christina: *Are Blocking Injunctions against ISPs Allowed in Europe? Copyright Enforcement in the Post-Telekabel Legal Landscape*, Journal of Intellectual Property Law & Practice, oktober 2014.

Andet:

Rapport fra udvalget om ophavsrettigheder på internettet, Kulturministeriet, 2011, tilgængelig på:
http://kum.dk/uploads/tx_templavoila/Ophavsrettigheder_pa_internettet_april2011.pdf

Advokatnævnets kendelse af 23. juni 2016, tilgængelig – med link til pdf-fil – på:
<http://viden.advokatsamfundet.dk/sager/643/>

Code of Conduct for håndtering af afgørelser om blokering af adgang til tjenester, der krænker immaterielle rettigheder, som senest revideret 12. december 2016. Tilgængelig på:
<http://www.teleindu.dk/wp-content/uploads/2013/01/TI-code-of-conduct-revideret-december-2016-public-1.pdf>