Tvistelovens regler om sikring og tilgang til elektronisk lagrede bevis utenfor rettssak, særlig ved krenkelser av rettighetshavers enerett til tilgjengeliggjøring av åndsverk på Internett.

Universitetet i Oslo

Det juridiske fakultet

Kandidatnummer: 207

Leveringsfrist:10.11.2011

(* regelverk for masteroppgave på:

www.uio.no/studier/emner/jus/jus/JUR5030/reglement/vedlegg_emnebeskrivelse_masteroppgaver_JUR5030_5060.html)

Til sammen 37488 ord

10.11.2011

Innholdsfortegnelse

1 Innledning

1.1 Rettslig grunnlag og hovedtema.

Ved vedtakelsen av lov om mekling og rettergang i sivile tvister av 17.juni 2005 nr. 90 (tvisteloven) ble det i kapittel 28 innført regler om **rett til å begjære sikring av bevis og å få tilgang til bevis** på et stadium forut for at det er reist ordinært søksmål om det materielle rettskravet.[1]

Hovedforutsetningene er at det enten foreligger bevisforspillelsesfare eller det "av andre grunner er særlig viktig å få tilgang til beviset før sak reises", jf. tvisteloven § 28-2.

Bevissikring utenfor rettssak er et sivilprosessuelt hjelpemiddel som skal gjøre det mulig for begjærende part å få sikret bevis og å få tilgang til bevis når det er nødvendig for at hun[2] skal kunne ivareta sine rettigheter i eller utenfor domstolene. Disse reglene omtales som "bevissikring utenfor rettssak", og er tema for denne avhandlingen[3].

I henhold til lov av 12. mai 1961 nr. 2 om opphavsrett til åndsverk m.v. (åndsverksloven) § 1 første ledd, har "[d]en som skaper et åndsverk (…) opphavsrett til verket", og i henhold til åndsverkslovens § 2 har "opphavsmannen"/"rettighetshaver" blant annet "enerett til å råde over åndsverket (…) ved å gjøre det tilgjengelig for

[1] Sondringen mellom sikring og tilgang behandles grundig i kapittel 3.

[2] Rettighetshaver omtales i denne avhandlingen som «hun», «saksøker» og liknende, mens krenkeren omtales som «han».

[3] Bevisreglene som gjelder på dette stadiet, er omtalt som ***bevissikringsreglene***. De bevisreglene som kommer til anvendelse etter at kravet er brakt inn for domstolen, under saksforberedelsen og hovedforhandlingen, kalles *de alminnelige bevisreglene.*

almenheten (…).” Denne **eneretten** omtales vanligvis og i denne avhandlingen som ”tilgjengeliggjøringsretten”.[4]

Begrunnelsen for at rettighetshaver er gitt en slik enerett, er at rettighetshaver skal kunne utnytte de økonomiske fordelene dette innebærer, og ha et incitament til å skape nye verk som kan komme samfunnet til gode.

Åndsverkloven er **teknologinøytral** og det innebærer at denne eneretten gjelder i alle ”medier”[5]. Å stille en fil med opphavsrettsbeskyttet materiale til disposisjon for andre på internett omtales som ”opplastning” av filen, og innebærer altså en ”tilgjengeliggjøring”[6]. En slik opplastning medfører at andre får muligheten til å gjøre seg kjent med innholdet, ved at filen eksempelvis kan “lastes ned”.[7] [8]

---

[4] Åndsverkloven sondrer mellom tre ulike former av tilgjengeliggjøringshandlinger; spredningsretten, visningsretten og fremføringsretten. I de tilfeller der verket deles ved bruk av tekniske hjelpemidler, vil dette anses som en fremføring av verket, jf. Ot.prp. nr.46 (2004-2005) side 24. Deling av opphavsrettsbeskyttet materiale via internett vil således anses som en fremføringshandling. Relevansen av denne sondringen knytter seg først og fremst til at det foreligger begrensninger i eneretten og at disse varierer avhengig av hvilken tilgjengeliggjøringsform som er aktuell. Tilgjengeliggjøringsretten omtales i punkt xxx. Rognstad (2009) side 156.

[5] Ot.prp. nr.46 (2004-2005) side 19 som omtaler “tilgjengeliggjøring for allmennheten” som et teknologinøytralt begrep.

[6] Se nærmere om tilgjengeliggjøringsbegrepet, dets innhold i kapittel xxx.

[7] Nedlastning av filer, er i henhold til åndsverksloven § 2 ansett for å være såkalt ”eksemplarfremstilling” og dette omfattes også av opphavsmannens enerett. De spørsmål som oppstår ved sikring av bevis for materielle opphavsrettskrenkelser i form av nedlastning/eksemplarfremstilling er ikke et direkte tema for denne avhandlingen og vil ikke bli behandlet eksplisitt. Her skal kun nevnes at de rettslig relevante spørsmålene ofte vil være likeartede, slik at innholdet i avhandlingen på mange punkter vil ha overføringsverdi.

[8] Siden opplastning er en forutsetning for nedlastning, og en opplastning kan medføre mange nedlastninger, kan opplastning ses som en ”grovere” handling. Kulturdepartementet har i et Høringsnotat fra 2011kommet med forslag til regulering av opplastningene, men har i første omgang ikke foreslått tiltaksom direkte retter seg mot de som foretar nedlastninger. Dette kan anses som et uttrykk for at også departementet anser opplastningshandlingene for å være grovere og at det er større behov for å stanse disse.

Den teknologiske utviklingen har medført at mulighetene for å dele informasjon de siste tiår er blitt betydelig forbedret og kan gjøres raskere, enklere og billigere enn gjennom de tidligere tradisjonelle (analoge) delingsmetoder. Dette har medført en betydelig utvidelse i den faktiske muligheten til å tilgjengeliggjøre opphavsrettsbeskyttede filer, særlig via internett. I utgangspunktet gir dette mange positive effekter for utnyttelse i lovlig øyemed, men har også den bivirkning at ulovlig fildeling[9] har fått meget stor utbredelse i dagens samfunn. Ulovlig tilgjengeliggjøring av opphavsrettsbeskyttet materiale, herunder særlig filmer, musikkfiler, datamaskinprogrammer og dataspill m.m. skjer nå kontinuerlig verden rundt.

1.2 Avhandlingens hovedproblemstillinger:

Det store omfanget av ulovlig tilgjengeliggjøring av opphavsrettsbeskyttet materiale på internett reiser mange utfordringer. Én særlig viktig utfordring er hvordan man skal redusere omfanget av slike opphavsrettskrenkelser på internett, i Norge og internasjonalt. Dette er særlig en utfordring som særlig må løses med myndighetenes hjelp via lovgivning[10] og internasjonale avtaler.[11]

For den enkelte rettighetshaver[12] eller interesseorganisasjon, som ønsker å håndheve sine rettigheter, medfører det forhold at internett er globalt, at et stort antall av **krenkelsene skjer på tvers av landegrensene**, og dette skaper flere jurisdiksjonsproblemer.

---

[9] Med fildeling brukes her som en fellesbetegnelse på ulike teknologiske fremgangsmåter som muliggjør deling av og tilgang for andre til elektronisk lagret informasjon.

[10] Eksempelvis Høringsnotatet fra Kulturdepartementet (2011) om forslag til "Endringer i åndsverksloven (tiltak mot ulovlig fildeling og andre krenkelser av opphavsrett m.m. på Internett").

[11] Agreement on Trade-Related aspects of Intellectual Property Rights, av 1.januar 1995 (TRIPS-avtalen).

[12] Når jeg i denne avhandlingen bruker uttrykket "rettighetshaveren", sondrer jeg ikke mellom den originære opphavsmannen og de som eventuelt har overtatt deler av opphavsmannens rettigheter. Også de såkalte "nærstående" rettigheter omfattes, altså utøvende kunstneres enerett til fremføringen, se nærmere punkt xxx.

Av større praktisk relevans for denne avhandlingens tema, er de særlige utfordringene knyttet til **bevissituasjonen**, herunder blant annet vanskeligheter med å kunne bevise **at** det er skjedd en ulovlig fildeling,[13] **omfanget** av rettsbruddet og særlig **hvem** som har foretatt opplastningen.

For at rettighetshaver skal kunne håndheve sine rettigheter, må rettighetshaver kunne **dokumentere** at det har skjedd en krenkelse av rettighetene hennes/hans[14]. Når man mistenker at noen har fortatt en ulovlig handling, må man sanke bevis for å klarlegge hvor god sak man har rettslig sett. Dette kan kalles "bevissankningsstadiet". På dette stadiet foretar man undersøkelser for å klarere hva som har skjedd hos den eventuelle fremtidige motparten, og i normale tilfeller skjer dette uten bistand fra domstolene. Dette kan vi kalle "privat etterforskning utenfor domstolene".

Ved opplastning av opphavsrettsbeskyttede verk på internett, knyttes brukerne til internett via såkalte IP-adresser,[15] og det medfører at deres identitet ikke blir umiddelbart tilgjengelig for andre, og dermed at heller ikke rettighetshaver uten videre kan skaffe seg tilgang til informasjon om hvem som har foretatt opplastningen. Internett-tilbyderne har rett til å lagre opplysninger om hvilken abonnent som er tildelt den aktuelle IP-adressen på det aktuelle tidspunktet, men det foreligger både rettslige og faktiske begrensninger i rettighetshavernes mulighet til å få tilgang til disse "abonnentopplysningene"[16]. Det medfører at det på dette området foreligger et særlig behov for bistand fra domstolene, for å gi rettighetshaver tilgang til abonnentopplysningene for å identifisere krenkeren[17]. **Ett tema for denne avhandlingen er i hvilken utstrekning tvistelovens regler om bevissikring utenfor rettssak kan ivareta rettighetshavers behov.**

---

[13] Fildeling forklares i kapittel xxx.

[14] I kapittel xxx gir jeg en nærmere redegjørelse for selve krenkelseshandlingen og det rettslige grunnlaget for opphavsmannens rettigheter.

[15] Dette forklares nærmere nedenfor i punkt xxx.

[16] Med «abonnentopplysninger» menes de kontaktopplysninger som registreres hos internettleverandøren ved opprettelse av et internettabonnement, herunder navn og adresse, jf. ekomforskriften § 6-2.

[17] Med «krenker» menes den som foretar en ulovlig opplastning.

Tilgang til abonnentopplysninger er imidlertid ikke tilstrekkelig for å oppfylle rettighetshavers behov for innsamling av alle de bevis som er nødvendig for å kunne identifisere og rettsforfølge en ulovlig opplastning. Jeg kommer tilbake til dette nedenfor i punkt 2.4. I tillegg kommer at rettighetshaver kan ha et ønske om å sikre pålitelige bevis for omfanget av krenkelsene av opphavsrettighetene, herunder også eventuelt omfanget av nedlastninger som er foretatt på grunnlag av denne opplastningen. Dette tilsier at rettighetshaver har behov for ytterligere bevis.

De relevante bevisene som underbygger dette, vil i hovedsak være elektronisk lagret og lokalisert hos abonnenten[18] på det lagringsmedium opplastningen har skjedd via, eksempelvis en datamaskin. Lokaliseringen medfører at rettighetshaveren ikke har direkte tilgang til disse sporene. Denne faktiske begrensningen i rettighetshavers mulighet til å sanke bevis ved privat etterforskning utenfor domstolene medfører at han også har behov for domstolenes bistand til å sikre slike bevis. Til dette kommer at dersom rettighetshaver hadde benyttet seg av den **ordinære fremgangsmåten** med å reise sak og begjære tilgang til bevis under saksforberedelsen etter tvisteloven kapittel 26 og 27, kunne motparten også lett ha manipulert og fjernet denne informasjonen. Dette viser behovet for å foreta bevissikring og det viser behovet for å kunne foreta slik bevissikring uten at motparten blir varslet om tiltaket på forhånd.

I denne avhandlingens kapittel 4 vil jeg redegjøre nærmere for de materielle og prosessuelle vilkår som må være oppfylt for å få medhold i en begjæring om sikring av bevis og tilgang til bevis ved mistanke om ulovlig opplastning av opphavsrettsbeskyttede verk på internett. Det er særlig to kategorier bevis det kan være relevant å sikre og disse er abonnentopplysninger og bevismateriale hos abonnenten.

I tillegg til rettighetshavernes viktige interesser, aktualiserer sikring og tilgang til abonnentopplysninger og elektroniske spor hos abonnenten også andre generelt tungtveiende interesser, herunder personvernhensyn, rettssikkerhetshensyn og hensynet til ytringsfriheten. I avhandlingen redegjøres for hvordan reglene ivaretar og avveier disse interesser ved løsningen av forskjellige spørsmål. Disse sterke motstridende

[18] Abonnenten kan enten være en privatperson eller en bedrift.

interessene er også fanget opp av internasjonale menneskerettigheter, og det gjør det nødvendig å drøfte om lovgiver og domstolenes konkrete grensedragninger er i overensstemmelse med menneskerettighetene, se punkt 4.10.

Tvisteloven åpner også for at slik bevissikring i enkelte tilfeller kan skje uten at motparten varsles og gis adgang til å bli hørt på forhånd. Dette unntaket fra kontradiksjonsprinsippet blir behandlet særskilt i punkt 5.3.

1.3 Nyere historisk utvikling og Norges folkerettslige forpliktelser til å sikre håndhevelsen av immaterielle rettigheter.

Bestemmelsene om bevissikring utenfor rettssak i tvisteloven er en videreføring av reglene om "bevisoptagelse utenfor retssak" i den tidligere tvistemålsloven kapittel 20[19].

Erfaringer fra anvendelsen av tvistemålslovens regler viste at reguleringen ikke var tilstrekkelig tilpasset de behov den teknologiske utviklingen medførte. Rettsutviklingen mot dagens ordning har skjedd i flere etapper, etter hvert som lovgiver har ansett det for nødvendig å foreta slike endringer. Behovet for regulering skyldes også internasjonale forhold.

I forbindelse med Norges inngåelse av WTO-avtalen[20] ble Avtale om handelsrelaterte sider ved immaterielle rettigheter (TRIPS-avtalen) vedtatt som vedlegg 1C.[21]

TRIPS-avtalen stiller krav til statenes lovgivning om vern av immaterielle rettigheter. I henhold til artikkel 50 nr. 1, pålegges medlemslandene å ha en ordning som sikrer at rettighetshaverne raskt og effektivt kan iverksette tiltak for å forhindre krenkelse av

[19] Tvistemålsloven av 13. august 1915 nr. 6 §§ 267-271a. Loven ble opphevet ved vedtakelsen av tvisteloven.

[20] Avtale av 15.april 1994 om opprettelsen av Verdens Handelsorganisasjon (World Trade Organization). Avtalen trådte i kraft 1.januar 1995.Se ot.prp. nr. 33 (2003-2004) punkt 2.

[21] Avtalen trådte i kraft 1.januar 1995.

immaterielle rettigheter (litra a), og for å ivareta relevant bevismateriale i forbindelse med den angivelige krenkelsen (litra b).

I en sak mellom Microsoft og Storbyguiden gjengitt i Rt 2000 side 1261 kom høyesteretts kjæremålsutvalg til at tvisteloven § 270 ikke gav hjemmel for å fatte endelig avgjørelse om bevissikring uten å la motparten fikk anledning til å uttale seg.

Avgjørelsen medførte at lovgiver i 2004 vedtok tvistemålsloven § 271a som innførte en rett til å sikre bevis uten at motparten får anledning til å uttale seg om dette før sikringen er gjennomført[22]. Det fremgår av forarbeidene[23] til endringsloven at Justis- og politidepartementet mente at norsk rett på dette punktet ikke var i samsvar med avtalen, og at "utvidelsen også [hadde] til hensikt å tilfredsstille kravene i artikkel 50 i (…) TRIPS-avtalen".[24]

Tvistemålslovens regler ble med noen endringer videreført ved tvisteloven.[25]

Siden TRIPS-avtalen bare pålegger medlemsstatene å ha et slikt system for ivaretakelse av immaterielle rettigheter, har mange av våre naboland innført tilsvarende spesielle regler[26] [27]. Tvistelovens regler om bevissikring utenfor rettssak er imidlertid gjort generelle.
Den 19. mai 2011 har Kulturdepartementet sendt ut et høringsforslag med forslag til endringer i åndsverkloven[28]. Kulturdepartementet argumenterer grundig for sitt forslag

---

[22] Bestemmelsen er nå videreført i tvisteloven § 28-3 fjerde ledd.

[23] Ot.prp. nr. 33 (2003-2004) punkt 2.2 siste avsnitt.

[24] Ot.prp. nr.33 (2003-2004) punkt 2.3

[25] Se spesialmotivene til kapittel 28 i Ot.prp.nr.51 (2004-2005) side 470 "*Tvistemålsloven har regler om bevissikring utenfor rettssak i §§ 267-271 a. Disse reglene videreføres i stor grad i lovforslaget. De viktigste endringene i forhold til gjeldende rett er for det første at virkeområdet for bevissikringsreglene utvides. For det annet innføres en adgang til* ***bevistilgang*** *utenfor rettssak.*"

[26] Sverige i Lag av 30. desember 1960 nr. 729 om upphovsrätt till litterära och konstnärliga verk, jf §§ 56a til 56h.

[27] Danmark i Retsplejeloven av 09.11.2010 kapitel 57a.

[28] Høringsnotat: Endringer i åndsverksloven (tiltak mot ulovlig fildeling og andre krenkelser av opphavsrett m.m. på Internet).

om å innføre spesielle bevissikringsregler i åndsverkloven, men alternativet om å gjøre endringer i tvisteloven synes ikke nærmere vurdert. I avslutningen, kapittel 7 vil jeg gi noen betraktninger om endringer bør skje i åndsverkloven, eller om endringene bør skje i tvisteloven.
De rettskildemessige spørsmålene som Norges forpliktelser etter TRIPS-avtalen reiser for tolkningen av reglene om bevissikring utenfor rettssak på immaterialrettens område, behandles i punkt 1. 7 rettskilder og metode.

1.4 Hovedformålene med bevissikringsreglene

Ved ulovlig opplastning av opphavsrettsbeskyttet materiale på Internett, gir åndsverkloven §§ 54-56 rettighetshaver forskjellige rettskrav, herunder for eksempel krav på erstatning. Jeg kommer nærmere inn på dette i punkt 4.4.1. Det er imidlertid "forskjell på å ha rett og å få rett". Bevissikringsreglene har flere formål som behandles nedenfor, men grunntanken bak alle disse formålene er at bevissikringsreglene skal bidra til at rettighetshaver skal kunne ivareta sine rettigheter, og slik "få rett".

Litt upresist kan det sies at rettighetshavers mulighet til å håndheve et eventuelt erstatningskrav på egen hånd, i utgangspunktet er begrenset faktisk og rettslig. Avgjørende for håndhevelsesadgangen beror i mange tilfeller på bevissikringsreglene, herunder i hvilken utstrekning disse hjemler en rett til å sikre de relevante bevisene. At det er mulig for en rettighetshaver til å håndheve sine rettigheter, er helt grunnleggende i en rettsstat.

1.4.1 Bevissikringsreglene skal bevirke materielt riktige avgjørelser:

Ett av hovedformålene med reglene om bevissikring utenfor rettssak er å sørge for at det faktiske grunnlaget retten baserer sin fremtidige avgjørelse på, er best mulig opplyst, og på den måten medvirke til at den avgjørelsen retten faller ned på er et **materielt riktig resultat**.[29] [30]

---

[29] Jamfør tvistelovens formål i tvisteloven § 1-1 første ledd.

Det mest grunnleggende hensynet bak en enhver god prosessordning er å sikre at rettsavgjørelsene blir materielt riktige, herunder å ha saksbehandlingsregler som sikrer at retten baserer seg på riktig faktum[31] og juss.[32]

Bevissikringsreglene skal medvirke til at rettens avgjørelse er korrekt hva gjelder det faktiske avgjørelsesgrunnlaget.[33]

Ett av formålene med bevissikringsreglene er således å hindre at saksøkte sletter bevis eller på annen måte gjør de utilgjengelige for rettighetshaver og domstolen, i situasjoner hvor det er fare for bevisforspillelse. Nedenfor i kapittel 4.6 redegjøres nærmere for de bevis det kan være aktuelt å sikre og hvorfor det er særlig fare for at opplaster kan gjøre slike bevis utilgjengelig for rettighetshaver.

---

[30] Vi sondrer mellom "materielt riktige" og "formelt riktige avgjørelser". Med "formelt riktige avgjørelser" forstår vi avgjørelser som er fattet i overensstemmelse med de prosessuelle regler. Dette trenger ikke nødvendigvis å være i overensstemmelse med de underliggende «realiteter». I den utstrekning prosessreglene setter grenser for partenes anledning til å føre de bevis de mener er relevante, og fremføre de argumentere de mener er relevante, kan resultatet bli materielt uriktig selv om det ikke er noe å utsette på avgjørelsen formelt sett. Begrensninger i den frie bevisføringsretten, kan medføre avvik mellom det virkelige hendelsesforløpet – "den materielle sannhet" – og det faktum retten legger til grunn som bevist – "den formelle sannhet", se Torgersen (2009) side 20-21.

[31] Ot.prp. nr. 51 (2004–2005) side 203.

[32] Tvisteloven har mange bestemmelser som skal sikre at rettsanvendelsen blir korrekt, se eksempelvis tvisteloven § 9-2, om kravene til stevningens innhold, som oppstiller en plikt for saksøker til å angi den rettslige begrunnelsen for sitt krav. Bestemmelsen skal besørge at en part på forhånd vet hvilke rettslige grunnlag og rettskildefaktorer som vil være relevante å påberope seg. Videre kan nevnes tvisteloven § 9-15 syvende ledd som gir partene rett til å få ordet under hovedforhandlingen for å argumentere blant annet for innholdet i rettsregler, samt § 29-3 om rett til å anke dersom tapende part mener at rettens avgjørelsesgrunnlag lider av rettsanvendelsesfeil. Kontradiksjonsprinsippet og prinsippet om rett til to-instansbehandling er således to prinsipper som skal medvirke til et rettsriktig resultat.

[33] Ot.prp. nr.51 (2004-2005) punkt 16.1.1 side 203.

1.4.2 Bevissikringsreglene skal bidra til å gjøre rettighetshaver i stand til å forutberegne sin rettsstilling:

Formålet med bevissikringsreglene er mer omfattende enn å sikre bevis som ellers kan gå tapt. Prosessreglene bør innrettes slik at rettighetshaver i størst mulig grad har mulighet til å **forutberegne sakens faktiske stilling før sak reises for domstolene**. Dette medfører at rettighetshaver gis mulighet til å vurdere hvor god sak hun har rettslig og faktisk, og å kalkulere risikoen for at hun eventuelt taper en sak og konsekvensene av dette, herunder et eventuelt ansvar for egne og motpartens sakskostnader. Ett av formålene med bevissikringsreglene er således å bidra til at rettighetshaver ikke reiser ubegrunnede søksmål, men også at rettighetshaver stilles i posisjon til å kunne reise søksmål i tilfeller hvor det er grunnlag for det.

For at rettighetshaver skal kunne forutberegne sin rettsstilling, er det ikke tilstrekkelig at rettighetshaver får medhold i en begjæring om **sikring** av de relevante bevisene. Det er også nødvendig at rettighetshaver får **tilgang** til disse bevisene.[34]

1.4.3 Bevissikringsreglene skal bidra til å få avgjort tvisten uten saksanlegg:

Ved å bidra til å gjøre rettighetshaver kjent med de faktiske forhold bidrar bevissikringsreglene også til å legge til rette for at parter skal kunne få avgjort sine tvister utenfor domstolene.[35]
Dette ble fremhevet som ett viktig formål med revisjonen av de sivilprosessuelle reglene.[36] [37]

---

[34] Se NOU 2001:32B side 987-988: "Uten regler om bevistilgang vil en part kunne bli stilt i en meget vanskelig situasjon i tilfeller hvor det kan være grunnlag for å fremme et krav eller å godta et krav som rettes mot parten. Parten kan bli stilt overfor valget mellom å reise sak eller ta til motmæle i saken på et uholdbart faktisk grunnlag eller avstå fra å reise sak eller ta til motmæle i en sak til tross for at faktiske forhold som han ikke kjenner, tilsier noe annet."

[35] Siden det er nødvendig med en avgjørelse fra domstolene, innebærer reglene det paradoksale at man benytter domstolene for å hindre at det blir nødvendig å benytte domstolene.

[36] Se Kommentar om bevissikringsreglene i Ot.prp.nr. 51 (2004-2005) side 470: «Reglene bør ses i sammenheng med lovens vektlegging av at tvister skal søkes løst før de når domstolene. (…) I denne sammenheng kan det være av stor betydning å oppnå bevissikring så tidlig som mulig».

Jo bedre klarlagt saken kan bli før sak reises, desto større sannsynlighet er det for at krenkeren forstår at han vil tape en sak, og desto større sannsynlighet er det for at han vil akseptere et tilbud om en minnelig løsning.[38]

I tillegg til at bevissikringsreglene bør kunne benyttes for å sikre bevis som underbygger at det er skjedd en ulovlig opplastning av opphavsrettsbeskyttet materiale, er det ønskelig at reglene kan benyttes for å sikre og gi tilgang til bevis for omfanget av rettsbruddet og andre forhold som er relevante for beregningen av et eventuelt erstatningskrav eller vederlagskrav. Slike bevis vil hjelpe rettighetshaver i argumentasjonen for å oppnå et godt forlik.[39]

Dette må også ses i sammenheng med ønsket om en prosessordning som sørger for et materielt riktig resultat også uten saksanlegg.

1.4.4 Bevissikringsreglene skal gi rettighetshaver mulighet til å gjøre seg kjent med hvem krenkeren er:

Reglene om bevistilgang utenfor rettssak har også det noe spesielle formålet å gi rettighetshaver større muligheter til å **gjøre seg kjent med hvem motparten er.**
I denne avhandlingen er dette særlig sentralt blant annet fordi opplastning på Internett skjer via en IP-adresse, og opplysningene om hvem som har abonnementet knyttet til denne IP-adressen, er underlagt taushetsplikt. Det medfører at reglene om bevissikring og bevistilgang utenfor rettssak er nødvendige for at rettighetshaver skal få tilgang til informasjon om hvem som har foretatt opplastningen, og på det grunnlaget kunne ivareta sine rettigheter ved domstolene eller ved en minnelig ordning.

---

[37] Se også NOU 2001:32B side 987-988: «Like viktig er at manglende mulighet for tilgang til bevis kan medføre at partene ikke forsøker å nå frem til en minnelig ordning gjennom forhandlinger…»

[38] Formålet er også sentralt bak reglene i tvisteloven kapittel 5 om partenes plikter før sak reises.

[39] NOU 2001: 32B side 988 punkt 31.1.

1.4.5 Bevissikringsreglenes preventive virkninger:

De ovenfor nevnte formål kan direkte bidra til at rettighetshaver i hvert fall i en viss grad får gjenopprettet den skade som opplastningen av den opphavsrettsbeskyttede filen har medført. Slik sett har det prosessuelle virkemiddelet en gjenopprettende funksjon.

I den utstrekning disse reglene fungerer slik at rettighetshaver kan ivareta sine opphavsrettigheter mer effektivt, og dette blir kommunisert til befolkningen, slik at folk ser at ulovlige opplastninger kan få store økonomiske konsekvenser for dem, vil reglene også kunne få en preventiv virkning. Slik situasjonen er nå, er det imidlertid liten grunn til å tro at reglene om bevissikring utenfor rettssak har noen særlige preventiv virkning, i hvert fall ikke på den som foretar opplastninger i liten skala.

1.4.6 Forholdet til andre grunnleggende hensyn:

Samlet skal reglene sikre rettighetshavernes mulighet til effektivt å kunne ivareta egne rettigheter med domstolenes hjelp, og dette er også ett av formålene med TRIPS-avtalen på immaterialrettens område.[40]

Formålene med bevissikringsreglene må imidlertid forstås på bakgrunn av de grunnleggende hensyn bak en god prosessordning, tvistelovens formål, og andre hensyn som taler for å foreta sikring og utlevering av bevis til rettighetshaver. Disse hensyn må også balanseres mot andre hensyn som kan tale mot slik sikring og tilgang, herunder personvernhensyn og øvrige rettssikkerhetshensyn.

Disse hensyn og avveininger av disse er selvfølgelig nært knyttet opp til spørsmålene om innholdet i de materielle vilkårene loven oppstiller for å anvende

[40] Se begrunnelsen for opphavsrett i Høringsnotat (2011) punkt 1.1.2: «Opphavsrett er bl.a. begrunnet i å sikre opphavsmenn muligheter til å få et økonomisk utbytte av sitt skapende arbeid. En grunntanke er at opphavsrett vil stimulere kreativitet og åndsproduksjon i samfunnet. Hvis opphavsmenn ikke hadde muligheten for økonomisk utbytte av sine verk, hadde de ikke hatt de samme incentivene til skapende arbeid. Lovens vern er altså ikke bare begrunnet i hensynet til den enkelte opphavsmann, men også i at skapende virksomhet er i samfunnets interesse.»

bevissikringsinstituttet, lovgivningens unntak og begrensninger og særtilfeller. Siden disse spesielle hensynene vil være relevante ved tolkingen av disse reglene, behandles disse motstridende hensynene i sin rette sammenheng i de enkelte kapitlene i avhandlingen.

1.5 Plass i rettssystemet

Tvistelovens regler om sikring av bevis er ett av tvistelovens[41] ulike virkemidler som skal sørge for at sakens bevis og faktiske forhold blir klarlagt forut for søksmål, under saksforberedelsen og under hovedforhandlingen.

Siden dette er helt grunnleggende, er det ikke overraskende at det er mange slike bestemmelser. I tillegg til bestemmelsene i kapittel 5 som gjelder før søksmål, nevnes her tvisteloven § 21-4 og 21-5 som pålegger partene plikt til på eget initiativ å opplyse om de sanne faktiske forhold og å opplyse om og tilby bevis også de som taler i egen disfavør.

Tvisteloven § 26-5 pålegger enhver å gi tilgang til bevis man har for hånden eller kan skaffe til veie, såkalt prosessuell **edisjonsplikt**.[42]

Slike regler **innebærer** at selv om saksøker ikke har tilstrekkelig bevis for hånden da sak reises, kan bevissituasjonen klarlegges under saksforberedelsen og under hovedforhandlingen. I mange tilfeller kan det imidlertid være dristig for en saksøker **å satse** på at motparten oppfyller denne sannhetsplikten, og det gjelder særlig fordi saksøker i mange tilfeller ikke vil klare å bevise at saksøkte holder tilbake relevante opplysninger og bevis.

Av slike grunner vil rettighetshaver være best tjent med å klarlegge bevissituasjonen **før** hun reiser søksmål, og ett av formålene med bevissikringsreglene er nettopp å bidra til "**å sikre bevis for en fremtidig rettssak**."[43]

---

[41] Utenfor tvisteloven kan nevnes straffeloven § 166 som oppstiller en straffesanksjonert plikt til å bidra til opplysning av en sak i og med at en part og et vitne skal fortelle hele sannheten.

[42] Ot.prp. nr.51 (2004-2005) side 204.

[43] Se Ot.prp.nr.33 (2003-2004) side 2.

Slik vil reglene om sikring og tilgang til bevis fungere som supplement til de alminnelige bevisreglene og tvistelovens edisjonsplikt som gjelder etter at saken er reist. Dette gjelder særlig i tilfeller hvor det kan være særlig grunn til å tro at saksøkte kommer til å misligholde disse pliktene, uten at saksøker kan gå ut i fra at retten kommer til å sanksjonere misligholdet.[44]

Selv om bevissikringsreglene ble noe utvidet ved gjennomføringen av TRIPS-avtalen i norsk rett, er reglene om bevissikring utenfor rettssak **generelle**. Dette betyr at de også har et tradisjonelt anvendelsesområde; å sikre bevis som kan gå tapt av **andre grunner** enn at saksøkte kan slette eller unndra bevis fra saksøker. Tradisjonelt er disse reglene benyttet i tilfeller hvor et vitne ikke vil kunne føres på et senere tidspunkt for eksempel når vedkommende ligger på dødsleiet, skal flytte fra landet eller skal på en lengre utenlandsreise.[45] [46]

1.6 Avgrensninger

Som overskriften viser er avhandlingens tema særlig anvendelsen av tvistelovens regler om bevissikring utenfor rettssak på krenkelser av tilgjengeliggjøringsretten på Internett, men redegjørelsen er ikke begrenset til dette. Tvistelovens regler er som nevnt gjort generelle, og selv om hovedfokuset er ovennevnte saksforhold, er redegjørelsene for vilkårene og virkningene i avhandlingen her gitt et innhold som medfører at de er ment å ha overføringsverdi til andre saksforhold. Jeg har også benyttet eksempler og rettspraksis fra andre materielle områder.

TRIPS-artikkel 50 nummer 1 regulerer midlertidig sikring for å hindre krenkelser, og nummer 2 tiltak for å hindre bevisforspillelse. Midlertidig forføyning, og bevissikringsregler i andre lovbestemmelser faller utenfor avhandlingen.

---

[44] Slike sannhets- og opplysningsplikter har et noe uklart innhold, og dermed vil det være **usikkert** om retten vil sanksjonere saksøktes brudd på pliktene.

[45] Schei (2007) Bind II side 1248.

[46] De tradisjonelle formål med bevissikringsreglene omtales ikke nærmere.

Særlig fordi plassen er begrenset har det vært nødvendig å avgrense mot en grundig behandling av reglene om saksomkostninger i tvisteloven § 28-5.
Jeg avgrenser også mot lovvalgspørsmål og jurisdiksjonsspørsmål.

Utenfor faller selvfølgelig også de straffeprosessuelle reglene om ransaking, beslag, krav på utlevering av abonnentopplysning i etterforskningsformål.

Tvistelovens regler gjelder **ikke** der **straffesanksjoner** er aktuelle, men siden brudd på opphavsrettigheter også er straffesanksjonert, jf åndsverksloven § 54, kan anvendelsen av reglene om bevissikring utenfor rettssak i en sivil sak reise spørsmål om forholdet til selvinkrimineringsforbudet i straffeprosessloven § 90 (parter), § 123 (vitneførsel som kan utsette vitnet for straff) og EMK art 6 og FN-konvensjonen om sivile og politiske rettigheter artikkel 14 nr. 3 bokstav g), jf. menneskerettighetsloven § 2. Jeg behandler ikke dette nærmere her.

1.7 Rettskilder og metode

I avhandlingen tar jeg sikte på å redegjøre for «gjeldende rett». Det innebærer at jeg tar vil redegjøre for rettsreglene slik jeg antar at Høyesterett vil forstå reglene dersom spørsmålet kommer for Høyesterett. Dette innebærer at jeg bruker «**vanlig» juridisk metode**, herunder alle relevante rettskildefaktorer.[47] Siden Høyesterettspraksis gir grunnlag for å bygge på prinsipper og reelle hensyn, vil også jeg gjøre dette i de tilfeller hvor jeg tror Høyesterett ville ha gjort dette. Dette er særlig aktuelt i de tilfeller hvor lovteksten er vag, for da gir ordlyden få føringer på løsningen og i tillegg fungerer lovteksten da mindre som en grense mot å oppnå gode resultater. De grunnleggende hensyn bak enhver god prosessordning, som nå er søkt lovfestet i tvisteloven § 1-1 er relevante for fastsettelsen av innholdet i alle avhandlingens relevante vilkår. Jeg viser til redegjørelsen nedenfor.

[47] Jeg vil også henvise til juridisk teori og avgjørelser fra tingretten og lagmannsretten, selv om jeg mener at dette ikke er rettskildefaktorer Høyesterett vil tillegge vekt. På samme måte som Høyesterett finner gode argumenter i slike kilder, bruker også jeg disse som argumentasjonskilder.

I den utstrekning tvistelovens regler er ment å være en videreføring av reglene i tvistemålsloven, vil Høyesterettsavgjørelser som angår tolkningen av de tilsvarende bestemmelser i tvistemålsloven være relevante tolkningsfaktorer.
Siden det er sparsommelig med rettspraksis om bevissikring utenfor rettssak, og forarbeidene til tvisteloven er forholdsvis nye og omfattende blir forarbeidene en sentral rettskildefaktor.
Nedenfor behandler jeg også Den europeiske menneskerettighetskonvensjonen (EMK). Behandlingen reiser imidlertid ikke tolkningsspørsmål som gir grunn til å redegjøre for hvilken juridisk metode Den europeiske menneskerettighetsdomstolen (EMD) benytter. Avhandlingens tema kan gi opphav til følgende problemstilling: Hvordan skal Høyesterett harmonisere Norges plikter etter EMK artikkel 8 og Norges plikter etter TRIPS-avtalen dersom disse er innbyrdes motstridende. Dette problematiseres ikke nærmere.

Anvendelsen av TRIPS-avtalen fortjener noen ord her. Avtalen/konvensjonen er en folkerettslig bindende avtale og den er søkt gjennomført i norsk rett ved tvistelovens kapittel 28. Dette medfører at denne blir en relevant rettskildefaktor ved tolkningen av tvistelovens regler om bevissikring utenfor rettssak.

Flere av bestemmelsene i avtalen kan etter sin ordlyd gi grunnlag for en slutning om at rettighetshaver pålegges bestemte plikter, se for eksempel artikkel 50 nummer 3 som tyder på at avtalen pålegger rettighetshaver å sannsynliggjør at hun er rettighetshaver. Det klare utgangspunktet er imidlertid at avtalen ikke kan tolkes på denne måten. Den pålegger statene plikt til å innrette det interne rettssystemet slik at det minst gir rettighetshaverne de rettigheter som følger av konvensjonen. Konvensjonen er ikke til hinder for at Norge vedtar internrettslige bestemmelser som stiller rettighetshaverne bedre. Dette innebærer at TRIPS-avtalen er en såkalt «minimumskonvensjon».[48]

[48] Se Ot.prp.nr 33 (2003-2004) Om lov om endringer i tvistemålsloven (bevisopptak utenfor rettssak) side 6.

Siden TRIPS-avtalen også binder andre WTO-land kan det være interessant å se hen til hvordan andre WTO-land har gjennomført avtalen i sitt interne rettssystem og hvordan dette er tolket i praksis. Særlig dansk og svensk rett kan være relevant i kombinasjon med hensynet til (nordisk) rettsenhet.

1.8 Oversikt over enkelte sammenhenger i avhandlingen:

Innledningsvis i kapittel 3 jeg funnet grunn til å presisere innholdet i de forskjellige rettsvirkningene sikring og tilgang til bevis og også sammenhengen med andre rettsvirkninger. Dette gir etter min mening nødvendige premisser for å forstå resten av avhandlingens tema, herunder de materielle vilkårene som behandles i kapittel 3 og de prosessuelle reglene som behandles i kapittel 4.

I kapittel 3 gis en nærmere redegjørelse for vilkårene for å få medhold i en begjæring om bevissikring. Ett av disse vilkårene er at det beviset som begjæres sikret må ha "*betydning i en tvist*"[49]. Dette vilkåret angir et krav om en **sammenheng** mellom **beviset** som begjæres sikret og et **materielt krav**. Siden rettighetshavers materielle krav i denne avhandlingen er basert på åndsverklovens regler, har det vært nødvendig å redegjøre oversiktlig for åndsverkslovens regler, herunder **tilgjengeliggjøringsbegrepet**, og jeg fant det hensiktsmessig å ta den redegjørelsen i punkt 4.4.1 i direkte sammenheng med vilkåret om betydning i en tvist. Redegjørelsen der har også relevans for andre deler av avhandlingen.
Siden innholdet i tvistelovens vilkår for bevissikring på denne måten skal anvendes på de materielle rettskrav som følger av brudd på åndsverkloven, fungerer åndsverkslovens regler på en måte som «**fakta**» i avhandlingen.
Siden brudd på åndsverkloven er en forutsetning for at det skal være aktuelt å kreve sikring av bevis, fungerer åndsverklovens regler som prejudisielle rettsforhold. I kapittel 2 redegjøres for hvordan opplastning av opphavsrettsbeskyttede verk foregår på Internett rent teknisk. Redegjørelsen der utgjør således fakta som må subsumeres under åndsverklovens regler, som altså er prejudisielle. Siden redegjørelsen i kapittel 2 også omfatter de spor som genereres ved opplastning på internett, har kapittel 2 også en

[49] Jf. tvl. § 28-2 første ledd.

direkte relevans for redegjørelsen for bevissikringsreglenes vilkår, virkninger og den konkrete gjennomføringen av bevissikring. Det har derfor vært nødvendig å skille dette ut i et eget kapittel tidlig i avhandlingen.

Sammenhengen med de øvrige kapitlene fremgår tilstrekkelig tydelig av innholdsfortegnelsen, så jeg redegjøre ikke nærmere for dette her.

2 Relevant fildelingsteknologi – de elektroniske spor

Nedenfor i inneværende kapittel vil jeg redegjøre for

- hvordan man laster opp en fil på internett,
- hvordan rettighetshaver kan få kunnskap om en ulovlig fildeling,
- hvilken informasjon rettighetshaver trenger for å identifisere hvilken abonnent som eier internettabonnement som er benyttet ved opplastningen,
- hvilke innsigelser rettighetshaver risikerer å bli møtt med fra en abonnent som blir konfrontert med mistanken, og
- hvilke bevis rettighetshaver kan benytte som forsvar mot slike innsigelser, herunder
- hvilke elektroniske spor som vanligvis oppstår ved opplasting av en fil, og
- hva disse sporene kan bevise om hvem som er den reelle opplaster av en fil

Jeg har forsøkt å gjøre det klart at rettighetshavers på grunn av faktiske og rettslige begrensninger i muligheten for å tilegne seg bevisene, har behov for bistand fra domstolene for å sikre og å få kunnskap om abonnentopplysninger og andre elektroniske bevis.

Fremstillingen gir det faktiske grunnlaget for behandlingen av betingelsene for bevissikring utenfor rettssak etter tvisteloven kapittel 28.

All bruk av elektroniske medier, herunder datamaskiner og kommunikasjon via internett, genererer «elektroniske spor». I tvistelovens systematikk er elektroniske spor «realbevis»,[50] og de er generelt relevante bevismidler. For å være **konkret relevant** i en

[50] Tvisteloven § 26-1 taler om «elektronisk lagret materiale». Ordlyden omfatter det vi vanligvis forstår med «elektroniske spor». Dette omfatter "[e]lectronically stored information, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy(…)", More (2010) note 12 side 149.

konkret sak, krever tvisteloven at de elektroniske spor «kan ha betydning for det faktiske avgjørelsesgrunnlaget i saken.»[51]

Beskrivelsen av den faktiske virkeligheten er også interessant for å forstå anvendelsen av de materielle opphavsrettslige reglene ved ulovlig fildeling på internett, se punkt 4.4.1. De materielle og prosessuelle betingelser som gjelder for å få medhold under hovedforhandlingen er også styrende for hvilke bevis rettighetshaver trenger å sanke forut for søksmål, og redegjørelsen tar hensyn til dette.[52]

Det finnes flere ulike teknologier som muliggjør fildeling. En hovedsondring går mellom såkalte «bruker – tjener»-nettverk eller «klient – server»-nettverk. I slike nettverk lastes filen opp til en sentral lagringsenhet (serveren), og fra denne serveren kan filen lastes ned/kopieres av andre med tilgang til nettsiden. Mer utbredt i dag, er den såkalte bruker-til-bruker-teknologien («peer-to-peer»-teknologien vanlig forkortet "p2p"). I p2p-teknologi overføres filene direkte mellom brukernes datamaskiner uten at filen lagres på en sentral lagringstjeneste. Opplastning av filen skjer dermed også på den enkelte brukers datamaskin og ikke på en sentral server.

Innenfor p2p-teknologier finnes det igjen ulike varianter[53]. Siden BitTorrent-protokollen[54] er den mest utbredte p2p-fildelingsteknologien, vil jeg i hovedsak redegjøre for hvordan opplastning av en fil skjer ved BitTorrent-protokollen.

2.1 BitTorrent-teknologien sett fra opplastingsperspektivet

Kronologisk fremstilt skjer opplastningen[55] i dette systemet ved at en person som ønsker å dele en fil[56] **først lager en oppdeling** av en kopi av filen i deler eller "blokker"

---

[51] Nedenfor i punkt xxx drøftes spørsmålet om hvilke krav til relevans som må være oppfylt på bevissikringsstadiet.

[52] Siden rettighetshavers rettslige og faktiske posisjon under hovedforhandlingen, vil ha stor betydning for forhandlingssituasjonen, har redegjørelsen også overføringsverdi til forhandlingssituasjonen.

[53] Vincents (2007) side 273.

[54] Med «protokoll» forstås et sett av regler som angir hvordan teknologien fungerer, herunder hvordan programmer og maskiner i et nettverk skal kommunisere, jamfør Unuth.

ved hjelp av en protokoll som er designet for nettopp dette formålet. Dette er en såkalt "**BitTorrent-protokoll**". Protokollen genererer en liten *.torrent-fil.[57] *.torrent-filen inneholder blant annet en liste over alle blokkene[58] som filen inneholder, generell informasjon som filens størrelse og type, og informasjon om hvor selve filen er tilgjengelig for nedlasting.[59] Selve filen er på dette tidspunktet gjort tilgjengelig for nedlasting, men for at andre skal kunne laste ned filen, må de få tilgang til informasjonen *.torrent-filen inneholder.

Denne *.torrent-filen distribueres vanligvis til en **tilrettelegger** som sprer slike *.torrent-filer, vanligvis via et nettsted. Den mest kjente tilrettelegger er The Pirate Bay, se www.thepiratebay.org[60] [61]. Spredningen gir potensielle nedlastere tilgang til *.torrent-filen.[62]

For å laste ned filen som *.torrent-filen peker på, må man laste ned et **BitTorrent-klientprogram** eller et peer-to-peer-klientprogram.[63] Dette klientprogrammet kobler alle brukerne opp til en **sporingstjener/**"trackeren".[64]

---

[55] Uttrykket "distribusjon" benyttes om første opplasters tilgjengeliggjøring. Første opplaster kalles «uploader». Senere opplastere kalles "peers". De såkalte "seedere" er opplastere som har lastet opp hele filen.

[56] En «fil» kan defineres som "en samling av data/informasjon lagret på en bestemt del av datamaskinen". Med «data» forstås "en hvilken som helst informasjon lagret på en datamaskin". Jf. Moore (2010) side 150 note 19.

[57] Jeg sondrer mellom *.torrent-filen og selve den opphavsrettsbeskyttede filen (heretter «filen»).

[58] Blokkene blir individualisert ved såkalte "hash-signaturer" som inneholder informasjon for å identifisere og autentisere de enkelte blokkene.

[59] Slik informasjon er data om data og kalles «metadata».

[60] Andre eksempler er Mininova, Torrentz, og det norske fildelingsnettverket Norbits.

[61] Tilretteleggeren har vanligvis også innebygget en søkemotor til å søke blant *.torrent-filene, og søkeresultatet kalles en "index".

[62] *.torrent-filen kan også distribueres via tradisjonelle kommunikasjonsmåter som e-post, og fysisk overlevering på CD, flashdisk etc.

[63] Eksempler her er µTorrent, Vuze og BitComet.

[64] Sporingstjeneren er en «server» som koordinerer brukernes handlinger i BitTorrent-fildelingsnettverket.

Når en bruker laster ned og åpner en *.torrent-fil, kontaktes sporingstjeneren og datamaskinen får en liste over de opplastere/brukere/klienter som deltar i svermen[65], og som maskinen skal koble seg opp mot. Den sentrale sporingstjeneren koordinerer kommunikasjonen mellom klientene i svermen, og er et nødvendig ledd i BitTorrent-teknologien. Under nedlastningen vil maskinen/programmet stadig kommunisere med sporingstjeneren om hvilke deler av filen som er lastet ned og opp, og fra hvilken maskin man laster ned.[66]

Fildelingen i BitTorrent-teknologien medfører at nedlasterne fortløpende også blir opplastere, og vi får dermed en rekke opplastere. **Åndsverkloven rammer også slike etterfølgende opplastere, og disse omfattes således også av fremstillingen her.**

2.2 Rettighetshavers forfølgelse av en ulovlig opplastning via spor i forskjellig teknologi:

Spørsmålene i det følgende er hvordan rettighetshaver kan oppdage ulovlig tilgjengeliggjøring av en fil på internett og hvilke undersøkelser rettighetshaver da kan gjøre for å oppklare hvem som står bak opplastningen.

Rettighetshaver kan typisk oppdage ulovlig tilgjengeliggjøring ved at rettighetshaver selv eller en representant foretar konkrete **søk** etter et konkret åndsverk i et fildelingsnettverk/tilrettelegger.

Muligheten for rettighetshaver til å foreta søk avhenger av hvor åpent nettverket er, og det kan sondres mellom **åpne**[67] og **lukkede**[68] **fildelingsnettverk**.

---

[65] En"sverm" omfatter samlingen av opplasterne.

[66] Avsnittene som beskriver BitTorrent-teknologien er basert på Vincents (2007), side 273-275.

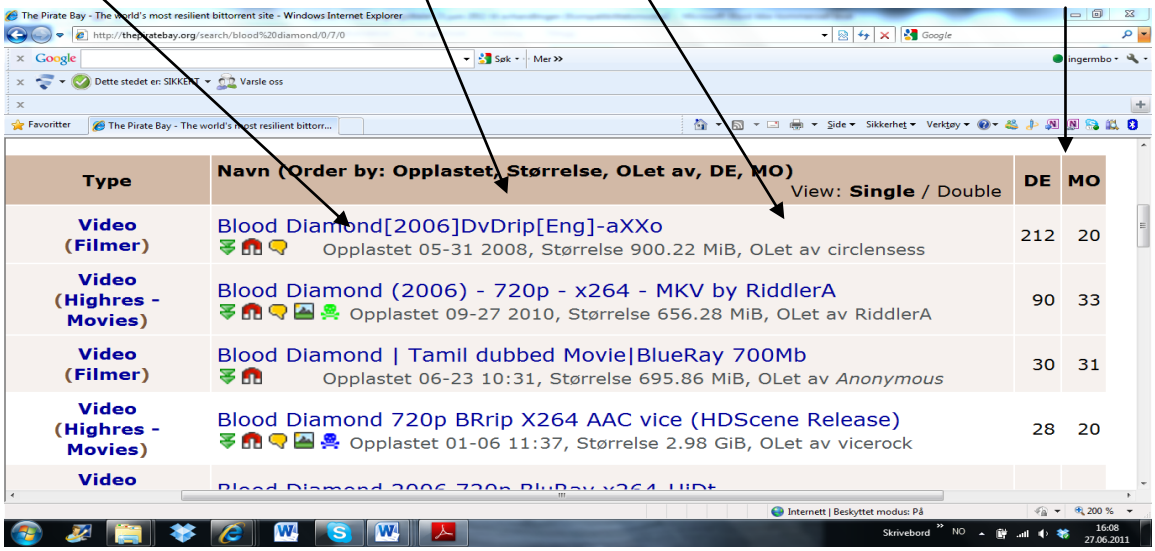
[67] Et åpent nettverk kjennetegnes ved som at det ikke foreligger tilgangsrestriksjoner, eksempelvis The Pirate Bay-nettverket.

[68] Anbefaling av eldre bruker og/eller krav om å bidra med nytt opphavsrettsbeskyttet innhold er vanlige autorisasjonskrav. Dette gjør undersøkelser mer tungvint og tidkrevende for rettighetshaver.

Siden *.torrent-filene vanligvis har søkekriterier som samsvarer med [illegible] etterspurte verket,[69] vil søkeindeksen gi en liste med relevante *.torre[illegible] rettighetshaver god grunn til å tro at hans verk er lastet opp i BitTorre[illegible] Søkeindeksen er i seg selv et relevant bevis, og rettighetshaver kan for eksempel sikre dette ved et Print Screen-bilde av søkeresultatet som vist nedenfor.

Antall personer med tilgang til

Opplastningstidspunktet | Torrent-filnavn | Opplasters



Figur 1: Print screen fra *.torrent-søkeindeksen på The Pirat Bay, søkeresultat på filmen Blood Diamond.

Som ovenfor vist inneholder *.torrent-filen metadata/informasjon som kan være relevant som bevis for å dokumentere hvem som konstruerte *-torrent-filen, og rettighetshaver bør derfor laste ned *.torrent-filen.

Det er alltid en mulighet for at *.torrent-fil**navnet** ikke samsvarer med filens innhold. Dette innebærer at rettighetshaver må laste ned filen som *.torrent-filen viser til for slik å sikre bevis for at det virkelig er det opphavsrettsbeskyttede verket som er lastet opp.

Det norske fildelingsnettverket Norbits hadde tidligere adressen www.norbits.net, men har nå byttet til en hemmelig adresse.

[69] Søker man for eksempel på "Blood Diamond", vil søkeindeksen angi hvilke *.torrent-filer som er laget med dette søkekriteriet.

Både sporingstjeneren og nettsiden kan inneholde informasjon om hvor mange brukere som har lastet opp hele eller deler av filen. Denne informasjonen er relevant for å bevise antall nedlastninger av verket og det igjen er relevant blant annet for å underbygge omfanget av det økonomiske tapet rettighetshaver har lidt.

Ved tilgjengeliggjøring i fildelingsnettverk, vil opplaster i utgangspunktet opptre **indirekte anonymt**, ved at det ikke eksisterer spor som direkte autentiserer/identifiserer opplaster (navn og adresse). Dokumentasjon i form av *.torrent-filen og filen med det opphavsrettsbeskyttede materialet er ikke tilstrekkelig til å si oss noe om **hvem** opplasteren er.

Spørsmålet i det følgende er hvor rettighetshaver kan finne bevis som lokaliserer opplasteren. Det er særlig to typer spor som kan benyttes for å komme på sporet av opplasteren. Disse er **registreringsinformasjon** og **IP-adressen**.

2.2.1 Registreringsinformasjon:

Opplaster av en *.torrent-fil **kan** ha registrert "**registreringsinformasjon**" hos tilrettelegger. På www.thepiratebay.org fordrer opplastning av *.torrent-filer at bruker registrerer brukernavn, passord og epost-adresse. Ved søk i *.torrent-indeksen er brukernavnet synlig for alle.

Tilretteleggere er lite tilbøyelige til å gi registreringsinformasjon videre. Siden registreringsinformasjonen heller **ikke blir autentisert/verifisert**, og brukeren dermed ikke trenger å oppgi korrekt informasjon, får informasjonen uansett mindre pålitelig som bevis.
Rettighetshaver trenger derfor andre typer identifiserende spor, se umiddelbart nedenfor. Registreringsinformasjon, særlig brukernavn kan likevel være en brikke i et større bevisbilde, se nedenfor i punkt 2.6.1.

2.2.2 Informasjon om hvilken IP-adresse som ble benyttet og opplastningstidspunktet:

2.2.2.1 Betydningen av IP-adressen og internettleverandørens tilkoblingslogg:

All kommunikasjon og overføring av data via internettet skjer via et adressesystem som baserer seg på TCP/IP-protokollene. "*IP (Internet Protocol) er den protokollen som brukes for entydig å adressere alle enheter som er tilkoblet internett. Alle data på internett må sendes mellom entydige adresser for å komme fram til riktig datamaskin. Slike adresser kalles IP-adresser*(…)".[70] Internettleverandørene[71] tildeler IP-adresser til sine abonnenter. Tilkobling til internett forutsetter derfor at bruker oppretter et internettabonnement med en ISP. ISP er forpliktet til å registrere informasjon som entydig identifiserer abonnenten, herunder abonnentens navn, adresse.[72] Denne informasjonen omtales som «abonnentopplysninger».[73]

Når abonnenten kopler seg til internett for å laste opp en *.torrent-fil tildeles han en unik IP-adresse.[74] Hvilke IP-adressen den enkelte abonnent tildeles på ethvert tidspunkt er informasjon som loggføres hos ISP (omtales som "tilkoblingsloggen")[75].

---

[70] Teknologirådet (2007)

[71] Uttrykket «internettleverandør» benyttes her om «tilbyder» av elektronisk kommunikasjonsnett eller –tjeneste (Internet Service Provider - ISP), se ekomloven § 1-5 nr.14. Eksempler er Telenor og NetCom, samt Universitetets senter for informasjonsteknologi (USIT) som er en lokal internettleverandør eller lokal nettverksadministratorer.

[72] Jf. ekomloven § 2-8 og ekomforskriften § 6-2.

[73] Uttrykket «abonnentopplysninger» ble benyttet av Høyesterett i en kjennelse gjengitt i Rt. 1999 side 1944, som gjaldt spørsmålet om politi- og påtalemyndighets rett til å få utlevert abonnentopplysninger etter den tidligere telekommunikasjonsloven av 1995 nr. 39 § 9-3 (3) ved mistanke om straffbare forhold, se nå det tilsvarende unntaket fra taushetsplikten i ekomloven § 2-9 (3).

[74] En IP-adresse kan enten være fast eller dynamisk. Med **fast IP-adresse** har abonnenten samme IP-adresse hver gang han kobler seg til Internett. Ved **Dynamisk IP-adresse** tildeles abonnenten en ny unik IP-adresse ved hver oppkopling til nettet. Dynamiske IP-adresser innebærer at én og samme IP-adresse blir tildelt flere forskjellige abonnenten, men på ulike tidspunkter. For at ISP skal kunne koble riktig abonnent til IP-adressen og slik identifisere hvilken abonnent som har benyttet en bestemt IP-adresse på et bestemt tidspunkt, er det derfor nødvendig å angi tidspunktet eller tidsrommet for bruken av den dynamiske IP-adressen. Basert på Casey (2004) side 455-456 og Teknologirådet (2007)

[75] Fremstillingen ovenfor er basert på NOU 2009:1 Individ og integritet side 290.

Dette innebærer at dersom rettighetshaver kjenner hvilken IP-adresse som ble benyttet ved opplastningen og tidspunktet for opplastningen, vil internettleverandørens koblingslogg vise hvilket abonnement som ble benyttet ved opplastningen, og ISP-ens registrerte abonnentopplysninger vil identifisere abonnenten og dermed lokalisere opplastningen.

Dersom rettighetshaver kobler seg til et fildelingsnettverk, laster ned den aktuelle *.torrent-filen, og kobler seg til sporingstjeneren, vil IP-adressen til den man laster ned fra være synlig i BitTorrent-klientprogrammet.[76]

Dette viser at rettighetshaver kan få tilgang til IP-adressen til opplaster ved vanlige private undersøkelser, og rettighetshaver trenger da ikke å benytte reglene om bevissikring utenfor rettssak for å få tilgang til denne informasjonen.[77]

Det neste spørsmålet blir om rettighetshaver kan få informasjonen registrert i tilkoblingsloggen og de abonnentopplysningene ISP-en har registrert.

2.3 Lovbestemt sletteplikt og taushetsplikt om internettleverandørens koblingslogg – Behovet for regler om bevissikring og bevistilgang utenfor rettssak.

Som vist er informasjonen internettleverandøren sitter på helt sentrale bevis. Inntil nylig påla ekomloven § 2-7 (2) internettleverandøren en sletteplikt med kort frist, og for rettighetshaver innebar dette tidligere at det hastet å hindre sletting av informasjonen.

Ved lov av 15. april 2011 nr. 11[78] er internettleverandørene i henhold til ny § 2-7a (1) pålagt en lagringsplikt av «trafikkdata,[79] lokaliseringsdata og data nødvendig for å identifisere abonnenten(…)» i 6 måneder. [80]

[76] BitTorrent-protokollen i utgangspunktet ikke er tilrettelagt for å skjule hvem som laster opp en fil.

[77] Slik tilgang forutsetter selvfølgelig at rettighetshaver får adgang til fildelingsnettverket enten fordi det er åpent eller fordi hun har fått innpass i et lukket nettverk.

Siden internettleverandøren har en sletteplikt etter 6 måneder, må rettighetshaver fortsatt sørge for å (forvare)/hindre sletting av informasjon om hvilket abonnement som ble benyttet og abonnentopplysningene. Siden sletteplikten er pålagt ved lov, er lovgrunnlag nødvendig for å gjøre unntak fra sletteplikten. Ett av temaene i denne avhandlingen er i hvilken utstrekning tvistelovens regler om bevissikring utenfor rettssak kan benyttes til dette formålet. Dette var også ett av flere tema i den såkalte Altibox-saken.[81] Tingretten påla internettleverandøren å oppbevare informasjonen, og anken ble forkastet.

For å kunne forfølge en ulovlig opplastning av opphavsrettsbeskyttet materiale på Internett ved rettslige midler er det **ikke tilstrekkelig** for rettighetshaver å hindre sletting av informasjonen.

data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring

For at rettighetshaver skal kunne forfølge en opplastning for retten, må hun ha kunnskap om hvem hun skal rette forfølgningen mot,[82] og hun trenger derfor å få **utlevert** denne informasjonen.

Et vesentlig poeng i denne sammenhengen er at rettighetshavers mulighet til å få identifisert krenkeren ved å få tilgang til abonnentopplysningene begrenses av ISP-ens **taushetsplikt** om abonnentopplysningene.[83]

---

[78] Lov om endring i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett). Loven ble vedtatt for å oppfylle Norges EØS-rettslige pliktene etter Datalagringsdirektivet.

[79] Ekomforskriften § 7-1 beskriver trafikkdata som «data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring».

[80] Loven trer i kraft fra den tid Kongen bestemmer. For å hindre at innholdet i dette punktet i avhandlingen blir foreldet, angis rettstilstanden etter den nye loven.

[81] Høyesterettsavgjørelsen er gjengitt i Rt. 2010 side 774. Jeg kommer tilbake til avgjørelsen i avhandlingen.

[82] Se blant annet tvisteloven § 9-2 (2) bokstav b) som pålegger saksøker å oppgi saksøktes navn i stevningen.

Denne taushetsplikten innebærer at rettighetshaver ikke kan få tilgang til disse opplysningene ved privat etterforskning utenfor rettssak. Det er derfor behov for et **rettslig grunnlag** som gir mulighet for å gjøre unntak fra taushetsplikten, og som gir rettighetshaver rett til å få tilgang til abonnentopplysningene. Anvendelsen av reglene i tvisteloven kapittel 28 er ett hovedtema i denne avhandlingen. Dersom Kulturdepartementets forslag til endringer i åndsverkloven blir vedtatt, vil også dette være et selvstendig rettslig grunnlag for å gjøre unntak fra taushetsplikten.

2.4 Abonnentens faktiske innsigelser - Andre kan ha benyttet abonnentens internettforbindelse:

Ovenfor viste jeg at rettighetshaver med hjelp av informasjon om IP-adressen og opplastningstidspunktet, samt internettleverandørens koblingslogg, kan knytte en opplastning til abonnentopplysningene.

I private hjem og på arbeidsplasser er det meget praktisk at flere datamaskiner kobles til internett via én router, se figur 2 nedenfor. Hver av datamaskinene i det lokale nettverket[84] benytter da samme IP-adresse i kommunikasjonen over Internett. Abonnentopplysningene knyttet til IP-adressen sier således intet om hvilken av disse datamaskinene som ble benyttet ved opplastningen, og heller ikke hvilken av arbeidstakerne eller familiemedlemmene som foretok opplastningen.[85] I slike tilfeller kan abonnenten innvende nettopp dette.[86]

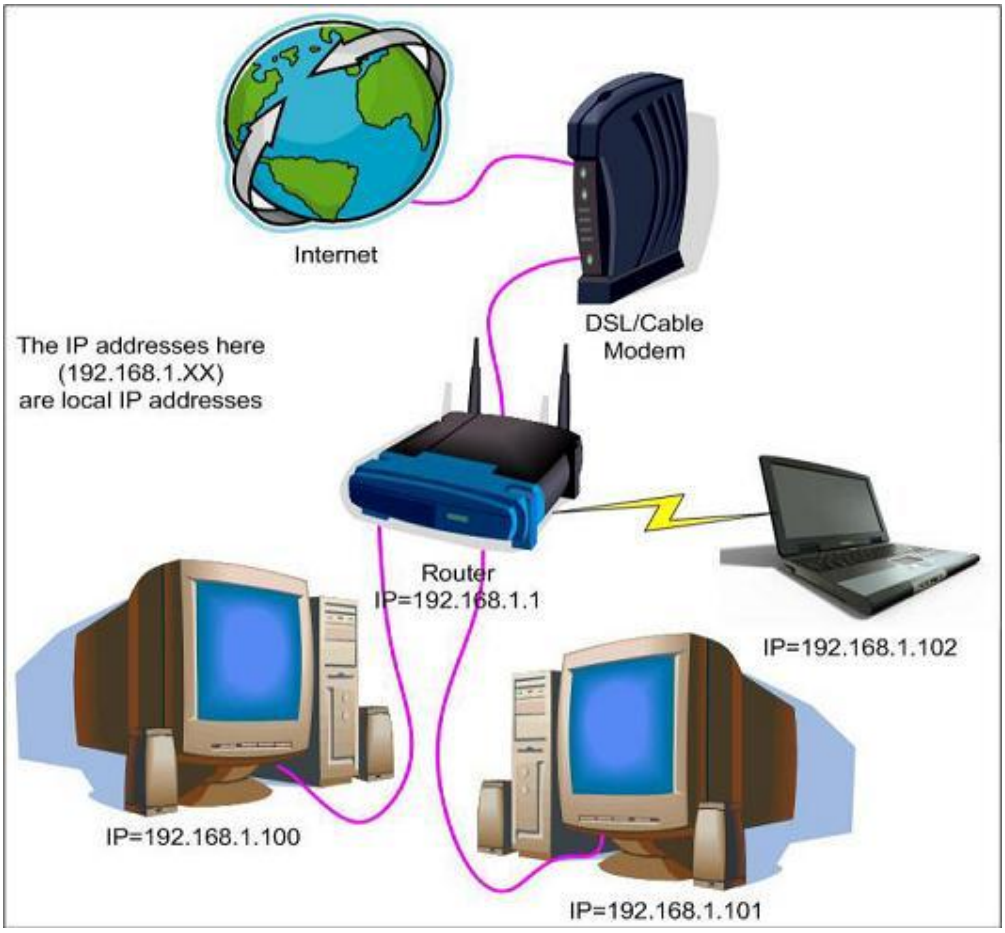
---

[83] Se ekomloven § 2-9. Brudd på taushetsplikten er straffbart etter ekomloven § 12-4 første ledd.

[84] Med «nettverk» forstås vanligvis at minst to datamaskiner kobles sammen. Det kan skje via internett, eller som i teksten via en hub/switch/router som felles aksesspunkt. Sistnevnte kaller jeg «lokalt nettverk».

[85] Teknologirådet (2007).

[86] Også nevnt av Generaladvokaten i «Promusicae»-saken for EU-domstolen, Case C-275/06 premiss 115.



Figur 2: nettverk med ruter-aksesspunkt.

I tillegg kommer at også uautoriserte/fremmede kan tilta seg adgang til internettforbindelsen via den trådløse routeren. Dersom nettverket er "åpent",[87] kan abonnenten dermed **innvende at uautoriserte har koblet seg til hans internettforbindelse**. Dersom nettverket er lukket, kan abonnenten innvende at **noen har hacket passordet**, og lastet opp åndsverket.[88]

Hvis det derimot kun er én datamaskin knyttet til ett abonnement, vil IP-adressen kunne identifisere datamaskinen. En datamaskin på en arbeidsplass eller i et privat hjem kan imidlertid være tilgjengelig for flere, og derfor kan abonnenten **alltid innvende at**

[87] Et "åpent nettverk" innebærer at datamaskiner som er innenfor nettverkets rekkevidde (og med trådløst nettverkskort), kan koble seg til routeren uten å logge inn, mens et "lukket nettverk" innebærer at bruken av internettforbindelsen krever pålogging med brukernavn og passord, jf. NORSISS.

[88] I Altibox-saken benyttet internettleverandøren dette som en innsigelse, se nærmere nedenfor i punkt xxx (forholdsmessighetsvurderingen i tvisteloven § 22-3).se LG-2009-105319-1.

andre familiemedlemmer, arbeidstakere eller andre besøkende kan ha foretatt opplastningen.[89]

Endelig kan abonnenten **innvende at noen har hacket seg inn på hans datamaskin via internett**, og lastet opp filen via denne datamaskinen.[90]

Disse forhold viser at abonnenten ikke nødvendigvis er den som har foretatt opplastningene. Det kan være abonnenten, men det kan også være andre. Dersom abonnenten i et senere søksmål innvender et eller flere av de ovennevnte forhold, vil retten i overensstemmelse med reglene for bevisføringsbyrde pålegge rettighetshaver bevisføringsplikten.[91]

Rettighetshaver kan ikke på forhånd kan vite om abonnenten vil bestride at han er opplaster eller eventuelt hvilke innsigelser han vil fremføre. For å styrke sine muligheter til å nå frem i forhandlinger eller søksmål, bør rettighetshaver derfor ta høyde for de nevnte innsigelsene. Hun har følgelig behov for å sikre og få tilgang til ytterligere bevis. Informasjon om abonnentens identitet er følgelig bare begynnelsen av rettighetshavers nødvendige bevissankning forut for søkmål.

Spørsmålene i det følgende er hvilke andre spor som vanligvis oppstår ved en opplastning, og hvordan disse kan benyttes i argumentasjon for å bekrefte eller avkrefte om abonnenten er den reelle opplaster.[92]

---

[89] Abonnenten kan også i slike tilfeller innvende at andre fysisk har koblet sin egen datamaskin til modemet/internettforbindelsen, og at det ikke er hans datamaskin som er benyttet.

[90] Abonnentens datamaskin er da benyttet som en mellommaskin/"proxy-server".

[91] Beviskravet for det faktiske påstandsgrunnlaget er alminnelige sannsynlighetsovervekt.

[92] Hvis det viser seg at abonnenten ikke er opplasteren, kan slike spor benyttes for å finne ut hvem som har foretatt opplastningen via abonnentens IP-adresse og datautstyr.

2.5 Innvendingen at det ikke er hans datamaskin(er) som er benyttet ved opplastningen:

Dersom abonnenten hevder at noen utenforstående, for eksempel en nabo, har benyttet hans nettilgang ved å koble seg til hans trådløse nettverk, så innebærer det at han anfører at ingen av datamaskinene i bedriften eller husstanden er benyttet.

2.5.1 Logg over trafikk igjennom router og brannmur[93]:

Siden internettilgangen ved trådløse nettverk går igjennom en router, vil denne registrere hvilken datamaskin som ble benyttet. Det første spørsmålet blir derfor om routeren **lagrer** informasjon om hvilken datamaskin som ble benyttet.

All trafikken igjennom routeren lagres i en logg, og denne loggen kan dermed gi opplysninger som kan benyttes for å avklare om abonnentens innsigelse er holdbar. Særlig dersom loggen viser at en utenforstående datamaskin var tilknyttet routeren i en periode hvor rettighetshaver lastet ned filen til sitt BitTorrent-klientprogram, se ovenfor, så vil dette bekrefte abonnentens innsigelse, og motsatt.[94]

Tilsvarende har brannmurer også en logg som lagrer all trafikk på hver datamaskin.[95]

Svakheter ved slike logger er at de har et begrenset minne, og at installatøren vanligvis kan gjøre innstillinger som medfører at trafikkdata enten ikke loggføres eller at loggen slettes etter kort tid. Disse forhold medfører at rettighetshaver enten ikke vil finne relevante bevis i routeren/brannmuren, eller at det haster med å sikre en utskrift av loggen dersom denne skal være et relevant bevis i en senere sak.

---

[93] Temaet basert på Casey (2004) side 467.

[94] Det finnes også programvare som gir eier mulighet til å overvåke og lagre all trafikk igjennom routeren.

[95] De fleste antiviruspakker kommer med en brannmur som skal hindre hackerangrep på datamaskinen.

2.5.2 Spor på abonnentens datamaskin(er):[96]

Dersom det finnes spor av opplastningen på abonnentens datamaskin eller en annen datamaskin i bedriften eller husstanden, så vil disse spor være bevismomenter som taler for at denne maskinen er benyttet.[97] Dersom man ikke finner spor som man ellers ville forvente å finne der dersom datamaskinen var benyttet ved opplastningen, så vil dette tale mot at denne datamaskinen er benyttet.

2.5.2.1 Spor av konstruksjonen av *.torrent-filen:

Eventuelle spor som bare oppstår ved konstruksjon av *.torrent-filen, vil være tungtveiende bevis som taler for at datamaskinen er benyttet til distribusjon av filen. Som redegjørelsen ovenfor i punkt 2.1 viser, konstrueres *.torrent-filen ved å benytte en BitTorrent-protokoll. Protokollen, og *.torrent-filen vil således være lagret på datamaskinen på et tidspunkt. Den som har konstruert *.torrent-filen er vanligvis også uploader, og eksistensen av slike bevis tilsier dermed at datamaskinen ble benyttet ved første distribusjon.

2.5.2.2 Spor av det opphavsrettsbeskyttede materialet:

Eksistensen av den opphavsrettsbeskyttede filen er et viktig spor som tilsier at datamaskinen er benyttet ved tilgjengeliggjøringen av filen.
Ved bruk av BitTorrent-teknologien, må hovedfilen være tilgjengelig via BitTorrent-klientprogrammet for at andre brukere skal kunne laste den ned. Vanligvis vil filen være lagret på harddisken i en filmappe.

Back-up-filer er også relevante spor, og særlig dersom hovedfilen er slettet.[98] Slike spor kan finnes på eksterne lagringsmedia, herunder ekstern harddisk, minnepinne, cd/dvd, e-post-konto.[99]

---

[96] I en bedrift eller privat husstand kan det som nevnt være mange datamaskiner.

[97] Abonnenten kan imidlertid fortsatt ha i behold sine innvendinger om at familiemedlemmer eller arbeidstakere har benyttet datamaskinen, og innvendingen om at hans maskin er benyttet som mellommaskin, se nedenfor.

[98] Back-up kan enten være automatisk eller manuell.

2.5.2.3 Spor etter sletting og manipulering av filer og programvare:

Hvilke filer og programmer som er lagret på en datamaskin er i stor grad brukerstyrt, hvilket innebærer at brukeren har mulighet til å fjerne relevante spor. Fullstendig sletting av programvare og filer er imidlertid vanskelig. En fil er ikke fullstendig slettet fra harddisken, før plassen hvor filen lå er overskrevet.[100]
Datamaskinens operativsystem omfatter også en "handlingslogg", som loggfører informasjon om handlinger som utføres, såkalt "**metadata**".[101] Tidligere handlinger kan således leses ut av loggen også etter slettingen av en fil.

Denne metadata omfatter filens «tidsstempel», som altså viser når filen ble opprettet, endret m.m. Slike metadata som sier noe om tidspunktet for handlinger, kan være viktige bevis som kan benyttes til forsvar mot abonnentens innsigelser. Dersom den den opphavsrettsbeskyttede filen ble lagret før *.torrent-filen ble lagret, så vil det tale for at datamaskinen ble benyttet til å konstruere *.torrent-filen.

Slik metadata kan imidlertid manipuleres, eksempelvis kan tidspunktet for når en fil er opprettet endres (endring av filens tidsstempel). Dette er noe rettighetshaver særlig må undersøke dersom *.torrent-filen ble lagret på datamaskinen etter at rettighetshaver er kjent med at *.torrent-filen er gjort tilgjengelig på et nettsted. Dette kan synes avansert, men det finnes programvare som endrer filenes tidsstempel. Dersom slik programvare er installert, vil programvaren i seg selv være et bevis som kan brukes som argument mot påliteligheten til den metadata som gjelder tidspunktet for filenes opprettelse, og eksistensen av programvare som endrer metadata eller på annen måte skjuler spor etter opplastning, kan svekke brukerens troverdighet generelt og spesielt med hensyn til når filen påstås opprettet.[102]

---

[99] Basert på Moore (2010) side151.

[100] Basert på Moore (2010) side151-152.

[101] «Metadata» kan defineres som data om data; "*elektronisk lagret informasjon som beskriver/angir egenskaper ved elektronisk lagret informasjon, herunder format og plassering*", jf. Moore (2010), note 39 side 152.

[102] Basert på Willassen (2009), Eoghan (2004) side 276, og Moore (2010) side152-153.

2.5.2.4 Metadata i webleserloggen:

Når en bruker kopler seg til internett, loggfører nettleseren[103] informasjon om hvilke websider brukeren besøker, herunder også tidspunktet. Webleserloggen vil således kunne bekrefte hvorvidt brukeren har vært inne på den nettsiden hvor *.torrent-filen ble publisert, og dette sporet vil følgelig kunne underbygge at abonnenten står bak tilgjengeliggjøringen. Eksistensen av disse sporene avhenger imidlertid av hvilke innstillinger brukeren har lagt inn om lagringstid, og brukeren kan også slette loggen.[104]

Sporene ovenfor kan i stor utstrekning si noe om én av abonnentens datamaskin(er) er benyttet, og således benyttes som forsvar mot en slik innsigelse.

2.6 Innsigelser om at andre har benyttet abonnentens datamaskin:

Som vi så kan abonnenten også innvende at datamaskinen(e) er benyttet av andre, herunder arbeidstakere, familiemedlemmer, budne og ubudne gjester (proxy-server-tilfellet).
Bevisene nevnt ovenfor vil også si noe om hvilken datamaskin som er benyttet, i og med at fraværet av spor eller eksistensen av spor på én datamaskin utelukker eller bekrefter at denne er benyttet.

2.6.1 Nødvendige spor som forsvar mot abonnentens «familiemedlemmer»-innvending:

Som vist ovenfor kan det brukernavnet/»artistnavnet» opplaster benyttet på nettstedet kunne gjenfinnes på datamaskinen eller i andre lagringsmedier hos opplaster. Dette var tilfellet TFRED-2006-177576, den såkalte «Pitbullterje»-dommen, hvor tiltalte hadde kopiert film-filen over på dvd- plater og merket disse med tilsvarende brukernavn som var benyttet på den aktuelle fildelingsnettsiden hvor filen var tilgjengeliggjort. Dette er et bevis som kan benyttes for å identifisere hvem som har benyttet datamaskinen.

---

[103] Eksempelvis Internet Explorer 7.

[104] Basert på Teknologirådet (2005).

Dersom flere benytter samme datamaskin, er det ikke uvanlig at de oppretter hver sin brukerkonto,[105] og metadata som lagrer informasjon om hvilken brukerkonto som ble benyttet vil være sentrale spor.
Påliteligheten av slik informasjon vil variere avhengig av hvor enkelt det har vært for andre å få adgang til den enkelte brukerkonto, herunder om den er passordbeskyttet.

I tillegg kan undersøkelser av nettleserloggen i tiden før og etter opplastningen, vise hvilke e-post-konti som ble benyttet og sammenholdt med annen informasjon om de forskjellige potensielle brukerne, herunder brukernavn, kan dette utelukke eller styrke mistanken mot enkelte. Siden flere kan benytte samme e-post-leverandør, kan også selve e-post-loggen, som viser hvilke e-poster som ble sent i dette tidsrommet, være viktige bevis. Slik informasjon kan være et bevis for at abonnenten var aktiv på datamaskinen i det tidsrommet filen ble lastet opp.

2.6.2 Nødvendige spor som forsvar mot proxy-server-innvendingen:

Dersom abonnenten hevder at han har vært utsatt for datainnbrudd og at noen har benyttet datamaskinen som «mellommaskin/proxy», blir spørsmålet hvilke spor som kan bekrefte/avkrefte dette. Ved «angrep» via routeren, vil dette som nevnt loggføres i routeren. Dersom sikkerhetsloggen på datamaskinen er slått av, kan dette tyde på inntrengning. Dette er noe abonnenten kan ha endret på selv, og er således ikke noe avgjørende bevis, men likevel et bevismoment. En inntrenger vil i alminnelighet forsøke å holde alle spor skjult for abonnenten, for så kunne beholde kontrollen over abonnentens datamaskin lengre, og en hacker vil således forsøke å skjule filer og loggdata. Funn av loggdata og filer som enkelt kunne skjules på abonnentens datamaskin taler derfor med styrke mot at det var en inntrenger.[106]

---

[105] Dette er for eksempel praktisk på Universitetet i Oslo.

[106] Dette var tilfellet i en straffesak for Oslo tingrett, hvor retten foretok en bevisvurdering basert på eksistensen av bevis og alminnelige antakelser om hvordan en inntrenger vanligvis vil opptre, se TOSLO-2010-62157.

2.7 Oppsummering – relevansen for den videre fremstillingen:

Ovenfor har jeg gitt en oversikt over enkelte av de spor som genereres ved opplastning på Internett.

De enkelte spor vil variere noe fra tilfelle til tilfelle, og de enkelte bevis må vurderes samlet og konkret. For rettighetshaver er det avgjørende at hun klarer å individualisere med tilstrekkelig sannsynlighet hvem som har foretatt opplastning av det opphavsrettsbeskyttede materialet, slik at hun kan benytte dette i vurderingen av hvorvidt og i tilfelle mot hvem hun skal innlede forhandlinger eller reise søksmål.

Jeg har vist at disse spor i mange tilfeller vil være avgjørende for rettighetshavers mulighet til å ivareta sine interesser og forfølge opphavsrettsbrudd. Jeg har vist at disse elektroniske spor kan forholdsvis lett kan fjernes eller manipuleres.[107]
Disse forhold tilsier henholdsvis at rettighetshaver bør ha anledning til å hindre at disse sporene blir gjort utilgjengelig for henne, og det tilsier også at hun positivt bør få tilgang til disse bevis.

Hovedtemaet nedenfor i kapittel 4 er innholdet i de materielle vilkår som må være oppfylt for at rettighetshaver skal få medhold i en begjæring om sikring og/eller en begjæring om tilgang til slike bevis.

Mer konkret er det særlig **to hovedspørsmål** som er aktuelle, og disse er:

- I hvilken utstrekning reglene bevissikringsreglene gir hjemmel til å begjære sikring og tilgang til abonnentopplysninger fra den aktuelle internettleverandøren, og enda mer interessant
- I hvilken utstrekning reglene gir hjemmel til bevissikring og tilgang til elektroniske spor på lagringsmedier hos abonnenten.[108]

---

[107] I innledningen og i kapittelet her har jeg også nevnt faktiske og rettslige forhold som medfører domstolenes bistand er nødvendig.

[108] I den videre fremstillingen forutsetter jeg at rettighetshaver har tilegnet seg bevis for hvilken IP-adresse som ble benyttet ved opplastningen, tidspunktet for opplastningen, og innholdet i filen med det

3 Rettsvirkningene ”sikring av bevis” og ”tilgang til bevis”

Det sentrale for en rettighetshaver som vurderer å begjære bevissikring utenfor rettssak er å vite hva «bevissikring utenfor rettssak» nærmere innebærer.

I denne avhandlingen er det derfor nødvendig først å redegjøre for **innholdet i rettsvirkningen(e)** bevissikring utenfor rettssak i tvisteloven kapittel 28.[109]

Som nevnt innledningsvis i kapittel 1, er det to rettsvirkninger kapittelet gir hjemmel til;

- krav om **sikring av bevis**, og
- krav om **tilgang til bevis**

Mens hovedformålet krav om sikring av bevis er å hindre at beviset går tapt, er hovedformålet med tilgang til beviset å gjøre rettighetshaver kjent med innholdet i beviset, slik at denne informasjonen kan benyttes for å forfølge kravet innenfor eller utenfor domstolene[110].

Når innholdet i rettsvirkningene er klarlagt, og rettighetshaver ser et behov for å begjære bevissikring, må rettighetshaver undersøke **om hun er i posisjon til å kreve dette**. Det er klart at ikke hvem som helst kan kreve sikring og tilgang til bevis i hvilken som helst situasjon, og dette medfører at det oppstilles skranker for **hvem** som kan få bevissikring og i **hvilke situasjoner** bevissikring kan kreves.

---

opphavsrettsbeskyttede materialet. Dette er bevis rettighetshaver kan sikre seg ved privat etterforskning utenfor domstolene.

[109] Som jeg skal vise her, er ikke lovteksten særlig klar på dette punktet, og ordbruken har heller ikke vært helt entydig i forarbeidene og rettspraksis.

[110] NOU 2001:32B side 987.

Før jeg går inn på de forskjellige materielle vilkårene, vil jeg altså kort redegjøre for innholdet i henholdsvis rettsvirkningene sikring til bevis og tilgang til bevis utenfor rettssak.

3.1 Det nærmere innholdet i rettsvirkningen sikring av bevis utenfor rettssak:

Tvisteloven § 28-1 angir etter sin ordlyd hva rettsvirkningen bevissikring kan gå ut på:

> *«Ved bevissikring utenfor rettssak kan det foretas rettslig avhør av parter og vitner og gis tilgang til og foretas undersøkelse av realbevis.»*

3.1.1 "rettslig avhør av parter og vitner":

Sikring av bevis kan for det første skje i form av **"rettslig avhør av parter og vitner".** Eksempelvis kan rettighetshaver kreve at internettleverandøren avhøres om registrert navn og adresse på det abonnementet som var tildelt den aktuelle IP-adressen på det aktuelle tidspunktet.[111]

Vi kan også tenke oss at rettighetshaver krever avhør av IT-ansvarlig i en bedrift om datatrafikk i et bestemt tidsrom.[112]

3.1.2 "tilgang til realbevis":

Sikring kan i henhold til bestemmelsen for det andre foretas ved **tilgang** til realbevis: Typiske eksempler er at en representant for namsmyndighetene får "tilgang" til realbeviset for eksempel ved å speilkopiere[113] harddisken og oppbevare speilkopien til senere.[114] [115]

---

[111] Dette var et subsidiært krav i TSTAV-2009-55827Altibox-saken.

[112] I arbeidstakertilfeller kan bedriften i mange tilfeller ønske å bidra til å oppklare forholdene, og i så fall er ikke bevissikring nødvendig. Jeg går ikke her inn på de personvernrettslige spørsmålene som slik frivillig bevissankning i bedriften reiser.

[113] Fordelen ved speilkopiering i motsetning til vanlig kopiering, er at førstnevnte innebærer at ikke bare filen blir kopiert, men også **metadata**.

[114] Uttrykket «tilgang» brukes her på samme måte som i tvisteloven § 26-5 tredje ledd, jf. første ledd, altså synonymt med at beviset/bevisgjenstanden **blir stilt til noens rådighet**. Siden slik sikring ved

Uttrykket ”realbevis” er definert i tvisteloven § 26-1:

> *«Realbevis er personer og gjenstander (fast eiendom, løsøre, dokumenter, elektronisk lagret materiale mv.) hvor personen eller gjenstanden, eller dens egenskaper, tilstand eller innhold, inneholder informasjon som kan ha betydning for det faktiske avgjørelsesgrunnlaget i saken».*

Bestemmelsen er etter sin ordlyd vid og i følge forarbeidene er den også ment å omfatte alle bevis som ikke er parts- eller vitneforklaringer.[116] Høyesterett har også lagt dette til grunn i Altibox-saken.[117]

Ovenfor i punkt 2.5 nevnte jeg eksempler på ”elektronisk lagret materiale” som er særlig aktuelle realbevis i denne avhandlingen.

3.1.3 ”foretas undersøkelse av realbevis”

Den tredje sikringsmåten etter tvisteloven § 28-1 er at det **«foretas undersøkelse av realbevis».** Dette vil typisk skje ved at en representant for namsmyndighetene får anledning til å undersøke realbeviset, jf tvisteloven § 26-3 jf. § 27-5 og deretter redegjøre for funnene (se tvisteloven § 27-6).

Som to former for sikring av bevis, er **forskjellen** på krav om tilgang til et realbevis og krav om undersøkelse av et realbevis, at sistnevnte typisk må benyttes i de tilfeller hvor

---

«tilgang» kan skje uten at motparten samtidig får **kunnskap om bevisets opplysninger**, så må uttrykket «tilgang» her holdes adskilt fra rettsvirkningen «tilgang» som behandles nedenfor. Tvistelovens uttrykk «tilgang» er altså **tvetydig**.

[115] Slik «tilgang» må holdes atskilt fra å gi en representant for namsmyndighetene «**fysisk tilgang»** til det stedet hvor beviset befinner seg. «Fysisk tilgang» kan være en nødvendig forutsetning for faktisk å sikre beviset og for å gi rettighetshaver tilgang til bevisets meningsinnhold, og reiser spørsmål om tvangsfullbyrdelse i tilfeller hvor motparten motsetter seg dette, se kapittel xxx (7).

[116] NOU 2001:32B side 977.

[117] Se Rt.2010 side 774 avsnitt 42 førstvoterende; ”[e]tter mitt syn følger det av § 28-4 at bevissikringen som utgangspunkt omfatter alle bevis som det vil kunne gis tilgang til i en aktuell tvist etter de alminnelige regler om bevis.”

beviset ikke kan flyttes, eller må tilbakeleveres før det kan fremlegges som bevis i (den senere) rettssaken, eller beviset vil endres over tid, slik at det er nødvendig å undersøke beviset på et bestemt tidspunkt og redegjøre for hvilken informasjon beviset gav på dette tidspunktet.

3.2 Nærmere om innholdet i rettsvirkningen tilgang til bevis:

Ovenfor har jeg nevnt at hovedrettsvirkningen sikring av bevis **ikke nødvendigvis** innebærer at rettighetshaver får rådighet over beviset, eller anledning til å gjøre seg kjent med meningsinnholdet i det sikrede beviset.

I punkt 1.3 nevnte jeg at den tidligere tvistemålsloven § 271a ikke gav rettighetshaver rettskrav på tilgang til beviset utenfor rettssak, og dette var en nyvinning med tvisteloven.

Tvistelovens forarbeider[118] fremhever at saksøker/rettighetshaver kan ha et særskilt behov for å få tilgang til innholdet i et bevis utenfor søksmål for å kunne forfølge kravet, se ovenfor i punkt 1.4 om lovens formål.

Spesielle hensyn kan også tilsi at retten beslutter sikring av et bevis (uten at motparten blir varslet), uten at verken representanter for domstol/namsmyndighet eller rettighetshaver får anledning til å gjøre seg kjent med bevisets innhold før motparten har fått anledning til å uttale seg om sikringen skal opprettholdes, og om hvorvidt og i så fall hvilke opplysninger rettighetshaver skal få kunnskap om.[119]

Dette viser at «tilgang til bevis» er en særskilt rettsvirkning i tvisteloven kapittel 28.

---

[118] NOU 2001:32B side 987.

[119] I punkt 5.3 opprettholdes sondringen mellom sikring og tilgang hva gjelder adgangen til å gjøre unntak fra kontradiksjonsprinsippet, se tvisteloven § 28-3 fjerde ledd.

Dette viser også at denne rettsvirkningen innebærer at rettighetshaver får rådighet over og kan gjøre seg kjent med hele eller deler av meningsinnholdet i beviset.[120] Dette følger også forutsetningsvis av tvisteloven § 26-7 «Tvist om bevistilgang», som etter § 28-4 gjelder tilsvarende utenfor rettssak.[121]

Det er ikke utelukket at sikring av beviset **kan** skje ved at retten beslutter at motparten skal gi rekvirenten[122] tilgang til et bevis,[123] men dette er i så fall et særskilt spørsmål.

Det er selvfølgelig heller ikke utelukket at rettighetshaver begjærer tilgang til et bevis utenfor rettssak, uten at det er nødvendig å kreve at det blir iverksatt særskilte tiltak for å hindre at beviset slettes. Jeg kommer tilbake til dette under behandlingen av vilkårene.

Hvordan tilgang til de aktuelle bevis konkret skal foregå, vil bero på de nærmere omstendigheter i det enkelte tilfellet, og er også først relevant etter at vilkårene er avgjort. Jeg har derfor funnet det hensiktsmessig å utsette behandlingen av hvordan beviset skal gjøres tilgjengelig for rettighetshaver til kapittel 6.

3.3 Tolkning av en begjæring om bevissikring:

Som vist kan uttrykket «sikring» bety sikring i snever og i vid forstand, og uttrykket ”tilgang” kan bli benyttet både når man mener rettsvirkningen tilgang og når man i realiteten snakker om en form for sikring i snever forstand. Av denne grunnen må retten tolke en begjæring for å avgjøre hva rettighetshaver egentlig ønsker.

---

[120] Det er også slik uttrykket «tilgang» til bevis for øvrig benyttes i tvisteloven.

[121] Dette følger også forutsetningsvis av tvisteloven § 28-3 fjerde ledd tredje punkt.

[122] I denne avhandlingen benyttes uttrykkene begjærende part/rekvirenten/saksøker/rettighetshaver som synonymer.

[123] I noen tilfeller vil selve prosedyren for bevissikring som hovedregel innebære at begjærende part får «tilgang til beviset». Dette er typisk ved parts- og vitneforklaringer hvor bevissikring i henhold til tvisteloven § 28-4 skjer i form av bevisopptak etter tvisteloven § 27-3, og hvor tvisteloven § 27-3 annet ledd bestemmer at partene skal varsles til rettsmøte hvor bevisopptak skal foretas. Dette er også forutsatt i forarbeidene uten nærmere drøftelse, se NOU 2001:32 side 990.

Tolkningen av en begjæring som lyder på krav om «sikring» eller «bevissikring» kan også bli avgjørende for hvilke vilkår som må være oppfylt, og hvilke saksbehandlingsregler som skal legges til grunn, herunder om motparten skal varsles og gis mulighet til å gjøre sitt syn gjeldende i saken. Dette gjelder eksempelvis de tilfeller hvor opplastningen er skjedd fra en IP-adresse tilhørende Universitetet i Oslo (eller en bedrift), og man vet at det er en student som har foretatt opplastningen. Det er da liten fare for bevisforspillelse, for USIT har ingen interesse i å slette sporene. I et slikt tilfelle er det ikke behov for å **kreve** sikring, og rettighetshaver vil bare kreve tilgang. Det er da de materielle vilkårene for tilgang som kommer på spissen, og i tillegg er det de prosessuelle vilkår og de prosessuelle saksbehandlingsregler som gjelder for tilgangsspørsmålet som kommer til anvendelse, herunder at det åpnes for kontradiksjon.

Retten har en veiledningsplikt og det vil falle innenfor denne å veilede rettighetshaver om at sikring og tilgang er to forskjellige rettsvirkninger, at vilkårene vil være forskjellige og at påstanden må presiseres.[124]

3.4 Sondringen mellom sikring/tilgang og **føring** av beviset.

Den siste sondringen som skal oppstilles her er sondringen mellom på den ene siden sikring og tilgang til beviset og på den annen side spørsmålet om **hvordan beviset skal føres for retten.**

Utgangspunktet om bevisføring finner vi i tvisteloven § 21-9 som bestemmer at et bevis skal føres mest mulig umiddelbart/direkte for den dømmende retten – ”bevisumiddelbarhetsprinsippet”[125].

Ved bevissikring i form av for eksempel «tilgang til realbevis», herunder elektroniske lagrede bevis, vil utgangspunktet være at beviset skal føres for den dømmende rett ved å

[124] Se tvisteloven § 11-5. Slik veiledning vil også indirekte gi motparten klarhet i sak og argumentasjonen, slik at det er mulig å komme med relevante motargumenter. Se Ot.prp.nr.51(2004-2005) side 169-170.

[125] Schei (2007) side 1021.

legge frem en kopi av beviset for retten, eller ved å la dommeren observere beviset direkte på en datamaskin. Ved bevissikring i form av observasjoner av realbevis, kan det være nærliggende at beviset føres ved å føre en rapport utarbeidet av representanten for namsmyndighetene eller en sakkyndig, se nærmere om de forskjellige gjennomføringsmåter nedenfor i punkt 6.

Spørsmålet om føringen av sikrede bevis er særlig interessant hva gjelder bevis i form av parts- og vitneforklaringer. Det er ikke gitt at gjengivelsen av forklaringen skal føres. I overensstemmelse med tvistelovens alminnelige regler om dette, er utgangspunktet heller at beviset skal føres direkte for den dømmende rett, og at det eventuelt kan være anledning til å benytte tidligere forklaringer til konfrontasjon.

Spørsmålet her blir om det gjelder et unntak for de tilfellene hvor beviset er sikret og/eller rettighetshaver har fått tilgang til beviset allerede før det ble reist søksmål.

Det er ikke nødvendigvis slik at anvendelsen av reglene om bevissikring også får betydning for hvordan et bevis skal føres for retten. Formålet med bevissikringen er å sikre beviset, eventuelt å gi tilgang til opplysningene som beviset inneholder slik at dette kan benyttes til de vurderinger som må foretas, herunder med hensyn til om det skal reises søksmål, forhandlinger, og hvilke andre bevis som skal innhentes. Dette tilsier **ikke** at det skal gjøres unntak fra de alminnelige reglene om bevisføring.

4 De materielle vilkårene

Når jeg nå har klarlagt at tvisteloven kapittel 28 i realiteten gir rettslig grunnlag for to forskjellige rettskrav, blir temaet i det følgende å redegjøre for **innholdet** i de vilkårene som å være oppfylt. Først gir jeg en **oversikt** over hvilke vilkår som må være oppfylt for at en begjæring om sikring av bevis og en begjæring om tilgang til bevis henholdsvis skal tas til følge.

§ 28-2 Vilkårene for bevissikring
Bevissikring kan begjæres når ***beviset kan få betydning i en tvist*** hvor den som setter fram begjæringen, ***vil kunne bli part eller partshjelper***, og det enten er en **nærliggende risiko for at *beviset vil gå tapt eller bli vesentlig svekket***, **eller** av **andre grunner er *særlig viktig å få tilgang*** til beviset før sak er reist.

4.1 «Grunnvilkåret»:

Etter ordlyden i lovens § 28-2 første ledd første punkt er det et vilkår at "beviset kan få betydning i en tvist hvor den som setter fram begjæringen, vil kunne bli part eller parthjelper". Dette vilkåret er i forarbeidene omtalt som "**grunnvilkåret**"[126]. Ved en lesning av vilkåret, ser vi at dette har **to sider.** For det første stilles et krav til relevansen av beviset eller begjæringen (heretter "**relevanskravet**") og for det andre oppstilles krav om personell tilknytning (heretter "**tilknytningskravet**"). Disse to sider av grunnvilkåret kunne ha vært behandlet samlet her slik lovgiver har lagt opp til i ordlyden og i forarbeidene.

Hensynet til klarhet og oversikt tilsier at det sondres mellom disse to sider av grunnvilkåret. Siden relevanskravet og tilknytningskravet reiser flere tolkningsspørsmål

[126] NOU 2001:32 side 988 til § 31-2.

uten noen større innbyrdes sammenheng, har jeg i den følgende redegjørelsen behandlet hver av de to sidene av «grunnvilkåret» separat som to forskjellige grunnvilkår.

4.1.1 De to «alternative» vilkår:

Loven oppstiller i tillegg vilkårene om **fare for bevisforspillelse**, og «sekkebestemmelsen» om «**andre grunner» som viser at det er «særlig viktig å få tilgang til beviset før sak er reist»**.

Forarbeidene angir at dette er to **«alternative»** vilkår for bevissikring.[127] Siden lovteksten binder de to vilkårene sammen med «eller», tilsier også lovteksten at dette er to alternative vilkår.

Jeg har imidlertid funnet grunn til å reise spørsmål ved om begge de "alternative" vilkår virkelig er alternative vilkår for begge rettsvirkningene eller om det er ett vilkår for bevissikring i snever forstand, og ett vilkår for tilgang.

4.1.2 Er det andre vilkåret et alternativt grunnlag for sikring av bevis?

Det andre "alternative" vilkår krever at det er særlig viktig for rekvirenten å få **"tilgang"** til beviset før sak er reist, og **ordlyden** taler således for at i hvert fall rettsvirkningen "tilgang" er den aktuelle rettsvirkningen. Vi må i utgangspunktet også legge til grunn at lovgiver har ment det som er skrevet, og dette taler derfor mot at vilkåret også gjelder sikring i snever forstand.

Det foreligger ingen **rettsavgjørelser** hvor sikring i snever forstand er besluttet uten at det forelå bevisforspillelsesfare. Der hvor vilkåret omtales i **forarbeidene** fremstår det av sammenhengene at det siktes til rettsvirkningen tilgang til bevis, selv om forarbeidene taler om «bevissikring».
Basert på én side av ordlyden, én side av forarbeidene, formålene og rettspraksis kan det synes merkelig at vilkårene omtales og fremstilles som «alternative». Min hypotese

[127] NOU 2011:32 side 988.

er at grunnen kan være at lovgiver ikke har vært tilstrekkelig bevisst sondringen mellom de to rettsvirkningene i lovgivningsarbeidet. Ordlyden og forarbeidene gir støtte for denne hypotesen, idet uttrykket ”bevissikring” gjennomgående brukes som samlebetegnelse på de to rettsvirkningene uten nyansering. Denne unyanserte språkbruken gjør slutningene fra forarbeidene mindre sikre, og det er derfor mindre grunn til å legge vekt på uttalelsene i forarbeidene som sier at de to vilkårene er ”alternative” vilkår.

Konklusjon: Jeg legger derfor til grunn at det andre vilkåret ikke er et alternativ vilkår for sikring.

4.1.3 Er bevisforspillelsesfare et alternativt grunnlag/vilkår for bevistilgang?

Ordlyden gir oss ingen holdepunkter for at bevisforspillelsesfare er et alternativt vilkår for å kreve tilgang til et bevis forut for rettssak.

Hva gjelder **formålene** med bevissikring i vid forstand er det ingen av disse som tilsier at rekvirenten skal få tilgang til et bevis bare fordi det foreligger bevisforspillelsesfare.

Rt.2010 side 774, Altibox-saken gjaldt både sikring og tilgang til bevis, og avgjørelsen gir ikke grunnlag for å slutte noe med hensyn til det temaet som her drøftes.

I tillegg kommer at uttrykket «andre grunner» i det andre vilkåret er så vid at dette vilkåret ikke utelukker at bevisforspillelsesfare kan være en slik annen grunn.[128]

Konklusjon: Bevisforspillelsesfarevilkåret er bare et vilkår og grunnlag for bevissikring i snever forstand.

[128] Dette kan tenkes dersom det er nødvendig at rettighetshaver får tilgang til ett bevis, slik at rettighetshaver har grunnlag for å fremsette en ny begjæring om sikring av andre bevis for å hindre bevisforspillelse av disse. Dette spørsmålet drøftes nærmere i relasjon til vilkårene for å få en begjæring behandlet uten at motparten blir varslet, se punkt xxx.

4.2 Oversikt over vilkårene:

For å få medhold i en begjæring om sikring av bevis, må følgende tre vilkår være oppfylt:

1. **Relevanskravet, eller «det materielle tilknytningskravet»**
2. **Tilknytningskravet eller «det personelle tilknytningskravet», og**
3. **Kravet om bevisforspillelsesfare**

For å få medhold i en begjæring om tilgang til et bevis, må følgende tre vilkår være oppfylt:

1. **Relevanskravet,**
2. **Tilknytningskravet,**
3. **Kravet om andre grunner som viser at det er særlig viktig å få tilgang til beviset.**

Nedenfor i punkt 4.4-4.6 behandles innholdet i de tre ovenfor nevnte vilkårene i relasjon til en begjæring om sikring i snever forstand. Deretter i kapittel 4 behandler jeg vilkårene for å få tilgang til et bevis. Det er da særlig det tredje vilkåret som tolkes.[129] Fortløpende og særskilt i punkt 4.8 drøftes spørsmålet om det i tillegg er grunnlag for å oppstille et ytterligere (ulovfestet) vilkår om **forholdsmessighet**, altså et fjerde vilkår som er felles for både sikring av bevis og tilgang til bevis.

4.3 Vilkår for bevissikring

Det materielle tilknytningskravet ved brudd på tilgjengeliggjøringsretten - "beviset kan få betydning i en tvist":

Etter ordlyden i tvisteloven § 28-2 er det bare anledning til å få sikret et bevis dersom "beviset kan få betydning i en tvist". Med "tvist" menes i denne sammenhengen et

[129] Jeg har ikke funnet grunn til å foreta en nærmere vurdering av om de to grunnvilkårene kan ha forskjellig innhold i relasjon til henholdsvis bevissikring og bevistilgang, så jeg problematiserer ikke det nærmere.

juridisk mellomværende mellom minst to parter som potensielt kan bringes inn for domstolene for en rettslig avgjørelse i henhold til gjeldende rett.[130]

4.3.1 Sammenhengen mellom de materielle (opphavsrettslige) rettskrav/beføyelsene etter åndsverksloven ved ulovlig opplastning av opphavsrettsbeskyttet materiale på Internett og de bevis som kan være aktuelt å begjære sikret: - de faktiske påstandsgrunnlag/det faktiske påstandsgrunnlaget.

I henhold til den grunnleggende bestemmelsen i tvisteloven § 1-3 første ledd er muligheten til å benytte domstolene som tvisteløsningsorgan begrenset til tvister om "rettskrav".[131] Dette kravet innebærer en avgrensning mot søksmål om faktiske forhold, interessetvister[132], politiske spørsmål[133] m.m. [134] [135]
At vilkårene for bevissikring utenfor rettssak på denne måten er koblet til kravet om «rettslig interesse», tilsier derfor **"negativt"** at det **ikke** er anledning til å benytte bevissikring utenfor rettssak for å skaffe "bevis" for krav som ikke samtidig vil være "rettskrav" i lovens forstand.[136] Dette tilsier altså at reglene ikke kan benyttes for å skaffe dokumentasjon for forhold som bare kan være relevante for å avgjøre faktiske forhold,[137] interessetvister[138] osv.

---

[130] Ot.prp. nr.51 (2004-2005) side 186 punkt 5.2.

[131] I følge NOU 2001:32 side 652 til § 1-3 er bestemmelsen ment å omfatte én side av kravet om "rettslig interesse" Siden lovgiver ikke tok sikte på å gjøre omfattende endringer i den eldre rettstilstanden etter tvistemålsloven §§ 54 og 55, er tidligere rettspraksis fortsatt relevant for å foreta avgrensningen av hvilke krav som kan bringes inn for domstolene til avgjørelse.

[132] Rt. 1979 side 468 eksklusjon Norsk Balalaikaorkester.

[133] Eksempelvis Rt. 1998 side 607 hvor en professor krevde å bli plassert i et bestemt lønnstrinn, basert på lønnspolitiske retningslinjer.

[134] Rettskravet skal fremgå av stevningen, se tvisteloven § 9-2 annet ledd bokstav c) som angir at ønsket domsresultat skal angis i påstanden.

[135] Ot.prp. nr.51 (2004-2005) side 186 punkt 5.2.

[136] NOU 2001:32B side 988 til § 31-2.

[137] Et eksempel på et mulig søksmål om faktiske forhold kunne være om en «fildelingsorganisasjon» skulle gå til domstolene med krav om å få dom for at rettighetshavernes markedsføringsfordeler ved den

Samtidig tilsier denne koblingen til rettskravbetingelsen "positivt" at det kan være aktuelt å benytte bevissikringsreglene til å sikre dokumentasjon for ethvert forhold som kan være relevant i et søksmål om ethvert materielt rettskrav.

Siden ordlyden i overskriften i kapittel 28 taler om bevissikring "utenfor rettssak", kan vi trygt slutte at bevissikringsinstituttet i hvert fall kan benyttes for å sikre bevis for forhold som kan være relevante i en fremtidig (hypotetisk) rettssak.[139] [140].

Ordet "betydning" betyr etter alminnelig språklig forståelse i hvert fall at beviset må være **relevant**.[141]

Sett i sammenheng innebærer vilkåret "betydning i en tvist" at beviset som begjæres sikret må **kunne** være **relevant** i en fremtidig rettssak om et materielt rettskrav. Dette vilkåret betegner jeg som «det materielle tilknytningskravet» eller «relevanskravet».

Hvilke bevis som kan være relevante beror på hvilke faktiske forhold som er relevante i saken.[142] Relevansen av de faktiske forhold[143] beror på hvilke vilkår det rettslige

---

ulovlige fildelingsvirksomheten overveier de uheldige økonomiske konsekvensene av fildelingen isolert sett.

[138] Et eksempel på en interessetvist ville være om noen ønsket dom for at opplastning av opphavsrettsbeskyttede musikkfiler må være lovlig med den begrunnelse at rettighetshavere har store markedsføringsgevinster av dette.

[139] Det samme fremgår av NOU 2001:32 side 987 punkt 31.1 og Ot.prp.nr.33(2003-2004) side 2 punkt 2.2. Dette gikk også uttrykkelig av ordlyden i den tidligere tvistemålsloven § 267.

[140] NOU 2001:32 side 987 punkt 31.1: "kapitlene om bevis forutsetter normalt at det verserer en tvist for domstolene, men er ikke begrenset til dette"

[141] Uttrykket "betydning" kan også bety noe mer, se nedenfor i punkt xxx om det er et vilkår at bevisene kan tillates ført, og punkt xxx om bevis med mindre bevisverdi.

[142] Se tvisteloven § 21-1.

[143] I tvistelovens terminologi er disse faktiske forhold omtalt som "det faktiske påstandsgrunnlaget"/de(t) relevante påstandsgrunnlag(et) og rettens "faktiske avgjørelsesgrunnlag", se henholdsvis tvisteloven § 11-2 første ledd, og § 21-1, jf. § 21-2 første ledd. "Det faktiske påstandsgrunnlaget" angår det parten mener

grunnlaget oppstiller som relevante. Hvilket rettslig grunnlag som er relevant, beror på hvilke rettsvirkninger det kan bli spørsmål om å kreve, for det er de aktuelle rettsvirkningene som styrer hvilke rettslig grunnlag rettighetshaver kan ønske å påberope seg.

For å avgjøre hvilke bevis som kan få betydning i en senere tvist er det derfor nødvendig å undersøke hvilke "rettskrav" som senere kan bli gjenstand for søksmål av rettighetshaver ved ulovlig opplastning av opphavsrettsbeskyttet materiale på Internett, hvilke rettsregler som regulerer disse, og hvilke vilkår som må være oppfylt.

I det følgende vil jeg derfor gi en redegjørelse for åndsverkslovens relevante rettsregler, herunder rettsvirkningene, og de vilkår som må være oppfylt for at rettighetshaver skal få medhold i den senere tvisten.

Siden åndsverklovens regler kun er et **indirekte tema**, faller det utenfor avhandlingens rammer å gå grundig inn på dette. Jeg gir derfor kun en nødvendig oversikt over åndsverkslovens regler om uberettiget tilgjengeliggjøring.

I punkt 2 er det redegjort for hvilke handlinger som anses som tilgjengeliggjøring. Jeg redegjorde også for hvilke spor som genereres ved opplastning på internett. Disse gir en oversikt over noen av de bevis det **faktisk**[144] kan være aktuelt å begjære sikret for å bevise de relevante faktiske forhold/påstandsgrunnlag/søksmålsgrunnlag, og redegjørelsen nedenfor må derfor ses i sammenheng med redegjørelsen i kapittel 2.[145]

---

hun kan dokumentere under **bevisførselen** i henhold til de **beviskrav** som oppstilles på området. Når retten senere skal ta standpunkt til hvilke faktiske forhold som er bevist og som skal legges til grunn for avgjørelsen, omtales disse som "rettens faktiske avgjørelsesgrunnlag".

[144] Selv om disse spor faktisk vil belyse det relevante faktum, er det ikke gitt at de rettslig sett kan sikres.

[145] Det skal presiseres at dette bare er et utgangspunkt. I norsk prosess er bevisføringsretten fri, jf tvisteloven § 21-3, og det er således i utgangspunktet ikke grenser for hvilke bevis/bevisdata man kan føre for retten. På sikringsstadiet skal ikke dommeren ta endelig standpunkt til det materielle kravet, og dette reiser spørsmål ved om retten på dette stadiet kan ta prejudisielt standpunkt til innholdet i de materielle rettsreglene etter åndsverkloven, og dermed hvilke faktiske forhold som kan bli relevante, og

På «håndhevingsstadiet», som innledes ved en stevning, må retten ta standpunkt til de ovenfor nevnte rettslige spørsmål. På «bevissikringsstadiet» er de imidlertid rettsspørsmål som får betydning for innholdet i det materielle tilknytningskravet. Når retten skal ta standpunkt til hvilke bevis som kan få betydning i en tvist, reiser dette flere spørsmål som retten må ta prejudisielt standpunkt til.

4.3.2 De materielle rettsregler ved krenkelser av åndsverksloven § 2 – prejudisielle rettsspørsmål.

"Den som skaper et åndsverk har opphavsrett til verket " [146] Slik lyder § 1 første ledd i lov om opphavsrett til åndsverk m.v. av 5.mai 1961 nr.2 (åndsverksloven). I henhold til åndsverksloven § 2 har "opphavsmannen" [147] /"rettighetshaver" blant annet "enerett til å råde over åndsverket (…) ved å gjøre det tilgjengelig for almenheten (…)." Dette omtales vanligvis og i denne avhandlingen som "tilgjengeliggjøringsretten". [148]
Dette er etter ordlyden i § 2 en "**enerett",** og innebærer positivt at det er rettighetshaver som kan tilgjengeliggjøre verket (**enerettens positive side**). Eneretten innebærer også at ingen andre har rett til å tilgjengeliggjøre verket (**enerettens negative side**). Fra disse utgangspunkter vil det gjelde unntak dersom det foreligger rettslig grunnlag for dette, herunder for eksempel avtale/samtykke eller lisens[149].

---

på denne måten setter grenser for hvilke bevis som kan få betydning i den senere tvisten. Jeg kommer tilbake til dette prosessuelle spørsmålet nedenfor i punkt xxx.

[146] Åndsverket er heretter omtalt vekselvis som verket og det opphavsrettsbeskyttede materialet.

[147] Med **opphavsmann** forstås her skaperen av åndsverket, eksempelvis musikere, forfattere, og komponister, jf. åndsverkloven § 1.

[148] Loven verner også innsatser og prestasjon som har tilknytning til åndsverket og opphavsretten, de såkalte "nærstående rettighetene", jf. Rognstad og Lassen (2009), side 15. Disse omfatter **utøvende kunstneres prestasjoner**, eksempelvis musikere, dansere og skuespillere som fremfører et åndsverk, jf. § 42. Tv- og filmprodusenter og andre **tilvirkere av åndsverk**, har også et tilgjengeliggjøringsvern, se åndsverkloven § 45. Relevant i denne avhandlingen er at spørsmålet om bevissikring, langt på vei aktualiseres de samme rettsspørsmål for nevnte rettighetshavere. Jeg sondrer derfor ikke mellom disse, og omtaler disse under et som *rettighetshavere*.

[149] Jf. åndsverksloven § 39 som oppstiller utgangspunktet om at eneretten helt eller delvis kan overdras.

Det er enerettens negative side som er relevant for **denne avhandlingens objekt**. Den negative retten innebærer et forbud mot at andre foretar handlinger som kvalifiserer til å være tilgjengeliggjøring i åndsverkloven § 2's forstand. Dette kan også formuleres som en plikt for andre til å unnlate å tilgjengeliggjøre verket.

Brudd på denne normen er i henhold til åndsverkloven sanksjonert[150] med et straffeansvar[151], erstatningsansvar for økonomisk[152] og ikke-økonomisk skade[153], og inndragningsansvar[154], samt at det i tillegg kan nedlegges påstand om forbud mot ytterligere bruk, såkalt "forbudsdom"[155].

Det er rettighetshavers forskjellige sivilrettslige beføyelser ved brudd på tilgjengeliggjøringsretten som er de relevante "rettskrav". Som angitt ovenfor er det disse som indirekte styrer hvilke bevis som vil være relevante i et konkret tilfelle.

Vilkårene kan igjen deles opp i to hovedspørsmål:

1. Det første spørsmålet er hvilke vilkår som må være oppfylt for at det skal foreligge et **åndsverk**:

I følge sikker rett må **tre kumulative vilkår** være oppfylt for at noe skal anses å være et åndsverk. Det må foreligge en frembringelse av et verk, dette verket må være av enten

---

[150] Uttrykket "**sanksjoner**" er fellesbetegnelse på de strafferettslige og sivilrettslige virkninger, mens ordet "**beføyelser**", "**rettskrav**" og "**rettigheter**" blir benyttet som betegnelse på de rent sivilrettslig sanksjonene.

[151] Den ordinære strafferammen for krenkelse av tilgjengeliggjøringsretten er etter § 54 første ledd bøter eller fengsel inntil tre måneder, men i tilfeller hvor det foreligger særlig skjerpende forhold, så øker øvre strafferamme til fengsel i tre år, jf § 54 fjerde ledd. Forsøk og medvirkning er straffbart.

[152] Åndsverkslovens henvisning til skadeserstatningslovens regler medfører altså at erstatningsansvaret for økonomisk tap dekker både lidt og fremtidig formuestap, jf. Lov om skadeserstatning av 13.juni 1969 nr. 26 kapittel 4.

[153] Jf åndsverkloven § 55 første ledd, jf § 2 (og § 42 og § 45).

[154] Etter åndsverkloven § 56 kan rettighetshaver / fornærmede kreve inndragning, mens § 55 annet ledd gir rett til å kreve utbetaling av den nettofortjeneste krenkeren har hatt som følge av den ulovlige handlingen. Dette gjelder uansett om krenker har vært i god tro eller ikke.

[155] Forankret i «eneretten» og rettspraksis.

litterær, kunstnerisk eller vitenskapelig art og for det tredje må dette kvalifiserer til å ha såkalt "verkshøyde".[156]

Disse vilkårene kan reise så vel rettslige spørsmål som bevisspørsmål. Det kan tenkes tilfeller hvor saksøker kan forvente at saksøkte under den senere hovedforhandlingen kommer med den innsigelse at det tvert imot er han som har skapt åndsverket, og at saksøker har kopiert hans verk. Dersom saksøker kan forvente en slik innsigelse, kan saksøker har interesse i å benytte bevissikringsreglene for å sikre bevis for de faktiske forhold som er relevante under frembringelsesvilkåret, særlig å sikre bevis for at saksøkte har kopiert hans verk. Dette er imidlertid lite praktisk. For denne avhandlingens formål forutsetter jeg derfor at det verket som er tilgjengeliggjort er et åndsverk og at saksøker/begjærende part har opphavsrettigheter til dette.

De nevnte vilkår er imidlertid også relevante i denne avhandlingen for det neste vilkåret om personell tilknytning til kravet. Jeg kommer tilbake til dette i punkt 4.5.

2. Det andre spørsmålet på "vilkårssiden" er hvilke tilfeller som kvalifiserer til å være "**tilgjengeliggjøring**" for "allmennheten" i åndsverkslovens § 2s forstand. Dette er av helt sentral betydning for å avgjøre det konkrete innholdet i det materielle vilkåret "betydning i en tvist" i tvisteloven § 28-2.

Et verk kan tilgjengeliggjøres på mange forskjellige måter, herunder på de **tradisjonelle** måter for eksempel visning av en film på kino, salg av musikk, bøker og lydbøker fra fysisk butikk. De relevante tilgjengeliggjøringshandlinger i denne avhandlingen er begrenset til tilgjengeliggjøring via Internett. Jeg viser her til kapittel 2 hvor jeg redegjorde for hvordan et verk kan tilgjengeliggjøres på internett via BitTorrent-teknologien.

[156] "Jul i Blåfjell"-dommen LB-2004-6608 hvor vilkårene benyttes. Se også Rognstad og Lassen (2009) side 77.

4.4 Den nærmere tolkningen av det materielle tilknytningskravet:[157]

4.4.1 Hvilke grenser setter de immaterialrettslig relevante påstandsgrunnlag?

Ovenfor har jeg redegjort for hvordan de materielle rettskrav rettighetshaver har etter åndsverkloven §§ 55-56 danner utgangspunktet for hvilke faktiske påstandsgrunnlag rettighetshaver kan påberope seg på håndhevingsstadiet, og dermed hvilke bevis som kan bli relevante. Når retten på bevissikringsstadiet skal ta standpunkt til innholdet i vilkåret "kan få betydning i en tvist", kan retten ta utgangspunkt i en slik redegjørelse/vurdering, og redegjørelsen ovenfor vil således danne **utgangspunktet** for fastsettelsen av hvilke faktiske påstandsgrunnlag det kan begjæres sikret bevis for.

Spørsmålet nedenfor er om resultatene av en slik redegjørelse for de immaterialrettslig relevante faktiske påstandsgrunnlagene også setter grensen for hvilke bevis som «kan få betydning i en tvist», **eller** om uttrykket "kan få betydning i en tvist" må tolkes videre (eller for så vidt snevrere).[158]

Det som særlig gjør dette problematisk er, at retten på bevissikringsstadiet ikke kan **vite** hva retten på håndhevingsstadiet vil mene om hvilke faktiske forhold som er relevante.[159]

Dette reiser spørsmål ved om retten skal ta standpunkt til slike prejudisielle rettslige spørsmål. Med andre ord er spørsmålet om retten har kompetanse til å avslå en begjæring om bevissikring med den **begrunnelse** at de faktiske påstandsgrunnlag det skal sikres bevis for ikke vil være rettslig relevante på håndhevingsstadiet.

Dette beror i prinsippet på en **tolkning** av uttrykket "kan få betydning i en tvist".

---

[157] Redegjørelsen nedenfor har også overføringsverdi for tilgangsspørsmålet.

[158] Dersom uttrykket tolkes videre, gir det mulighet til å sikre bevis i større utstrekning enn disse bevis kan føres under hovedforhandlingen, og motsatt.

[159] På bevissikringsstadiet vet kanskje heller ikke rettighetshaver nøyaktig hvilke faktiske anførsler hun vil fremsette under den senere saken, og hvilke de da vil vurdere som uholdbare.

Vi finner det rettskildemessige utgangspunktet i ordlyden. Den bruker uttrykket ”kan”. Bestemmelsen bruker ikke uttrykket ”vil” få betydning i en tvist. Etter en alminnelig språklig forståelse av ordlyden tilsier ordet ”kan” at det er tilstrekkelig med en **mulighet** for at beviset vil kunne få betydning, og dermed at det er tilstrekkelig at det er en mulighet for at det faktiske påstandsgrunnlaget vil være relevant under den senere tvist. Ordlyden taler følgelig for at uttrykket tolkes vidt, og det taler mot at retten kan avslå en begjæring om bevissikring med den begrunnelse at det faktiske forhold beviset skal sikre ikke vil være relevant.

Det tilsvarende spørsmålet kan også oppstå på under saksforberedelsen på håndhevingsstadiet, hvis en part anfører at et faktisk forhold er irrelevant i saken og at bevisførsel om forholdet derfor skal avskjæres. Det rettslige grunnlaget for løsning av et slikt prosessuelt krav er tvisteloven § 21-7 første ledd. Det foreligger en rekke Høyesterettsavgjørelser om tolkningen av bestemmelsen og dens forgjenger i tvistemålsloven, og bestemmelsen reiser flere spørsmål som faller utenfor denne avhandlingen. Her skal imidlertid nevnes at særlig hensynet til et materielt riktig resultat tilsier at retten på håndhevingsstadiet er **tilbakeholden** med å avskjære bevis om faktiske forhold på et tidlig stadium, for i mange tilfeller kan det være usikkerhet ved om et faktisk forhold er relevant helt frem til prosedyrene er ferdig.

Dette har overføringsverdi til vårt spørsmål.[160] Dersom retten må være tilbakeholden med å avskjære bevisførsel om faktiske forhold under hovedforhandlingen, kan dette tilsi at den i hvert fall bør være tilbakeholden med å avslå en begjæring om bevissikring med denne begrunnelse, for på bevissikringsstadiet er det ofte enda mer uklart hvilke faktiske forhold som vil bli påberopt.

Til dette kommer at tvistens rammer i utgangspunktet beror på det faktiske påstandsgrunnlaget en part anfører. Utgangspunktet er at rettighetshaver har frihet til å

[160] Som rettskildemessig grunnlag for direkte overføringsverdi kan nevnes Altibox-saken avsnitt 37 hvor Høyesterett gir uttrykk for at § 28-4 må tolkes slik «at det ikke kan gis tilgang til bevis som ikke også kan fremlegges i en aktuell tvist».

fremsette rettslige anførsler om hvilke faktiske påstandsgrunnlag som vil omfattes av lovens vilkår.
På den annen side finnes det faktiske anførsler som vil være fullstendig irrelevante.

Nedenfor i kapittel 4 skal vi se at det gjennomgående gjør seg sterke mothensyn ved begjæringer om bevissikring, herunder særlig personvernhensyn, og disse kan tilsi at bevissikringsreglene i hvert fall ikke bør kunne benyttes til å sikre bevis for slike fullstendig irrelevante påstandsgrunnlag. Dette innebærer at det bør gå en grense ett sted.

I følge ordlyden og forarbeidene er det heller ingen tvil om at det er meningen at uttrykket "kan få betydning i en tvist" skal utgjøre et «**grunnvilkår»** og dette må forstås slik at dette rettslig skal utgjøre en grense for hvilke bevis som kan begjæres sikret.[161]

Problemstillingen i det følgende blir hvor grensen skal trekkes for domstolens rett til å avslå en begjæring om bevissikring med den begrunnelse at det faktiske påstandsgrunnlaget beviset skal underbygge ikke vil være relevant på håndhevingsstadiet. Det beror på en nærmere tolkning av bestemmelsen. Et mulig faktisk grensetilfelle er hvis rettighetshaver ønsker å sikre bevis for at motparten har lastet ned andre opphavsrettslige verk enn de rettighetshaver har rettigheter til. Det er ikke helt utelukket at slike faktiske forhold kan være relevante, men det er heller ikke gitt at de er relevante, uten at jeg her går nærmere inn på dette.

Som ovenfor nevnt tilsier ordlyden at uttrykket tolkes vidt, men uttrykket "kan" er så upresist at det ikke sier noe nærmere om hvor grensen skal trekkes. Vi må derfor se på de øvrige relevante rettskildefaktorene.

I de klare tilfeller kan begjærende part og retten ta utgangspunkt i redegjørelsen for åndsverklovens regler ovenfor i punkt 4.3.1 og den faktiske redegjørelsen i kapittel 2.

[161] NOU 2001:32B side 988.

Når ordlyden er forholdsvis åpen, og forarbeidene og rettspraksis er tause, åpner rettskildeprinsippene for å legge relativt større vekt på formålet og de reelle hensyn, og i det følgende foretar jeg en de lege lata-drøftelse av formålene og de reelle hensyn.

Formålet med bevissikringsreglene er som nevnt i punkt 1.4 først og fremst å sikre et materielt riktig resultat. Som nevnt kan ikke retten på bevissikringsstadiet kjenne rammene for den tvist som senere blir reist, og har dårlig grunnlag for å vurdere hvilke faktiske forhold som vil være relevante. Hensynet til et materielt riktig resultat tilsier derfor at retten er tilbakeholden med å avslå en begjæring om bevissikring med den begrunnelse at de faktiske påstandsgrunnlag beviset skal underbygge vil være irrelevante på håndhevingsstadiet.[162]

Videre kommer at begjæringen om bevissikring i mange tilfeller også vil være kombinert med en begjæring om at motparten ikke varsles, og det medfører at retten ikke får de nødvendige motargumenter presentert fra motparten, og det innebærer at retten i så fall på eget initiativ må ivareta motpartens interesser ved å søke i de relevante rettskildene som altså etter forutsetningen her gjelder prinsipielle immaterielle grensetilfeller. Dette kan gå på bekostning av domstolenes effektivitet, som også er ett av formålene i tvisteloven, jf § 1-1. Også dette taler derfor mot at retten har omfattende kompetanse til å avslå en begjæring med den begrunnelse at de faktiske forhold beviset skal dokumentere vil være irrelevante, og dermed ikke ”kan få betydning i en tvist”.

Endelig kommer at motparten kan bli pålagt å dekke rettighetshavers saksomkostninger (med dette) i den senere saken, og det endog uten at motparten fikk muligheten til å akseptere kravet på bevissikringsstadiet.
Alle disse argumenter tilsier at vilkåret ”kan få betydning i en tvist” ikke tolkes så snevert at det setter (snevre) grenser for hvilke mulige faktiske påstandsgrunnlag rettighetshaver kan påberope som relevante på bevissikringsstadiet. En slik løsning støttes også av hensynet til effektivt å ivareta rettighetshavers immaterielle rettigheter,

[162] Dette støttes også av Rt.1998 side 484 hvor retten uttalte at man bør være forsiktig med en for sterk avgrensning av bevistemaer under saksforberedelsen.

og dette hensynet må også tillegges forholdsvis stor vekt for å sikre at Norge oppfyller våre folkerettslige forpliktelser etter TRIPS-avtalen.

På den annen side må det ikke tapes av syne at for gjennomføring av bevissikring utenfor rettssak kan det gjøre seg gjeldende flere sterke mothensyn, herunder personvernhensyn og rettssikkerhetshensyn, samt at det også foreligger en fare for at en rekvirent benytter dette instituttet for å legge hindringer i veien for en konkurrent, påføre en konkurrent dårlig omdømme, eller til og med for å få tilgang til informasjon om en konkurrents forretningshemmeligheter.[163] Dette taler for at bevissikringsinstituttet ikke bør kunne benyttet til å sikre bevis for forhold som ikke er relevante, og dette taler således for en snevrere tolkning av vilkåret. Disse mothensyn får særlig vekt i tilfeller hvor retten skal ta standpunkt til begjæringen uten å varsle motparten, se kapittel 5.3.

Oppsummering – forholdet til et forholdsmessighetsvilkår.
Vi ser her at det foreligger mange motstridende hensyn, og tilstedeværelsen og vekten av disse vil variere med de **konkrete** omstendigheter på et vidt spekter av mulige tilfeller. Når det er mange motstridende interesser som vil få forskjellige vekt avhengig av de nærmere omstendigheter, så tilsier dette at regelen åpner for en konkret skjønnsmessig helhetsvurdering.

Jeg nevner her at jeg nedenfor i punkt 4.8 argumenterer for å oppstille et ytterligere vilkår om at bevissikringstiltaket må være forholdsmessig, og i denne forholdsmessighetsvurdering vil en rekke omstendigheter være relevante. Siden et slikt forholdsmessighetsvilkår vil medføre at retten får anledning til å trekke inn alle de relevante omstendigheter i det konkrete tilfellet, og gi dem den vekten de fortjener i det konkrete tilfellet, vil det antakeligvis også være mer hensiktsmessig å benytte forholdsmessighetsvilkåret som et kriterium for å trekke grensen for hvilke faktiske påstandsgrunnlag som kan benyttes som grunnlag for en begjæring om bevissikring etter reglene i kapittel 28, enn å legge til grunn en snever tolkning av inngangsvilkåret ”betydning i en tvist”.

[163] Dette siste er nevnt i Schei m.fl. (2007) side 1249.

Konklusjonen på drøftelsen ovenfor blir dermed at vilkåret "kan få betydning i en tvist" må tolkes vidt i overensstemmelse med ordlyden, men at det antakeligvis går en grense, slik at vilkåret medfører at retten kan avslå en begjæring om sikring av bevis for faktiske påstandsgrunnlag som åpenbart vil være irrelevante.

Prosessuelt innebærer dette at retten **i utgangspunktet** må (kan) [164]legge til grunn begjærende parts pretensjon med hensyn til hvilke påstandsgrunnlag som vil være relevante. Dette er også i overensstemmelse med vanlig lære hva gjelder spørsmålet om retten skal legge til grunn pretensjoner om innholdet i rettsregler for spørsmål som har relevans under saksforberedelsen og som også vil få relevans for avgjørelsen av hovedkravet under hovedforhandlingen.[165] Dersom begjæringen om bevissikring var blitt fremmet under saksforberedelsen, ville nok denne læren fått direkte betydning, men i dette tilfellet er altså bevissikringsreglene skilt ut til et stadium forut for saksforberedelsen. De samme hensyn gjør seg som ovenfor nevnt gjeldende, og det tilsier for så vidt at Høyesteretts syn på dette området også gis overføringsverdi til vår problemstilling.

4.4.2 Neste problemstilling – egenskaper ved beviset som medfører at det ikke "kan få betydning i en tvist"

Ovenfor har jeg konkludert med at de materielle opphavsrettslige rettsregler som bestemmer hvilket faktisk påstandsgrunnlag som vil være relevant i den senere saken, bare i unntakstilfeller vil sette en grense for hvilke bevis som «kan få betydning i en tvist». Spørsmålet nedenfor er om egenskaper ved selve beviset kan medføre at retten avslår en begjæring om bevissikring med den begrunnelse at beviset ikke «kan få betydning i en tvist.»

[164] Se også tvisteloven § 9-6 tredje ledd.

[165] Eksempelvis Rt.2003 side 998.

Det kan også reises spørsmål ved om **egenskaper ved et bevis** kan medføre at det ikke er anledning til å benytte bevissikringsreglene for å sikre dette.

Her er det særlig **to grupper** av forhold ved bevisene som kan være aktuelle å drøfte.

1. For det første kan det foreligge omstendigheter som medfører at beviset på håndhevingsstadiet kan/vil bli nektet ført.
2. For det andre kan det hende at beviset kan/vil ha relativt liten beviskraft.

4.4.2.1 Beviset vil bli nektet ført under hovedforhandlingen:

Hva gjelder den første gruppen av bevis er det klare rettslige utgangspunktet i norsk rett **prinsippet om fri bevisføringsrett**,[166] men at det foreligger en rekke bestemmelser som setter grenser for denne frie bevisføringsretten. Reglene om bevisforbud danner en særskilt skranke for å få sikret og eventuelt tilgang til bevis også på bevissikringsstadiet.[167] For de tilfeller hvor det er **helt på det rene** at ett av disse unntak vil komme til anvendelse under den senere hovedforhandlingen, "kan" ikke beviset få betydning i en tvist, og ordlyden tilsier at begjærende part ikke bør kunne kreve et slikt bevis sikret.[168] Dette har også støtte i Altibox-saken, se avsnitt 37 hvor det fremgår at «det ikke kan gis tilgang til bevis som ikke også kan fremlegges i en aktuell tvist». I slike tilfeller har dette grunnvilkåret en klar funksjon som avgrensningskriterium, og dette standpunktet må i utgangspunktet legges til grunn. Siden verken ordlyden i § 28-4, forarbeidene eller Høyesterett foretar noen nyansert drøftelse av om standpunktet skal gjelde for alle bevisforbudsreglene, og det heller ikke er problematisert om standpunktet i alle tilfeller vil være i overensstemmelse med TRIPS-avtalen, kan dette imidlertid ikke legges til grunn som bastant regel i alle tilfeller.

I tilfeller hvor det foreligger mulighet for at retten ikke kan få tilstrekkelig grunnlag for å vurdere spørsmålet om beviset vil bli tillatt ført eller avskåret, kan det likevel være grunn til å være noe tilbakeholden. Dette gjelder også i tilfeller hvor anvendelsen av

---

[166] Se tvisteloven § 21-3 første ledd første punkt, NOU 2001:32B side 943.

[167] NOU 2001:32B side 990.

[168] Som et eksempel kan her nevnes bevisforbudet om abonnentens betroelse til presten om sine syndige ulovlige opplastninger, jamfør tvisteloven § 22-5 første ledd.

bevisforbudsreglene beror på skjønnsmessige vurderinger som vanskelig kan bli tilstrekkelig opplyst allerede på bevissikringsstadiet.[169]

Videre kan hensynet til å gi rettighetshaver bevis som kan benyttes i forliksforhandlinger tilsi at vilkåret ikke tolkes for strengt, jf at også dette er ett av formålene med bevissikringsreglene.[170]

Drøftelsen ovenfor viser også at det kan være behov for en konkret vurdering av om et bevis bør nektes sikret fordi det kan bli nektet ført under hovedforhandlingen. Dette taler for å oppstille et forholdsmessighetsvilkår. Dette vil også være i overensstemmelse med lovgivningen på de punkter hvor bevisforbudsreglene oppstiller en helhetsvurdering eller en forholdsmessighetsvurdering, se særlig bevisføringsforbudet i tvisteloven § 22-3 som er særlig aktuelt ved bevissikring av abonnentopplysninger.

4.4.2.2 Liten bevisverdi:

Den andre gruppen er, som nevnt, de tilfeller hvor beviset som ønskes sikret (kan være lite aktuelt eller) har liten bevisverdi. Spørsmålet er da om begjæring om sikring av slike bevis omfattes av vilkåret "kan få betydning i en tvist". Ordlyden er vid, og dette taler mot at det er anledning til å begrense bevissikringsreglene på denne måten. Særlig gjelder det dersom beviset nok vil ha lav bevisverdi, men hvor det rettskrav rettighetshaver ønsker å sikre bevis for er av betydelig verdi, for eksempel et erstatningskrav i millionklassen.

Det rettslige grunnlaget for å avskjære et bevis i en sak med den begrunnelse at det har liten bevisverdi er tvisteloven § 21-7 annet ledd bokstav b) (og § 21-8). Også her er det grunn til å være tilbakeholden med å trekke grensen i og med at retten på bevissikringsstadiet ikke kan vite hvilke andre bevis som vil bli påberope og derfor ikke

[169] Dette ble fremhevet i Rt.2002 side 976.

[170] Selv om motpartens motivasjon for å inngå forlik vil være mindre dersom bevisene mot ham ikke kan føres i retten, så er det ikke gitt at motparten forstår dette.

ha full innsikt i den **relative** betydningen av beviset som begjæres sikret, og heller ikke se betydningen av beviset i det samlede bevisbildet.

Også på dette punktet vil de argumentene som taler for å tolke det materielle tilknytningsvilkåret snevert variere med de konkrete omstendigheter, som vist ovenfor.

Alt i alt tilsier disse forhold at muligheten for at beviset vil ha liten bevisverdi ikke medfører at det faller utenfor lovens uttrykk "kan få betydning i en tvist", men at også dette forhold ved et bevis trekkes inn i den forholdsmessighetsvurderingen som retten må foreta. Jeg viser her til drøftelsen av dette vilkåret nedenfor i punkt 4.4

4.5 Hvem kan begjære bevissikring – det personelle tilknytningskravet

Bestemmelsens andre vilkår for å få medhold i bevissikring (i vid forstand) er et krav om personell tilknytning til det fremtidige rettskravet.

Lovens vilkår er at begjærende part "*vil kunne bli part eller partshjelper*". Vilkåret innebærer en begrensning med hensyn til **hvem** som kan fremsette en begjæring om bevissikring, og innebærer et kvalifikasjonskrav ved at begjærende part må ha en så sterk tilknytning til rettskravet og/eller den fremtidige tvisten at vedkommende vil kunne bli part eller partshjelper i denne tvisten. Det omtales her som et "personelt tilknytningskrav".

Et slikt personelt tilknytningskrav samsvarer godt med den alminnelige prosessforutsetningen om tilknytning til søksmålsgjenstanden, som innebærer at saksøker må være innehaver av kravet/ være materielt berettiget til kravet jf tvisteloven § 1-3 annet ledd[171].

[171] NOU 2001:32 side 988 (punkt 31.2 § 31-2 annet avsnitt)

4.5.1 Personell tilknytning som part:

For å kunne bli ”part” i den senere tvist, må den som fremmer en bevisbegjæring for domstolen anføre at hun er innehaver av en eller flere rettigheter som er krenket og at vedkommende er rette innehaver av et materielt rettskrav som følger av brudd på rettighetene. Hun må altså anføre være «kravssubjekt».

Ved krenkelse av tilgjengeliggjøringsretten ved opplastning av opphavsrettsbeskyttede verk på internett er det åndsverksloven som angir hvem som er kravssubjekt. For eksempel tilkommer retten til erstatning i henhold til åndsverkloven § 55 rettighetshavere, herunder opphavsmannen, utøvende kunstner eller tilvirker av verket[172]. Begjærende part må følgelig anføre at hun opptrer i egenskap av å være rettighetshaver av det aktuelle verket krenkelsen knytter seg til på minst én av disse måter.

Ved rettens vurdering av om det personelle tilknytningskravet er oppfylt, vil dette bero på en vurdering av det rettslige grunnlaget, herunder om åndsverklovens vilkår som angir hvem som er personell kompetent til å fremme et krav er oppfylt.

I henhold til åndsverkloven § 42 og § 45 vil også flere persongrupper kunne være rettssubjekter i forhold til forskjellige rettigheter. Jeg legger uten videre til grunn at flere rettssubjekter kan være ”part” i relasjon til det personelle tilknytningskravet, og således at flere rettssubjekter kan ha tilstrekkelig personell tilknytning til en opplastet fil på internett, og således kunne begjære sikring av bevis for en uberettiget opplastning.

Jeg legger uten videre problematisering til grunn at kravet om at begjærende part ”vil kunne bli part” innebærer at begjærende part bare kan kreve sikret bevis for en opplastning av et verk på internett i den utstrekning opplastningen er uberettiget i forhold til vedkommende. For eksempel vil ikke kunstneren kunne bli part i en senere tvist dersom kunstneren har solgt de rettigheter som nå er krenket. I overensstemmelse med dette vil kunstneren selvfølgelig kunne bli part i en senere tvist dersom det er

[172] Åndsverkloven §§ 55, 56, jf. 54, jf. 45, 42 og 2.

kunstnerens ideelle uoverdragelige rettigheter som er krenket i forbindelse med opplastningen. [173]

4.5.2 Personell tilknytning som partshjelper – Partshjelperbegrepet:

Av mer interesse er at bestemmelsen også gir (en fremtidig) **partshjelper** adgang til å fremme begjæringen.[174] Den personelle adgangen til å begjære bevissikring omfatter altså også personer som i en eventuell fremtidig rettssak, vil kunne opptre i egenskap av å være partshjelper, jf. ordlyden "*vil kunne bli (...) partshjelper*"[175]. I følge forarbeidene skal dette begrepet forstås som en henvisning til at de alminnelige vilkårene for å kunne yte partshjelp etter tvisteloven § 15-7.[176]

I henhold til bestemmelsen er det to alternative forhold som kan gi grunnlag for partshjelperstatus. 1. Anvendt på vårt tilfelle vil vilkåret være oppfylt dersom vedkommende dokumenterer å ha et reelt behov for at rettighetshaver, som senere kan opptre som part, vinner, og dette reelle behovet begrunnes i **rettsstillingen** hos den som ønsker å ha partshjelperstatus, jf § 15-7 første ledd bokstav a).

2. Alternativt kan foreninger, stiftelser eller offentlige organer kunne bli partshjelper i saker "som ligger innenfor deres formål og naturlige virkeområde etter § 1-4" forutsatt at disse har oppgave å fremme særskilte interesser. Hva gjelder vårt rettsforhold er Norsk forening for opphavsrett aktuell, samt forvaltningsorganisasjoner som TONO[177] og GRAMO[178].

---

[173] De alminnelige reglene om partsevne og prosessdyktighet må selvfølgelig være oppfylt da begjæringen fremsettes, se henholdsvis tvisteloven § 2-1 og § 2-2.

[174] For ordens skyld presiserer jeg at spørsmålet her er om partshjelperen alene kan fremsette en begjæring om sikring eller tilgang til bevis, og ikke hvem som kan erklære partshjelp hvis rettighetshaver allerede har begjært bevissikring. Det siste var et spørsmål i Altibox-saken, hvor Videogramforeningen erklærte partshjelp for tingretten. Tingretten avslo begjæringen med den begrunnelse at reglene passet dårlig, og at det ikke forelå noe behov på det stadium i saken. Jeg er enig i det siste.

[175] Dette innebærer en utvidelse i forhold til tidligere rett, se den tidligere tvistemålsloven § 267 hvor det kun var parten som kunne begjære bevissikring.

[176] NOU 2001:32 side 988

[177] Forvalter fremføringsrettigheter til komponister.

Ved en begjæring om bevissikring, må altså vedkommende person eller organisasjon anføre at det foreligger en tilknytning til det materieller kravet, og retten må vurdere om denne tilknytningen kvalifiserer til å oppfylle de rettslig relevante vilkårene for at denne skal anses som partshjelper.

Denne utvidelsen av kretsen av de som skal anses å ha tilstrekkelig personlig tilknytning, fra de som kan bli part i en sak til også å omfatte de som kan bli partshjelper, er i forarbeidene begrunnet i behovet for å kunne handle raskt.[179] I disse tilfeller kan det selvfølgelig være hensiktsmessig at ikke bare den direkte kravshaveren har mulighet til å begjære bevissikring. Når flere personer gis adgang til å sikre bevis, styrkes også muligheten for oppfyllelse av formålet om å gjøre bevissikringen mer effektiv, og dermed styrke rettens avgjørelsesgrunnlag[180]. Dette behovet gjør seg særlig gjeldende i de tilfeller hvor parten/rettighetshaver ikke selv har mulighet til å begjære bevissikring. Slik manglende mulighet kan typisk være tilfelle dersom rettighetshaver ikke har det nødvendige utredningsapparatet eller den nødvendige økonomi som kreves for å fremme en begjæring. I mange tilfeller vil også forfølgning av brudd på tilgjengeliggjøringsretten på internett være motivert av et ønske om å skape presedenser og kommunisere til andre opplastere at de risikerer forfølgning ved domstolene. Det er altså allmennpreventive hensyn som kan tilsi en slik forfølgning, og da er det også rimelig at rettighetsorganisasjoner påtar seg kostnadene med bevissikringen. Lovens utvidelse åpner således for dette.

4.5.3 Hvilke krav stilles til dokumentasjon for den personelle tilknytning?

Kravet til personell tilknytning henviser til hvem som vil kunne bli part eller partshjelper i den fremtidige tvist. Hvorvidt vedkommende vil kunne bli part[181] i en fremtidig tvist er et prejudisielt rettsforhold. Som andre prejudisielle rettsforhold beror

---

[178] Sikrer vederlag for produsenter og utøvende kunstnere for kringkastingsverdlag.

[179] NOU 2001:32B side 988 § 31-2.

[180] Jf. NOU 2001:32 side 988 § 31-2 annet avsnitt. Hvorvidt de hensyn som har begrunnet denne utvidelsen foreligger i et konkret tilfelle, er uten relevans for partshjelpers adgang til å begjære sikring.

[181] Redegjørelsen vil for alle praktiske formål bli lik for part og partshjelper.

løsningen på både faktiske forhold og rettslige forhold. Dette reiser dermed spørsmål om hvilke krav som stilles til begjærende parts dokumentasjon av disse prejudisielle spørsmål på bevissikringsstadiet.

Hva gjelder argumentasjon for opphavsretten, er lovens klare utgangspunkt at retten har ansvaret for at rettsanvendelsen blir riktig, jf. tvisteloven § 11-3. Jeg kan ikke se at det skulle finnes tilfeller hvor det er tilstrekkelig grunn til å gjøre unntak fra dette.

4.5.3.1 Krav til bevis for faktiske forhold under det prejudisielle rettsforholdet:

Relatert til spørsmålet om begjærende part vil kunne bli "part" kan det være nødvendig at vedkommende dokumenterer at hun er "rettighetshaver" til en fil. For at vedkommende skal være rettighetshaver til en opplastet fil, må vedkommende ha skapt filen. Dette er et faktisk forhold og spørsmålet er her om tvisteloven § 28-2 forutsetter at dette bevises eller om retten skal legge til grunn begjærende parts pretensjoner med hensyn til dette faktiske forholdet, og dersom det kreves bevis, oppstår spørsmålet om hvilket beviskrav som stilles.

For at retten skal kunne ta en begjæring om bevissikring til følge, så må begjærende part i det minste pretendere å ha en slik personlig tilknytning at hun vil kunne bli part eller partshjelp i den senere sak. Retten er imidlertid i utgangspunktet forpliktet til å prøve dette av eget tiltak. Så langt er dette helt parallelt med tolkningen av tvisteloven § 1-3.[182]

Når det gjelder rettens standpunkt til rettighetshavers begjæring om tilgang til opplysningene/bevisene, er det heller ikke grunnlag for å gjøre unntak fra dette.
Det kan imidlertid stilles spørsmål ved om retten bør gjøre unntak når den behandler en begjæring om sikring av bevis, og da særlig hvis det er fare ved opphold. Til støtte for et slikt synspunkt kan anføres at tvisteloven § 34-1 annet ledd må anvendes analogisk, samt at dette vil være best i samsvar med formålene med bevissikringsreglene og TRIPS-avtalen. Jeg går ikke nærmere inn på dette her.

[182] Schei m.fl.(2007) side 80.

4.6 Bevisforspillelsesfare - Vilkåret om risiko for tap eller svekkelse[183]

Det tredje vilkåret for å få medhold i en begjæring om sikring av bevis er i henhold til tvisteloven § 28-2 at det må foreligge en **risiko** for at beviset **"*kan gå tapt* *eller bli vesentlig svekket*"** dersom beviset ikke sikres **"før sak er reist"**, og i henhold til lovens ordlyd kreves i tillegg at denne risikoen er kvalifisert slik at den må være "**nærliggende**" i bestemmelsens forstand.

Dette vilkåret innebærer et krav om kvalifisert **bevisforspillelsesfare**, altså at det foreligger en kvalifisert risiko for at beviset ikke vil kunne føres eller føres på samme måte i en fremtidig rettssak[184]. Dette er også fremhevet i TRIPS-avtalen artikkel 50 første ledd bokstav b.[185]

Det umiddelbare formålet er at gjennomføringen av en beslutning om sikring av beviset skal avhjelpe bevisforspillelsesrisikoen, slik at de øvrige formål ivaretas, se punkt 1.4 ovenfor.

For å forstå vilkåret er det nødvendig å **se det i sammenheng med de ordinære reglene** om bevisførsel **under** rettssak,[186] de ordinære reglene om bevisopptak under rettssak[187] og den **prosessuelle edisjonsplikten**[188] som gjelder etter at søksmål er reist. Det fremgår av bestemmelsens ordlyd at risikoen for bevisforspillelse må gjelde "før

---

[183] Som utledet i punkt xxx gjelder dette vilkåret bare sikring av bevis i snever forstand. Hva gjelder de forskjellige sikringsmetoder, viser jeg til punkt 6.3 og punkt 6.4. Jeg behandler spørsmålene om å behandle og gjennomføre bevissikring uvarslet i punkt xxx.

[184] Eksempler på dette er at beviset slettes fra en datamaskin eller ødelegges.

[185] TRIPS artikkel 50 bokstav b lyder: «Rettsmyndighetene skal kunne pålegge raske og effektive midlertidige tiltak for å ivareta relevant bevismateriale i forbindelse med den angivelige krenkelsen».

[186] Se tvisteloven § 21-2. Et alternativ til bevissikring før rettssak er å benytte reglene om fjernavhør i tvisteloven § 21-10 i tilfeller hvor et vitne skal reise langt av sted i en lengre periode.

[187] Se tvisteloven §27-2.

[188] Se tvisteloven § 26-5.

sak er reist".[189] Ordlyden viser også at bevissikringsinstituttet skal være et unntak fra de alminnelige reglene i den forstand at dersom det ikke er tilstrekkelig fare forbundet med å vente med bevissikringen til etter at søksmål er reist, så skal den ordinære fremgangsmåten velges.[190]

Dette tolkningsresultatet er også best i overensstemmelse med de hensyn som ligger bak kravet om aktuell interesse i tvisteloven § 1-3 annet ledd. Før sak er reist hviler det fortsatt en usikkerhet med hensyn til om rettighetshaver vil forfølge den ulovlige opplastningen, mens når sak er reist er det på det rene at beviset vil/kan bli benyttet for å forfølge rettighetshavers rettigheter, og den aktuelle interesse for tiltak for å sikre et bevis har dermed **større aktuell interesse** når søksmål faktisk er reist.
Av dette kan vi slutte at dersom rettighetshaver ikke løper noen risiko ved å vente med å begjære bevis fremlagt til etter at søksmål er reist, så skal denne fremgangsmåten benyttes.

Bevissikring er også et **alternativ til de vanlige undersøkelser** rettighetshaver kan gjøre uten domstolens hjelp ("privat etterforskning") før rettssak. I Altibox-saken fremhevet retten at beviset (abonnentopplysningene) ikke kunne sikres på annen måte enn ved bevissikring utenfor rettssak, og det forelå således intet handlingsalternativ[191]. Selv om Høyesterett ikke sier det uttrykkelig, er det mulig å tolke førstvoterende dithen at dersom det er mulig å hindre bevisforspillelse uten å benytte bevissikring, så vil det tale mot å benytte disse reglene. Dette synspunktet kan i så fall plasseres under vilkåret om "bevisforspillelsesfare", slik at dette ikke vil være oppfylt i et tilfelle hvor beviset kan sikres på annen måte. Alternativt kan løsningen rubriseres under forholdsmessighetsvilkåret, se nedenfor i punkt 4.8, og synspunktet er at det er

[189] Uttrykket "før sak er reist" står riktignok i slutten av bestemmelsen direkte i tilknytning til det andre alternative vilkåret, men basert på ordlyden i kapitteloverskriften, ordlyden i § 28-1 og uttalelser i forarbeidene kan vi trygt legge til grunn at uttrykket "før sak er reist" også refererer til sikring av beviset.
[190] Dette kan også formuleres slik at i den utstrekning **bevisforspillelsesrisikoen** kan **avhjelpes** ved de ordinære bevisregler under rettssak, tilsier det at slike regler skal benyttes. I så fall vil bevissikringstiltak forut for rettssak lettere må kunne karakteriseres som unødvendig eller i hvert fall uforholdsmessig, se nedenfor i punkt xxx.
[191] Rt.2010 side 774 avsnitt (57).

unødvendig å benytte bevissikring utenfor rettssak hvis beviset kan sikres på annen måte, og unødvendige tiltak som er inngripende må vurderes som "uforholdsmessige".

Spørsmålet i dette punktet er dermed hvilke tilfeller som kvalifiserer til å gi rett til bevissikring før sak er reist, altså hva som nærmere ligger i dette bevisforspillelsesfarevilkåret,[192] og for denne avhandlingens tema er spørsmålet deretter under hvilke omstendigheter det kan være aktuelt å sikre de bevis som er gjennomgått ovenfor i kapittel 2, og som kan være aktuelle etter ulovlig opplastning av opphavsrettsbeskyttede verk på Internett.

Nedenfor er analysen systematisert ved at jeg først undersøker hvilke tilfeller som dekkes av henholdsvis alternativene "kan gå tapt" og kan bli "vesentlig svekket", og deretter undersøker hva som kan utgjøre risikofaktorer, før jeg deretter tolker og finner innholdet i uttrykket "nærliggende".

4.6.1 Tilfeller hvor beviset "kan gå tapt":

Sett i sammenheng med alternativet om at beviset kan bli "svekket" nedenfor vil tap-alternativet omfatte de tilfeller hvor et bevis blir fjernet herunder permanent slettet.[193]

Som nevnt i punkt 2.5.2 kan det være nødvendig å foreta sikring av **datamateriale hos abonnenten**. Slike bevis kan opplasteren/saksøkte lett fjerne enten ved **fysisk** å fjerne datamaskinen og andre lagringsmedier fra eget hjem eller kontorlokaler, eller ved **teknisk** å slette filer og logger på datamaskinen. En sentral egenskap ved elektronisk lagrede bevis er at de lett lar seg slette. Dette vil i mange tilfeller medføre at beviset går "tapt".

---

[192] Jeg taler om vilkåret i entall selv om tap av beviset og vesentlig svekkelse av beviset er to alternative vilkår eller to sider av vilkåret om bevisforspillelsesrisiko. Kvalifiseringen "nærliggende" som drøftes nedenfor gjelder begge sider av vilkåret. Jeg gjør ikke noe større poeng ut av dette.

[193] Dersom et vitne eller en part er alvorlig syk og det dermed er fare for at vedkommende vil dø før sak er reist eller før hovedforhandlingen, så vil dette omfattes av alternativet "kan gå tapt". Schei m.fl. (2007) side 1248. Dette reiser imidlertid ingen spesielle spørsmål i relasjon til denne oppgavens tema.

Et annet illustrerende eksempel på tilfeller hvor beviset kan gå tapt, er risikoen for at en internettleverandør sletter abonnentopplysninger, se punkt 2.3 ovenfor.
Dette ble anført i Altibox-kjennelsen. Retten kom her til at vilkåret om bevisforspillelsesfare klart var oppfylt. [194]

Når endringslov om Datalagringsdirektivet i norsk trer i kraft, er ikke risikoen for sletting av slike spor lenger så stor[195], og det er særlig tilgang til slike opplysninger som er den interessante rettsvirkningen.

4.6.2 Tilfeller hvor beviset vil bli "vesentlig svekket":

Ordlyden "svekket" krever at det må skje en svekkelse av beviset på en eller annen måte. Etter en alminnelig språklig forståelse av uttrykket "svekket" vil dette omfatte tilfeller hvor beviset blir svekket i sin **bevisverdi**.

I uttrykket "bevisverdi" legger jeg her ikke bare graden av bevisstyrke, som særlig vil bero på en **pålitelighetsvurdering og en troverdighetsvurdering**, men også hvilket faktum beviset sier noe om.[196] Dersom beviset er manipulert slik at det gir klare indikasjoner mot at motparten har foretatt en opplastning, så sier det noe om et uriktig faktum. Dette var tilfellet i TOSLO-2010-62157, behandlet ovenfor i punkt 2.6.2. I saken hadde siktede plantet bevis som tilsa at noen hadde benyttet hans datamaskin som en proxy-server. For denne oppgavens relevante problemstillinger kan vi tenke oss at distributør/uploader sletter den opprinnelige filen etter at *.torrent-filen er konstruert og opplastningen er foretatt, og at han deretter på nytt legger filen inn på sin datamaskin fra en DVD, slik at denne filens metadata viser at han har lagret filen **etter** at *.torrent-filen ble konstruert og opplastet. Det foreligger ingen "feil" ved et slikt bevis, så beviset

---

[194] I vurderingen la retten avgjørende vekt på det forhold at internettleverandøren var pålagt en sletteplikt av den aktuelle koplingen innen 21 dager fra oppkoplingen til internett. Unnlatelsen av å sikre beviset ville medføre at det ikke var mulig å identifisere/kople abonnenten, og det forelå ingen andre bevis som kunne identifisere brukeren. Retten anså derfor vilkåret for å være oppfylt.

[195] Se Lovvedtak 46 (2010-2011) til ny § 2-7a i ekomloven, som oppstiller en lagringsplikt på 6 måneder.

[196] Se også NOU 2001:32A side 458.

vil ha pålitelighet og troverdighet, men dersom dette beviset legges til grunn, så vil dette med styrke tale for at vedkommende ikke er distributør.

Det neste spørsmålet er om uttrykket «svekket» også omfatter de tilfeller hvor det blir vanskeligere å føre beviset, uten at beviset blir svekket i sin bevisverdi.
At det blir **vanskeligere** å føre beviset omfattes **ikke** av en alminnelig språklig forståelse av uttrykket "svekket", og dette taler derfor mot at dette omfattes av svekkelsesvilkåret.[197]
I følge forarbeidene er det imidlertid meningen at dette vilkåret skal dekke de tilfeller hvor det foreligger en risiko for **endringer i bevissituasjonen**[198]**.** Eksempler på dette kan være at det blir **mer kostbart** å føre beviset, eller andre vanskeligheter tilsier at det allerede før saksanlegg er **behov** for å tilrettelegge for at bevisførselen under hovedforhandlingen kan skje uten store ulemper. Dette følger blant annet av at forarbeidene gir uttrykk for at dette vilkåret er en videreføring av den tidligere tvistemålsloven § 267 som uttrykkelig omfattet det tilfellet "at det vilde bli særlig vanskelig at føre det".[199]

Når vi ser uttrykket "**vesentlig**" i sammenheng med den tolkningen som ovenfor er gjort av uttrykket "svekket", innebærer dette for det første at det er et vilkår at bevisverdien blir vesentlig svekket, eller for det andre at det blir vesentlig vanskeligere å føre beviset. Selve ordlyden "vesentlig" krever en kvalifisering av de to nevnte alternativene, slik at ikke enhver endring i bevissituasjonen vil være tilstrekkelig.

---

[197] Se den samme tankegangen i tvisteloven § 33-2 om grunner som være «sikringsgrunn» og dermed kan gi grunnlag for arrest.

[198] NOU 2001:32B side 987 hvor hensynet fremheves i proporsjonalitetsvurderingen til tvisteloven § 21-7side.

[199] Se NOU 2001:32 side 988 § 31.2 hvor det fremgår at det er en videreføring i dagens språkdrakt. Etter alminnelig språkbruk har uttrykket "vesentlig svekket" bevis en annen betydning enn at det blir "særlig vanskelig at føre" beviset, så det er ikke særlig dekkende å si at det er det samme i "dagens" språkdrakt, men uttalelsene i forarbeidene tilsier derfor at det ikke var meningen å foreta noen realitetsendring på dette punktet, og at vilkåret skal ha et innhold i overensstemmelse med en alminnelig språklig forståelse av ordlyden i den tidligere tvistemålsloven § 267.

Jeg viser her til at hovedregelen om umiddelbar bevisførsel som vi finner i tvisteloven § 21-9 legislativt står sterkt, og at det skal gode grunner til for å fravike dette. Jeg viser her til avgjørelsene i Rt 1999 side 109. Det er således ikke tilstrekkelig om bevisførselen under hovedforhandlingen vil bli lettere. Det kreves altså også at bevissikringen vil avhjelpe en situasjon som er slik at den innebærer et avvik fra det normale.[200]

Hva gjelder **datamateriell hos abonnenten**, vil sletting av elektroniske spor på opplasterens datamaskin i mange tilfeller medføre at beviset ikke kan gjenskapes. I slike tilfeller kan det imidlertid innvendes at det skapes nye spor når en fil slettes, og disse "slettespor" kan i så fall anvendes som "indirekte" bevis ("indisier") i kombinasjon med en anførsel om at filen er slettet for å skjule spor av opplastning. Slike bevis og slik bevisførsel vil imidlertid være vanskeligere å føre enn om man kunne ha ført selve den opprinnelige filen. I et slikt tilfelle vil nok bevisverdien bli svekket, og det vil ofte også være vanskeligere å finne slike slettespor og vanskeligere å redegjøre for hvordan disse kan vise at motparten har foretatt opplastninger. Hvorvidt endringen vil være tilstrekkelig til å utgjøre en "vesentlig" svekkelse vil bero på de konkrete omstendigheter. Siden det vanligvis vil kreves spesialkompetanse for å finne slettespor, vil vilkåret om risiko for at beviset blir vesentlig svekket gjennomgående være oppfylt i de tilfeller hvor det foreligger risiko for at motparten vil slette filer på sin datamaskin.

I andre tilfeller vil sletting av enkelte spor helt eller delvis kunne gjenopprettes ved hjelp av "gjenopprettingsteknologi". Slik gjenoppretting forutsetter imidlertid spesialkunnskap som de fleste rettighetshavere ikke er i besittelse av, slik at det blir nødvendig å engasjere en sakkyndig. Også slike tilfeller vil dermed omfattes av tilfellet "vesentlig svekket". Dette medfører at dersom det er en **risiko for at filen vil bli slettet**, så vil bevissikring altså (likevel) kunne besluttes selv om beviset ikke er "tapt".

Spørsmålet i det følgende er hvilke krav loven stiller til de situasjoner hvor slik bevisforspillelse kan forekomme.

---

[200] Jeg ser her bort i fra de tilfeller hvor selve bevissikringstiltaket medfører at faren for svekkelse av beviset avhjelpes, slik at beviset kan føres på ordinær måte under hovedforhandlingen.

4.6.3 Oversikt over innholdet i kravet om «risiko» for bevisforspillelse:

Etter ordlyden i bestemmelsen er det et vilkår for bevissikring at det foreligger en risiko for bevisforspillelse. Dette er godt i overensstemmelse med flere av formålene med reglene.
Uttrykket "**risiko**" innebærer etter en alminnelig språklig forståelse at det i det minste må foreligge en **mulighet for noe negativt**; her konkret mulighet for sletting av et bevis eller andre handlinger som medfører at beviset blir vanskeligere å føre.[201]

Som vi har sett, kan sletting enten utføres av en person eller av en teknisk innretning for eksempel et program som er innstilt slik at det sletter innholdet i en logg etter et visst antall dager. Vilkåret krever at det foreligger en mulighet for at en person vil foreta en slik handling, eller at det foreligger et slikt innrettet teknisk program. I så fall foreligger det en risiko for bevisforspillelse. I så fall tilsier det at man nå bør kunne foreta en bevissikringshandling for å hindre at denne risikoen materialiserer seg.

I følge forarbeidene[202] er ordlyden "nærliggende risiko" en videreføring av den tidligere tvistemålsloven § 267 hvoretter kravet var at det var "grund til at frygte". I følge forarbeidene var ikke omformuleringen ment å innebære en realitetsendring, men utelukkende å formulere det samme innholdet i "dagens språkdrakt". Basert på forarbeidene kan vi derfor tolke "nærliggende risiko" slik at det er synonymt med "grund til å frykte", altså at "nærliggende risiko" skal tolkes i overensstemmelse med alminnelig språklig forståelse av uttrykket "grund til at frygte".

Jeg er enig med forarbeidene i at grunn til å frykte etter alminnelig språklig forståelse har det samme innholdet som "risiko". Uttrykket "nærliggende" er imidlertid ikke reflektert i grunn til å frykte. Uttrykket "nærliggende" gir som vi skal se nedenfor uttrykk for en kvalifikasjon av risikoen. Sett i den eldre språkbruk, synes det som om lovens innhold nå er at det må foreligge en nærliggende grunn til å frykte

[201] Jeg bruker uttrykket "slettehandlinger" som fellesbetegnelse på disse negative handlingene
[202] NOU 2001:32B side 988.

bevisforspillelse. I det følgende legger jeg til grunn at disse to uttrykkene er synonyme. Det interessante blir å se hva vi ellers kan si om innholdet i vilkåret, og hvordan dette kan gi veiledning i konkrete tilfeller.

Det er rekvirenten som må **anføre** et mulig scenario som vil skje dersom bevissikring ikke blir foretatt. Rekvirenten må underbygge dette med å anføre **bestemte forhold** og å vise **hvordan disse forhold gir grunn til å tro** at dette scenariet vil realiseres dersom retten ikke beslutter iverksatt bestemte tiltak som skal sikre beviset.

Nedenfor skal jeg vise at blant de **forhold** som typisk kan tilsi at det er grunn til å frykte at en **person** kan komme til å foreta slettehandlinger, er at motparten **forstår** at han risikerer å få et søksmål mot seg på grunn av ulovlig opplastning av opphavsrettsbeskyttet materiale på internett. Frykten for å tape et erstatningssøksmål kan i alminnelighet altså virke **motiverende** på de som er i posisjon til å slette et spor. Et annet **forhold** som typisk kan innebære at det foreligger grunn til å frykte at en logg vil bli slettet, er en lovpålagt sletteplikt. I slike tilfelle er det altså et påbud i lov som kan «**motivere»** til å foreta en slettehandling, og dette gjelder uansett om dette slettepåbudet er implementert i et program eller om slettepåbudet må oppfylles manuelt.

Basert på de foregående avsnitt er det allerede her grunn til å presisere at realiteten i vilkåret er at **det må foreligge (bestemte) omstendigheter/forhold** som alt i alt **viser** at det foreligger grunn til å frykte eller foreligger nærliggende risiko for bevisforspillelse. Dette viser at verken tvistemålslovens uttrykk ”grund til å frykte” eller tvistelovens uttrykk ”nærliggende risiko” er særlige gode formuleringer av dette vilkåret, i og med at ingen av disse angir at **det må foreligge bestemte forhold**. Lovens formulering sier således intet om **årsaksfaktorene**, men sier bare at det må foreligge en årsakssammenheng.
For å være mer dekkende, burde lovens formulering således hatt det understrekede tillegget, ”og det enten [foreligger omstendigheter som viser at det] er en nærliggende risiko for at beviset vil gå tapt eller bli vesentlig svekket, (…)”

Før jeg nedenfor går nærmere inn på hvilke omstendigheter som kan tale **for og mot** at det foreligger grunn til å frykte at bevis vil bli slettet, skal jeg først undersøke det

nærmere innholdet i vurderingstemaet ”risiko”/ ”grund til at frygte” og innholdet i kvalifikasjonskriteriet ”nærliggende” risiko eller grunn til å frykte.

4.6.4 Det nærmere innholdet i ”risiko” og kvalifikasjonskriteriet ”nærliggende”:

Vi kan i utgangspunktet legge til grunn at dersom det er 100 % sikkert at et spor vil bli slettet, så vil det foreligge en ”nærliggende risiko” for sletting.
Dersom det på den annen side er 0 % sannsynlighet for sletting, foreligger det ingen risiko, og dermed heller ikke ”nærliggende risiko” for bevisforspillelse.

Disse tilfellene er de klare tilfeller og de viser at spørsmålet om ”nærliggende risiko” **i hvert fall** er et spørsmål om sannsynlighetsgrad.[203]

Det kan reises spørsmål ved om kravet om ”nærliggende risiko” gir anvisning på en **ren sannsynlighetsvurdering** eller om det skal bero på en helhetsvurdering hvor også **andre forhold** enn sannsynlighet vil være relevante. Før jeg går inn på dette spørsmålet vil jeg først behandle spørsmålet om hvilket krav til sannsynlighet som kreves etter rettskildefaktorene.

4.6.4.1 Sannsynlighetskravet: kreves sannsynlighetsovervekt?

Ikke en hvilken som helst risiko for bevisforspillelse kvalifiserer til å gi grunnlag for sikring utenfor rettssak. Den relevante bevisforspillelsesrisikoen, er den risikoen som anses som “*nærliggende*” i bestemmelsens forstand. Dette innebærer at det må foreligge en kvalifisert bevisforspillelsesfare.

Ordlyden “nærliggende” er etter en alminnelig språklig forståelse et strengere krav enn at det bare foreligger **en mulighet** for bevisforspillelsesfare. Isolert sett kan ordlyden derfor tilsi at bevisforspillelsesrisikoen må være forholdsvis stor.

[203] Spørsmålet om hvilket sannsynlighetskrav som oppstilles behandles nedenfor.

På den annen side sier ikke ordlyden at det må foreligge en sannsynlighetsovervekt. Ordlyden bruker ikke engang uttrykket sannsynlig, og det ville være nærliggende dersom lovgiver hadde ment at det skulle være et krav om sannsynlighetsovervekt.

Bakgrunnen for innføringen av disse reglene er at Norge har ønsket å gjennomføre våre folkerettslige forpliktelser i henhold til TRIPS-avtalen, se punkt 1.3. Ordlyden i TRIPS-avtalen artikkel 50 nummer 1 bokstav b) taler heller ikke om noe sannsynlighetskrav for bevissikring, i motsetning til hva som gjelder for å kunne foreta andre tiltak som skal hindre brudd på immaterielle rettigheter, sammenlikne artikkel 50 nummer 1 bokstav a).[204]

Det foreligger heller ingen andre rettskildefaktorer som sier at det er et krav om 50 % sannsynlighet.
Tvisteloven § 33-2 oppstiller et krav om 50 % sannsynlighet for at skade vil skje dersom ikke beslutter arrest, men siden bestemmelsen gir hjemmel for mye mer inngripende tiltak enn bevissikring, har bestemmelsen liten overføringsverdi. Riktignok kan det også tenkes tilfeller hvor bevissikringen vil være inngripende, men siden jeg nedenfor oppstiller et forholdsmessighetsvilkår, så kan graden av inngrep i privatlivets fred og andre argumenter trekkes inn i en helhetsvurdering, og dette kan i konkrete tilfeller medføre at retten avslår en begjæring dersom det ikke er sannsynlighetsovervekt for sletting, eller i spesielle tilfeller endog kvalifisert sannsynlighetsovervekt.

Etter dette er jeg derfor kommet til at loven **ikke** oppstiller noe krav om sannsynlighetsovervekt, og som sagt finner jeg støtte for dette standpunktet i ordlyden.

4.6.4.2 Graden av sannsynlighet:

Ordlyden sett i sammenheng med den øvrige lovteksten - "*før sak er reist*", tilsier at den aktuelle risikoen må overstige den risikoen som i alminnelighet foreligger og som til enhver tid knytter seg til muligheten for at føringen av et bevis vil bli umulig eller

[204] For ordens skyld gjentar jeg at konvensjonen gir minimumsrettigheter, se punkt 1.7

vanskeligere. Dette kan med en innarbeidet terminologi fra erstatningsretten omtales som et krav om at den aktuelle tapsrisikoen må overstige "dagliglivets risiko". Dersom risikoen ikke er høyere enn den risikoen som i alminnelighet alltid foreligger for at et vitne skal forsvinne eller et dokument bli slettes hos motparten, så tilsier det at vilkåret ikke vil være oppfylt. Dette tilsier at det må kreves noe mer.

Krüger Kaldnes-kjennelsen[205] **er et eksempel hvor risikoen ikke oversteg den dagligdagse risikoen - det forelå ikke en "nærliggende risiko".**

Den materielle tvisten stod mellom Krüger Kaldnes as (heretter Kaldnes) og et konkurrerende selskap Biowater. Det var tidligere inngått et rettsforlik mellom Kaldnes og Biowater, hvoretter Biowater var forpliktet til å avstå fra aktiv rekruttering blant de ansatte hos Kaldnes.

Tvisten om bevissikring stod mellom Kaldnes og Top Temp Bemanning Tønsberg AS (heretter Top Temp). Kaldnes begjærte bevissikring hos Top Temp, med det formål å finne bevis som kunne avklare om Top Temp hadde fått et rekrutteringsoppdrag fra Biowater i strid med rettsforliket. Kaldnes anførte at rekrutteringsselskapet Top Temp hadde forsøkt å rekruttere en ansatt fra Kaldnes, og ønsket å sikre bevis for at dette var skjedd etter oppdrag fra Biowater.

Det relevante spørsmålet for vår del var om det forelå en nærliggende risiko for at (Biowater ville kontakte) Top Temp og forsøke å slette de relevante dokumentene/bevisene. **Retten besvarte dette benektende.**

De rettssetninger retten la vekt på var at bevissikringen skulle skje hos en profesjonell tredjepart, som ikke stod i noe konfliktforhold til begjærende part. Det forhold at Top Temp eventuelt hadde et kundeforhold til Biowater, medførte ikke en tilstrekkelig stor risiko for at Top Temp ville slette de relevante bevisene/dokumentene. Det forelå heller ikke holdepunkter for at det ville bli vanskelig å få tak i kontaktpersonen hos Top Temp under en senere hovedforhandling.

Den rettskildemessige verdien av en tingrettskjennelse er ikke nevneverdig, men den illustrerer at dersom beviset er hos en tredjemann som ikke har noen direkte og stor personlig interesse i å slette bevisene, så vil det ikke foreligge en bevisforspillelsesfare som overstiger dagliglivets risiko.

---

[205] TTONS-2009-126809.

Konsekvensbetraktninger tilsier at man ikke setter sannsynlighetskravet høyt. I motsatt fall vil retten måtte avslå en begjæring i de tilfeller hvor det er lavere sannsynlighet for bevisforspillelse, men hvor konsekvensene av bevisforspillelse vil være meget store. Dette tilsier at sannsynlighetskravet settes **forholdsvis lavt** slik at dette vilkåret ikke får noen sentral funksjon som **avgrensningskriterium** i tilfeller hvor andre forhold med styrke kan tilsi at bevissikring bør kunne foretas. Graden av sannsynlighet kan trekkes inn i den senere forholdsmessighetsvurderingen sammen med de øvrige forholdene som taler for og mot bevissikringstiltaket.

Etter dette er det vanskelig å si noe sikkert om hvilken grad av sannsynlighet som kreves ut over at det ikke kreves 50 % sannsynlighet, og at det på den annen side heller ikke må være en rent hypotetisk/teoretisk sannsynlighet for bevisforspillelse. Hensynet til å hindre misbruk av bevissikringsreglene tilsier også at det må være en nedre grense. Et alternativ kunne være at retten varierte terskelen for hvilken sannsynlighet som kreves avhengig av om det gjør seg gjeldende forhold som kan tilsi at rekvirenten vil ha andre uberettigede grunner til å benytte bevissikringsreglene, for eksempel misbruk for å "kikke en konkurrent i kortene".[206]
Det er imidlertid ikke nødvendig å nyansere dette sannsynlighetskravet med slike forhold, for slike forhold kan trekkes inn i den forholdsmessighetsvurderingen som jeg gir anvisning på nedenfor i punkt 4.8.

På den annen side kan det være grunn til å nyansere sannsynlighetskravet slik at det kan settes lavere i de tilfeller hvor rekvirenten kan påvise at det haster veldig med å sikre beviset. Denne løsningen er valgt hva gjelder vilkårene for midlertidig forføyning, se tvisteloven § 34-2 annet ledd, hvor vilkåret om å sannsynliggjøre kravet er lempet dersom det foreligger fare ved opphold.[207]

[206] Eksempel hentet fra Schei m.fl. (2007) side 1249.

[207] Det bemerkes at tvisteloven ikke gjør unntak fra plikten til å sannsynliggjøre sikringsgrunn i disse tilfeller.

Siden jeg er kommet til at sannsynlighetskravet i alle tilfeller vil være lavere enn 50 %, og det ikke er mulig å si noe nærmere om hvilket sannsynlighetskrav som gjelder, er vilkåret så **fleksibelt** at retten kan komme til et ønsket resultat[208], særlig sett i sammenheng med forholdsmessighetsvilkåret.

4.6.4.3 Er "nærliggende risiko" en ren sannsynlighetsvurdering?

Det kan stilles spørsmål ved om kravet om "nærliggende risiko" en **ren sannsynlighetsvurdering** eller kan **andre forhold** være relevante i en helhetsvurdering.

Det som aktualiserer dette spørsmålet, er særlig at det kan tenkes tilfeller hvor sannsynligheten for bevisforspillelse er meget lav, men hvor konsekvensene av bevisforspillelse er meget høye, for eksempel i de tilfeller hvor de bevis som kan slettes ville være avgjørende for rettighetshavers mulighet til å dokumentere et erstatningskrav i millionklassen.

Hensynet til rettighetshaver tilsier at det bør være anledning til å foreta bevissikring også i disse tilfellene. Videre vil hensynet til sakens opplysning tale for at slike tilfeller omfattes av vilkåret.
Med grunnlag i formålet med bevissikringsreglene og hensynet til et materielt riktig resultat, jf. tvisteloven § 1-1, er det rettskildemessig grunnlag for å tillegge disse hensynene stor vekt.

Siden jeg ovenfor er kommet til at "nærliggende risiko" ikke oppstiller et krav om sannsynlighetsovervekt, men at det for øvrig er vanskelig å si noe sikkert om hvilke krav til sannsynlighet som stilles, gir bestemmelsen tilstrekkelig grad av fleksibilitet til å fange opp de tilfeller hvor det alt i alt er grunnlag for å beslutte bevissikring.

Siden jeg har funnet grunnlag for å oppstille et ytterligere vilkår om at tiltaket må være konkret forholdsmessig, gir også denne løsningen grunnlag for å trekke inn øvrige

[208] Se også NOU 2001:32A side 458.

momenter i den vurderingen. I denne vurderingen er det godt grunnlag for å trekke inn både bevisets potensielle bevisverdi, og graden av sannsynlighet for bevisforspillelse. Hensynet til forenkling av regelverket kan tilsi at det kun oppstilles én slik helhetsvurdering.

Jeg er etter dette kommet til at ”nærliggende risiko” kun gir anvisning på en ren sannsynlighetsvurdering, og at øvrige momenter vurderes etter forholdsmessighetsvilkåret.

Jeg er nå kommet til at ”nærliggende risiko” gir anvisning på en ren sannsynlighetsvurdering, og at sannsynlighetskravet er forholdsvis lavt. Retten må foreta en vurdering av hvor sannsynlig det er at beviset vil slettes eller svekkes på annen relevant måte. Retten må da basere seg på de **forhold** rekvirenten anfører og som etter rekvirentens mening viser at det er grunn til å frykte at bevis vil bli slettet. I neste punkt behandler jeg de omstendigheter som kan være relevante i vurderingen. Nedenfor i punkt 4.6.5.2 behandler jeg spørsmålet om hvilke krav til bevis som kreves for at retten skal kunne legge rekvirentens anførte momenter til grunn for sin vurdering.

4.6.5 De omstendigheter som kan tale for og mot at det foreligger en bevisforspillelsesfare:

Temaet i dette punktet er å vise hvilke **omstendigheter** som kan tilsi at det er grunn til å frykte for at opplaster, særlig abonnenten, eller en ”tredjemann” vil utføre ”bevisforspillelseshandlinger”.

Den mest sentrale **omstendighet** i denne avhandlingen er at en person risikerer å få et søksmål mot seg og som dermed viser at vedkommende har en **interesse** i å slette de bevis som kan vise at han foretok en opplastning. Den omstendighet at en person risikerer å få et søksmål mot seg, er imidlertid ikke tilstrekkelig til at det faktisk foreligger en risiko for bevisforspillelseshandlinger. Det sentrale er at vedkommende **forstår** dette, for det er denne subjektive forståelsen av realitetene som vil virke **motiverende** på vedkommende for å foreta slettehandlinger. Det er derfor grunn til å tro at både objektive forhold og subjektive forhold er relevante.

I det følgende redegjør jeg for de **objektive** momenter, men forutsetningen er hele tiden at motparten blir kjent med disse forhold før søksmål, og at det derfor reises et spørsmål om det foreligger en risiko for bevisforspillelse før søksmål. Jeg skal også legge til at dersom vedkommende har en urealistisk forestilling om de objektive omstendigheter, for eksempel dersom motparten tror at det potensielle erstatningskravet vil være meget høyt, så vil motpartens **subjektive** forestillinger være avgjørende for i hvilken grad dette vil motivere til slettehandlinger, slik at en urealistisk forestilling om et høyt erstatningskrav kan virke sterkt motiverende, og motsatt. De objektive og subjektive forhold må derfor ses i sammenheng.

Ved vurderingen av om det skal foretas en **uvarslet bevissikring**, vil mange av de samme momenter være relevante, men særlig de subjektive forhold vil være sentrale, for varselet medfører at motparten blir kjent med rettighetshavers krav om sikring av bevis. Jeg kommer tilbake til dette nedenfor i kapittel 5.3.

Størrelsen på det potensielle søksmålet eller rettskravet vil altså være relevant. Jo større potensielt erstatningskrav, desto sterkere blir motpartens interesse i å foreta slettinger.[209]

Videre vil det selvfølgelig være relevant **om vedkommende faktisk er den som har foretatt opplastningen eller om vedkommende er "uskyldig"**. Ovenfor i kapittel 2 viste jeg eksempler på hvordan andre enn abonnenten kan foreta opplastning via abonnentens IP-adresse. Og selv om abonnenten er den som har foretatt opplastningen, viste jeg i kapittel 2 også en rekke innsigelser som abonnenten kan ha og som vil gjøre det vanskeligere å bevise at abonnenten er opplaster. Jo mer bevisst abonnenten er på slike innsigelser, og jo større tro han har på at han vil få gehør for disse, desto mindre sannsynlig vil abonnenten anse et tap for å være, og desto mindre motiverende kan et søksmål virke på hans tilbøyelighet til å slette. Dette siste vil nok sjelden være realistisk, og det er særlig på grunn av det neste momentet.

---

[209] Se NOU 2001:32B side 949.

Som tidligere nevnt vil elektroniske lagrede bevis være **enkle å slette**, og jo mer **fagkunnskap om hvordan sporene kan slettes** motparten har, desto større sannsynlighet vil det være for at vedkommende også vil benytte disse enkle midler for å slette spor. På den annen side, dersom vedkommende vet eller **tror at manipuleringen med bevisene vil bli oppdaget**, så kan det tale mot at vedkommende vil forsøke på dette.[210]

I alminnelighet må vi gå ut i fra at de fleste har **naturlige motforestillinger mot å slette eller manipulere bevis** som er relevante i en sak, og dette tilsier derfor at det i alminnelighet er slik at det skal en del til for at vedkommende vil utføre slettehandlinger. Hvis det foreligger forhold som tilsier at motparten ikke har særlig respekt for loven, så kan det tilsi at vedkommende ikke har slike naturlige motforestillinger, og det vil dermed tale for at vedkommende kan komme til å slette relevante bevis.

Opplistingen av momenter er ikke ment å være uttømmende.

Redegjørelsen viser at noen forhold kan tilsi at det er risiko for sletting, mens andre forhold kan tale mot. Dette viser at retten må foreta en helhetsvurdering av alle momentene som fremkommer i saken, og retten må vurdere momentene opp mot det som er **vanlig handlemåte i liknende situasjoner**.

Jeg vil i det følgende illustrere hvordan disse momentene kan virke med relevante avgjørelser.

Dun & Bradstreet-kjennelsen[211]:
Tvisten stod her mellom kredittinformasjonsbyråene Dun & Bradstreet Norway AS og AAA Soliditet AS (heretter samlet D&B) og Kredittopplysningen AS (heretter KO). D&B begjærte sikring av KOs elektroniske kundelister, med det formål å få sikre bevis for om og i hvilken utstrekning KOs ansatte hadde misbrukt D&Bs kundelister. **Det**

[210] Willassen (2007).

[211] Oslo Tingretts kjennelse av 24. januar 2011 (Saksnummer: 10-197602TVI-OTIR/05).

anførte faktumet var at tidligere ansatte i D&B hadde tatt med seg D&Bs kundelister og urettmessig benyttet seg av disse for å skaffe kunder til det konkurrerende selskapet KO. **Det relevante spørsmålet** for vår del var om det forelå en nærliggende risiko for at KOs ansatte ville slette eller endre informasjonen. Direkte var spørsmålet også om det var en risiko for at de ansatte ville slette eller endre informasjonen dersom de ble varslet om kravet om bevissikring. **Retten besvarte dette bekreftende.**
De rettssetninger retten la vekt på var at (siden) det var motparten som hadde **kontroll** over de aktuelle kundelistene, og at det var i deres **interesse** at bevisene ikke ble meddelt D&B, så forelå det en risiko for at bevisene ville bli slettet eller manipulert. For at denne risikoen skulle anses nærliggende la retten vekt på at de aktuelle kundelistene var elektronisk lagret, hvilket innebar at disse **enkelt** kunne slettes/manipuleres. Retten la også vekt på konfliktnivået mellom partene.
Kjennelsens overføringsverdi:
Kjennelsen illustrerer at sannsynligheten for sletting eller manipulering varierer med **hvor enkelt det er å slette eller manipulere bevisene**. Dette er i overensstemmelse med alminnelige erfaringssetninger som også tilsier at jo enklere det er å slette et bevis, desto større er risikoen for risikoen realiseres.

I saken risikerte KO å få rettet et betydelig erstatningskrav mot seg, dersom de hadde misbrukt D&Bs kundelister, og dette tilsa at det var nærliggende at KO kunne komme til å slette eller manipulere bevis dersom D&B ventet med å kreve fremleggelse av bevis til etter søksmål, eller for så vidt dersom KO ble varslet om begjæringen om bevissikring.

I Krüger-Kaldnes saken, var beviset hos tredjemann, men rekvirenten mente likevel at det var en risiko for at Top Temp ville slette bevisene. Dette illustrerer at retten må vurdere om relasjonen mellom tredjemann som har bevisene i sin besittelse og den potensielle motparten er så sterk at det foreligger en risiko for at tredjemann vil velge å slette eller manipulere bevisene. Denne risikoen må vurderes opp mot momentet muligheten for at det kan oppdages at beviset er slettet eller manipulert. At beviset er hos tredjemann taler i alminnelig mot at tredjemann vil være interessert i å slette eller manipulere beviset. Det taler således mot å få sikret beviset, men samtidig taler jo det også mot at det vil bli sannsynliggjort i ettertid at tredjemann faktisk har slettet eller

manipulert beviset. Dette medfører at tredjemann lettere vil komme unna med det, og det igjen får den betydningen at det kan øke sannsynligheten for at tredjemann kommer til å slette eller manipulere beviset. Dette må retten ta i betraktning, og vurderingen må gjøres konkret. Ved vurderingen av hvor sterk relasjonen mellom tredjemann og den potensielle saksøkte er, vil det være relevant å se på om det er en **familietilknytning**, **hvor langvarig relasjonen har vært**, om tredjemann har mer eller mindre **klare økonomiske interesser** i saksøktes posisjon/økonomiske stilling osv.

I Altibox-saken var abonnentopplysningene det sentrale beviset. Dette var selvfølgelig i internettleverandørens besittelse og internettleverandøren hadde ingen egeninteresse i å slette dette beviset. Situasjonen var imidlertid slik at koblingen mellom den benyttede IP-adressen og abonnentopplysningene ville bli slettet dersom internettleverandøren ikke tok aktive grep for å hindre sletting. Frem til rekvirentene begjærte beviset sikret forelå det således en meget stor sannsynlighet for at beviset ville bli slettet, men selve begjæringen medførte at Altibox noterte beviset slik at det deretter ikke forelå noen bevisforspillelsesfare. Sakens reelle spørsmål var deretter om rettighetshaverne kunne kreve **tilgang** til beviset.
Denne avgjørelsen viser at det må sondres mellom de tilfeller hvor det kreves en aktiv handling for å slette eller manipulere beviset, og de tilfeller hvor beviset vil bli slettet automatisk etter en tid, og hvor det er nødvendig å gå inn med en aktiv handling for å **hindre** at beviset blir slettet.

Avgjørelsene ovenfor illustrerer at retten ved vurderingen må sondre mellom de tilfeller hvor beviset er hos den potensielle motparten, og hvor det er hos en tredjemann. Dette har sammenheng med at egeninteressen til den potensielle motparten er større enn en tredjemann. Det er imidlertid grunn til å påpeke at vurderingen må være konkret.
Dette reiser et særlig spørsmål ved krav om sikring av bevis hos abonnenten, for det vil i de fleste tilfeller være vanskelig for rettighetshaver å vite om abonnenten har foretatt opplastningen, eller om noen andre har benyttet abonnentens IP-adresse til å foreta opplastning. Dette er jo nettopp grunnen til at det er ønskelig med bevissikring hos abonnenten, for å skaffe bevis som kan benyttes mot de potensielle innsigelser abonnenten kan komme med under den senere rettsprosessen, se ovenfor punkt 2.4.

Dette fører oss over i spørsmålet om hvilke bevis eller hvilken dokumentasjon som kreves for at retten skal kunne legge til grunn et moment i denne vurderingen.

4.6.5.1 Hvilke krav stilles til dokumentasjon for eksistensen av de enkelte momenter?

Spørsmålet her er om og i hvilken utstrekning rekvirenten må dokumentere momentene for at retten skal legge de til grunn i vurderingen av om det er sannsynlig at en slettehandling vil bli foretatt.[212] [213]

Hensynet til rettssikkerhet tilsier at retten ikke kan legge til grunn et moment uten noen form for dokumentasjon. Dette taler derfor mot at retten kan bygge på rekvirentens **pretensjoner**.

Det ligger i bevissikringsreglenes "natur" at det kan haste med å få foretatt en bevissikring. Dette tilsier at kravene til dokumentasjon for de enkelte momenter ikke stilles så høyt at det blir vanskelig for rettighetshaver å oppfylle disse i et konkret tilfelle. Dersom kravene settes for høyt mister bevissikringsreglene sin praktiske betydning. Det vil være i strid med TRIPS-avtalen.

Basert på dette legger jeg til grunn at det i alminnelighet ikke kan kreves at rekvirenten dokumenterer de enkelte omstendigheter med sannsynlighetsovervekt. Retten må imidlertid foreta en konkret vurdering av hvor sannsynlig de enkelte momentene er, og kravet til dokumentasjon bør nyanseres med hvor vanskelig eller enkelt det synes å være for rekvirenten å bevise de enkelte omstendigheter. Hensynet til motpartens rettssikkerhet tilsier at rekvirenten beviser de omstendigheter som kan bevises uten større vanskeligheter og tidsspille. Loven er imidlertid ikke tilstrekkelig presis til at det er mulig å oppstille noen klare krav til dokumentasjon for de enkelte omstendigheter.

---

[212] Som illustrerende eksempler kan nevnes om rekvirenten må bevise størrelsen på det potensielle erstatningskravet, og om motparten har kunnskap om sletteteknologi.

[213] Dette spørsmålet må holdes adskilt fra spørsmålet om hvor sannsynlig det er at slettehandlinger vil bli utført, som for så vidt er **hovedtemaet** i dette punktet.

4.6.5.2 Særlig om momenter som viser at motparten har en interesse i å slette beviset – pretensjoner:

Hva gjelder momentet, abonnentens interesse i å slette beviset, så vil det gjennomgående være slik at:

- dersom abonnenten ikke har gjort opplastningshandlingen, så vil han ikke ha noen særlig interesse i å slette bevisene, og det vil således heller ikke foreligge noen sannsynlighet for dette (jeg ser her bort i fra at bestefar sletter filer for å hindre at sønnesønnen blir tatt for opplastninger). Og på den annen side vil det være slik at
- dersom abonnenten har foretatt opplastningen, så vil han gjennomgående ha en sterk interesse i å slette bevisene, og denne interessen vil gjennomgående være tilstrekkelig sterkt til at det foreligger tilstrekkelig sannsynlighet for at han vil forsøke å slette bevisene.

Dette viser at hvorvidt abonnenten er krenkeren eller ikke er krenkeren, får avgjørende betydning for graden av interesse i å foreta sletting, og dette vil igjen ha meget stor betydning i vurderingen av hvor nærliggende risikoen er for at han vil foreta en slettehandling. Dette innebærer altså at bevisførsel med hensyn til om vedkommende er krenkeren kan få avgjørende betydning for om vilkåret om nærliggende risiko for bevisforspillelse er oppfylt.

Dette medfører at dersom retten skulle kreve at rekvirenten sannsynliggjorde at abonnenten/motparten også er den reelle opplasteren, så ville bevissikringsreglene miste mye av sin betydning/effekt i mange tilfeller. Denne konsekvensbetraktningen tilsier derfor at det ikke stilles særlige krav om at hun må bevise momentet at abonnenten har foretatt opplastningen.

Etter min mening taler dette for at retten i **utgangspunktet** må kunne legge til grunn at abonnenten har foretatt opplastningen, se dog modifikasjonen umiddelbart nedenfor. I

juridisk terminologi kan dette uttrykket slik at retten kan legge til grunn rekvirentens pretensjoner med hensyn til om abonnenten har foretatt opplastningen.[214]

Dette må undergis en modifikasjon/presisering. Dette medfører imidlertid ikke at retten ikke **kan** foreta en vurdering av enkelte sider ved motparten som også kan være relevante for å avgjøre om vedkommende er opplaster, og følgende kan tilsi at retten bør foreta en slik vurdering:
Dersom det foreligger bestemte omstendigheter som tilsier at det er lite sannsynlig at abonnenten er den reelle opplasteren, så vil det tale mot å legge dette til grunn. Et eksempel her er hvor abonnenten er en bedrift og IP-adressen benyttes av mange ansatte. Et annet eksempel er de tilfeller hvor abonnentopplysningene viser at abonnenten er foresatt i et hjem med flere familiemedlemmer.[215] Dersom slike opplysninger foreligger, kan ikke retten se bort i fra disse. Det medfører at det må påligge rekvirenten å redegjøre for slike opplysninger i de tilfeller hvor disse opplysningene enkelt kan fremskaffes uten å gå på bekostning av bevissikringsreglenes effektivitet. Dette gjelder særlig i de tilfeller hvor retten har besluttet å behandle begjæringen om bevissikring uten å varsle motparten.

Siden det ikke foreligger noen høyesterettsavgjørelser om dette, foreligger det ikke rettskildemessig grunnlag for å oppstille noen grense for hva retten har anledning til å vurdere, men samtidig viser den rettslige drøftelsen ovenfor at det ikke vil være hensiktsmessig om retten var forpliktet til å kreve dokumentasjon for at abonnenten hadde foretatt opplastningen. Dette kan uttrykkes slik at retten "**kan**" legge til grunn rekvirentens pretensjon i den utstrekning det er nødvendig for å ivareta hensynet til å gjøre bevissikringsreglene effektive. Som redegjørelsen ovenfor viser er det imidlertid

---

[214] Dette spørsmålet likner også noe på den situasjonen hvor faktiske påstandsgrunnlag som ligger til grunn for en prosessforutsetning (rettslig interesse) er de samme faktiske påstandsgrunnlag som må dokumenteres for å få medhold i hovedkravet. I disse tilfeller har Høyesterett lagt til grunn at det ikke er hensiktsmessig at saksøker allerede under saksforberedelsen er nødt til å bevise disse faktiske påstandsgrunnlagene, og at retten dermed kan legge til grunn saksøkers pretensjoner. Se Rt. 2009 side 209 avsnitt 15.

[215] I Altibox-saken var tilrettelegger sønnesønn til abonnenten.

sjelden grunn for retten til å unnlate å kreve fremlagt informasjon om hvem abonnenten er (arbeidsgiver med flere ansatte, alder på abonnenten m.m.).

Konsekvensen av at retten i mange tilfeller kan legge rekvirentens pretensjoner til grunn med hensyn til om motparten er krenkeren, er at vilkåret om fare for bevisforspillelse i mange tilfeller vil være oppfylt ved en begjæring om sikring av datamateriale hos abonnenten i tilfeller hvor rettighetshaver pretenderer at abonnenten er opplasteren, og det ikke foreligger bestemte opplysninger som tyder på at abonnenten ikke er den reelle opplasteren. Konsekvensen av dette blir videre at bevisforspillelsesvilkåret ofte vil være oppfylt når det foreligger en begjæring om sikring av datamateriale hjemme hos en privat abonnent. Redegjørelsen ovenfor viser imidlertid at retten må foreta en sannsynlighetsvurdering basert på en rekke momenter. Dette er noe problematisk, for det er i alminnelighet ikke sannsynlig at rekvirenten vil redegjøre for de bevismomenter som taler mot at abonnenten/motparten er den reelle opplaster. Det medfører at i hvert fall i de tilfeller hvor det prosessuelt skal foretas en vurdering av om vilkårene er oppfylt uten at motparten blir varslet, er det særlig viktig at retten har kunnskap om de forskjellige momenter som er nevnt ovenfor og som generelt vil være relevante.[216]

4.7 Bevistilgangsbehov: "av andre grunner er særlig viktig å få tilgang til beviset før sak er reist"[217]

Etter ordlyden kan det kreves tilgang til bevis dersom det foreligger "*andre grunner*" som gjør det "*særlig viktig*" å få tilgang til beviset før kravet er brakt inn for domstolen, selv om det ikke foreligger risiko for bevisforspillelse.

I en sak gjengitt i **Rt.1997 side 713** var spørsmålet om en kvinne kunne begjære bevisopptak av to vitneforklaringer med det formål å få avklart hvem erstatningskravet

[216] I redegjørelsen her har jeg særlig fokusert på en begjæring om bevissikring hos abonnenten, men synspunktene får tilsvarende anvendelse på en begjæring om bevissikring hos andre enn abonnenten.

[217] For ordens skyld henviser jeg her til punkt xxx hvor jeg viste at loven må forstås slik at dette er et vilkår for å kreve å få **tilgang** til beviset.

skulle rettes mot. Høyesterett kom her til at det ikke var rettslig grunnlag for dette, og begrunnet det med at nevnte formål med bevissikring ikke var omfattet av loven. Det forelå i det tilfellet heller ikke noen tapsrisiko. Det alternative vilkåret om andre grunner som gjør det særlig viktig å få tilgang til beviset innebærer således en utvidelse i forhold til det som fulgte av den tidligere tvistemålsloven. Hva gjelder bakgrunnen og formålet med utvidelsen viser jeg til redegjørelsen ovenfor i punkt 1.3, samt tolkningen av vilkåret nedenfor.

Tolkingen av vilkåret reiser først spørsmål om hvilke **andre grunner** som kan begrunne at rettighetshaver får tilgang til et bevis før sak reises for domstolene. Dernest reises spørsmål om hvilke tilfeller som kvalifiserer til å være "**særlig viktig**" i bestemmelsens forstand.[218]

4.7.1 Hva er "andre grunner"?

Ordlyden – *"andre grunner"* – er vid og oppstiller få begrensninger om hvilke forhold som kan være relevante, men bestemmelsen krever altså at det må foreligge "grunner" som tilsier at rekvirenten har ett eller annet **behov** for å få tilgang til opplysningene.

Ved krenkelser av rettighetshavers enerett til opplastning av åndsverk på Internett opptrer opplasteren anonymt. For at rettighetshaver skal kunne forfølge et brudd på opphavsretten ved å reise søksmål for domstolene med påstand om erstatning eller andre rettskrav som nevnt i punkt 4.3.1, må hun få kunnskap om hvem krenkeren er. Det er for så vidt selvsagt at rettighetshaver må ha kunnskap om hvem hun skal stevne for å kunne reise søksmål. I følge tvisteloven § 9-2 annet ledd bokstav b) må en stevning angi hvem saksøkte er, og uten kunnskap om hvem krenkeren er, vil rettighetshaver heller ikke kunne dokumentere at hun har aktuell interesse i søksmålet i henhold til kravene i § 1-3 annet ledd. Identifiseringen av krenkeren er også relevant for å avgjøre hvilken domstol som vil være rett verneting..

[218] Det vil gjennomgående være slik at vurderingen av om det foreligger andre grunner og om de er særlig viktige, vil foretas under ett. Det er imidlertid prinsipielt to forskjellige spørsmål, og jeg behandler de derfor separat.

Dette viser at rettighetshaver har et særlig **behov** for **tilgang** til bevis som kan **identifisere** krenkeren. Dette vil særlig være abonnentopplysninger som altså identifiserer abonnenten. Som vist ovenfor i punkt 2.5 er imidlertid ikke dette alltid tilstrekkelig til å identifisere den reelle krenkeren. Det medfører at rettighetshaver også har behov for å få tilgang til andre bevis som enten kan identifisere krenkeren **direkte**, eller som rettighetshaver **indirekte** kan benytte som utgangspunkt for ytterligere undersøkelser/"etterforskning" enten utenfor domstolene eller ved ytterligere begjæringer om bevissikring.

Som angitt ovenfor i punkt 1.4.3 er ett av formålene med tvisteloven at tvister også skal kunne løses **utenfor domstolene**. For at rettighetshaver skal være i stand til å kunne gå i forhandlinger med den antatte krenkeren, trenger hun også tilgang til abonnentopplysninger og andre identifiserende bevis.

Alle disse behov for å identifisere den antatte krenkeren vil altså være "andre grunner" som tilsier at rettighetshaver gis tilgang til bevis som direkte eller indirekte **identifiserer** krenkeren.

4.7.2 "særlig viktig" å få tilgang

Det neste spørsmålet blir dermed om dette er tilstrekkelig til å oppfylle kriteriet om at det skal være "**særlig viktig**" å få tilgang til disse opplysningene.

I følge bestemmelsens ordlyd må det foretas en avgrensning mot de grunner som anses som viktige, men altså ikke "*særlig viktig*[e]". Hvilke forhold som kvalifiserer til å være "særlig viktig" i bestemmelsens forstand er ikke angitt nærmere, og den upresise ordlyden tilsier at det vil bero på en **skjønnsmessig helhetsvurdering**. En alminnelig språklig forståelse av **ordlyden isolert sett** tilsier at normen er streng, og at det skal mye til før kravet er oppfylt. Dette samsvarer også godt med uttalelser i **forarbeidene**

hvor det fremheves at bestemmelsen gir anvisning på en streng vurderingsnorm, [219] og at vilkåret har et "***snevert anvendelsesområde***".[220]

Ordlyden gir ikke særlig grunnlag for å trekke inn hensynet til motparten i denne vurderingen av om det er særlig viktig. Siden hensynet til motparten vil variere med de konkrete omstendigheter, og dette kan trekkes inn i den ulovfestede forholdsmessighetsvurderingen, er det heller ikke nødvendig å trekke inn et slikt forvanskende element her. Hensynet til klarhet og oversiktlighet tilsier også at dette holdes utenfor. Dette er etter min mening også i overensstemmelse med Høyesteretts synspunkter i Altibox-saken.

Ut over dette gir ordlyden liten veiledning. Ved vurderingen av hvilke bevis som det kan være "særlig viktig" for rettighetshaver å få tilgang til, skal jeg derfor se hen til øvrige rettskildefaktorer. Spørsmålet er i første omgang om abonnentopplysninger og andre bevis som kan identifisere krenkeren forut for søksmål, kvalifiserer til å være "særlig viktig" å få tilgang til i bestemmelsens forstand, basert på de grunner som er omtalt ovenfor.

Når et sentralt hensyn bak utvidelsen av reglen fra bevissikring til bevistilgang på denne måten har vært å gi tilgang til **identifiserende bevis**, så tilsier det at behovet for å få tilgang til identifiserende bevis i de fleste tilfeller vil være "særlig viktig" i bestemmelsens forstand.

Temaet var oppe i den såkalte Altibox-saken gjengitt i Rt 2010 side 774.
For Høyesterett dreide saken seg om rekvirentene Sandrew Metronome Norge AS og Filmkameratene AS som var rettighetshavere til henholdsvis spillefilmene "Max Manus" og "Kautokeino-opprøret", kunne kreve sikring og å få tilgang til

---

[219] Ot.prp.nr.51 (2004-2005) annen spalte side 470.

[220] NOU 2001:32 side 988: "Kriteriet «særlig viktig å få tilgang til beviset» svarer til vilkårene for bevisopptak under saksforberedelsen etter [§ 27-1 annet ledd].(…) Det er mulig at bevissikring før rettssak vil fremstå som et (enda) mer ekstraordinært virkemiddel, og at terskelen i praksis kan bli noe høyere enn for å tillate bevissikring under saksforberedelsen."

abonnentopplysninger fra internettleverandøren (Altibox as). Rettighetshaverne anførte at abonnenten hadde brutt åndsverksloven. Spørsmålet om grunnvilkårene for bevissikring var oppfylt ble rettskraftig avgjort i tingretten. Nedenfor i punkt 4.9 kommer jeg tilbake til flere spørsmål som var tema for Høyesterett. Høyesterett gav rettighetshaverne medhold i kravet om utlevering av abonnentopplysninger.

Selv om spørsmålet om grunnvilkårene var oppfylt var rettskraftig avgjort av tingretten, og temaet for Høyesterett var om taushetsplikten skulle oppheves, så er sammenhengen med spørsmålet om rettighetshaver skulle få tilgang til opplysningene etter § 28-2 så nær at de synspunkter Høyesterett gir uttrykk for etter min oppfatning har **overføringsverdi** til det temaet jeg drøfter her.

Med henvisning til lagmannsrettens vurdering fremhever Høyesterett at de anførte handlinger antas å være både straffbare og erstatningsbetingende, at den påståtte krenkelsen var av en art som må anses som et betydelig problem, og at det derfor foreligger et behov for å kunne gripe inn overfor slik virksomhet, hvor sivilt søksmål er den eneste måten som rettighetshaverne kan ivareta sine rettigheter på fordi politiet og påtalemyndighet ikke prioriterer slike saker, og at abonnenten av den aktuelle IP-adressen ikke kan ha en berettiget forventning om rettsstridig bruk av denne.

Jeg fremhever særlig at retten la vekt på at konsekvensen av at det ikke ble gitt tilgang til beviset, ville være at rettighetshaver var avskåret fra å få håndhevet sine rettigheter etter åndsverksloven. Det er følgelig sentrale rettssikkerhetshensyn og rettsstatshensyn som gjør seg gjeldende. Til dette kom at det kun var internettleverandøren som kunne identifisere parten, og at abonnenten således ikke kunne identifiseres på andre måter.

Videre skal jeg her trekke frem at Norges folkerettslige forpliktelser i henhold til TRIPS-avtalen innebærer at vi er forpliktet til å ha et system som medfører at rettighetshaverne har muligheten til å håndheve krenkelser av immaterialrettigheter. Også dette tilsier med styrke at det er ”særlig viktig” at i hvert fall rettighetshaver på det området som dekkes av TRIPS-avtalen gis tilgang til slike identifiserende bevis.

Hva gjelder abonnentopplysninger vil det springende punktet her ofte være om vilkårene for å gjøre unntak fra taushetsplikten er oppfylt, se om dette nedenfor i punkt 4.9. Hvis det er tilfellet, så vil det gjennomgående også være slik at det er "særlig viktig" for rekvirenten å få tilgang til opplysningene før sak reises.

4.7.3 Tilgang til andre bevis enn de identifiserende:

Det neste spørsmålet er om vilkåret kan være oppfylt dersom rettighetshaver begjærer tilgang til **andre bevis** enn de identifiserende. Som sentralt eksempel her er rettighetshavers begjæring om tilgang til datamateriale hos abonnenten. Dette materialet kan vise **omfanget** av krenkerens opplastninger.

Basert på forhistorien til bestemmelsen, om utvidelse fra bare bevissikring til også å gi hjemmel for bevistilgang, finner vi synspunkter som trekker i denne retningen. Jeg skal her nevne forarbeidenes uttalelser om ett av formålene med denne utvidelsen:

> "Uten regler om bevistilgang vil en part kunne bli stilt i en meget vanskelig situasjon i tilfeller hvor det kan være grunnlag for å fremme et krav eller å godta et krav som rettes mot parten. Parten kan bli stilt overfor valget mellom å reise sak eller ta til motmæle i saken på et uholdbart faktisk grunnlag eller avstå fra å reise sak eller ta til motmæle i en sak til tross for at faktiske forhold som han ikke kjenner, tilsier noe annet. Like viktig er at manglende mulighet for tilgang til bevis kan medføre at partene ikke forsøker å nå frem til en minnelig ordning (...)".[221]

Dette viser at rettighetshaver kan ha behov for tilgang til slike bevis forut for at søksmål reises, og at slike behov kan være "særlig viktig[e]" i bestemmelsens forstand.

Uttrykket «før sak er reist» i § 28-2 tilsier at retten må foreta en vurdering av i hvilken utstrekning rettighetshavers interesser vil være ivaretatt ved å vente med å kreve tilgang til opplysningene til **etter** at det er reist søksmål. Særlig tvistelovens formål om å legge

[221] NOU 2011:32B side 987-988.

til rette for å få avgjort tvister utenfor domstolene vil imidlertid medføre at det i de fleste tilfeller vil være nødvendig å få tilgang til slike opplysninger som er relevante for beregningen av kravet m.m. før søksmål. Til illustrasjon kan nevnes at i de tilfeller hvor det er på det rene at saken ikke vil bli avgjort ved utenrettslig forlik, og det er på det rene at rettighetshaver vil forfølge krenkelsen, enten fordi rettighetshaver har tilstrekkelige opplysninger til å avgjøre hvilket nivå erstatningskravet vil ligge på, eller rettighetshaver ønsker å reise søksmål av prinsipielle grunner herunder for å statuere et eksempel som kan virke preventivt på andre potensielle opplastere, så vil dette tale mot å gi rettighetshaver tilgang til slike bevis allerede før det er reist søksmål.

Det kunne reises spørsmål ved om det er grunnlag for å anse behovet for å få tilgang til bevis som mindre viktig i saker hvor tilgang ønskes som ledd i **"privat etterforskning"**. Dette ble anført av Altibox i Altibox-saken, og mindretallet i lagmannsretten hadde fremhevet at tilgang til taushetsbelagt materiale ville innebære "en uheldig utvidelse av adgangen til å drive privat etterforskning". Høyesterett fant ikke rettskildemessig grunnlag for dette. Tvert imot fant førstvoterende at når lovgivningen hjemler erstatningsrett ved opphavsrettskrenkelser, så kunne ikke rettighetshaver være forpliktet til å forfølge krenkelsen via det strafferettslige systemet. Retten fant også at det en slik ordning ville "være i dårlig samsvar med Norges folkerettslige forpliktelser etter TRIPS-avtalen".

4.8 Forholdsmessighetskravet

Spørsmålet i det følgende er om det i tillegg til de vilkår som er angitt ovenfor også gjelder et forholdsmessighetsvilkår. Dersom det gjelder et slikt vilkår, så innebærer det at selv om vilkårene i § 28-2 er oppfylt, så kan retten likevel avskjære en begjæring om sikring eller tilgang etter en helhetsvurdering.

Det første spørsmålet blir om det foreligger rettskildemessig grunnlag for å oppstille et slikt forholdsmessighetsvilkår, og i så fall, blir spørsmålet dernest hvilke momenter som er relevante å ta i betraktning i denne interesseavveiningen/forholdsmessighetsvurderingen. Behandlingen nedenfor er felles for både rettskravet sikring av bevis og rettskravet tilgang til bevis.

4.8.1 Det rettslige grunnlaget for forholdsmessighetsvilkåret.

Ordlyden i tvisteloven § 28-2 gir ingen holdepunkter for positivt å oppstille et forholdsmessighetsvilkår. Lovgivningsteknisk kunne lovgiver ha oppstilt en slik vurdering ved å angi at bevissikring «kan» besluttes når vilkårene er oppfylt. Siden ordlyden i § 28-2 sier at «[b]evissikring kan begjæres når(…)», og på den måten angir at bevissikring kan begjæres fremfor å angi at retten «skal» eller at retten «skal» beslutte bevissikring, får vi ikke denne veiledningen i ordlyden. Ordlyden taler således ikke for et det oppstilles et særskilt forholdsmessighetsvilkår, men siden det heller ikke står «skal», blir ordlyden heller ikke en skranke eller motargument.

Høyesterett uttalte i Altibox-saken[222] at «[b]evissikring i medhold av kapittel 28 skjer således etter de alminnelig bevisreglene i tvisteloven kapittel 21 og 22.» Blant disse bestemmelser finner vi tvisteloven § 21-8 som oppstiller en begrensning i den frie bevisføringsrett ut i fra proporsjonalitet, og bestemmelsen fremhever at det skal være «et rimelig forhold mellom den betydning tvisten har og omfanget av bevisføringen».[223] Bestemmelsen er i forarbeidene omtalt som «den alminnelige proporsjonalitetsregel».[224] Det korrekte er nok å si at denne bestemmelsen angir en generell proporsjonalitetsregel hva gjelder saksbehandlingsregler knyttet til **bevisførsel**, og er et utslag av et **alminnelig** forholdsmessighetsprinsipp som angis i § 1-1 annet ledd fjerde strekpunkt, som angir at «saksbehandlingen og kostnadene [skal] stå i et rimelig forhold til sakens betydning».

---

[222] Rt.2010 side 774 avsnitt 37 tredje setning.

[223] Jeg forstår henvisningen slik at dersom føringen av et sikret bevis under hovedforhandlingen vil bli nektet med hjemmel i denne bestemmelsen, så vil det materielle tilknytningskravet i § 28-2 i noen tilfeller ikke være oppfylt, altså fordi beviset ikke «kan få betydning i en tvist». Som vist ovenfor i punkt xxx vil det sjelden være mulig å avgjøre allerede på bevissikringsstadiet om vilkårene for å avskjære et bevis på dette grunnlaget er oppfylt, og det taler for at det materielle tilknytningskravet vanskelig kan benyttes som avgrensningskriterium i kombinasjon med en bestemmelse som § 21-8.

[224] NOU 2001:32B side 974.

Endelig skal nevnes at det også fremgår av forarbeidene at en alminnelig forholdsmessighetsbegrensning må leses inn i § 21-4.[225]

Når loven og forarbeidene i en rekke tilfeller fremhever at de konkrete reglene må suppleres med en proporsjonalitetsvurdering, så taler dette for at det også kan oppstilles en slik forholdsmessighetsvurdering ved avgjørelsen av om retten skal beslutte sikring eller tilgang til bevis.

De øvrige bestemmelsene gir grunnlag for å foreta en interesseavveining hvor tidsbruk og kostnader ved saksbehandlingen vurderes opp mot sakens betydning. Ved anvendelsen av bevissikringsreglene kan det også være grunnlag for å foreta en vurdering av om kostnader og tidsbruk er for store sett i forhold til betydningen av beviset og betydningen av den mulige tvistegjenstanden.
Jeg skal tilføye at etter min mening gir følgende momenter **enn mer grunn** til å oppstille et slikt forholdsmessighetsvilkår ved bevissikring:
For det første er lovens bevissikringsvilkår, som vist ovenfor, ikke særlig presise i sitt innhold, og det åpner for å legge vekt på rettsanvenderens syn på hva som er en rimelig og rettferdig løsning.
For det andre har jeg vist at de forskjellige sider av saken kan variere meget fra sak til sak, og at det derfor kan være hensiktsmessig å foreta en samlet helhetsvurdering.
For det tredje gjelder at på områder som faller inn under anvendelsesområdet til Den europeiske menneskerettighetskonvensjonens artikkel 8, så må retten uansett foreta en forholdsmessighetsvurdering etter artikkel 8 nummer 2, og siden domstolen ved denne konkrete skjønnsmessige forholdsmessighetsvurderingen vil bli gitt en stor skjønnsmargin[226], så kan det hevdes at en ulovfestet forholdsmessighetsvurdering etter tvisteloven kapittel 28 vil eller kan ha samme innhold som den forholdsmessighetsvurderingen retten må foreta etter artikkel 8 nummer 2.[227]

---

[225] NOU 2001:32B side 946-947.

[226] NOU 2001:32A side 169.

[227] Se Altibox-kjennelsen, Rt.2010 side 774 avsnitt (24).

For det fjerde gjelder at når loven åpner for å begrense bevisførselen ut i fra hensynet til å begrense **kostnader** og **tidsbruk**, så bør det også være anledning til å legge vekt på **personvernhensyn** og **rettssikkerhetssyn**[228], slik jeg foreslår nedenfor.[229]

Konklusjon: Etter dette har jeg kommet til at det er grunnlag for å oppstille et forholdsmessighetsvilkår.[230][231]

4.8.2 De relevante momenter i forholdsmessighetsvurderingen:

Forholdsmessighetsvurderingen gir retten grunnlag for å foreta en skjønnsmessig helhetsvurdering av alle de relevante forhold i det konkrete tilfellet. Det neste spørsmålet blir dermed hvilke momenter som vil være relevante i denne vurderingen. Ordlyden i § 1-1 styrer i en viss grad hvilke momenter som kan være relevante å ta i betraktning også her.[232] I forarbeidene er det også nevnt at formålet med en proporsjonalitetsregel i relasjon til tvisteloven § 21-8 er å komme til et rimelig forhold mellom saksbehandlingen og tvistens betydning.[233]

Jeg legger til grunn at følgende momenter generelt vil være relevante:

---

[228] Dette fremheves som sentrale hensyn i Høringsnotat (2011) side 4.

[229] Som ytterligere støtteargumenter kunne følgende være fremhevet: Likheten mellom det sivilrettslige virkemiddelet bevissikring og de straffeprosessuelle tvangsmidler, særlig ransaking, tilsier også at det bør gjelde et forholdsmessighetsprinsipp på samme måte som i straffeprosessloven § 170a. Særlig for abonnentopplysninger gjelder også, som vist ovenfor i kapittel 2, at disse er underlagt ISP-ens taushetsplikt etter ekomloven § 2-9 og at det derfor er nødvendig å foreta en forholdsmessighetsvurdering etter tvisteloven § 22-3, se Altibox-saken avsnitt 48-54. Videre er bevissikringsreglene et alternativ til den prosessuelle edisjonsplikten som gjelder på håndhevingsstadiet og da oppstiller tvisteloven § 26-5 tredje ledd et proporsjonalitetsvilkår. Endelig oppstiller tvisteloven et forholdsmessighetsvilkår for å beslutte midlertidig forføyning etter tvisteloven § 34-1 annet ledd.

[230] Oppstilling av et slikt forholdsmessighetsvilkår foreslås også i Høringsnotat (2011) punkt 1.1.1

[231] Siden dette forholdsmessighetsvilkåret ikke har støtte i ordlyden i § 28-2, kaller jeg dette for et «**ulovfestet** forholdsmessighetsvilkår».

[232] I NOU 2001:32B er det i mange sammenhenger angitt momenter som er relevante.

[233] NOU 2001:32B side 950.

1. **Tidsmomentet**:

Dersom bevissikringsreglene vil medføre at avgjørelsen av en tvist trekker betydelig ut i tid, taler dette mot å tillate bevissikring. Det klare tilfellet er hvis en part skulle begjære bevissikring for å trenere en sak. Jeg kan ikke se at dette er særlig praktisk for de tilfeller som omfattes av denne avhandlingens tema.

2. **Kostnader:**

På stadiet for bevissikring er kostnadene knyttet til behandlingen av bevissikringsbegjæringen og sikringen av beviset de aktuelle utgiftspostene.
Dette omfatter kostnader for **begjærende part**, **motparten** og **staten**, herunder **domstolen**[234] **og namsmyndighetene**.
Utgangspunktet er at rekvirenten må dekke egne og motpartens saksomkostninger, jf tvisteloven § 28-5 første ledd. Dette er imidlertid en sannhet med modifikasjoner, for dersom det kommer til sak, vil disse omkostningene være kostnader med saken, som kan løftes over på krenkeren etter bestemmelsene i tvisteloven kapittel 20, særlig § 20-2. Jeg går ikke nærmere inn på de nærmere regler om dette. Som utgangspunkt må det være rettighetshaver som avgjør om han ønsker å benytte midler til å få sikret et bevis, men retten kan altså trekke dette inn i helhetsvurderingen.
Her skal også særlig nevnes at utgiftene med gjennomføringen av sikringen og kanskje særlig gjennomføringen av en begjæring om **tilgang** kan bli særlig høye. Jeg viser her til Normarc-saken som har versert for det norske rettssystemet i flere år.[235] Jeg viser til behandlingen av saken nedenfor.[236]

3. **Sakens betydning:**

Dette momentet fremheves i § 1-1, men også flere ganger i forarbeidene. Først og fremst omfatter dette sakens **økonomisk** betydning, men også **andre interesser** hos

---

[234] Se NOU 2001:32 B side 950 som fremhever dette.

[235] Se blant annet Rt. 2006 side 626, og TOSLO-2004-42431.

[236] Jeg nevner også avgjørelsen fra Borgarting lagmannsrett (LB-2010-202642), hvor kostnadene ble vurdert å være høye, men ikke uforholdsmessige høye. Det ble der også nevnt muligheten for å benytte IKT for å begrense utgiftene.

partene kan være relevante. I tillegg kan saken ha **prinsipielle implikasjoner**[237] eller en **rettsavklarende funksjon**.[238]

Anvendt på vår virkelighet vil typisk det potensielle erstatningskravets størrelse være relevant, sammenlikne opplastning av én mindre etterspurt film, sammenliknet med en såkalt «blockbuster». Det er ikke utenkelig at rettighetshaver(e) kan ønske bevissikring mot en mindre opplaster for å avklare muligheten for dette, og å gi et signal til alle de mindre opplasterne om at de kan bli utsatt for forfølgning. Siden dette er et stort og anerkjent problem, antar jeg at Høyesterett vil legge stor vekt på dette i forholdsmessighetsvurderingen.[239]

4. **Hvor aktuelt kravet er:**

Dersom det er meget sannsynlig at rettighetshaver vil reise og nå frem med et søksmål, eller nå frem i forhandlinger, så taler det for å tillate bevissikring, og motsatt.

5. **Bevisets bevisverdi:**

På bevissikringsstadiet er dette spørsmål om hvor viktig det aktuelle bevis vil være for å underbygge påstandsgrunnlaget på håndhevingsstadiet. Momentet har nær sammenheng med sakens betydning, og hensynet til et materielt riktig resultat. Jo høyere bevisverdi, desto større vekt får dette i forholdsmessighetsvurderingen.[240] Betraktningen er altså at jo lavere bevisverdi et bevis synes å få i en senere sak, desto mindre grunn er det til å akseptere et inngripende bevissikringstiltak.

6. **Sannsynligheten for å finne bevis som taler mot saksøkte:**

I en avgjørelse gjengitt i Rt.2009 side 1689 ble et avslag på begjæring om tilgang til innholdet på avdøde brors PC, og tilgang til informasjon om hvem som hadde vært ekteskapsvitner/forlovere da broren giftet seg kort tid før han døde, avslått. Høyesteretts ankeutvalg fant at anken over lagmannsrettens avgjørelse åpenbart ikke kunne føre

---

[237] NOU 2001:32B side 651.

[238] NOU 2001:32B side 949 siste setning.

[239] Et støtteargument for dette er TRIPS-avtalen. Synspunktet er at dersom en begjæring avslås med den begrunnelse at det er et uforholdsmessig tiltak å rette skytset mot én enkelt og mindre opplaster, så vil norsk rett ikke være i overensstemmelse med TRIPS-avtalen artikkel 50.

[240] Se Ot.prp.nr.51 (2004-2005) side 467: til § 26-4 Personer som bevis.

frem. Lagmannsrettens begrunnet sin avgjørelse med at ikke på noen måte var sannsynliggjort at begjæringen ville lede til bevis som kunne underbygge begjærende parts påstandsgrunnlag.

7. **Rettssikkerhetshensyn og personvernhensyn:**[241]

Særlig personvernhensyn[242] vil være et vektig moment ved en begjæring om **sikring**[243] av datamateriale hjemme hos en abonnent.[244] Det er også relevant ved sikring av datamateriell hos en bedrift[245] eller konkurrent.[246]

Dette er også relevant i forhold til hvorvidt et krav om **tilgang** til bevis kan være forholdsmessig.

For å hindre at dette hensynet får avgjørende utslag i forholdsmessighetsvurderingen, kan og bør rettighetshaver spesifisere begjæringen, slik at det ikke kreves tilgang til informasjon som i alminnelighet kan være personvernsensitiv. Rettighetshaver bør således enten unnlate å kreve tilgang til privat e-postkorrespondanse, selv om det, som ovenfor vist, kan finnes relevante spor der, eller kreve at dette bare skal gjøres tilgjengelig dersom også andre bevis taler for at motparten er opplaster.[247]

8. **Om den potensielle motpart blir varslet eller ikke.** Dette har blant annet betydning for om han får mulighet til å avverge kostandene knyttet til gjennomføringen
9. **Om begjæringen er rettet mot den antatte krenkeren eller en tredjemann.**

---

[241] Dette er generelle relevante hensyn i Norge. Dessuten er dette fremhevet av lovgiver i relasjon til § 26-4, se Ot.prp.nr.51 (2004-2005) side 467.

[242] Hva gjelder tilgang til abonnentopplysninger ved opphavsrettskrenkelser på internett, uttalte retten i Rt.2010 side 774 at abonnenten ikke kunne ha noen berettiget forventning om å opptre anonymt.

[243] Her mener jeg sikring i snever forstand.

[244] Som redegjørelsen i kapittel xxx viser, vil den praktiske gjennomføringen av slik bevissikring gå ut på at namsmannen drar hjem til abonnenten for å sikre bevisene. De fleste privatpersoner vil oppleve dette som en særlig integritetskrenkelse. Dette gjelder særlig ved uvarslet bevissikring.

[245] I konkurranseloven § 25 er det oppstilt strengere vilkår for å foreta bevissikring hjemme hos en privatperson.

[246] Jeg viser her til det som tidligere er nevnt om faren for å misbruke reglene om bevissikring for å kikke motparten i kortene eller å stikke kjepper i hjulene på en konkurrent.

[247] Jeg viser ellers til det jeg skriver nedenfor i punkt 5.4 om spesifikasjonskravet.

10. Om sikring forutsetter at namsmyndighetene benytter tvang.

11. **Hvor godt underbygget begjæringen er**. Dette kan omfatte hvor sannsynlig det er at «motparten» er krenkeren, og hvor godt de øvrige vilkårene er dokumentert.

12. **Kan saken oppklares på annen måte**.[248]

Avslutning:
Retten må foreta en konkret skjønnsmessig vurdering av de momentene som er relevante i det konkrete tilfellet. Dersom det begjæres uvarslet bevissikring må retten først og fremst basere seg på rettighetshavers påstandsgrunnlag og dokumentasjon, mens ved varslet bevissikring, vil også motparten bidra til å opplyse saken med bevis og argumentasjon.
Avslutningsvis skal nevnes at det ikke er gitt at forholdsmessighetsvurderingen vil slå ut med samme resultatet for alle de begjærte bevis, og heller ikke for sikring og tilgang.[249]

4.9 Tilgang til abonnentopplysninger - tvisteloven § 22-3:

Ett av hovedspørsmålene for Høyesterett i Altibox-saken var om tvisteloven § 22-3 annet og tredje ledd kommer til anvendelse ved spørsmålet om å gi rettighetshaver tilgang til abonnentopplysninger som er underlagt internettleverandørens taushetsplikt etter ekomloven § 2-9. Høyesterett kom til at bestemmelsen kom til anvendelse, og at det var nødvendig å foreta en interesseavveining. I saken hadde Post- og teletilsynet samtykket i bevissikring i saken,[250] og spørsmålet for Høyesterett var om den interesseavveiningen lagmannsretten hadde foretatt etter § 22-3 tredje ledd var basert på

[248] Et eksempel her er om vitneforklaringer kan oppklare saken.

[249] Hva gjelder sistnevnte sondring er det imidlertid en sammenheng: Dersom retten vet at rettighetshavers begjæring om tilgang vil være uforholdsmessig, taler det også mot at det vil være forholdsmessig å tillate sikring.

[250] Altibox-saken avsnitt 49.

korrekt lovforståelse. Høyesterett besvarte dette spørsmålet bekreftende.[251] På dette punktet synes rettstilstanden nå klarlagt. Retten må foreta en bred interesseavveining hvor de hensyn som tilsier inngrep i taushetsplikten, må veies opp mot de hensyn som begrunner taushetsplikten. Høyesterett gir også uttrykk for at interesseavveiningen har «stor likhet med den proporsjonalitetsvurdering som EF-domstolen forutsetter foretatt, når medlemsstatene i nasjonal lovgivning åpner for å pålegge en forpliktelse til å gi private parter tilgang til opplysninger om hvem som innehar en IP-adresse, slik at de kan forfølge rettighetsbrudd i en sivil sak.»[252]

4.10 EMK artikkel 8 om rett til privatliv og korrespondanse:

Spørsmålet om tilgang til abonnentopplysninger omfattes av EMK artikkel 8 ble ikke drøftet av Høyesterett i Altibox-saken, for retten fant at vilkårene i annet ledd uansett var oppfylt.[253] Jeg legger uten ytterligere drøftelse til grunn at sikring og tilgang til datamateriell hjemme hos en privat abonnent vil være et inngrep i vedkommendes rettigheter etter artikkel 8.

Hva gjelder spørsmålet om sikring og tilgang til abonnentopplysninger kan være inngrep i noens rett til privatliv og korrespondanse tar jeg utgangspunkt i en avgjørelse fra EMD av 3. april 2007 i saken Copland mot Storbritannia.[254] Av den norske oversettelsen publisert på Lovdata fremgår at telefonen, e-post og internettbruken til klageren, som var ansatt som assistent til rektoren ved en skole i Wales, var blitt overvåket grunnet mistanke om overdreven bruk av skolens utstyr til personlig bruk. Domstolen fant at innhentingen og lagringen av informasjon om hennes telefonbruk, e-post og internettbruk, uten at hun var klar over det, innebar et inngrep i hennes rett til privatliv og korrespondanse etter artikkel 8.[255]

Selv om innhenting og lagring av informasjon om internettbruk skiller seg fra abonnentopplysninger, legger jeg under noen tvil til grunn at både sikring og tilgang til abonnentopplysninger kan omfattes av EMK artikkel 8.

---

[251] Altibox-saken avsnitt 52-54.

[252] Se avsnitt 53 med videre henvisninger.

[253] Se avsnitt 56.

[254] EMK-2000-62617.

[255] Siden skolen ikke hadde lovhjemmel for å foreta slik overvåkning, kom ikke annet ledd til anvendelse.

EMK artikkel 8 annet ledd oppstiller tre kumulative vilkår for at et inngrep etter første ledd

For det første må i inngrepet ha lovhjemmel. Tvistelovens regler om bevissikring utenfor rettssak tilfredsstiller dette kravet.

For det andre må det foreligge et «legitimt formål». De aktuelle inngrep vil være begrunnet i hensynet til å beskytte rettighetshavers rettigheter, og dette er et klart legitimt formål.®[256]

For det tredje må inngrepet være «forholdsmessig». Jeg viser her til redegjørelsen for det ulovfestede forholdsmessighetsvilkåret ovenfor.

[256] Se Altibox-saken avsnitt 57.

5 Prosessuelle spørsmål ved bevissikring

For at en bevisbegjæring skal kunne behandles for domstolen, er det flere prosessuelle vilkår som må være oppfylt. I dette kapittelet belyses prosessuelle problemstillinger som er særlig aktuelle for denne avhandlingens tema. Dette er spørsmålet om i hvilke tilfeller loven åpner for at en bevisbegjæring kan behandles uten at motparten varsles, og som følgelig begrenser motpartens kontradiktoriske rettigheter. Deretter behandles spørsmålet om hvilke krav som stilles til spesifiseringen av de bevis som begjæres sikret. Dette spørsmålet har særlig aktualitet ved uvarslet bevissikring[257].

Situasjonen hvor disse problemstillingene aktualiseres innebærer en begrensning i motpartens rettigheter, og det synes derfor hensiktsmessig først å redegjøre kort for motpartsbegrepet i tvistelovens bestemmelser om bevissikring utenfor rettssak[258].

5.1 Motparts-begrepet:

Den som opptrer i egenskap av å være motpart, har anledning til å utøve partsrettigheter.
I følge tvl. § 28-3 annet ledd anses som motpart "*den begjæringen retter seg mot*" og den et eventuelt fremtidig rettskrav mest "*nærliggende*" vil bli rettet mot.
At også tredjepersoner som pålegges å bistå ved bevissikringen har anledning til å utøve **partsrettigheter, er begrunnet** i at tredjemann vil ha et legitimt behov til å komme med innsigelser[259] og således at retten må ta disse i betraktning ved vurderingen av om de øvrige vilkårene for bevissikring er oppfylt.

---

[257] Grunnen til det er dels at motparten ikke har anledning til å komme med innvendinger hva gjelder holdbarheten av de bevis og anførsler begjærende part presenterer, og dels ved at internettleverandøren (som også vil anses som motpart,) ikke representerer tilsvarende interesser som abonnenten.

[258] Avslutningsvis behandles kort vernetingsspørsmålet.

[259] NOU 2001:32B § 31-3 side 989.

Den som risikerer å få et krav mot seg, skal også gis anledning til å fremme sine innsigelser. Som redegjørelsen i kapittel 2.4 viser, kan det tenkes flere innvendinger mot at abonnenten også er den som står bak opplastningen, og det er således usikkert om kravet vil bli rettet mot denne. Tilknytningen må kvalifisere til å være "*nærliggende*", og dette tilsier at det kreves visse holdepunkter. Dersom begjærende part skal ha mulighet til å få klarlagt bevis forut for rettssak, tilsier dette at kravet ikke skal tolkes for strengt, og at det må anses tilstrekkelig å fremlegge IP-adressen og de handlinger som knyttes til denne. Dette ble også ansett som tilstrekkelig i Altibox-kjennelsen.[260]

5.2 Vernetingsspørsmålet

Utgangspunktet for rettens vurdering av om denne er stedlig kompetent til å behandle en bevissikringsbegjæring, er i følge tvisteloven § 28-3 første ledd den domstolen der «*sak i tilfelle kunne vært reist*». I følge de alminnelige vernetingsreglene i § 4-4 skal sak fremmes ved «*saksøktes alminnelige verneting*»[261]. Ved en begjæring om sikring av abonnentopplysninger, vil begjærende part naturligvis ikke ha kjennskap til dette. I disse tilfellene gir forarbeidene anvisning på at man skal legge til grunn rettskretsen der saksøkte mest sannsynlig har alminnelig verneting eller der begjæringen mest hensiktsmessig kan behandles[262]. Siden det er internettleverandøren som skal bistå ved sikringen av abonnentopplysningene, kan det være praktisk at domstolen i dennes rettskrets behandler begjæringen.

5.3 Varslet eller uvarslet bevissikring

Når en begjæring om sikring eller tilgang til bevis bringes inn for domstolene er det klare alminnelige utgangspunktet at retten må varsle motparten om begjæringen, og slik at motparten får anledning til å ta til motmæle mot denne.[263] Det kan imidlertid foreligge fare for at motparten vil slette bevis dersom han blir varslet om begjæringen

[260] TSTAV-2009-55827 avsnitt (3).

[261] Dette vil være domstolen som tilhører rettskretsen der privatpersonen har sin bopel, og for foretaksregistrerte virksomheter der denne har registrert hovedkontor, jf. § 4-4 annet og tredje ledd.

[262] NOU 2001:32B § 31-3 side 989. Se også bestemmelsens annet punktum.

[263] Se § 28-3 tredje ledd annet punktum., se også den alminnelige regelen i tvisteloven § 13-2.

før bevissikring blir besluttet og gjennomført.[264] Som redegjort for i kapittel 2 gjør det seg gjeldende mange spesielle forhold som medfører at risikoen for bevisforspillelse kan være særlig stor for de tilfeller som omfattes av denne avhandlingens tema. Siden bevissikringsfaren består i at motparten kan ødelegge bevisene[265], oppstår **spørsmålet om loven har virkemidler som avhjelper denne risikoen**. Siden retten til å bli hørt står sterkt i norsk rett, krever unntak fra dette en klar lovhjemmel. Det rettslige grunnlaget for å gjøre unntak fra kontradiksjonsprinsippet er tvisteloven § 28-3 fjerde ledd. Bestemmelsen gir retten kompetanse til å «*treffe avgjørelse om at bevissikring skal holdes før motparten varsles*», dersom det «*er grunn til å frykte at varsel til motparten vil hindre at beviset sikres*».[266]

Bestemmelsen viderefører den tidligere bestemmelsen i tvistemålsloven § 271a, som ble vedtatt som følge av avgjørelsen i en sak gjengitt i Rt. 2000 side 1261 (Microsoft mot Storbyguiden). I saken krevde Microsoft Corp. og Adobe Systems Inc. gjennomføring av bevisopptak utenfor rettssak i medhold av tvistemålslovens regler for å sikre bevis med tanke på en eventuell senere rettssak om erstatning på grunnlag av mistanke om at Storbyguiden as hadde installert programvare i strid med bestemmelser i åndsverksloven. Spørsmålet for Oslo byrett var om tvistemålsloven § 270 gav hjemmel til å avsi slik kjennelse uten at Storbyguiden ble hørt. Byretten kom til at det ikke var anledning til å avsi kjennelse uten at motparten ble hørt, og avslo begjæringen om dette. For høyesteretts kjæremålsutvalg var spørsmålet om lagmannsretten hadde anvendt loven korrekt da lagmannsretten nektet å behandle kjæremålet uten først å forkynne dette for motparten. Det ble anført at forkynnelse for motparten ville medføre at adgangen til å foreta bevisopptak ble illusorisk. Høyesteretts kjæremålsutvalg kom til at loven ikke gav hjemmel for å gjøre unntak fra flere sider av kontradiksjonsprinsippet, og stadfestet lagmannsrettens kjennelse. [267]

---

[264] Om gjennomføringsmåtene, se nedenfor i kapittel 6.

[265] Schei Bind II (2007) side 1253.

[266] Bestemmelsen gir etter sin ordlyd grunnlag for å **behandle begjæringen** om bevissikring uten å varsle motparten, mens § 28-3 fjerde ledd annet punktum synes å gi hjemmel for å kunne **gjennomføre** bevissikringstiltaket uten å varsle motparten.

[267] I henhold til TRIPS-avtalens artikkel 50 annet ledd plikter norske myndigheter å ha et regelverk som åpner for at domstolene skal kunne beslutte midlertidige tiltak uten at motparten blir hørt, særlig dersom

Kjæremålsutvalget uttalte at TRIPS-avtalen ikke kunne/måtte tolkes slik at den påla Norge en plikt til å ha en slik regel, og at det heller ikke var grunnlag for å anta at lovgiver hadde lagt til grunn at norsk rett hadde en slik regel.

En slik fremgangsmåte innebærer at motpartens kontradiktoriske rettigheter settes på vent, og avviker således fra et helt grunnleggende prinsipp i norsk sivil- og straffeprosess. Det sentrale spørsmålet blir hvilke tilfeller som gir tilstrekkelig grunn til å gjøre unntak fra kontradiksjonsprinsippet, og jeg kommer tilbake til dette nedenfor.[268] Lovens formuleringer gir ikke noen særlig veiledning med hensyn til innholdet i vilkårene for å gjøre unntak fra varslingsplikten. Siden tolkningen av vilkårene må bero på de grunner som tilsier å gjøre unntak veiet opp mot hvor stort inngrep vedtaket vil være i kontradiksjonsprinsippet, har jeg funnet grunn til først å redegjøre kort for den rettskildemessige vekten dette prinsippet har i norsk rett.

5.3.1 Kontradiksjonsprinsippets status i norsk prosessrett:

Kontradiksjonsprinsippet innebærer i korthet at partene skal gis innsyn i sakens dokumenter og få anledning til å uttale seg om forhold av betydning før det treffes en avgjørelse[269]. Det følger allerede av tvistelovens formålsbestemmelse i § 1-1 at retten til

---

det er nødvendig for å hindre at rettighetshaveren lider uopprettelig skade eller når det er en påviselig risiko for at bevismaterialet ødelegges.

[268] Det kan reises spørsmål ved om retten kan beslutte å unnlate å varsle motparten av eget tiltak, eller om rettighetshaver/begjærende part må kreve slik behandling og gjennomføring. Ordlyden sier ikke at det er nødvendig med en begjæring, men siden begjærende part er nærmest til å vite om det er ønskelig, og nødvendig med slik behandling, og det er snakk om å gjøre unntak fra den grunnleggende rettigheten til å bli hørt, samt at det ofte vil gjøre seg gjeldende sterke personvernhensyn, legger jeg uten videre til grunn at retten ikke kan unnlate å varsle motparten dersom dette ikke begjæres. Det er ikke dermed sagt at ikke en begjæring kan tolkes slik at det også begjæres uvarslet behandling av begjæringen, men en eventuell uklarhet bør avklares med rettighetshaver. Jeg nevner også at retten har en veiledningsplikt som vil omfatte dette, jf tvisteloven § 11-5.

[269] Ot.prp. nr.51 (2004-2005) til punkt 13.2.2 side 167. «*Kontradiksjonsprinsippet berører også rettens forhold til partenes prosesshandlinger. Det sentrale i prinsippet går ut på at partene må gis anledning til å få gjøre rede for sitt syn på de faktiske omstendigheter, og at de må få adgang til å uttale seg om hverandres anførsler. Det siste forutsetter også rett til innsyn i dokumenter".*

kontradiksjon er et sentralt virkemiddel for å sikre en "*rettferdig, forsvarlig, rask, effektiv og tillitsskapende behandling av rettstvister*".
Ved at partene gis anledning til å uttale seg, vil dette i alminnelighet styrke rettens avgjørelsesgrunnlag som igjen vil styrke muligheten for et materielt riktig resultat, se eksempelvis § 9-6 som oppstiller en uttalelsesrett for partene. Kontradiksjonsprisnippet kommer også til uttrykk i tvisteloven § 11-1 tredje ledd som begrenser rettens avgjørelsesgrunnlag til forhold partene har hatt anledning til å uttale seg om.
Dette understrekes også i forarbeidene hvor det fremgår at tvisteloven § 11-1 tredje ledd «*gir en fundamental regel om rett til kontradiksjon*», hva gjelder det faktiske avgjørelsesgrunnlaget.[270]
Prinsippet er også vernet av EMK artikkel 6: Forarbeidene "*Prinsippet om forsvarlig saksbehandling kan utledes av kravet i EMK artikkel 6 nr. 1 om rettferdig rettergang for en upartisk og uavhengig domstol, og det gir ikke bare uttrykk for en sammenfatning av de øvrige prinsippene som er omhandlet foran. Ut fra en totalvurdering av hele saksbehandlingen vil det også kunne påberopes uten at noen særskilt rettergangsbestemmelse er overtrådt*".[271]
Manglende kontradiksjon, vil kunne bedømmes som en **saksbehandlingsfeil**, med opphevelse av avgjørelsen som mulig virkning, jf. tvisteloven § 29-21 første ledd. Dette innebærer at retten til kontradiksjon ikke bare er et prinsipp, men også en **prosessuell rettighet**.[272] [273]

---

[270] NOU 2001:32B til punkt 5.2 § 5-1(3) side 702

[271] Ot.prp. nr. 51 (2004-2005) punkt 4.1.

[272] I Rt.2010 side 1025 i den såkalte «Muggsopp-dommen» uttalte retten at det skal lite til for at fravær av kontradiksjon må vurderes som en «*alvorlig saksbehandlingsfeil*» og «*det skal ikke mye til før en slik feil vil bli ansett å kunne ha hatt virkning på resultatet*».

[273] «Borettslagsleilighetene» Rt.1990 side 8 hvor kontradiksjon omtales som en «grunnsetning i vår rettergangsordning».
I Rt.2005 side 1590 hvor Høyesterett omtaler kontradiksjonsprinsippet som en "bærebjelke i vår prosessordning".

Dette tilsier at det kreves kvalifiserte grunner for å gjøre begrensninger i denne rettigheten. Dette er relevant for tolkningen av lovens vilkår.

Når motargumenter gjør seg gjeldende, må det foretas en avveining:

Som vist hensynet til et materielt riktig resultat et hensyn som også begrunner kontradiksjonsprinsippet. Hvis det foreligger risiko for at beviset vil bli slettet dersom motparten varsles, så står hensynet til et materielt riktig resultat og muligheten til å kunne få sine (immaterielle)[274] rettigheter[275] ved rettssystemets[276] hjelp på den ene siden mot retten til kontradiksjon på den andre siden. Det må da foretas en interesseavveining. For bevissikring utenfor rettssak har lovgiver foretatt denne avveiningen, og spørsmålet i det følgende er hvilke tilfeller som gir tilstrekkelig grunn til å beslutte uvarslet bevissikring.

5.3.2 Vilkår for å gjøre unntak fra varslingsplikten

Tvisteloven § 28-3 fjerde ledd oppstiller ett vilkår, og dette er at det må foreligge **«grunn til å frykte at varsel til motparten vil kunne hindre at beviset sikres»**. Dette vilkåret minner veldig om ordlyden i den eldre tvistemålsloven 267, om «grund til at frygte». Som vist ovenfor i punkt 4.6.3 er dette bevisforspillelsesfarevilkåret videreført i tvisteloven § 28-2 som vilkår for å begjære sikring av bevis, men i ny språkdrakt. Spørsmålet etter bevisforspillelsesfarevilkåret var om det var fare for bevisforspillelse ved å unnlate å sikre beviset før søksmål. Her er temaet formelt et litt annet, altså om selve varselet gir grunnlag for å konstatere bevisforspillelsesfare. Siden mange av de grunner som tilsier at det foreligger bevisforspillelsesfare er at motparten vil foreta slettehandlinger, så er forskjellen for de fleste av de bevis som omhandles i denne avhandlingen imidlertid bare formell. De spor som genereres på en datamaskin

---

[274] Se TRIPS-avtalen artikkel 50 nummer 2.

[275] Dette er også hensyn som er blitt løftet opp til menneskerettigheter. Om EMK artikkel 6 uttales det i NOU 2001:32A side 456: "Reglene om bevis må være slik at de gir partene rimelige muligheter for å presentere sin sak gjennom bevistilbud og bevisføring (…) Det må være mulighet for kontradiksjon om bevisføringen"

[276] Ot.prp.nr.33 (2003-2004) side 5: "Faren for materielt uriktige realitetsavgjørelser på grunn av bevisforspillelse fra motpartens side må anses som et større rettssikkerhetsproblem".

og som er nødvendige for å underbygge at særlig abonnenten er opplaster, som nevnt enkle å slette eller manipulere.

Dette innebærer at de omstendigheter som er nevnt ovenfor i punkt 4.6.5 også vil være relevante å trekke inn i en vurdering av om det foreligger grunn til å frykte at varsel til motparten vil hindre at bevisene sikres.[277] For å hindre dobbeltbehandling viser jeg derfor til momentene ovenfor.

Det er imidlertid grunn til å presisere om at retten må foreta en selvstendig vurdering av begge spørsmålene, og som nevnt ovenfor innebærer uvarslet bevissikring et inngrep i kontradiksjonsprinsippet og dette tilsier at avveiningen kan falle forskjellig ut.

I Altibox-saken krevde rettighetshaverne bevissikring av abonnentopplysninger og datamateriale hjemme hos abonnenten. For sistnevnte ble avslått med endelig virkning av lagmannsretten, slik at bare spørsmålet om sikring av abonnentopplysninger ble prosedert for Høyesterett. Likevel blir ikke abonnenten varslet om saken. Dette kan jo synes merkelig, for det var jo åpenbart ingen grunn til å frykte at varsel til abonnenten ville hindre at ISP-en sikret abonnentopplysningene. Når dette ses opp mot vekten av kontradiksjonsprinsippet, blir dette også temmelig oppsiktsvekkende.[278] Ingen av instansene presiserer hvilke forhold de la vekt på for å gjøre unntak fra varslingsplikten.

5.3.3 Behandling av rettighetshavers rettskrav om å få tilgang til det sikrede beviset:

Ordlyden i tvisteloven § 28-3 fjerde ledd tredje punkt omhandler spørsmålet om når rettighetshaver kan få tilgang til de sikrede bevis. Etter ordlyden er det bare i de tilfeller hvor «det kan være viktig for motparten å hindre» at rettighetshaver får tilgang til beviset, at tilgang skal utstå til «avgjørelsen er endelig». Ordlyden oppstiller således et utgangspunkt om at rettighetshaver skal få tilgang **før** sikringsavgjørelsen er endelig.

---

[277] Mange av rettskildene som der ble nevnt som grunnlag for å oppstille de relevante momentene gjaldt også direkte uvarslet bevissikring.

[278] Jeg legger til grunn at abonnenten kunne varsles og gjøre sine synspunkter gjeldende uten at rettighetshaver ble gjort kjent med hvem abonnenten var. En slik særordning ville bare ivareta kontradiksjonsprinsippet, og krever ikke et særskilt rettslig grunnlag.

I de tilfeller hvor det er skjedd uvarslet sikring av bevis, og det dermed er gjort inngrep i kontradiksjonsprinsippet, bør dette i hvert fall i de aller fleste tilfeller praktiseres[279] slik at rettighetshaver ikke får tilgang til beviset før motparten er varslet om sikringen og gitt mulighet til å begjære etterfølgende muntlige forhandlinger etter tvisteloven § 28-3 fjerde ledd fjerde punkt, som gir tvisteloven § 32-8 tilsvarende anvendelse. Lovens ordlyd er imidlertid såpass fleksibel her, se særlig at loven bruker uttrykket «kan», at den gir retten mulighet til å komme til rimelige løsninger. Dersom det imidlertid i ettertid skulle vise seg at motparten hadde gode grunner for å holde informasjonen skjult for rettighetshaver, vil en beslutning om å gi rettighetshaver tilgang til bevis uten at motparten er varslet og gitt mulighet til å argumentere for sitt syn,[280] innebære at skaden er skjedd. For disse tilfeller gir tvisteloven § 28-3 femte ledd rettslig grunnlag for å pålegge rettighetshaver en erstatningsplikt. I andre tilfeller kan «skaden» avhjelpes ved å nekte rettighetshaver å føre bevisene på håndhevingsstadiet.[281]

Ordlyden gir som nevnt hjemmel for å gi rettighetshaver tilgang til bevisene før avgjørelsen er endelig. Det kan være særlig hensiktsmessig i tilfeller hvor det haster for rettighetshaver å få tilgang til opplysningene.

Bestemmelsen gir imidlertid ikke hjemmel for å unnlate å varsle motparten så snart bevissikring er gjennomført.[282] Dette reiser et problem i tilfeller hvor rettighetshaver først trenger tilgang til abonnentopplysninger for å kunne vurdere og eventuelt begrunne og spesifisere en begjæring om sikring av datamateriale hos abonnenten. Dette kan særlig være aktuelt i tilfeller hvor rettighetshaver ønsker å vite hvem abonnenten er for å foreta undersøkelser med hensyn til om abonnenten tidligere har foretatt opplastninger.

---

[279] Jeg synes loven har fått en uhensiktsmessig struktur på dette punktet.

[280] Når motparten ikke er varslet vil han heller ikke ha fått anledning til å argumentere for hvorfor det «kan være viktig for motparten å hindre det».

[281] Se særlig tvisteloven § 22-7 om utilbørlig innhentede bevis.

[282] Ordlyden i § 28-3 fjerde ledd annet punkt kunne kanskje gi opphav til et spørsmål om retten kunne vente i seks måneder, men sett i sammenheng med retten til å kreve etterfølgende muntlig behandling, kan det ikke være mye tvil om at lovgiver har ment at motparten skal varsles så snart bevissikringen er gjennomført.

5.4 Spesifikasjonskravet

Ved fremsettelsen av en begjæring om sikring eller tilgang til elektroniske spor hos abonnenten, oppstår spørsmålet om det gjelder noe krav til begjæringens innhold, særlig med hensyn til spesifisering av hvilke bevis rettens avgjørelse skal omfatte.[283]

De prosessuelle bestemmelsene i tvisteloven § 28-3 er tause om dette spørsmålet. **Det rettslige grunnlaget** for at det gjelder et spesifikasjonskrav finner vi i tvisteloven § 28-4 som gir § 26-6 tilsvarende anvendelse.[284] At det gjelder krav til spesifiseringen av en begjæring om bevissikring utenfor rettssak fremgår også av forarbeidene[285] og rettspraksis.[286]

Formålet med spesifikasjonskravet er å gi **motparten** grunnlag for å vite hvilke bevis begjæringen gjelder, og således gi reell mulighet til å vurdere om kravet skal oppfylles frivillig eller hvilke innsigelser han skal komme med.[287] Dette viser også at dette er en side av kontradiksjonsprinsippet.[288]
Et ytterligere formål er å gi **retten** grunnlag for å avgjøre om vilkårene er oppfylt. [289]
Anvendt på denne avhandlingen skal spesifikasjonskravet hindre at retten fatter en beslutning som ikke oppfyller de materielle vilkårene.[290]

---

[283] Jeg legger uten ytterligere problematisering til grunn at dette er et materielt krav, men med den modifikasjon at retten antakelig kan avvise en begjæring uten realitetsbehandling dersom begjæringen er fullstendig upresis. Det rettslige grunnlaget er i så fall en analogi fra tvisteloven § 9-2 annet ledd bokstav c), jf § 16-5 fjerde ledd. Det er et saksbehandlingskrav for avvisning er at begjærende part er gitt mulighet til å rette, jf § 16-5 første ledd, og er gitt veiledning om dette, jf § 11-5.

[284] NOU 2001:32B side 990.

[285] NOU 2001:32B side 990 til § 31-4.

[286] Se avgjørelsene som omtales i dette kapittelet.

[287] Ot.prp.nr.51 (2004-2005)side 204.

[288] Se mer om dette i kapittel xxx

[289] NOU 2001:32B side 990 til § 31-4.

[290] Spesifikasjonskravet har således sterke likhetstrekk med kravene til angivelsen av det straffbare forholdet i en tiltalebeslutning, se Rt 1992 side 445.

I henhold til § 26-6 første ledd[291] skal en begjæring "*spesifiseres slik at det er klart hvilke bevisgjenstander kravet gjelder*". Den kvalifiserende angivelsen er den som «klart» angir hva som begjæres sikret. Utover at ordlyden isolert sett synes å oppstille et strengt krav, sier den lite om hvilke forhold som kvalifiserer.

Ved krav om **bevissikring av abonnentopplysninger** knyttet til en dynamisk IP-adresse,[292] må en begjæring rettet mot internettleverandøren spesifiseres med angivelse av datoen og klokkeslettet for når IP-adressen ble benyttet slik at internettleverandøren kan individualisere abonnenten.[293] [294]
Hensynet til å kunne gjennomføre bevissikring tilsier følgelig at begjæringen presiseres, og dette reiser i alminnelighet få rettslige spørsmål.[295]

Høyesterett har uttalt seg om spesifikasjonskravet i et obiter dictum i Normarc-kjennelsen Rt.2006 side 626.
Faktum i saken var at selskapet Normarc AS mistenkte at tidligere ansatte hadde kopiert og tatt med seg opphavsrettsbeskyttet informasjon og annet elektronisk materiale til et konkurrerende selskap NSM. Normarc begjærte og fikk medhold i at det skulle foretas **uvarslet bevissikring** hos det NSM, ved at namsmannen med medhjelpere skulle speilkopiere alt materiale på selskapets servere, Cd'er, tapes og andre lagringsmidler, på arbeidsstasjonene til 4 tidligere ansatte, samt alle backup-filer.
I den etterfølgende muntlige forhandlingen, var det relevante **spørsmålet hvilke krav som måtte stilles til spesifiseringen av beslaget**. NSM anførte at begjæringen på sikringsstadiet ikke var tilstrekkelig spesifisert, slik at materialet måtte tilbakeleveres.
NSM anførte også at <u>rettssikkerhetsgarantier</u> tilsa at det måtte spesifiseres og at det

---

[291] Bestemmelsen viderefører individualiseringskravet som fulgte av tvistemålsloven § 253 første ledd, se ot.prp. nr.51 (2004-2004) til § 26-6 side 467.

[292] Se kapittel 2 om sondringen mellom dynamiske og faste IP-adresser.

[293] Rt.1999 side1944 – en straffesak hvor retten la tilsvarende individualiseringskrav til grunn for at politiet skulle få tilgang til abonnentopplysninger.

[294] I Rt. 2007 side 920 avsnitt (46), legger retten til grunn at angivelse av kontonummeret er tilstrekkelig til å individualisere bankkontoen som begjærende part krevde kontoutskriften til.

[295] Siden dette uten videre lagt til grunn i Altibox-kjennelsen, kan vi slutte at dette ikke representerte et grensetilfelle.

ikke kunne være adgang til å foreta et "**altomfattende generalbeslag**". For kjæremålsutvalget var **spørsmålet** også om lagmannsretten hadde tatt feil da de hadde lagt til grunn at begjæringen måtte spesifiseres **før** bevissikringen ble foretatt, og at det således ikke var anledning til å utfylle denne før utleveringen. **Kjæremålsutvalget** mente at lagmannsretten hadde foretatt en gal lovtolkning på dette sistnevnte spørsmålet og opphevet lagmannsrettens avgjørelse. Spørsmålet om spesifikasjonskravet var derfor ikke avgjørende for sakens utfall, men ble likevel kommentert i et **obiter dictum**. **Avgjørelsens overføringsverdi til vårt tema:** Høyesterett gir uttrykk for at man ikke generelt kan angi presise spesifikasjonskrav, og at kravene må fastsettes etter en **konkret vurdering** i det enkelte tilfellet basert på de **formål** og **reelle hensyn** som gjør seg gjeldende. I overensstemmelse med det **viser** avgjørelsen også at **kravene til spesifisering forut** for selve sikringen av bevisene må være mindre strenge enn forut for **utlevering av bevisene**.

Siden det gjennomgående gjør seg gjeldende forskjellige rettssikkerhetshensyn og personvernhensyn ved gjennomføring av henholdsvis en begjæring om sikring og en begjæring om tilgang, sondrer jeg mellom disse stadier når jeg nedenfor redegjørelsen nærmere for innholdet i spesifikasjonskravet.

5.4.1 *Kravene til spesifikasjon av en begjæring om sikring:*

Basert på uttalelsene fra Høyesterett i Normarc-saken blir spørsmålet i det følgende hvilke hensyn som kan gjøre seg gjeldende ved sikring av elektroniske spor hjemme hos privatpersoner og i en bedrift. I tillegg til formålene som er angitt ovenfor, og som gjennomgående vil tale for større grad av spesifisering, skal også nevnes at kravet må «ses i lys av muligheten for å foreta en nærmere individualisering og kan ikke stilles så høyt at det kan hindre klarlegging av faktiske forhold av betydning i saken».[296] I overensstemmelse med formålet med tvisteloven § 1-1 må retten også ta i betraktning de økonomiske konsekvensene av å stille for høye krav til spesifisering av begjæringen. Videre må ikke kravene være så strenge at det i stor grad reduserer den reelle adgangen til å få brakt et krav inn for domstolen.[297] [298]

[296] Rt. 2004 side 442 avsnitt 30.

[297] Ot.prp. nr. 51 (2004-2005) punkt 1.2 side 14.

En begjæring om sikring av bevis i form av speilkopiering av **alle lagringsmedier** hos abonnenten vil i de fleste tilfeller som utgangspunkt[299] være for generelt angitt.[300] Det er mulig å angi dette mer presist, og retten har behov for en noe mer spesifisert angivelse for å se om hvert enkelt av disse bevis «kan få betydning i en tvist».[301] Retten må ha grunnlag for å vurdere om beviset kan ha noen som helst beviskraft i forhold til påstandsgrunnlaget, og retten trenger grunnlag for å vurdere om det påstandsgrunnlaget beviset skal dokumentere kan være relevant i en senere tvist.
Bevissikring hos personer er inngripende, og generelle rettssikkerhetsbetraktninger tilsier at begjæringen spesifiseres. For privatpersoner gjør sterke personvernhensyn seg gjeldende særlig ved speilkopiering i en privatpersons hjem. Formålet tilsier dermed at begjæringen spesifiseres så godt at retten kan foreta en realistisk forholdsmessighetsvurdering, herunder bør det også angis om det er mulig eller sannsynlig at andre enn motparten har lagret informasjon på de aktuelle lagringsmedier.

Et utgangspunkt kan være de elektroniske bevis som genereres hos abonnenten og andre ved opplastningen, og jeg viser her til redegjørelsen ovenfor i kapittel 2. I den grad det er mulig å individualisere de enkelte spor ved å nevne tidspunktet for opprettelsen av de forskjellige bevis, så må det gjøres. I de tilfeller hvor det er mulig at flere beboere/arbeidstakere har benyttet aktuelle datamaskiner, kan begjæringen spesifiseres slik at det bare kreves sikring av spor som finnes på en bestemt brukers brukerkonto.

Hvilke krav som nærmere stilles må bero på de konkrete omstendigheter. Siden det ikke er gitt at rettighetshaver skal få tilgang til alle de bevis som er sikret, kan personvernhensyn ivaretas ved å kreve ytterligere spesifikasjon for å få tilgang til de

---

[298] På opphavsrettens område er TRIPS-avtalen et støtteargument for dette.

[299] Når jeg skriver i utgangspunktet er det fordi § 26-6 annet ledd åpner for å lempe på spesifikasjonskravet.

[300] NOU 2001:32B side 978 til punkt 29.1. Hvor det uttales at retten har behov for et konkret faktum å anvende jussen på.

[301] Se behandlingen av relevanskravet i kapittel xxx.

enkelte bevis. Dette reiser dermed spørsmål om hvilke krav til spesifikasjon som gjelder for å få medhold i en begjæring om tilgang. Dette er det neste temaet.

5.4.2 Spesifikasjonskravet ved krav om tilgang til bevisene:

På dette stadiet er bevisene sikret, og hensynet til rask behandling får da gjennomgående mindre vekt.
Når kravet er utlevering av opplysningene til rettighetshaver er det særlig personvernhensyn som begrunner at man må stille strengere krav til spesifiseringen av begjæringen. I mange tilfeller kan IP-adressen og det aktuelle datautstyret hos abonnenten være benyttet av flere enn bare abonnenten. Hensynet til tredjemanns personvern er derfor også relevant. Disse hensyn tilsier at begjæringen spesifiseres slik at ikke uvedkommende får tilgang til informasjon som ikke er relevant og som er personvernsensitiv eller som motparten eller tredjemann ikke ønsker at rettighetshaver skal få kunnskap om.[302]

For det tilfellet at begjærende part bor i et bokollektiv hvor oppkoplingen til internett skjer via en trådløs ruter, vil alle i kollektivet være potensielle krenkere, og det kan være vanskelig å klarlegge hvilken person som står bak opplastningen uten å få tilgang til informasjon som bare gjelder øvrige brukere av datautstyret.[303]

Mot at spesifikasjonskravet skal forstås strengt i slike tilfeller er det forhold at dette kan avhjelpes ved at begjærende part ikke gis tilgang til bevisene før motparten er gitt anledning til å kommentere bevissikring i den etterfølgende muntlige behandling. Det kan også avhjelpes ved å overlate til retten eller en representant for namsmyndighetene å undersøke bevisene.[304]

---

[302] Dette kan vi kalle «overskuddsinformasjon», se Yulex 2008 side 169, Hjort.

[303] Siden alle brukerne i utgangspunktet har forklaringsplikt/vitneplikt er ikke dette til hinder for å kreve fremlagt bevis som er generert av andre brukere på abonnentens datamaskin. Se tilsvarende synpunkter i Rt. 2002 side 442 avsnitt 32-33.

[304] Se kapittel 6 om de forskjellige sikringsmetodene.

De spor som genereres på en datamaskin ved en ulovlig opplastning vil variere med hensyn til synbarhet, lagringssted og varighet. Dette påvirkes dels av automatiske innstillinger og egendefinerte innstillinger. I den utstrekning egendefinerte innstillinger synes å begrense muligheten til å klarlegge hvem som har generert sporene, og de aktuelle brukere av datamaskinen ikke bidrar til oppklaring ved forklaringer, tilsier dette at retten lemper på spesifikasjonskravet.

Risikoen for "misbruk" av systemet tilsier at det settes krav til spesifikasjon i begjæringen, men kan også i en viss grad avhjelpes noe ved bestemmelsen i § 28-3 femte ledd som angir et ansvarsgrunnlag for (på nærmere angitte vilkår) å pålegge begjærende part å betale **erstatning** for den **skade** motparten har lidt som følge av en ubegrunnet begjæring om bevissikring.

For å hindre begjærende part å kikke motparten i kortene, kan man for eksempel kreve at rettighetshaver selv legger frem dokumentasjon på at hun har en kopi av den informasjonen som anføres å være krenket.[305] Dette er særlig aktuelt dersom begjæringen gjelder tilgang til programkode hos motparten.

Hensynet til å begrense utgiftene på tilgangsstadiet kan også tilsi et strengere krav. Normarc-saken har vist at et sentralt hensyn på sikringsstadiet bør være å begrense omfanget av det som skal kopieres, for dermed å redusere den etterfølgende gjennomgangen av materialet og dermed redusere kostnadene. Hensynet illustreres godt av Normarc-saken hvor det ble sikret informasjon tilsvarende flere millioner A4-ark.

[305] Se TRIPS-avtalen artikkel 50 nummer 5.

6 Den praktiske gjennomføringen - Særlige prosessuelle spørsmål

I kapittel 3 redegjorde jeg oversiktlig for innholdet i rettsvirkningene sikring og tilgang til bevis. Redegjørelsen nedenfor bygger på dette og de øvrige kapitlene.
Tvisteloven kapittel 28 angir ikke noe uttrykkelig om fremgangsmåten, men henviser i tvisteloven § 28-4 til de alminnelige bevisreglene, herunder reglene om tilgang til realbevis i lovens kapittel 26 og reglene for bevisopptak i rettssak, i kapittel 27, så langt de passer.[306]
Gjennomføringen av sikring av bevis reiser spørsmål om hvem som skal foreta sikringen og hvilken sikringsmetode som skal benyttes. Endelig oppstår spørsmål om hvordan beviset eller de opplysninger beviset inneholder skal gjøres tilgjengelig for rettighetshaver.

6.1 Spørsmålet er hvem som skal sikre beviset

6.1.1 Utgangspunktet – retten har kompetanse:

I følge tvisteloven§ 28-4, jf. § 27-2 tredje ledd, skal/kan bevisopptaket "*foretas av den rett som har saken*".
Hva gjelder sikring av **abonnentopplysninger** vil en hensiktsmessig fremgangsmåte være at ISP-en pålegges å oversende den relevante informasjonen til retten.[307]
For det tilfellet at bevissikringen går ut på å sikre en **forklaring fra parter eller vitner**, vil det være praktisk at en dommer foretar bevisopptak i rettslokalet.[308] Det vil også

[306] NOU 2001:32B § 31-4 side 990 som presiseres at bevisforbudsreglene og bevisfritaksreglene kommer tilsvarende til anvendelse.

[307] Denne fremgangsmåten ble valgt i Altibox-saken.

[308] Ved varslet bevissikring vil denne gjennomføringsmåten medføre at både rettighetshaver og antatt motpart blir innkalt og får anledning til å stille spørsmål i overensstemmelse med kontradiksjonsprinsippet.

medføre at de hensyn som ligger til grunn for bevisumiddelbarhetsprinsippet langt på vei ivaretas.

For det tilfellet at det skal foretas uvarslet bevissikring av **elektroniske spor hos abonnenten**, har dommeren kompetanse til å reise ut til abonnenten, men dette er helt upraktisk, se nedenfor.
Sett fra motpartens ståsted, kan bevissikringen oppleves som problematisk, særlig dersom bevissikring blir konfliktfylt. I disse tilfellene tilsier hensynet til rettens nøytralitet og særlig at motparten opplever retten som nøytral, og dermed dennes tillit til at domstolen fatter en materielt riktig avgjørelse, at retten ikke er til stede ved den praktiske gjennomføringen av bevissikringen.[309]

6.1.2 Kan dommeren la seg bistå av namsmyndighetene?

Statens apparat for gjennomføring av fullbyrdelsesavgjørelser, herunder fullbyrdelsesdommer og kjennelser om midlertidig sikring,[310] er namsmyndighetene.[311] Spørsmålet her er om retten kan overlate gjennomføringen til namsmannen.

I tvl § 33-5 første ledd, som regulerer gjennomføringen av en arrest, har retten kompetanse til å overlate dette til namsmannen, og i følge forarbeidene bør dette overlates til namsmannen i de tilfeller hvor gjennomføringen nødvendiggjør forretning utenfor domstolens kontor.312 Siden dette også kan være tilfellet ved bevissikring, tilsier det at retten også på bevissikringsstadiet skal kunne overlate dette til namsmannen.

Til dette kommer at namsmannen har et apparat, herunder personer som har erfaring fra denne type saker, og det tilsier at det er hensiktsmessig å overlate dette til namsmannen.

---

[309] At dette er et relevant hensyn, kommer blant annet til uttrykk i ot.prp. nr. 51 (2004-2005) side 34 og tvistelovens formålsparagraf, jf. § 1-1, samt EMK artikkel 6 som slår fast at partens rett til å få avgjørelsen truffet av en domstol som er objektiv og uavhengig av sakens aktører.

[310] Tvisteloven kapittel 32-34.

[311] Lov om tvangsfullbyrdelse av 26.juni 1992 nr.86 første del, kapittel 2, særlig § 2-2, jf. § 2-1.

[312] Ot.prp. nr.65 (1990-1991) side 279.

Som nevnt ovenfor vil dette også styrke hensynet til rettens nøytralitet og tillit i befolkningen. Namsmannens kompetanse til å bistå ved sikring av bevis er lagt til grunn i flere avgjørelser.[313] [314] På dette grunnlaget konkluderer jeg med at retten har anledning til å la namsmannen bistå.

For det tilfellet at begjæringen går ut på å sikre elektroniske spor fra abonnentens datamaskin og andre elektroniske lagringsmedier vil de aktuelle bevisene lagres og oppbevares elektronisk, dels på de harddisker som er montert inn i datamaskinen og andre eksterne lagringsmedier, eksempelvis cd-er og tapes.[315] Slike data er svært følsom og enhver bruk av datamaskinen vil kunne endre dataene.

Dersom namsmannen ikke besitter særlig kunnskap om dette foreligger det en risiko for at beviset ikke sikres på riktig måte og igjen en risiko for at beviset går tapt eller mister bevisverdi.[316] **Dette reiser spørsmål ved om det er anledning til å oppnevne sakkyndige med relevant kompetanse til å bistå namsmannen ved bevissikringen**.[317]

Tvisteloven § 28-4, jf. § 27-2 fjerde ledd, jf. § 25-2 åpner for at det kan oppnevnes sakkyndige[318] dersom dette er «nødvendig» for å sikre et «forsvarlig faktisk avgjørelsesgrunnlag», og spørsmålet vil således bero på en konkret vurdering.

Ved vurderingen av hvilke elektroniske spor det skal gis tilgang til, viser redegjørelsen i neste punkt at enkelte sikringsmetoder for elektroniske spor nødvendiggjør en sortering av det sikrede materialet. I disse tilfellene vil det også være aktuelt å oppnevne sakkyndige til å foreta denne sorteringen.[319]

---

[313] Rt.2006 side 626 Normarc-kjennelsen.

[314] RG 2007 side 736 Funbox as, Dun & Bradstreet saksnummer; 10-197602TVI-OTIR/05, LB-2010-202642.

[315] Se kapittel 2.

[316] Willassen (2006) side 6-7.

[317] Datarekonstruksjonsselskapet IBAS as er et praktisk eksempel.

[318] NOU 2001:32B § 31-4 side 990.

[319] Retten har kompetanse til å pålegge aktørene taushetsplikt, jf tvisteloven § 22-12.

6.2 Har retten kompetanse til å gjennomføre bevissikring med tvang?

Et særskilt spørsmål oppstår for de tilfeller hvor den som oppbevarer beviset nekter å la retten/namsmannen å få beviset eller å slippe inn i lokalet hvor beviset befinner seg.

For det tilfellet at gjennomføringen av bevissikringen går ut på å sikre bevis hos motpart/tredjemann, innebærer dette at namsmannen må få tilgang til lokalet hvor bevismidlene er. I alminnelighet foreligger en risiko for at motparten vil nekte namsmannen tilgang. Siden dette vil kunne medføre at formålet med en den uvarslede bevissikring forfeiles, oppstår spørsmålet om retten kan pålegge motparten å gi tilgang til lokalet hvor beviset er.

For at motparten kan ilegges denne plikten, er at dette er lagt til grunn i flere rettsavgjørelser, herunder i Funbox-kjennelsen[320] og Normarc-kjennelsen.[321]

For det tilfellet at motparten nekter å etterkomme pålegget eller ikke er hjemme, oppstår spørsmålet om det er adgang til å bryte seg inn. Tvisteloven § 28-4, jf. § 27-5 første ledd om formålet, oppstiller i utgangspunktet ingen begrensninger med hensyn til hvilke tiltak som kan gjøres. På annen side må dette anses som et inngrep, og **legalitetsprinsippet** krever derfor at det foreligger et rettslig grunnlag. I så henseende tilsier hensynet til forutberegnelighet og klarhetskravet at den generelle formålsangivelsen i tvl. § 27-5, ikke oppfyller dette kravet. Det kreves således et annet rettslig grunnlag for at man kan bryte seg inn hos abonnenten.[322]

---

[320] TAHER-2006-184362. Foruten at det i kjennelsen vises til at formålet med bevissikringen ivaretas på denne måten, kan ikke det rettslige grunnlaget for plikten utledes av kjennelsen.
Et mulig rettslig grunnlag, er den prosessuelle edisjonsplikten i tvl. § 28-4, jf. tvl.26-5 første ledd, som pålegger "*enhver…å stille til disposisjon…bevisgjenstander*", og som ifølge ordlyden og NOU 2001:32 § 29-5 annet avsnitt side 979, innebærer en plikt til å gi adgang til beviset.

[321] Rt.2006 side 626.

[322] Dette ble også lagt til grunn i Funbox-kjennelsen, TAHER-2006-184362.

6.3 Hvilken sikringsmetode kan anvendes ved sikring av elektroniske spor

Om sikringsmetoden fastsetter tvisteloven § 28-4, jf. § 27-5 første ledd at denne skal være egnet til å ivareta formålet med bevissikringen, som vil være å sikre bevisets pålitelighet og integritet.[323] [324]Som nevnt kan det tenkes flere innvendinger fra abonnenten om at denne ikke står bak opplastingen, og begjærende part vil av den grunn være interessert i at spor som kan underbygge/avkrefte en slik innsigelse sikres. Det er flere metoder som kan tenkes anvendelige for sikring av elektronisk lagret materiale.[325]

Ved filkopiering er det kun de filer som spesifikt angis som kopieres. For det tilfellet at filnavnet på filen som skal sikres er endret eller slettet, vil ikke filkopiering avhjelpe dette problemet. Ved filkopiering foreligger det således en risiko for at resultatet av bevissikring blir mangelfullt.[326]

Siden speilkopiering også sikrer metadata, er dette en hensiktsmessig og praktisk sikringsmetode.

6.4 Spørsmålet om hvordan rettighetshaver får tilgang til bevisene:

Utgangspunktet finnes i § 28-4 jf. § 26-7 tredje ledd, hvor det fremgår at retten i "*nødvendig utstrekning*" fastsetter "*måten beviset skal gjøres tilgjengelig på*", og dette tilsier at det er retten som skal ta den endelige avgjørelsen. Forutsetningen er her selvfølgelig at de materielle vilkårene for å gi rettighetshaver tilgang til bevisene er oppfylt, herunder at rettighetshaver har spesifisert begjæringen om tilgang i

---

[323] NOU 2001:32B side 986 § 30-5.

[324] Ved valg av sikringsmetoder må retten også kunne beslutte en hensiktsmessig sikringsmetode basert på rettighetshavers begjæring. Det følger også av tvisteloven § 28-4, jf. § 25-4 at retten fastsetter et mandat for sakkyndiges fremgangsmåte ved bevissikringen, og retten kan også pålegge partene å komme med forslag, se NOU 2001:32B side 974 § 28-4.

[325]Eksempelvis kan namsmannen ta med seg datamaskiner og andre lagringsmedier, ta bilde av skjermbildet, elektroniske kopi. Siden fysisk beslag av de elektroniske lagringsmediene medfører at innehaver ikke kan benytte disse, kan dette få uheldige følger, herunder økonomiske eller praktiske konsekvenser. Dette alternativet vil også kunne oppleves som mer inngripende enn om det aktuelle innholdet kopieres, og det vil således kunne være et uforholdsmessig inngrep å ta med lagringsmediene fremfor å kopiere disse.

[326] Avsnittet er basert på Ot.prp. nr.1 (2008-2009) punkt 22.5.2.2 side 121-122.

overensstemmelse med kravene. Som nevnt ovenfor skal motparten også varsles og gis rett til å kreve muntlige forhandlinger før rettighetshaver får tilgang til bevisene.

7 Oppsummering og bemerkninger til Høringsnotat (2011).

Redegjørelsen viser at for at rettighetshaver skal kunne håndheve sine rettigheter overfor opphavsrettskrenkelser på Internett vil i de fleste tilfeller være av avgjørende betydning at hun i det minste gis tilgang til abonnentopplysninger. Redegjørelsen viser også at rettighetshaver er nødt til å be om domstolenes bistand for å få utlevert slike opplysninger. Dette er selvfølgelig kostbart, og gir slik sett et dårlig vern til små rettighetshavere.

Kulturdepartementet har foreslått nye regler som skal gjøre det enklere for rettighetshaver å få tilgang til slike «identifiserende» opplysninger. Blant annet foreslås det at Medietilsynet skal overta domstolens oppgave med å foreta vurderingen av om internettilbyderne skal pålegges å gi tilgang til abonnentopplysningene. Siden dette nok vil ivareta hensynene til rask og billig saksbehandling, er dette etter min mening et godt forslag.

Et mulig tiltak er også varselbrev til motparten.[327] Dette er ment å skulle ha en preventiv og informativ virkning. Det kan også stilles spørsmål ved om dette er relevant i en medvirkningsvurdering. I avhandlingen har jeg påpekt forskjellige innsigelser abonnenten kan komme med når han blir konfrontert med en mistanke om opplastning. Dersom rettighetshaver kan påvise at abonnenten tidligere har fått varselbrev[328] og likevel ikke har foretatt tiltak for å hindre at hans internettilgang benyttes til opplastninger, kan dette være et bevismoment mot abonnenten, men det kan nok også få betydning ved at krenkelsene blir påregnelige for abonnenten, og det vil være relevant i forhold til et erstatningsansvar på grunnlag av uaktsomhet, og for så vidt også et mulig strafferettslig medvirkningsansvar etter åndsverkloven § 54.

---

[327] Se Høringsnotatet (2011) kapittel 4.

[328] Dette må ses i sammenheng med Høringsnotatets forslag om at rettighetshaverne skal kunne lage og lagre registre med abonnentopplysninger.

Høringsutkastet foreslår at endringene gjøres i åndsverkloven fremfor i tvisteloven. Hva gjelder særlig de foreslåtte unntak fra varslingsplikten som kan gi rettighetshaver mulighet til å foreta nærmere vurderinger av om andre sikringstiltak skal iverksettes, er også aktuelle for andre saksøkere, og dette vil nok stadig bli mer aktuelt etter hvert som større og større deler av dagen brukes på Internett, og disse reglene kunne nok med fordel ha vært innført i tvisteloven.

8 Litteraturliste

Se http://www.ub.uio.no/skrive-referere/hvordan-referere/

Norske lover:

- Lov om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) av 15.april 2011 nr.11.
- Lov om mekling og rettergang i sivile tvister av 17.juni 2005 nr.90 (tvisteloven).
- Lov om konkurranse mellom foretak og kontroll med foretakssammenslutninger av 5.mars 2004 nr. 12 (konkurranseloven)
- Lov om elektronisk kommunikasjon av 4.juli 2003 nr.83 (ekomloven).
- Lov om tvangsfullbyrdelse av 26.juni 1992 nr.86 (tvangsfullbyrdelsesloven).
- Lov om rettergangsmåten i straffesaker av 22. mai 1981 nr. 25 (straffeprosessloven).
- Lov om skadeserstatning av 13.juni 1969 nr. 26 kapittel 4 (skadeserstatningsloven).
- Lom om opphavsrett til åndsverk m.v. av 12. mai 1961 nr. 2 (åndsverksloven).

- Lov om rettergangsmåten for tvistemål av 13. august 1915 nr. 6 (opphevet) (tvistemålsloven).

Utenlandske lover:

- Svensk rett: Lag av 30. desember 1960 nr. 729 om upphovsrätt till litterära och konstnärliga verk, jf §§ 56a til 56h.
- Dansk rett: Retsplejeloven av 09-11-2010, kapitel 57a.

Forarbeider:

- Prop. 49 L (2010-2011) Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett).
- NOU 2001:32 Bind A Rett på sak, Lov om tvisteløsning (tvisteloven).
- NOU 2001:32 Bind B Rett på sak, Lov om tvisteløsning (tvisteloven).
- NOU 2009:1 Individ og integritet, Personvern i det digitale samfunnet.
- Ot.prp. nr.51 (2004-2005) Mekling og rettergang i sivile tvister (tvisteloven).
- Ot.prp. nr. 33 (2003-2004) Om lov om endringer i tvistemålsloven (*bevisopptak utenfor rettssak*).
- Høringsnotat: Endringer i åndsverksloven (tiltak mot ulovlig fildeling og andre krenkelser av opphavsretten m.m. på Internett), av 19.mai 2011, Kulturdepartementet.

Forskrifter:

- FOR-2004-02-16-401: Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften).

Internasjonale avtaler:

- Agreement on Trade-Related Aspects of Intellectual Property Rights, 1. Januar 1995.
- Avtale av 15.april 1994 om opprettelsen av Verdens Handelsorganisasjon (World Trade Organization). Norge ratifiserte avtalen 7.desember 1994.

Konvensjoner:

- Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter. Roma, 4.november 1950.(EMK).

Tidsskrifter og artikler:

- Willassen, Svein. *Om speilkopiering av data i sivile tvister*. Lov & Data nr.87 2006, side 6-7.
- Willassen, Svein. *Tidsstempel og elektronisk bevis*. Lov & Date nr. 98 2009, side 13.
- Jonathan L. Moore. "*Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of ESI in Civil Litigation*"**.** Jurimetrics, Volume 50, Winter 2010, Number 2, side 147-193.
- Vincents, Okechukwu Benjamin. "*When Rights Clash Online: The Tracking of P2p Copyright Infringements Vs. the EC Personal Data Directive*". International Journal of Law and Information Technology, Volume 16 Number 3. Oxford University Press 2007, side 270-296.

Nettdokumenter:

- Teknologirådet. *IP-adresser og oppkoplingslogger*. 2007. http://www.teknologiradet.no/FullStory.aspx?m=104&amid=3130 [sitert 25. april 2011].
- Teknologirådet: *Spor på PC og brannmur*. 2005. http://www.teknologiradet.no/FullStory.aspx?m=104&amid=490 [sitert 10. februar 2011].
- Willassen, Svein. *Sikring av elektroniske spor*. 2007. Ibas AS: http://www.willassen.no/svein/pub/espor.pdf. [sitert 2. november. 2010]
- Unuth, Nadeem.What is a Protocol? About.com Guide

http://voip.about.com/od/voipbasics/g/protocoldef.htm [sitert 3. november 2010].

- NORSISS - Norsk Senter for Informasjonssikring. Trådløst nettverk: http://www.norsis.no/veiledninger/teknisk/Tradlost_nettverk.html [sitert 29. mai. 2011]

Litteratur/ Bøker:

- Rognstad, Ole-Andreas, Stuevold Lassen, Birger. Opphavsrett. Oslo 2009. Universitetsforlaget.
- Schei, Tore med flere. Tvisteloven Kommentarutgave Bind I og Bind II. Oslo, Bergen og Skien 2007. Universitetsforlaget.
- Torgersen, Runar. Ulovlig beviserverv og bevisforbud i straffesaker. Oslo 2009. Lobos Media AS.
- Casey, Eoghan. Digital evidence and computer crimes. Forensic science, computers and the internet. Second edition 2004. Elsevier Academic Press.

9 Lister over tabeller og figurer m v