RETTEN PÅ FREDERIKSBERG
RETSBOG

Den 20. april 2020 kl. 13.00 holdt Retten på Frederiksberg offentligt retsmøde i retsbygningen.

Dommer Dan Bjerring behandlede sagen.

Sag BS-1440/2019-FRB

Copyright Management Services Ltd.
(advokat Jeppe Brogaard Clausen)

mod

L
(advokat Mikkel Kleis)

Ingen var tilsagt eller mødt.

Retten bemærkede, at Østre Landsret ved domme af 8. april 2020 i sagerne BS-39423/2019-OLR, BS-41550/2019-OLR og BS-41559/2019-OLR har fastslået, at Copyright Management Services Ltd. ikke har godtgjort, at selskabet har søgsmålskompetencen til i eget navn at føre sag om de tre film, som disse sager angik. Ved dommene afviste landsretten derfor sagerne fra domstolene.

Landsrettens præmisser i sag BS-39423/2019-OLR, der er enslydende med præmisserne i sag BS-41550/2019-OLR, er som følger:

> "Copyright Management Services Ltd. har til støtte for, at selskabet er påtaleberettiget henvist til en aftale, underskrevet den 8. og 9. juni 2016, om "generiske tjenester", indgået med det cypriotisk indregistrerede selskab M.I.C.M., som selv har fået overdraget

rettighederne af filmens producent, det amerikanske selskab Third Degree Films, Inc.

Dette understøttes imidlertid ikke af det fremlagte materiale. Landsretten har herved navnlig lagt vægt på, at aftalen om generiske tjenester alene er fremlagt i uddrag og fremstår som indgået mellem en rettighedshaver på den ene side og M.I.C.M. på den anden side. I henhold til aftalen antager rettighedshaveren bl.a. M.I.C.M. til at organisere retssager til håndhævelse af ophavsrettigheder. Det fremgår ikke af det fremlagte, at M.I.C.M skulle have overdraget nogen rettigheder til den anden part. I aftalen omtales endvidere et unavngivet advokatkontor, men dette ses ikke at have underskrevet aftalen som part. Allerede derfor godtgør aftalen ikke, at M.I.C.M. som rettighedshaver skulle have overdraget en påtaleret til Copyright Management Services Ltd.

Dertil kommer, at det af registreringen i "Companies House" fremgår, at Copyright Collections Ltd., der er angivet som part i aftalen, flere måneder før aftalens indgåelse skiftede navn til Copyright Management Services Ltd.

Landsretten finder på den baggrund, at Copyright Management Services Ltd. ikke har godtgjort, at selskabet har søgsmålskompetence til at føre sagen i eget navn. Den fremlagte mail af 9. oktober 2019 fra en person ved navn Ioannis Papapetrou, der bl.a. oplyser at være direktør i M.I.C.M., og at selskabet har overdraget retten til i Danmark at anlægge sag for ophavsretskrænkelser, herunder i denne sag for landsretten, kan ikke føre til en anden vurdering.

Landsretten tager derfor appellantens principale påstand til følge, således at den indankede dom ophæves, og sagen afvises fra domstolene."

Disse domme ligger i forlængelse af Retten på Frederiksbergs kendelse af 23. januar 2020 i sag BS-43373/2018-FRB, hvorved Retten på Frederiksberg ligeledes afviste sagen (bl.a.) under henvisning til, at der ikke kunne lægges vægt på den samme "Generic Service Agreement", som landsretten nu også har taget stilling til.

Det er samme dokument, som CMS har påberåbt sig i nærværende sag, og nærværende sag skal dermed også – alene af den grund – afvises fra domstolene.

Retten finder imidlertid anledning til også at bemærke følgende:

Indledning

Nærværende sag er én af over 150 sager, som selskaberne Copyright Management Services Ltd. (CMS) og M.I.C.M. - MIRCOM International Content Management & Consulting Ltd. (MIRCOM) tilsammen har anlagt alene ved Retten på Frederiksberg med påstand om, at sagsøgte skal betale 7.500 kr. for ulovlig download og deling af et angiveligt ophavsretligt beskyttet værk via et såkaldt peer-to-peer-, P2P-, BitTorrent-netværk.

Efter de udtalelser, som CMS og MIRCOM's advokat har givet til forskellige medier og efter antallet af borgere, der er berørt af de kendelser, som Retten på Frederiksberg tidligere har afsagt om, at borgernes identitets- og adresseoplysninger skulle udleveres af borgernes teleselskaber til CMS og MIRCOM, kan det endvidere lægges til grund, at nærværende sag er én ud af flere tusinde, måske 50.000 eller flere, alene i Danmark, hvor CMS og MIRCOM har sendt breve ud til borgerne med krav om betaling for ulovlig download og deling af film via BitTorrent-netværk.

Efter i øvrigt offentlige tilgængelige oplysninger, herunder på Maverickeye UG's hjemmeside, der dog ikke ses opdateret siden januar 2018, og fra diverse svenske og norske medier, samt oplysningerne fra andre retssager, herunder EU-Domstolens sag C-597/19, kan det endvidere lægges til grund, at CMS og MIRCOM tilsammen har opnået, eller har ønsket at opnå, identitets- og adresseoplysninger på i hundredtusindvis af europæiske borgere.

Der er herunder tale om borgere i Finland, Sverige og Norge, hvor CMS er, eller har været, repræsenteret af samme advokat eller advokatfirma, som i Danmark, og der er ligeledes tale om, at man også i disse lande på baggrund af de indhentede oplysninger har skrevet til et meget stort antal borgere med krav om betaling for ulovlig download og deling af film på tilsvarende vis, som det er sket forud for sagsanlægget i denne sag og de øvrige sager i sagskomplekset ved Retten på Frederiksberg.

Det har i offentligheden, herunder bl.a. også i Norge og Sverige, været debatteret og kritiseret – herunder fra advokatside – at Njord Law Firms udsendelse af disse breve, og fremgangsmåde i øvrigt, i vidt omfang har været egnet til at presse borgere, der meget muligt har været uskyldige, til at indgå forlig.

En sådan kritik er bl.a. også kommet til udtryk i et brev af 24. januar 2017, som Forbrukerrådet i Norge og IKT-Norge ifølge oplysninger på Forbrukerrådets hjemmeside har sendt til advokat Jeppe Brogaard Clausen med opfordring til at stoppe med at udsende de pågældende breve, herunder under henvisning til, at man fremkom med urigtige og vildledende oplysninger og ikke ville kunne bevise, at man havde et krav mod de pågældende borgere.

Forbrukerrådet i Norge har endvidere på deres hjemmeside i et opslag den 5. juni 2018 under overskriften "Ikke betal svindelkrav fra Hengeler & Latham" sammenstillet breve fra advokatfirmaet Hengeler & Latham med de breve, der er udsendt af Njord Law Firm. Det fremgår bl.a., at Hengeler & Latham i de pågældende breve henviser til, at deres bevis er tilvejebragt ved anvendelse af Maverickeye UG, og dermed er der tale om samme fremgangsmåde i forhold til den tekniske fremskaffelse af beviser, som CMS og MIRCOM også har baseret samtlige sager i Danmark på.

Advokat Jeppe Brogaard Clausen er i en artikel, bragt i K-News den 13. januar 2020, citeret for, at der er indgået forlig i 60 procent af sagerne i Danmark, og at dette ikke omfatter retssager.

Da de breve, der indgår i sagskomplekset ved Retten på Frederiksberg, og som må betegnes som standardbreve, alle lægger op til et forlig mod betaling af nogle tusinde kroner, og da retten også har kunnet konstatere, at der i en række sager er indgået forlig på et større beløb end de 7.500 kr., der var stævnet for, og i hvert fald i et enkelt tilfælde forlig på 39.000 kr., kan der, selv efter et forsigtigt skøn, være tale om, at sagerne samlet set – over hele Europa – har indbragt, eller har potentiale til samlet at indbringe, CMS og MIRCOM et trecifret millionbeløb.

CMS og MIRCOM er imidlertid ikke indehavere af ophavsretten til de film, de har anlagt sag om – og efter landsrettens ovennævnte domme af 8. april 2020 har de altså heller ikke på det i disse sager fremlagte grundlag søgsmålskompetence til i eget navn at forfølge eventuelle krænkelser af ophavsretten. Der foreligger endvidere ingen oplysninger om, i hvilket omfang de beløb, som sagerne – indenretligt såvel som udenretligt – har indbragt, er kommet indehaverne af ophavsretten til gode.

Østre Landsrets domme af 8. april 2020 kan siges at ligge i forlængelse af de i alt 13 sager, som Retten på Frederiksberg tidligere har afvist med den begrundelse, at CMS og MIRCOM ikke var rette sagsøger. Disse sager med tilhørende retsbøger er omtalt på Retten på Frederiksbergs hjemmeside ved opslag den 26. marts 2020.

Retten på Frederiksberg kan imidlertid konstatere, at det forhold, at såvel Retten på Frederiksberg som Østre Landsret har fastslået, at CMS og MIRCOM har ageret på et påstået aftalegrundlag, der ikke gør selskaberne til rette sagsøger i sagerne, ikke for nærværende har fået CMS og MIRCOM til af egen drift at hæve samtlige de resterende verserende sager ved Retten på Frederiksberg.

Retten har endvidere bl.a. noteret sig, at Ritzau har citeret advokat Jeppe Brogaard Clausen for at have udtalt, at man overvejer at søge

Procesbevillingsnævnet om tilladelse til at anke landsrettens domme til Højesteret, og at rækkevidden af landsrettens domme i forhold til de øvrige sager afhænger af aftalegrundlaget i disse sager, og at "man skal drøfte med filmproducenten, om man ønsker at indtræde direkte i de her sager."

Sagernes bevismæssige stilling

Generelle bemærkninger

Det kan konstateres, at alle sagerne i sagskomplekset er identiske i forhold til de overordnede bevismæssige spørgsmål, de rejser.

Der er således for det første tale om, at det er det samme grundlæggende tekniske bevis, som CMS og MIRCOM har fremlagt i samtlige sager, i form af logoplysninger om den ip-adresse, der angiveligt var knyttet til den sagsøgte borgers internetabonnement på tidspunktet for den påståede krænkelse af ophavsretten. Disse logoplysninger er angiveligt i samtlige tilfælde tilvejebragt af programmet MaverikMonitor, som selskabet Maverickeye UG angiveligt står bag.

Der er for det andet tale om, at dette bevis i bedste fald siger noget om, hvilke data der er blevet overført fra én ip-adresse til en anden, men ikke i sig selv noget om, hvem der måtte stå bag de pågældende dataoverførsler eller hvilken computer, tablet eller smartphone, der måtte være anvendt hertil.

Det kan lægges til grund, at flere tusinde af de borgere, der har modtaget breve fra Njord Law Firm, og flere hundrede af de borgere, der siden er blevet stævnet, alle har afvist at kende noget til ulovlig download og fildeling overhovedet.

Mens der i sagens natur ikke uden videre kan ses bort fra muligheden af, at visse af disse borgere ikke fortæller sandheden – eller den fulde sandhed – i den forbindelse, kan der i hvert fald ses bort fra muligheden af, at samtlige af disse helt almindelige borgere, hvoraf formentlig størstedelen aldrig har været i kontakt med retssystemet, allesammen lyver.

Der kan herunder ses bort fra muligheden af, at en 84-årig dement kvinde, som omtalt i en artikel i Berlingske Tidende den 22. juli 2019, skulle have gjort sig skyldig i ulovlig download og deling af film ved hjælp af BitTorrent-teknologi, mens hun i øvrigt var indlagt som følge af sin demenssygdom.

Der kan også ses bort fra muligheden af, at alle de borgere, der har kunnet dokumentere eller sandsynliggøre, at de ikke var hjemme, og herunder f.eks. var bortrejst, på tidspunktet for de påståede ophavsretskrænkelser, også lyver, men

blot har sat deres BitTorrent-klienter til automatisk at downloade film, mens de f.eks. var ude af landet i uge- eller månedsvis.

Der kan ligeledes ses bort fra muligheden af, at borgere, der (angiveligt) har kunnet dokumentere, at de har betalt for legale tjenester som Netflix, HBO, Spotify m.fl., ved siden af dette skulle have en interesse i at downloade og fildele primært amerikanske b-film og pornofilm via BitTorrent-netværk.

Der er derfor en formodning for, at som minimum en vis - ukendt - procentdel af de borgere, der er blevet kontaktet af Njord Law Firm, og herunder de borgere, der siden er blevet sagsøgt, rent faktisk ikke har haft noget med ulovlig download og fildeling at gøre.

Der kan allerede på den baggrund siges at være en risiko for, at – i hvert fald en del af – forklaringen herpå er, at der er en fejlkilde i CMS/MIRCOM's bevisindsamling og håndtering af beviserne, eller eventuelt hos de teleselskaber, der har udleveret oplysningerne om de pågældende ip-adresser og borgere.

Det forhold, at der således er en forhåndsformodning for, at i hvert fald en vis - ukendt - procentdel af de sagsøgte borgere ikke selv har foretaget ulovlig download eller fildeling, indebærer, at det bliver et potentielt betydeligt retssikkerhedsmæssigt problem i den enkelte sag, hvis retstilstanden skulle være den, som hævdet af CMS og MIRCOM, at domstolene – blot som følge af nogle tekniske beviser, som er tilvejebragt af CMS/MIRCOM selv – ved en eventuel realitetsprøvelse af det rejste krav i den enkelte sag skulle tage udgangspunkt i en formodning om, at sagsøgte er ansvarlig for de påståede krænkelser, hvis ikke sagsøgte selv kan bevise det modsatte, herunder manglende ansvar for andres, f.eks. en bofælles, handlinger.

Dette retssikkerhedsmæssige problem bliver så meget desto større som følge af den passivitet, som CMS/MIRCOM har udvist i forbindelse med deres håndtering af samtlige sager, og som har bevirket, at de påståede krænkelser alle ligger meget lang tid forud for tidspunktet for stævningens indlevering. I nærværende sag er der tale om, at den påståede krænkelse skal have fundet sted den 25. juni 2016, og stævningen er indleveret den 14. januar 2019. CMS skrev angiveligt til sagsøgte om det påståede krav første gang den 15. juni 2017.

Dette bevirker for det første, at det må antages at være umuligt på nuværende tidspunkt for den enkelte sagsøgte borger selv at indhente oplysninger fra den pågældendes teleselskab om, hvilken ip-adresse borgeren var tildelt på et givent tidspunkt, så langt tilbage i tiden.

Borgeren kan således ikke få efterprøvet det centrale bevis, og om der eventuelt kan være sket fejl i forbindelse med CMS/MIRCOM's indsamling og håndtering

af data, netop på det for den konkrete sag relevante tidspunkt, eller om der eventuelt kan være sket fejl i teleselskabets håndtering af data i forbindelse med selskabets tilvejebringelse og udlevering af oplysningerne om ip-adressen og abonnenten bag, ligesom der heller ikke er adgang til at kontrollere CMS/MIRCOM's håndtering af de udleverede oplysninger.

Borgeren vil i mange tilfælde, f.eks. hvor den pågældende router og/eller computer ikke længere eksisterer, heller ikke kunne foranstalte tekniske undersøgelser heraf på nuværende tidspunkt, herunder i forhold til om eventuelle hackerangreb (eller lignende) eller tekniske problemer af betydning for sagen kan have gjort sig gældende på daværende tidspunkt.

Da alle sagerne endvidere vedrører ét - og kun ét - konkret tidspunkt flere år tilbage i tiden vil det i sagens natur også i mange tilfælde kunne være vanskeligt for borgeren præcist at redegøre for, hvem der ellers måtte have kunnet benytte borgerens netværk på det pågældende tidspunkt.

Den af CMS/MIRCOM udviste passivitet kan således i sig selv udgøre et betydeligt retssikkerhedsmæssigt problem i sagerne.

Hvis en realitetsprøvelse af sagerne skulle komme på tale, ville de ovennævnte forhold gøre det nødvendigt at vurdere alle sagerne og de spørgsmål, som de overordnet rejser, i et samlet perspektiv i forhold til de fremlagte beviser og tilvejebringelsen af disse, samt i forhold til selskaberne CMS, MIRCOM og Maverickeye UG's forhold og den måde, som sagerne hidtil er ført på.

En konkret vurdering af beviserne i hver enkelt sag, der alene forholdt sig til den konkrete sagsøgte borgers eventuelle fremlagte oplysninger til støtte for dennes uskyld, men som ikke forholdt sig generelt til pålideligheden og troværdigheden af – og usikkerhedsmomenterne i – de af CMS og MIRCOM fremlagte oplysninger, og hvad – om noget – man med sikkerhed måtte kunne udlede heraf, ville således allerede af de ovenfor anførte grunde indebære en stor risiko for, at der blev truffet materielt urigtige afgørelser, hvor hensynet til generelt at kunne bekæmpe ulovlig fildeling og stille enkeltindivider til ansvar for deres eventuelle krænkelser af ophavsretten ville komme til at indebære en tilsidesættelse af hensynet til den enkelte borgers retssikkerhed.

Denne risiko er selvsagt stor, når borgerens muligheder for at bevise, at borgeren ikke har været ansvarlig for en eventuel krænkelse, reelt ikke er til stede. De anførte retssikkerhedsmæssige betænkeligheder gælder endvidere så meget desto mere i de – indtil videre mange – tilfælde i dette sagskompleks, hvor borgerne tillige er selvmødere i småsagsprocessen. Som følge af sagernes karakter, er det er således ikke uden videre muligt for retten at give borgeren den vejledning, der er forudsat i forarbejderne til retsplejelovens regler om

småsagsprocessen, med henblik på at sikre borgeren mod materielt urigtige resultater og sikre, at borgeren opnår den retsstilling, som borgeren efter lovgivningen har krav på.

Hvad kan der udledes af de tekniske beviser, som CMS og MIRCOM har fremlagt, med hensyn til spørgsmålet om sagsøgtes "delinger" af et værk og omfanget heraf?

CMS og MIRCOM har fremlagt en række sagkyndige rapporter med henblik på at dokumentere pålideligheden og ufejlbarligheden af det program, MaverikMonitor, som angiveligt har indhentet de dataoplysninger, der i samtlige sager i sagskomplekset udgør det eneste bevis, når sagsøgte i øvrigt ikke har oplyst noget kendskab til forholdet.

Af disse sagkyndige rapporter, som CMS og MIRCOM har fremlagt til støtte for, at retten kan forlade sig på de angiveligt indsamlede data – og kan udlede præcis dét af disse data, som CMS og MIRCOM hævder – er der imidlertid kun én, der udtaler sig om forhold af betydning for vurderingen af det for samtlige sager centrale spørgsmål om, hvorvidt der er sket "deling" af den i den konkrete sag omhandlede fil – og i givet fald i hvilket omfang – og om det uden videre kan lægges til grund, at der i så fald er tale om en "deling", som en bruger af det pågældende netværk har foretaget bevidst eller tilstrækkeligt uagtsomt til at ifalde ansvar.

Den pågældende rapport af 18. oktober 2018 er udarbejdet af Norges teknisk-naturvitenskapelige universitet (NTNU) og bærer titlen "En drøfting rundt bevisene som er lagt frem i CMS-saken" (i det følgende betegnet som NTNU-rapport 2).

Rapporten har også en første del, ligeledes af 18. oktober 2018, der bærer titlen "Generell rapport om fildeling-teknologier med et spesielt fokus på BitTorrent" (i det følgende betegnet som NTNU-rapport 1).

Rapporterne er udarbejdet til brug for en ankesag i Norge mellem Telenor og CMS, efter at Telenor m.fl. i første instans blev dømt til at udlevere personoplysninger om ca. 23.000 kunder til CMS.

Rapporterne beskriver BitTorrent-teknologiens virkemåde og formål, nemlig at muliggøre, at der via et netværk hurtigt og effektivt kan deles meget store filer, som f.eks. film, mellem flere computere på samme tid.

BitTorrent-teknologien går således grundlæggende ud på, at en stor fil, altså f.eks. en film, i forbindelse med, at den gøres tilgængelig i det pågældende BitTorrent-netværk deles op i meget mindre dele, og at disse dele siden (i

vilkårlig rækkefølge) kan hentes af en computer i netværket fra andre computere i netværket, der måtte være i besiddelse af den ene eller anden del. Computerne i netværket er hver især kommet gradvist i besiddelse af flere og flere dele af den samlede fil efter at have efterspurgt de pågældende dele i netværket, og derved at alle de computere i netværket, der har hentet en del, samtidig automatisk via BitTorrent-teknologien stiller denne del til rådighed for de andre computere i netværket. Til sidst vil alle delene så automatisk kunne samles til den oprindelige fil – film – på samtlige af de computere i netværket, der har ønsket at hente filen.

Pointen er, at fildelingen på denne måde bliver hurtigere og mere effektiv, end hvis én server stillede hele filen til rådighed alene og samtlige andre computere, der efterspurgte filen, hver især skulle hente hele filen på denne server.

Rapporterne fra NTNU (der i øvrigt bruger forkortelsen "MM" for MaverikMonitor) indeholder bl.a. følgende definitioner af betydning for forståelsen af terminologien på området:

> "**capture** En capture refererer i denne rapporten til én enkel dataoverføring fra en peer i ett P2P nettverk til MM.
>
> **klient** En klient er i denne rapporten brukt om en gitt bit programvare som kommuniserer med andre. Om man starter et program for å delta i ett BitTorrent nettverk har man startet en BitTorrent klient.
>
> …
>
> **leech** er en peer i et BitTorrent nettverk som laster ned data. Dette betyr at peeren ikke enda sitter med 100% av datasettet.
>
> **peer** er en klient som deltar i ett BitTorrent nettverk.
>
> …
>
> **seed** En seed er en peer i et BitTorrent nettverk som laster opp data. Dette betyr at peeren sitter på minst en liten bit av datasettet.
>
> **sverm** Alle peers i et BitTorrent nettverk som deltar i delingen av et gitt datasett på et gitt tidspunkt."

Rapporterne påkalder sig særlig opmærksomhed i forhold til den omstændighed, at CMS og MIRCOM i samtlige sager har støttet det rejste krav på, at der kan sættes lighedstegn mellem antallet af delinger af det i sagen omhandlede værk og den såkaldte "swarmsize", som programmet MaverikMonitor angiveligt har indhentet oplysninger om.

Oplysningerne om "swarmsize" indgår imidlertid ikke i de af CMS og MIRCOM sædvanligvis fremlagte logoplysninger i sagerne, men er først blevet indleveret af CMS/MIRCOM på rettens eller sagsøgtes advokaters forespørgsel.

I replik indleveret i rettens sag BS-3148/2019-FRB har CMS endvidere i stedet blot anført følgende:

> "CMS bemærker i samme forbindelse, at hver fildeling af et filmværk i gennemsnit sker til et publikum på 500 (såkaldt swarm-size). Hvis dette gennemsnit lægges til grund for fildelingen af filmværket "*Survivor*", vil det rimelige vederlag udgøre kr. 35.000 (500 spredninger x 70 kr. pr. spredning). CMS udregner ikke på nuværende stadie swarm size for de enkelte fildelinger, men fastsætter kravet skønsmæssigt til kr. 7.500."

Ud over, at denne "gennemsnitsbetragtning" er udokumenteret, er den i modstrid med de oplysninger og anbringender, som CMS og MIRCOM i øvrigt er fremkommet med i forhold til spørgsmålet om, hvorledes det kan godtgøres, at den sagsøgte borger på det tidspunkt, som der er sagsøgt for, har foretaget et bestemt antal "delinger" af den pågældende film, filmsekvens eller episode af en serie.

Af NTNU-rapport 2, s. 23, fremgår følgende om spørgsmålet om muligheden for at indkredse omfanget af deling af information via et BitTorrent-netværk:

> "For å kunne si noe om i hvilket omfanget en gitt peer driver å deler informasjon i et BitTorrent-nettverk må man dessverre drive med estimering. Å nøyaktig påvise hvor mye en kunde deler i et BitTorrent-nettverk er krevende da det krever tilgang til å overvåke all trafikken fra denne kunden. Det finnes ikke en sentral oversikt over dataoverføringene da utvekslingen av data skjer direkte mellom peers. Det man derimot kan er å konstatere at en peer deltar i en sverm, og man vet at en peer som deltar i en sverm normalt sett alltid er der for å laste ned datasettet og som en konsekvens av det vil den også samtidig laste opp datasettet til andre peers. Etter å ha konstatert at en peer deltar i en sverm kan man konstatere omfang ved å se på tilstedeværelse over tid. Man kan ikke si hvor mye en peer har delt med andre, men det er veldig sannsynlig at en peer som er i en sverm over lang tid har delt mer enn en som er i en sverm i kort tid.
>
> Omfang kan også konstateres utifra antall verk som er delt. At en gitt abonnent har delt små deler av 5 verk vil bety at den sannsynligvis har lastet ned disse 5 verkene, da deltakelse i en sverm i all hovedsak

> handler om at en ønsker at få tak i verket. En usikkerhet her er at en IP-adresse som er overvåket over tid kan ha hørt til mer enn en abonnent …
>
> Nesten alle verdiene som er lagt frem i denne saken er uegnet for a si noe sikkert om omfanget verkene CMS håndterer blir delt. Dette inkluderer feltene "swarm-size", … , enten fordi de ikke sier noe om omfang i det hele, eller fordi de inkluderer verk som ikke CMS håndterer rettighetene til. Det eneste feltet som egner seg til a si noe om omfang for delingen av CMS sine verk er feltet "Captures/title" da denne verdien beskriver antall ganger MM har observert denne IP-adressen dele informasjon som CMS har rettighetene til. Dette tallet alene er dog dessverre ikke en god indikasjon på omfang. Man må ha en tidsangivelse for hver capture i tillegg, og selv da vil det være en usikkerhet knyttet til koblingen mellom en IP-adresse og den faktiske bruker."

Det bemærkes, at dét som rapporten her beskriver, er problemerne i forhold til at kunne skønne over et samlet omfang af den enkelte bruger af netværkets "delinger", herunder over længere tid og af flere værker.

De beskrevne problemer bliver imidlertid så meget desto større, når dét, som CMS og MIRCOM hævder at kunne godtgøre i den enkelte sag, er hvor mange "delinger", sagsøgte har foretaget på det i stævningen anførte klokkeslæt.

I forhold til spørgsmålet om betydningen af størrelsen af en "swarm-size" fremgår af NTNU-rapport 1, s. 9 og s. 16, bl.a.:

> "Alle peers som deltar i distribusjonen av et gitt datasett regnes som dette datasettets sverm. Hvert datasett har sin egen sverm med peers. En BitTorrent-klient vil normalt sett kun aktivt kommunisere med ca 50 andre peers selv om det er mange flere peers i svermen. …
>
> Om man justerer opp eller ned størrelsen på svermen … vil prinsippene forbli de samme. Hver enkelt peer vil i gjennomsnitt dele like mye. Hovedforskjellen når en sverm blir større er at hver enkelt peer deler med flere andre peers, samtidig som at de deler en mindre andel av datasettet med hver enkelt peer. Totalen blir den samme. Det er dette som gjør at BitTorrent skalerer så godt. Når en sverm blir veldig stor er det mange som vil laste ned data, men det er samtidig like mange som laster opp data. Dermed vil ikke lasten øke, sett fra en peers synspunkt selv om den totale datatrafikken i svermen er mye høyere."

Det anførte uddybes i afsnit 4.1.1 på side 12 ff i NTNU-rapport 2:

> ”Størrelsen på en gitt sverm, altså hvor mange som aktivt tar del i delingen av et gitt datasett, er ikke en indikasjon på hvor aktiv en gitt peer er i nettverket. Det påstås at en stor sverm betyr at det er mange andre man *kan* dele data med, men man må samtidig huske at en stor sverm også betyr at det er mange andre en gitt peer kan spørre for å hente en del. Man har altså flere peers å dele data med, men med hver enkelt peer deler man mindre deler av datasettet. Når alt kommer til alt vil forholdet mellom nedlasting og opplasting innenfor en sverm alltid være én, og om da noen peers deler mye mer enn andre ender man opp med at de fleste som deltar i en sverm deler mindre enn omfanget av ett datasett.
>
> De allerfleste BitTorrent klienter har som en del av sine innstillinger en begrensning på hvor mange andre peers den tar kontakt med … [fodnote 14: Både Transmission v2.92 på Ubuntu og uTorrent v.3.5.4 på Windows opererer med maks 50 peers per sverm og maks 200 peers totalt sett]. Dermed er det enda et moment som bidrar til at det i praksis ikke er noen forskjell for en gitt peer om svermen har 1 000 eller 10 000 peers når det kommer til hvor mye en gitt peer kommer til å dele.
>
> CMS har påpekt i et av sine prosessskriv at mange peers i en sverm minker sannsynligheten for at MM logger en gitt peer, fordi det er så mange andre peers man kan koble seg til i tillegg til MM. CMS skriver:
>
> > Ettersom utvelgesen skjer automatisk vil det således være mindre og mindre sannsynlig at brukeren kun kobler seg opp mot rettighetshaver jo større Swarm-size det er snakk om.
>
> Denne argumentasjonen er å snu opp ned på hvordan BitTorrent fungerer. Det er ikke den som ønsker å dele datasettet som tar kontakt med andre peers, men det er den som ønsker å få tak i datasettet som gjør det. Når MM jobber mot BitTorrent nettverkene tar den rollen til en peer som ønsker å laste ned en del av datasettet, og det er med andre ord MM som tar initiativet til oppkoblingen. …
>
> CMS legger stor vekt på at en stor sverm betyr at deltakerne av denne svermen er mer aktive, og med det driver fildeling i et større omfang enn deltakere i en sverm som er mindre. De uttaler blant annet at det å dokumentere størrelsen på en sverm dokumenterer at en deltaker har deltatt i svermen over tid selv om de bare har en eneste capture. I sitt anketilsvar skriver CMS på side 39 hvordan størrelsen på svermen

betyr et bedre dokumentert omfang enn hva som ble lagt frem i scanbox saken, hvor det bare var lagt frem 1 capture uten informasjon om svermen:

> Herunder er det ført bevis for at "swarmsize" på dagen krenkelsen tok sted. Som tidligere beskrevet sannsynliggjør dette at krenkeren har vært i svermen over tid. Videre viser verdien usannsynligheten for at man kun kobler seg opp til MaverickMonitor. Verdien sannsynliggjør også deling med andre brukere, og dermed en krenkelse av et visst omfang, jft punkt 3.3

At det er mange som deltar i en sverm betyr ikke at alle i svermen har deltatt i lengre tid. Så lenge svermen er fungerende er det ikke mer sannsynlig at en er tilstede lenge selv om det er en større sverm. CMS sikter muligens til at det er lite sannsynlig at en peer kobler seg opp mot MM når det er mange andre i svermen fordi det er så mange andre den kan koble seg opp til istedet, men dette setter virkemåten i svermen på hodet all den tid at det er MM som tar initiativ til oppkoblingen fordi det er MM som opererer som nedlaster. Da MM faktisk ikke er på jakt etter å laste ned datasettet vil det ikke være noen grunn til at MM ikke skal be om å få den samme delen av datasettet fra alle peers i en sverm.

Når det kommer til sannsynligheten for å dele data er den ikke større i en stor sverm. Dersom det i svermen er mange peers som sitter på hele datasettet, samtidig som at det er få leechere, vil faktisk sannsynligheten bli lavere for at en gitt peer deler data enn om en er i en sverm hvor de este er leechere, fordi det er så få som har behov for å laste ned datasettet. I motsatt fall, hvor en peer besitter hele datasettet for en sverm hvor det bare er leechere som ikke har noe særlig av datasettet, vil det faktum at peers deler de deler av datasettet de allerede har gjøre at det ikke er noen peers som kommer til a dele mye mer enn andre."

Den eneste sagkyndige rapport, der udtaler sig om spørgsmålet om MaverikMonitors mulighed for at påvise antallet af "delinger", afviser altså, hævet over enhver tvivl, at der kan sættes nogen form for lighedstegn mellem antallet af "delinger"og swarmsize.

Det kan således konkluderes, at det allerede af den grund er faktuelt forkert, når CMS og MIRCOM sætter lighedstegn mellem størrelsen af en "swarm" og antallet af delinger på et bestemt klokkeslæt og hævder, at en "swarmsize" på mere end 110 viser, at der er sket "delinger" i tilsvarende antal. Der er således

ingen dækning for, at CMS/MIRCOM kræver betaling for den påståede ophavsretskrænkelse, som om det var bevist, at sagsøgte på det pågældende tidspunkt havde foretaget 110 selvstændige ophavsretskrænkelser, "delinger", svarende til fuld "eksemplarfremstilling" og videredistribution af disse eksemplarer til (mindst) 110 andre, og der er dermed ingen dækning for at kræve et vederlag på 70 kr. gange 110, der netop hviler på en beregning svarende til, at der var sket en sådan eksemplarfremstilling og videredistribution.

Det kan endvidere konkluderes, at CMS og MIRCOM og deres advokat har været klar over, at der ikke har været tilstrækkeligt belæg for at argumentere således med hensyn til bevisets stilling, som man har gjort i samtlige sager.

Tilbage står, at CMS/MIRCOM i samtlige sager i bedste fald alene kan bevise, at sagsøgte i ét enkelt tilfælde (dét tilfælde på dét tidspunkt, der er sagsøgt for) har foretaget helt eller delvist download af det i sagen omhandlede værk, og at MaverikMonitor har kunnet hente den tilsvarende del af værket via sagsøgtes ip-adresse.

Dette flugter for så vidt udmærket med det forlig om betaling af 56 kr., som CMS indgik i rettens sag BS-25462/2018-FRB, og hvor CMS gjorde gældende, at man skulle anses for at have vundet sagen – uagtet, at sagsøger ifølge forligsteksten ikke havde anerkendt nogen form for krænkelse. CMS anførte i den forbindelse ikke desto mindre, at CMS med forliget havde opnået det, som CMS ønskede med sagsanlægget, nemlig at få sagsøgtes ophavsretskrænkelser bragt til ophør samt at have opnået "et rimeligt vederlag."

CMS/MIRCOM har derimod ikke ført – og vil ikke kunne tilvejebringe – bevis i den enkelte sag for, at der er sket flere "delinger" (fuldt ud) af det i sagen omhandlede værk fra den i sagen omhandlede ip-adresse.

Når det således i NTNU-rapport 2 anføres "Å nøyaktig påvise hvor mye en kunde deler i et BitTorrent-nettverk er krevende da det krever tilgang til å overvåke all trafikken fra denne kunden", er der tale om en konstatering af, at en sådan adgang til overvågning er MaverikMonitor ikke i besiddelse af.

Når det videre i rapporten anføres, at der ikke findes "en sentral oversikt over dataoverføringene da utvekslingen av data skjer direkte mellom peers", er der ligeledes tale om en konstatering af, at MaverikMonitor ikke kan overvåge, hvilken dataudveksling – og dermed eventuel "deling" – der måtte foregå mellem de enkelte "peers". MaverikMonitor kan alene foretage registreringer af, hvilken dataudveksling der foregår mellem MaverikMonitor og de "peers", som MaverikMonitor selv er i forbindelse med.

CMS og MIRCOM har navnlig heller ikke noget bevis for, hvem af deltagerne i en "swarm" i et BitTorrent-netværk, der måtte have gjort det ophavsretligt beskyttede værk tilgængeligt i netværket til at starte med (altså har ageret som den oprindelige "seeder"). Det bemærkes, at sagerne herved adskiller sig fra omstændighederne i dommen gengivet i U 2011.1736 H, hvor den sagsøgte – efter en konkret vurdering af det anvendte peer-to-peer-netværks virkemåde – blev dømt for at have stillet sit eget digitale musikbibliotek til rådighed for andre brugere af netværket, og altså for at have ageret som oprindelig "seeder", mens han i øvrigt blev frifundet for den del af sagen, der vedrørte, at han skulle have skaffet sig musiktitler via det pågældende netværk.

Det er imidlertid den oprindelige "seeders" tilgængeliggørelse af en fil, der udgør overførslen til almenheden af det eventuelt ophavsretligt beskyttede værk via netværket. Det pågældende netværk og den pågældende "swarmsize" vil til enhver tid have en given størrelse, som ikke i sig selv øges derved, at én eller flere brugere af netværket giver sig til at downloade det pågældende værk via netværket. Den enkelte brugers anvendelse af BitTorrent-teknologien indebærer således ikke, at der sker en overførsel til almenheden (deling) udover den, der allerede er gjort mulig, fordi nogen har placeret filen i netværket til at starte med.

Således som teknologiens virkemåde er beskrevet, er den enkelte brugers "seeding" (deling) af brudstykkerne af filen ikke nogen nødvendig forudsætning for, at de andre brugere af netværket kan hente den allerede tilgængeliggjorte fil (så længe bare én anden "seeder" filen), og den enkelte brugers adfærd bidrager således ikke til en spredning til andre brugere af netværket, der ikke ville være sket alligevel (blot eventuelt langsommere), når disse brugere selv har besluttet sig for at gå i gang med at hente (downloade) filen. Er der f.eks. kun én anden bruger end den oprindelige "seeder", vil download af filen således antageligt blot gå langsommere, og der sker ingen yderligere spredning af filen.

Brugernes samlede adfærd har altså i realiteten primært betydning for, hvor hurtigt brugerne, der hver især via netværket har foretaget (ulovlig) download af (dele af) filen, kommer i besiddelse af den fulde fil, og som beskrevet i NTNU-rapport 2 vil der i praksis være tale om, at den enkelte bruger kobler sig op til maksimalt 50 andre computere i netværket for at opnå den bedst mulige udnyttelse af teknologien og dermed det hurtigste og mest effektive download af filen.

Der er således også af den grund ikke tale om, at der i en "swarm" i et givent netværk sker "delinger" af det ophavsretligt beskyttede værk svarende til antallet af deltagere i denne "swarm".

Den retvisende beskrivelse er derimod, at hvis der er 110 deltagere i en "swarm", så vil disse deltagere – hvis de alle har downloadet den pågældende fil fuldt ud

ved hjælp af BitTorrent-teknologien – alle have udnyttet denne teknologi til at hente forskellige dele af filen hos hinanden (men altså kun i et samspil med i alt maksimalt 50 computere) med henblik på hurtigst muligt at kunne downloade og åbne den pågældende fil på deres egen computer uden at betale herfor.

Som ovenfor anført betyder dette imidlertid netop ikke, at hver af de 110 deltagere har foretaget 109 "delinger" til de øvrige deltagere i netværket af det pågældende værk, men blot at ophavsretsindehaveren i 110 tilfælde er gået glip af den betaling for download af filmen, som ophavsretsindehaveren havde krav på.

Det må derfor også antages, at EU-Domstolen i sag C-597/19 som svar på det præjudicielle spørgsmål 1 a, der er rejst i den sag, vil fastslå, at "seeding" af i sig selv uanvendelige "pieces" af et ophavsretligt beskyttet værk ikke som sådan udgør en overføring til almenheden som omhandlet i artikel 3, stk. 1, i direktiv 2001/29 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet.

Hvorledes kan et eventuelt krav herefter gøres op?

CMS/MIRCOM, der ved anvendelsen af MaverikMonitor i sagens natur må have overvåget og indsamlet oplysninger om ip-adresserne på samtlige deltagere i den pågældende "swarm", kan herefter alene med rette sagsøge samtlige 110 deltagere for 70 kr. hver (hvis den af CMS/MIRCOM under henvisning til U 2005.60 V anførte beregning af filmens pris i øvrigt lægges til grund).

Alternativt skulle der være tale om et synspunkt om, at alle brugere af et BitTorrent-netværk må hæfte hver især og solidarisk for hinandens handlinger og dermed det totale antal gange det pågældende værk måtte være downloadet fuldt ud via netværket. Et sådant synspunkt har hverken CMS eller MIRCOM imidlertid gjort gældende, og synspunktet støder desuden bl.a. på det problem, at det – som omtalt straks nedenfor – ikke uden videre kan konkluderes, at den enkelte deltager i et netværk er klar over, at dennes download af en fil også bevirker, at andre brugere potentielt får nemmere og hurtigere adgang til samme fil. Hertil kommer som ovenfor anført, at den enkelte brugers download er uden selvstændig betydning for det samlede antal downloads, og at der, som følge af teknologiens virkemåde, for den enkelte bruger i det enkelte tilfælde – alt andet lige – vil være tale om, at alene en begrænset del af filen "deles" med en begrænset del af sværmen.

CMS og MIRCOM har i samtlige sager rejst krav opgjort under henvisning til dommen refereret i U 2005.60 V – og dermed til en vederlagsberegning ud fra en anslået, reduceret salgspris af en dvd i fuld spillefilmslængde med fradrag i øvrigt af udgifter til fremstilling og distribution samt andre driftsudgifter.

CMS og MIRCOM har imidlertid i en række sager undladt at oplyse om, at sagen ikke drejede sig om et værk i fuld spillefilmslængde, men derimod f.eks. en scene fra en pornofilm, der kunne erhverves til en langt mindre pris.

Dette gør sig således gældende i nærværende sag, hvor retten ved retsbog af 5. marts 2020 anførte:

> "Retten bemærker i øvrigt, at CMS ved at henvise til dommen gengivet i U 2005.60 V har begrundet sin påstand om betaling af 7.500 kr. med udgangspunkt i, at der skal laves en beregning for hver enkelt "deling" ud fra kostprisen på en dvd-film i fuld længde.
>
> Retten bemærker i tilknytning hertil, at følgende fremgår af de logoplysninger vedrørende den påståede krænkelse den 25. juni 2016, kl. 14.00, som CMS har fremlagt som sagens bilag 2:
>
> "[PrettyDirty]
> Penny PaxChanel Preston
> James Deen
> Sugar Babies: Part One
> (22.04.2016)
> 544p"
>
> Det påståede download ses således ikke at vedrøre filmen "Sugar Babies", men derimod "Sugar Babies: Part One" med de medvirkende skuespillere Penny Pax, Chanel Preston og James Deen.
>
> Af det som sagens bilag 8 fremlagte cover fremgår, at filmen "Sugar Babies" indeholder et "Chapter One" med medvirken af Penny Pax, Chanel Preston og James Deen.
>
> Retten skal på den baggrund opfordre CMS til at redegøre for, om CMS gør gælende, at der tale om en "deling" af en film i fuld længde eller om et kapitel eller en scene fra en film, og – hvis der alene er tale om en scene, der evt. har kunnet erhverves selvstændigt til en lavere pris end en fuld dvd – hvorvidt dette giver CMS anledning til at justere det påståede udgangspunkt på 70 kr. pr. deling."

Ved processkrift af 19. marts 2020 anførte CMS om dette spørgsmål:

> "Hvis Venstre Landsrets beregningsmodel lægges til grund vil det rimelige vederlag ved en pris på 70,00 kr. og en swarm-size på 201 udgøre: 70,00 kr. x 1 film x 201 delinger = 14.070,00 kr.

> For så vidt angår overvejelsen, om der er delt en film i fuld længde eller mindre, skal CMS henvise, at som eksemplarfremstilling anses både "*hel eller delvis eksemplarfremstilling på en hvilken som helst måde*", jf. ophavsretslovens § 2, stk. 2, 1.pkt.
>
> Filmværket udbydes til salg på hjemmesiden Adultdvdempire.com, der mod betaling giver adgang til pornofilm på DVD eller via internettet, herunder filmen i denne sag.
>
> Som bilag 36 fremlægges skærmbilleder fra Adultdvdempire.com, hvoraf fremgår, at filmværket "Sugar Babies" kan købes på DVD for 22,99 amerikanske dollars, svarende til 159,15 kr.
>
> Hvis Venstre Landsrets beregningsmodel lægges til grund vil det rimelige vederlag ved en salgsprispå 159,15 kr. udgøre: 159,15 kr. x 1 film x 201 delinger = 31.989,15 kr.
>
> Retten på Frederiksberg har anført, at den påståede download ses at vedrøre "Sugar Babies: Part One" med de medvirkende skuespillere Penny Pax, Chanel Preston og James Deen.
>
> Det fremgår af bilag 36, at det også er muligt at købe sig adgang til hver af de fire sceneværker, som filmen består af. Adgang til ét enkelt sceneværk koster 5,99 amerikanske dollars, svarende til 41,48 kr. Det fremgår af bilagets side 2, at i første sceneværk i filmen medvirker skuespillere Penny Pax, Chanel Preston og James Deen.
>
> Hvis Venstre Landsrets beregningsmodel lægges til grund vil det rimelige vederlag ved en scenepris på 41,48 kr. udgøre: 41,48 kr. x 1 film x 201 delinger = 8.337,48 kr.
>
> CMS gør på den baggrund gældende, at påstandsbeløbet fastsat til 7.500 kr. udgør et rimeligt vederlag i denne sag."

Det ses, at CMS herved har set bort fra, at retten i retsbogen også anførte følgende:

> "Retten skal endvidere opfordre CMS til i den forbindelse at forholde sig til det anførte i afsnit 4.1.1 i den rapport, som CMS har fremlagt som sagens bilag 14, og det i samme rapport i afsnit 5.1 anførte om, at "Nesten alle verdiene som er lagt frem i denne saken er uegnet for at sie noe sikkert om omfanget verkene CMS håndterer blir delt. Dette inkluderer feltene "swarmsize", …",…"

I stedet anførte CMS blot i processkriftet:

> "I kolonnen benævnt "SwarmSize" er angivet det antal IP-adresser, som filen er blevet delt med. Det fremgår af række 728, markeret gul, at MaverickMonitor har registreret en SwarmSize på 201, svarende til at værket er delt med 201 brugere. Filmen er således blevet delt over 100 gange som nævnt i stævningen."

Det ses også, at CMS ved de to sidst anførte beregninger i sit processkrift ser bort fra, at landsretten i U 2005.60 V foretog fradrag i den officielle kostpris for at nå frem til beregningen af det rimelige vederlag.

Det kan herefter samlet set konstateres, at CMS og MIRCOM med de allerede indgåede forlig og afsagte domme i sagskomplekset potentielt (ud over, at de i øvrigt ikke er at anse for rette sagsøgere i sagerne) har opnået en meget stor overkompensation for de enkelte, eventuelle ophavsretskrænkelser, og at det i hvert fald ikke har været med rette, at den enkelte bruger er blevet afkrævet et beløb, der i givet fald også har dækket fuldt ud for andre brugeres selvstændige og egenhændige ophavsretskrænkelser.

Andre bevisproblemer

NTNU-rapport 2 udtaler sig også om en række andre forhold, der viser, at der er yderligere grunde til, at CMS og MIRCOM ikke har godtgjort, at det rejste krav i de enkelte sager er berettiget.

Bevisproblemer i forhold til dynamiske ip-adresser og logoplysninger over længere tid

På s. 4 og s. 5 i NTNU-rapport 2 berøres spørgsmålet om dynamiske ip-adresser:

> "Da det er mulig at en IP-adresse bytter eier er det viktig at internettleverandør (Internet Service Provider, ISP) kan verifisere at en gitt abonnent har hatt en gitt IP-adresse i alle de tidspunktene CMS har gjort captures for denne adressen. …
>
> I detaljerte eksempel som CMS har lagt frem, …, ser man tydelig at fildelingen har skjedd over lang tid. Skal man konstatere at det er samme abonnent som har deltatt i alle disse svermene må man sjekke at det er denne abonnenten som har hatt denne adressen fra 28. mai 2016 til 25. januar 2017.
>
> I prosessskriv av 15. august på side 16 skriver CMS følgende:

> Retten opplyses om at CMS ikke har kjennskap til systemene til de ulike internettleverandørene, og når en IP har blitt overvåket over lang tid, vil det derfor være umulig for CMS å vite hvorvidt IP-Adressen har gått over til en annen abonnent. Dette bør likevel ikke være avgjørende. For det første vil det i de overveiende fleste tilfellene dreie seg om samme bruker som deler filmen fordi et annet scenario forutsetter at IP-adressen går over til en annen bruker som deler akkurat samme hash som den forrige brukeren. For det andre vil Telenor mfl. kunne se om abonnenten er den samme nå som på tidspunktet for de midlertidige forføyingene.

Her er det flere momenter som er veldig viktige fra et teknisk perspektiv, dersom man ønsker å knytte aktiviteten til en gitt abonnent. CMS har rett i at det for CMS vil være umulig å vite hvorvidt en IP-adresse går over til en annen abonnent. Det er det bare ISP som kan sjekke. … Det er … veldig viktig at alle tidspunktene det er gjort captures i overvåkingen av en gitt adresse blir oppgitt, fordi det er bare slik ISP kan kontrolleres at det er samme abonnent.

…

Det er til slutt et punkt til fra det CMS skriver på side 43 av ankesvaret sitt som må kommenteres når man drøfter innvirkningen av dynamiske IP-adresser:

> Det er først etter en eventuell utlevering at CMS har mulighet til å undersøe det reelle omfanget bak krenkelsen og abonnenten vil først da kunne gi informasjon som indikerer at IP-adressen er re-allokert.

Her vil CMS at det skal være opp til abonnenten å bevise at IP-adressen er reallokert, men slik kan det ikke fungere. De aller fleste abonnenter av en ISP har ikke kontroll på hvilken adresse de benytter når, fordi det er noe man ikke trenger å forholde seg til. Da er det selvfølgelig umulig at det er abonnenten som skal bevise dette. Det er helt klart at man må sjekke at de aktuelle captures hører til en gitt abonnent *før* personopplysninger utleveres."

Det ligger fast, at noget sådant ikke er blevet tjekket i sagerne i dette sagskompleks, inden de sagsøgtes personoplysninger blev udleveret. Det ligger også fast, at det ikke siden er blevet tjekket, om den i den enkelte sag omhandlede ip-adresse vitterlig også har været tildelt den sagsøgtes internetabonnement på samtlige de tidspunkter, som den af CMS/MIRCOM fremlagte log indeholder.

Det er (bl.a.) derfor et problem, når CMS og MIRCOM standardmæssigt i alle sager fremhæver og gør gældende, at der er konstateret (en lang række) yderligere krænkelser via sagsøgtes ip-adresse, end den krænkelse, der er stævnet for, og anfører, at "det fulde omfang af krænkelserne bør indgå som et element i den samlede culpabedømmelse."

CMS og MIRCOM kan ikke med føje anmode retten om lægge vægt på yderligere eventuelle krænkelser, når CMS og MIRCOM ikke har stævnet for disse krænkelser og ikke har ført– og ikke på nuværende tidspunkt kan føre – bevis for, at ip-adressen på samtlige i loggen anførte tidspunkter har været knyttet til sagsøgtes internetabonnement.

Hertil kommer, at CMS og MIRCOM heller ikke har ført noget bevis for, at eventuelle øvrige værker, som er nævnt i logoplysningerne, er værker, for hvilke der er sket en ophavsretskrænkelse og i den forbindelse, hvem der måtte have været indehaver af ophavsretten.

Udover at CMS og MIRCOM efter landsrettens domme af 8. april 2020 ikke kan anses som rette sagsøger i de anlagte sager, foreligger der således heller ingen oplysninger i den enkelte sag om CMS eller MIRCOM's eventuelle beføjelser i forhold til eventuelt øvrige nævnte værker i logoplysningerne.

Bevisproblemer i forhold til spørgsmålet om uagtsomhed

NTNU-rapport 2 behandler også spørgsmålet om, hvorvidt det uden videre kan lægges til grund, at en bruger af et BitTorrent-netværk ved, at et download af en fil via netværket også indebærer et (delvist) upload. På side 5 f anføres således:

> **"2.2 Med hvilket overlegg skjer deling/opplasting?**
>
> Et moment som er diskutert en del er i hvor stor grad en vanlig bruker er kjent med at man laster opp data samtidig som at man laster ned data ved hjelp av BitTorrent. Om det har en relevans for saken at opplasting skjer med overlegg bør man tenke igjennom hvilke indikatorer man har for at opplastingen faktisk skjer med overlegg. Deretter kan man vurdere om det er sannsynlig at overlegg finner sted for de fleste eller ikke.
>
> Det er en rekke faktorer som er lagt frem i saken. CMS argumenterer med at det er sannsynlig at de fleste kjenner til at det lastes opp fordi:

- **Diskusjonfora:** Det finnes diskusjonsfora på nett hvor brukere av BitTorrent-klienter diskuterer hvor lenge de skal laste opp etter de selv har lastet ned et datasett, slik at svermen fortsatt kan leve.

- **Lisenstekst (End User License Agreement, EULA):** Bilag 2 i anketilsvar fra CMS viser bilder fra installasjonen av uTorrent, hvor det et stykke ned i EULA er opplyst at programmet automatisk vil dele med andre.

- **Advarsler:** En del BitTorrent-klienter gir advarsler når det lastes ned som varsler brukerne om at de kommer til å dele data med andre om de benytter programmet. Det er gitt eksempler fra PopcornTime og BitTorrent-klienten qBitTorrent i bilag 2 av anketilsvaret fra CMS

- **Brukergrensesnitt:** De fleste BitTorrent-klienter viser opplastingshastighet i brukergrensesnittet.

At det er flere kilder til advarsler taler i første omgang i retning av at de fleste brukerne vet at de deler samtidig med at de laster ned. Om man derimot går igjennom samme liste punkt for punkt for å lage hypoteser som sannsynliggjør at brukeren ikke får med seg advarselen, så er det ikke så åpenbart at de fleste deler med overlegg:

- **Diskusjonsfora:** Det er usannsynlig at de fleste diskuterer fildeling i en så detaljert grad at man inkluderer opplasting. De aller fleste som benytter en BitTorrent klient er etter all sannsynlighet ute etter å laste ned en fil. De som er interessert nok i å bidra inn til BitTorrent-nettverket til at de faktisk oppsøker ulike fora må regnes å være i mindretall.

- **EULA:** Det er studier som viser at brukere i gjennomsnitt bruker så lite som 7 sekunder på å tolke en lisenstekst. Om man tenker på antallet slike tekster en gjennomsnittlig bruker blir utsatt for er det ikke overraskende at mange bare klikker seg forbi uten å lese. Advarselen uTorrent presenterer i sin lisenstekst kan man derfor ikke anta at de fleste har lest.

- **Advarsler ved nedlasting:** Brukere har en tendens til å klikke seg gjennom alle advarsler som dukker opp for å få gjort det de ønsker, uten å lese eller bry seg om hva advarslene faktisk sier. For eksempel er det observert at det er betydelig antall brukere som åpner nettsted som nettleseren aktivt advarer om at inneholder

virus eller lignende. Det er dermed rimelig å anta at mange brukere ikke leser advarsler og istedet bare klikker seg videre.

- **Brukergrensesnitt:** Selv om en BitTorrent-klient tydelig viser at du laster opp i f.eks 4MB/s må en bruker som leser dette faktisk forstå hva dette innebærer for å ta stilling til hva det betyr.

Gitt de fire punktene over er det urimelig å påstå at de fleste brukerne kjenner til at de laster opp data. Samtidig er det også urimelig å påstå at de fleste ikke kjenner til at det lastes opp data. Sannheten er nok et sted midt i mellom. Det er verdt å merke seg at det er universitet som har laget en tjeneste for å varsle sine brukere når de laster opp i P2P-nettverk fordi de erkjenner at det er mange brukere som ikke vet at de gjør dette.

2.3 Identifisering av ulike klienter

Som en del av diskusjonen rundt overlegg, altså hvor bevisst er en bruker på at det han gjør er ulovlig, har det i prosessskriv, anke og ankesvar blitt diskutert rundt klienten "popcorn time". Grunnen til at akkurat denne klienten bliver diskutert flere ganger er at dette er en klient som i veldig stor grad skjuler at det skjer fildeling, samtidig som at den har et grensesnitt som til forveksling kan ligne på lovlige tjenester som "Netflix"og "YouTube". …"

I forhold til spørgsmålet om, hvorvidt brugeren også nødvendigvis vil være bevidst om, at der kan ske en fortsat og længerevarende automatisk deling af en fil, anføres i rapporten s. 19 f:

"Om videre deling skal skje med overlegg må to kriterier være på plass. Først må brukeren faktisk være klar over at nedlasting også medfører opplasting, og dette aspektet drøftes kort i kapittel 2.2. For det andre må brukeren faktisk la klienten kjøre med overlegg over lang tid. Da mange av klientene er konstruert slik at de legger seg i bakgrunnen istedet for å avslutte når man klikker på lukkeknappen er det absolutt en mulighet at man bare glemmer at den kjører i bakgrunnen."

Dette kan sammenholdes med en af de andre sagkyndige rapporter, som CMS og MIRCOM har fremlagt, "Evaluation of the System *MaverikMonitor*" af 2. april 2014, udarbejdet af Dr. Simone Richter, hvor det i punkt 11.41 bl.a. anføres:

> "A user who has acquired the Complete Data Set will continue to transmit pieces of that file to other users unless the client is instructed to stop doing so. …"

Hvis de fremlagte logoplysninger i denne sammenhæng (antallet af "captures" af samme fil over en længere periode) i øvrigt er pålidelige, må det umiddelbart anses for plausibelt, at de i rapporterne således beskrevne tekniske forhold er forklaringen på det billede, der tegner sig i mange af sagerne i sagskomplekset, hvor den samme (porno)filmtitel går igen og igen i logoplysningerne, time efter time og dag efter dag over flere måneder (og alternativt må der være tale om en for brugeren særdeles tilfredsstillende (porno)film, siden den skal downloades så mange gange om og om igen).

Problemet med brugerens eventuelle ukendskab til, at brugeren foretager sig noget ulovligt og (efter omstændighederne) tillige ukendskabet til, at brugerens klient (eventuelt over længere tid) automatisk uploader fildele, som brugeren har downloadet, bliver i øvrigt så meget desto større, hvis man – som CMS og MIRCOM – vil hævde, at sagsøgte under alle omstændigheder hæfter for andres handlinger, foretaget via sagsøgtes ip-adresse, f.eks. hvis sagsøgte har overladt brugen af netværket til andre eller har ændret den forudindstillede kode til at tilgå netværket.

Sagsøgte vil således ikke have mulighed for nærmere at påvise, at en anden person, hvis handlinger sagsøgte så skulle hæfte for, faktisk ikke har handlet i ond tro eller tilstrækkeligt uagtsomt i forhold til at have "delt" den omhandlede fil (over længere tid).

Hertil kommer, som retten har anført i den vejledning, som retten har offentliggjort på sin hjemmeside den 5. februar 2020, at det ikke nødvendigvis vil forholde sig således, at CMS/MIRCOM har et grundlag for deres krav, selv om det måtte forholde sig således, at sagsøgte (eller en person, hvis handlinger sagsøgte måtte hæfte for) har downloadet den pågældende film(sekvens). Et ansvarsgrundlag vil tillige forudsætte, at det efter bevisførelsen i sagen også kan lægges til grund, mod sagsøgtes eventuelle benægtelse, at sagsøgte (eller en person, hvis handlinger sagsøgte måtte hæfte for) i forbindelse med et sådant download handlede uagtsomt i forhold til en eventuel ophavsretskrænkelse.

I de sager, der handler om download af pornofilm(sekvenser), har retten i den forbindelse særligt påpeget, at pornofilm, i fuld længde såvel som i brudstykker, igennem flere år har været stillet – i hvert fald tilsyneladende – gratis og lovligt til rådighed for almenheden på forskellige internetsider. Retten har herefter bemærket, at det på den baggrund ikke uden videre er givet, at en sagsøgt (eller en person, hvis handlinger sagsøgte måtte hæfte for) har handlet uagtsomt ved

et eventuelt download af en given pornofilm(sekvens), uanset om dette måtte være sket via et fildelingsnetværk.

Retten har yderligere bemærket, at det i den forbindelse muligvis også kan være af betydning, at visse af disse internetsider har så store besøgstal, at der tilsyneladende skabes en forretning alene ved bannerreklamer og tillægsydelser, fremfor afkrævning af betaling for at se de pågældende pornofilm, og herunder at sådanne sider kan hævdes at blive bekræftet i at være legitime foretagender, når bannerreklamer også indrykkes f.eks. af et medlem af Folketinget op til et folketingsvalg.

Mens det kan hævdes, at enhver bør kunne sige sig selv, at man ikke kan gå ud fra, at det er en lovlig handling at downloade "Fasandræberne" fra internettet kort tid efter premieren, uden at betale herfor, kan vurderingen altså formentlig stille sig anderledes under andre omstændigheder, herunder når der er tale om mindre kendte titler, herunder pornofilm eller scener fra pornofilm.

En eventuel uagtsomhedsvurdering i sagerne i dette sagskompleks må af de ovenfor anførte grunde formentlig tage et andet og mere nuanceret udgangspunkt, end hvad der var påkrævet under omstændighederne i U 2011.1736 H, hvor tiden og teknologien endvidere var en anden.

MaverikMonitors bevisværdi i øvrigt

I NTNU-rapport 2, s. 10, betegnes den af Dr. Simone Richter udarbejdede rapport af 2. april 2014, "Evaluation of the System *MaverikMonitor*", som "forholdsvis tynn", og det anføres, at den "utelater mange detaljer".

På s. 22 f, anføres endvidere følgende konkluderende bemærkninger:

> "Et annet spørsmål som har været viktig er hvor pålitelig MM faktisk er, og hvorvidt verdiene som er dokumentert er riktige. Basert på den dokumentasjonen som er fremlagt er det ingen grunn til å tvile på at informasjonen er korrekt samlet inn. Der det er tvil er i den videre håndteringen av bevisenen når oppsummeringene ble laget, og hvordan de ulike verdiene tolkes. Det er i denne rapporten grundig redegjort for at ikke alle verdiene bør tolkes slik de har blitt gjort i denne saken, fordi det gir et feil bilde på hva som foregår."

De øvrige af CMS/MIRCOM fremlagte rapporter, der skal dokumentere, at MaverikMonitor er ufejlbarligt, er alle generelle og siger stort set intet om, hvilke mulige fejlkilder, der kan have været netop på det eller de tidspunkter, hvor det konkrete bevis i den konkrete sag angiveligt blev indhentet af MaverikMonitor.

I en række sager, herunder nærværende sag, har de sagsøgtes advokater endvidere henvist til sagkyndige rapporter, der har været fremlagt i amerikanske retssager, og som konkluderer, at MaverikMonitor ikke er pålideligt.

Det drejer sig bl.a. om en rapport af 27. februar 2018, udarbejdet af Ph. D. Kalman Toth, til brug for sagen Dallas Buyers Club, LLC, v. John Huszar. Rapporten forholder sig bl.a. til Dr. Simone Richters rapport af 2. april 2014 "Evaluation of the System *MaverikMonitor*", hvis konklusioner afvises, bl.a. med følgende bemærkninger, s. 6 og s. 8:

> "Paige conducted a simple confidence test asserting his tests confirm that the "infringement detection system works" - not stating how consistently or reliably. Richter conducted similar rudimentary tests. Neither Paige nor Richter configured or ran tests simulating the actual operating environment, namely, a swarm of Bit Torrent computers at many unknown locations sharing a significant number media files among peer computers in the swarm, a tracker, and the MaverickMonitor system.
>
> …
>
> Richter describes how she analyzed the code, line by line, to detect logic and other errors – she found none.
>
> Given the large code base of over 140,000 lines of code, I venture that it would have been infeasible for her to review all the code. Furthermore, the lack of technical specifications would have made it impossible for her to determine if the code correctly implements the required functionality as intended."

I stedet konkluderer Kalman Toth på s. 8:

> "In the absence of verifiable evidence, an objective software professional cannot conclude that MaverickMonitor detects the IP adresses of infringing bit torrent users correctly, consistently and reliably."

Tilsvarende konkluderes om systemet Exipio, der angiveligt svarer til MaverikMonitor, i en rapport udarbejdet af Bradley Wittemann og fremlagt den 2. februar 2017 i sagen Malibu Media, LLC vs. John Doe. Om mulighederne for, at der registreres forkerte ip-adresser, anfører Bradley Wittemann bl.a.:

> "The Excipio system attempts to identify a specific user, however, there are a number of reasons why the IP address recorded could be incorrect.

6.1 IP addresses in the BitTorrent protocol can be easily spoofed
To achieve high bandwidth connections, the BitTorrent protocol uses UDP, which allows spoofing of the source addresses of Internet traffic.

Protocols that communicate over the User Datagram Protocol (UDP), unlike the Transmission Control Protocol (TCP), do not perform handshakes and therefore do not perform source IP address validation. This means someone can send a UDP packet with a forged header that specifies someone else's IP address as the source.

6.2 The IP address could have been in use by other entities
The user's IP address could have been in use by another subscriber during some of the period of time in question. Without having solidified that this was the one and only user of that IP address for the period in question, some or all of the traffic shown in the Excipio system's report may not belong to the individual identified in this suit.

…

6.3 Common BitTorrrent trackers inject random IP addresses into the results returned in swarm lists
Starting in 2008, a number of the largest BitTorrent tracker sites started to inject random IP address into their swarm list results. The result is that these fake IP addresses are perpetuated in a swarm as having been a swarm member, and introduced to the new swarm members as being valid. However, this IP address could have been a coincidental match with a real individual's IP address.

…

6.4 The computer could be infected and acting as a member of a bot-net
There have been reports of cyber-criminals creating Virtual Private Networks (VPNs) on top of bot-nets of compromised or exploited devices, then selling the ability to send traffic out of those devices.

This possibility introduces further doubt of the association between IP address and this individual.

6.5 VPN software could be providing inaccurate IP of swarm members

> The use of Virtual Private Network (VPN) software, or the intentional misconfiguration of it, could provide an inaccurate IP address of a swarm member.
>
> This possibility introduces further doubt of the association between IP address and this individual."

Om sin baggrund oplyser Bradley Wittemann bl.a.:

> "I worked from 2011 to 2015 as a Senior Director of Product Management for BitTorrent Inc., the software company founded by the inventor of the of the BitTorrent Protocol. While with BitTorrent I remained involved with building systems for content distribution."

Hvordan er filerne havnet i et BitTorrent-netværk?

CMS/MIRCOM kan endvidere som ovenfor nævnt ikke føre bevis for, hvem der har placeret de pågældende filer i de pågældende netværk. Det kan imidlertid konstateres, at i hvert fald dele af det fremlagte aftalegrundlag i visse af sagerne, efter sin ordlyd udtrykkeligt giver MIRCOM ret til at placere de værker, som aftalen angiveligt angår, i fildelingsnetværk. Der kan herved bl.a. henvises til retsbog af 26. november 2019 i rettens sag BS-30249/2019-FRB, hvoraf fremgår bl.a.:

> "…A har opfordret MIRCOM til at dokumentere, at "de er indehaver af rettighederne til den i sagen omhandlende film", og … hun har gjort gældende, at filmen først udkom den 6. februar 2017, og således ikke var udgivet på det påståede krænkelsestidspunkt den 26. januar 2017.
>
> Da MIRCOM ikke i sin replik har bestridt sidstnævnte forhold, må retten på det foreliggende grundlag derfor umiddelbart antage, at der også i nærværende sag vil opstå et spørgsmål om, hvordan de film for hvilke, der hævdes at være sket ophavsretskrænkelser – i det konkrete tilfælde "Amazing Female Orgasms" – overhovedet havnede i de pågældende fildelingsnetværk, hvorfor, og med hvilken retsvirkning, jf. herved også Retten på Frederiksbergs dom af 22. maj 2018 (som refereret i retsbogen af 7. november 2019), og det af Telenor for landsretten i U 2019.2019 Ø anførte i anbringendernes punkt 5.3 om MaverikMonitors virkemåde og herunder om, at "CMS har alene bevist provokerede krænkelser af meget begrænset omfang", hvilket anbringende, så vidt ses, ikke blev imødegået af CMS under sagens behandling for landsretten.

Det bemærkes i den forbindelse, at det af den aftale, som MIRCOM har fremlagt som sagens bilag 6, og hvor rettighedshaver er betegnet "licensor" og MIRCOM som "licensee" bl.a. fremgår:

> "LICENSOR grants LICENSEE the exclusive rights to make the Works available to the public in remote computer networks, so-called peer-to-peer and intemet file sharing networks ("P2Pnetworks").
> …
> For each of the Works, LICENSOR will provide LICENSEE with: a.) 2 DVDs as they are supplied to the retailers; or, b.) a website or server link, where such Works can be legally downloaded by LICENSEE."

I USA afsoner to advokater langvarige fængselsstraffe efter domfældelse i den såkaldte "Prenda Law" sag. De pågældende advokater blev fundet skyldige i bedrageri, bl.a. idet de selv havde placeret pornofilm i fildelingsnetværk, hvorefter de overvågede disse netværk og fremsatte krav for erstatning for ophavsretskrænkelser over for de borgere, som angiveligt havde downloaded og delt de pågældende film i de pågældende netværk.

Af referat af sagen på United States Department of Justices hjemmeside den 9. juli 2019 fremgår bl.a.:

> "United States Attorney Erica H. MacDonald today announced the sentencing of JOHN L. STEELE, 48, to 60 months in prison for his role in a multi-million dollar fraud scheme to obtain payments from extortion victims to settle sham copyright infringement lawsuits by lying to state and federal courts throughout the country. STEELE, who pleaded guilty on March 6, 2017, was sentenced earlier today before Judge Joan N. Ericksen in U.S. District Court in Minneapolis, Minnesota.
>
> According to his guilty plea and documents filed in court, between 2011 and 2014, STEELE and his co-defendant PAUL R. HANSMEIER, both practicing lawyers, executed a scheme to obtain millions of dollars by threatening copyright lawsuits against individuals who allegedly downloaded pornographic movies from file-sharing websites. STEELE admitted in court during his plea that he and HANSMEIER created a series of sham entities, which they surreptitiously controlled, to obtain copyrights to pornographic movies – some of which they filmed themselves – and then uploaded those movies to file-sharing websites like "The Pirate Bay" in order to lure people to download the movies. STEELE and HANSMEIER then

> filed bogus copyright infringement lawsuits that concealed both their role in distributing the movies, and their personal stake in the outcome of the litigation. After filing the lawsuits, the defendants gained authority from the courts to subpoena internet service providers ("ISPs") for identification information of the subscriber who controlled the IP address used to download the movie. …
>
> In total, STEELE and HANSMEIER obtained approximately $3 million from the fraudulent copyright lawsuits."

"Prenda Law" er – så vidt vides – det eneste tilfælde, hvor det er påvist, at det i realiteten var sagsøgerne selv, der havde placeret de pågældende film i BitTorrent-netværk, og derved formentlig opnåede større fortjeneste på forlig og retssager om påståede ophavsretskrænkelser, begået via disse netværk, end der kunne have været opnået ved at afsætte filmene på markedet.

Uanset at retten ikke har noget grundlag for at fastslå, at noget tilsvarende gør sig gældende i nærværende sag, er det et retssikkerhedsmæssigt problem, hvis domstolene skulle konstatere, at der foreligger en krænkelse af ophavsretten, uden viden om, eller klare indikationer på, hvordan det omhandlede værk er havnet i fildelingsnetværket.

Det påhviler CMS/MIRCOM at sandsynliggøre, at der ligger en ophavsretskrænkelse bag, såfremt den omhandlede fil er delt i det omhandlede netværk, og herunder at det ikke er nogen med tilknytning til ophavsretsindehaveren, der har placeret værket i netværket og dermed delt det i netværket.

Retten har i den forbindelse noteret sig, at det i NTNU-rapport 2 to steder på s. 13, som citeret ovenfor, bemærkes, at CMS vender tingene på hovedet, når CMS i deres processkrifter fremkommer med synspunkter, der synes at være baseret på en forudsætning om, at brugerne i netværket kobler sig op til MaverikMonitor. Rapporten fastslår, at det forholder sig omvendt, da det er MaverikMonitor, der tager initiativ til opkoblingen med henblik på at finde brugere, der tilbyder filen.

En anden mulig forklaring på det af CMS i de pågældende processkrifter anførte, er imidlertid, at MaverikMonitors virkemåde i virkeligheden ikke blot er at efterspørge filer i de pågældende netværk, men også at stille filer til rådighed med henblik på at registrere, hvem der giver sig til at downloade disse filer.

Kontrol af data

I nærværende sagskompleks er det kun CMS/MIRCOM, der har haft mulighed for – ved gennemsyn – at undersøge om f.eks. to filer, navngivet f.eks. "London has Fallen" og "It Started With a Kiss for Riley and Elsa", som hentes i et BitTorrent-netværk, også reelt indeholder netop filmen "London has Fallen" henholdsvis scenen " "It Started With a Kiss for Riley and Elsa" fra pornofilmen "Girls that Like Girls".

Det er også kun CMS/MIRCOM, der har kunnet sammenholde filernes såkaldte hash-værdier med andre filers tilsvarende værdier.

Det er endvidere kun CMS/MIRCOM, der ved, hvor mange servere MaverikMonitor måtte have anvendt til at efterspørge filer i de pågældende netværk, og dermed i hvilket omfang MaverikMonitor selv kan have medvirket til at få en "swarm" til at fremstå større, end den i virkeligheden var.

På tilsvarende vis er det alene CMS/MIRCOM, eller måske snarere Maverickeye UG, der kan indestå for, at samtlige de angiveligt af MaverikMonitor indsamlede ip-adresser vitterlig er de ip-adresser, via hvilke den pågældende datatrafik har fundet sted. Det bemærkes herved, at det er uproblematisk at fremstille en talrække, der vil dække over en vilkårlig ip-adresse.

Hverken retten eller de sagsøgte har nogen reel mulighed for at efterprøve beviserne i disse henseender.

Spørgsmålet om hacking eller lignende

Det må i øvrigt konstateres, at CMS/MIRCOM's tilgang til spørgsmålene om, hvorvidt fejl i dataindsamlingen og datahåndteringen eller hacking eller beslægtet kriminalitet kan spille en rolle i sagerne, fremstår forsimplet.

Spørgsmålet om hacking eller beslægtet kriminalitet kan således ikke reduceres til alene at være et spørgsmål om, hvorvidt det er muligt og sandsynligt, at en sagsøgts routers accespoint kan være hacket.

Der findes andre former for hacking og it-kriminalitet, der vil kunne indebære, at den ip-adresse, som en abonnent er tildelt, enten er – eller blot fremstår som at være – den ip-adresse, hvorfra der begås kriminalitet, selvom det ikke er den pågældende abonnent, der står bag kriminaliteten, og uden, at den pågældende ved, at ip-adressen på den ene eller ande måde misbruges.

I rettens sag BS-29767/20109-FRB har sagsøgte fremlagt en rapport af 29. august 2019, "IP-adresser og brug i Danmark for Advokatgruppen.dk", udarbejdet af Henrik Lund Kramshøj, Zencurity ApS. I rapporten, s. 16 ff, anføres bl.a.:

”Der er også andre måder at få tilgang til IP-adresse og et netværk på. Private forbrugere har ofte ikke styr på IT-sikkerhed. Det er et komplekst emne som selv virksomheder i Danmark stadig kæmper med. Emnet omtales ofte som malware, virus og orme.
…
Udover at bryde ind i routeren er der mange enheder som tilbyder funktioner til at åbne forbindelser. En af disse er UPnProxy som giver angribere mulighed for at benytte andres internetforbindelser.

Når denne type funktion misbruges vil det se ud som om trafikken kommer fra forbrugerens enhed, men reelt er det en proxy funktion der blot videresender via denne forbindelse.

…

Det er meget sandsynligt at private computere som har været brugt til almindelig hjemmebrug har skadelig software. Mange private benytter enten ingen eller gratis anti-malware software til beskyttelse, som er utilstrækkelig.

Når man køber adgang til internet leveres typisk til privatbrugere en router-enhed. Denne enhed benytter udbyderens valgte teknologi, ADSL kobber, Fiber eller coax-antennekabel.

Disse enheder forbindes til internet men er i mange tilfælde ikke sikre. Enhederne skal være billige på grund af stor konkurrence mellem udbydere, og kunderne vil ikke betale en høj oprettelsespris.

Derfor er kvaliteten ikke god nok. Værre endnu kommer der ofte ingen opdateringer, og eventuelle opdateringer lægges ikke automatisk på enhederne.

…

Det betyder at kriminelle har næsten uhindret adgang til 100.000-vis af router-enheder over hele verden.

Eksempelvis kunne et botnet, Mirai botnet fra 2016 inficere omkring 900.000 enheder hos Deutsche Telekom.

…

> Almindelige forbrugere har ikke selv mulighed for at beskytte sig, og må forlade sig på den sikkerhed som udbyderen har valgt - ved valg af enhederne."

En rapport fra maj 2019 om et omfattende research-studie lavet af forskere fra bl.a. Indiana University, "Resident Evil: Understanding Residential IP Proxy as a Dark Service", beskriver, hvorledes ganske almindelige ip-adresser (i meget betydeligt antal på verdensplan) er gjort til en vare, som kan købes, med henblik på at lade adresserne blive udnyttet til at begå kriminelle handlinger, hvor det sløres, hvem der i virkeligheden står bag.

Flere hjemmesider udbyder angiveligt denne vare. Som et eksempel kan nævnes www.smartproxy.com, hvor man under overskriften "Why use a residential proxy network" anfører bl.a.:

> "You might want to hide your IP address for various reasons. Or you might need to scrape data from several websites, run many accounts from the same machine, upload or download torrents via P2P connections or stream geo-blocked content.
>
> Whatever the case is, a **residential proxy network is a great for hiding your true online identity**. It allocates genuine, residential IPs to you and hides your IP from servers for more online anonymity."

Der kan antageligt ses bort fra, at sådanne løsninger og den beskrevne handel med ip-adresser reelt anvendes af "almindelige" brugere af BitTorrent-netværk, der blot er interesserede i at downloade film uden at blive opdaget, bl.a. fordi det formentlig vil være billigere at betale for lovlig download end for sådanne løsninger.

De ovenfor nævnte kilder giver heller ikke i øvrigt retten noget sikkert grundlag for at konkludere noget med hensyn til, hvorvidt beviserne i nærværende sagskompleks – i form af de fremlagte ip-adresse-oplysninger – kan være misvisende i de enkelte sager, allerede som følge af, at der kan foreligge en kriminel udnyttelse af de pågældende ip-adresser.

Det synes imidlertid at ligge fast, at der eksisterer flere muligheder for at få datatrafik til at fremstå som om, den kommer fra en anden ip-adresse, end den i virkeligheden gør, eller for, at andre på anden vis kan udnytte en abonnents ip-adresse, uden at abonnenten er klar over det.

Sådanne it-tekniske forhold vil være ukendte for de fleste borgere, og de sagsøgte i sagskomplekset vil reelt heller ikke have mulighed for konkret at sandsynliggøre, at et eller flere af sådanne forhold kan have været en forklaring

på, hvorfor deres ip-adresse kan være kommet i spil som en adresse, hvorfra der angiveligt er begået ophavsretskrænkelser, og navnlig ikke, når den påståede krænkelse ligger flere år tilbage i tiden.

Teledata som bevis – og håndteringen heraf – indenfor strafferetsplejen, er endvidere i dag er af en sådan beskaffenhed og kompleksitet, at justitsministeren, som en udløber af den såkaldte teledatasag, har fundet det påkrævet at tage initiativ til at etablere et uafhængigt tilsyn med politiets og anklagemyndighedens behandling af de tekniske beviser, som politiet og anklagemyndigheden anvender i straffesager.

Der ses ikke, blot fordi en i øvrigt strafbar handling gøres til et bevistema under en civil sag, at være grundlag for en lempeligere behandling af spørgsmålet om pålideligheden af data, når disse er tilvejebragt – ikke af en offentlig myndighed, underlagt et objektivitetsprincip – men af et privat selskab, i hvert fald til dels med henblik på videreoverdragelse til andre selskaber, alle med potentielt store økonomiske interesser i at påberåbe sig validiteten af netop disse data.

Sammenfattende bemærkninger om ip-adressen som udgangspunkt for bevisførelsen i sagerne

Af samtlige de ovenfor nævnte grunde kan en af CMS/MIRCOM angiveligt registreret ip-adresse ikke stå alene som det eneste bevis i sagen og kan heller ikke danne grundlag for præsumptionsansvar, omvendt bevisbyrde eller lignende for den abonnent, der på det i stævningen konkret oplyste tidspunkt angiveligt var tildelt den pågældende ip-adresse.

EU-Domstolens dom i sag C-149/17 indebærer heller ikke, at det efter gældende dansk ret er udgangspunktet, at den person, der hos et teleselskab står anført som betaleren for et internetabonnement, ifalder et ansvar for eventuel kriminalitet begået ved hjælp af den pågældende internetforbindelse, med mindre den pågældende konkret kan pege på en bestemt anden gerningsmand end sig selv. Dette gælder selvsagt så meget desto mere, når det, som i sagerne i nærværende sagskompleks, end ikke som udgangspunkt kan anses for bevist, at en ophavsretskrænkelse har fundet sted, og at krænkelsen i givet fald er sket via den i den enkelte sag konkret angivne ip-adresse.

Selskaberne CMS, MIRCOM og Maverickeye UG m.fl.

CMS og MIRCOM

Retten har konstateret, at der ikke findes mange offentligt tilgængelige oplysninger om MIRCOM og de personer, der står bag dette selskab, der er baseret på Cypern. MIROM ses således bl.a. ikke at have nogen hjemmeside.

I processkrift af 20. januar 2020 i rettens sag BS-43373/2018-FRB har CMS om MIRCOM anført:

> "CMS har til brug for to verserende ankesager, der behandles ved Østre Landsret, indhentet yderligere dokumentation fra MIRCOM, der bekræfter, at de to virksomheder samarbejder, og at MIRCOM har overdraget påtaleretten til CMS i blandt andet Danmark."

CMS og Maverickeye UG

CMS's hjemmeside er ikke særlig rig på indhold og information. Der er bl.a. ingen information om de personer, der står bag selskabet, og der er heller ikke nogen navne på ansatte. Siden ses ikke opdateret siden januar 2018.

Flere sagsøgte i sagskomplekset har påpeget, at CMS er stiftet af Patrick Achache, der ligeledes har stiftet Maverickeye UG, der står bag MaverikMonitor.

Af et opslag af 10. november 2015 på Maverickeye UG's hjemmeside fremgår bl.a.:

> "**NJORD and Maverickeye to endorse awareness campaign in Finland**
>
> Maverickeye (ME) has just closed a new deal with NJORD, a Scandinavian law firm that specializes in data protection, intellectual property law, and many other areas, and has been ME's partner law firm in Denmark for quite some time now. Together, the 2 companies aim to take over Finland and spread better awareness on copyright infringement.
>
> …
>
> FINLAND TAKEOVER
>
> NJORD Now, Finnish citizens can expect getting settlement demands as NJORD takes over Finland by storm. Unless an ISP account owner answers questions raised in a demand letter, he or she runs the risk of being prosecuted as an infringer under the Finnish law. NJORD will also make examples of those who have ignored the notices or have not engaged with them.

…

THE PARTNERSHIP

Patrick Achache of Maverick Eye closed the deal with Njord because he trusts in the expertise of the firm's lawyers. He supports the claims made in Denmark (especially for DBC ["Dallas Buyers Club"]) and strongly considers illegal downloading as stealing from rights holders.

THE GOAL

The main goal of the partnership between Maverickeye and Njord is to protect client's data, particularly their movies, and the whole entertainment industry not just in Finland and Denmark but around the world. …

At Maverickeye, we see a chance to protect our clients, their movies, and the whole entertainment industry by working with other companies that share the same advocay. This bold move is just one of our ways to show to the public that we constantly innovate to fight infringement. We want people to understand that what we aim for goes beyond reducing piracy; we want to prevent illegal downloading entirely."

Af et opslag af 11. november 2016 på hjemmesiden fremgår endvidere bl.a.:

"Movie piracy battle strengthened in Scandinavia

Last year, MaverickEye and NJORD Law Firm announced a joint enforcement program in Finland. Since then, enforcement has started related to more than 30 movies also but also in Denmark, Norway, and Sweden. Now the effort is being further strengthened.

On October 12 2016, the Danish Producers Association confirmed a cooperation with NJORD Law Firm using MaverickEye data to offer its members a subscription to attack individual up-/downloaders.

…

This broad approach will strengthen NJORD Law Firm's and MaverickEye's ongoing battle against movie piracy in Denmark, says XX at MaverickEye:
(Quote by person from MaverickEye)
Full service approach at a fixed rate

> The first members have already signed up and MaverickEye is now investigating the scope of the infringement for some of the biggest Danish film producing companies.
>
> Meanwhile NJORD is this Autum sending out several thousand letters a week alone in Denmark.
>
> "Based on previous experience, we expect that all subscribers will receive positive payoff, meaning the settlements paid by the receivers of the letters will exceed the costs for our reports and administrative work", says Partner Jeppe Brogaard Clausen, who initiated the approach at NJORD Law Firm."

Dette opslag ses bl.a. at kunne sammenholdes med de sager i sagskomplekset vedrørende Zentropa-film, som Retten på Frederiksberg tidligere har afvist, bl.a. under henvisning til, at det fremlagte aftalegrundlag bl.a. bestod i en e-mailkorrespondance af 1. og 2. november 2016 mellem advokat Jeppe Brogaard Clausen og Zentropas managing director, hvor der i øvrigt ikke blev nævnt noget om CMS. Retten bemærkede endvidere, at Zentropa ved advokat Jeppe Brogaard Clausen herefter optrådte som rekvirent i sagerne om isoleret bevisoptagelse og edition.

Det må således – også på baggrund af informationerne på Maverickeye UG's hjemmeside – konstateres, at det fremstår uklart, hvilken nødvendig rolle CMS skulle have spillet, og hvilket behov CMS skulle have udfyldt i Maverickeye UG's og Njord Law Firms "ongoing battle against movie piracy in Denmark." CMS ses heller ikke umiddelbart omtalt på øvrige dele af Maverickeye UG's hjemmeside.

Af en artikel bragt i K-News den 17. januar 2020 og sammenholdt med oplysninger tilgængelige via Companies House, beta.companieshouse.gov.uk, fremgår, at Patrick Achache den 19. november 2019 har overdraget kontrollen med CMS fra sig selv til Lubesly Tellidua, der er skønhedsdronning på Filippinerne.

CMS, Maverickeye UG og Hatton & Berkeley

Den sagsøgte borger i rettens sag BS-6619/20 (hvor CMS' påståede krav i øvrigt var forældet) hæftede sig i sine processkrifter bl.a. ved CMS' beskedne økonomiske forhold, således som de fremgår af de tilgængelige oplysninger hos Companies House.

Af de af Patrick Achache den 8. juli 2019 underskrevne, ikke reviderede regnskabsoplysninger for CMS for 2018, som disse er indleveret hos Companies House fremgår bl.a.:

”Cash at bank and in hand	$ 92,802

Average number of employees, including directors during the year was as follows: 1

Due within one year	
Trade debtors	$ 190,039
Prepayments and accrued income	-
Other debtors	$ 1,163
…	

Creditors: Amounts Falling Due Within One Year

Trade creditors	$ 260,763
Corporation tax	$ 3,742
Other Creditors	$ 990

Share Capital

Alloted, Called up and fully paid	$ 1”

Sagsøgte hæftede sig endvidere ved, at der tilsyneladende er et meget stort antal selskaber, der har samme adresse som CMS – 43 Berkeley Square i London – uagtet at bygningen på denne adresse ifølge Google Streetview skulle være af relativ beskeden størrelse.

Af selskabet Hatton & Berkeleys hjemmeside fremgår, at dette selskab har adresse i London på 43 Berkeley Square. Det fremgår også, at Hatton & Berkeley blandt mange andre ydelser tilbyder ”copyright protection”. En billedtekst herom på hjemmesiden lyder:

> “Pictured above here with Robert Croucher (Hatton & Berkeley) is Patrick Achache, the talented young tech entrepreneur who turned his hand to developing software that tackles digital piracy for the film and TV industries.”

Herudover tilbyder Hatton & Berkeley oprettelser af såkaldt ”virtual offices”. Der anføres følgende herom på hjemmesiden:

> “At **Hatton & Berkeley**, we understand how important the reputation of your business is. Your prestigious Berkeley Square address will create the right impression and will make your clients assured of the quality and service of your business.”

Af et opslag af 24. september 2015 på Maverickeye UG's hjemmeside fremgår bl.a.:

> "Hatton & Berkeley and Maverick Eye to support one of the biggest anti-piracy efforts in the UK. Together with international sales and distribution partners, the 2 notable companies will work together to tackle issues of digital piracy.
>
> On its official press release published on www.hattonandberkeley.com, Hatton & Berkeley said:
>
> "Hatton & Berkeley stands alongside our colleagues in an international operation that has so far yielded drastic reductions in streaming, torrenting, and illegal downloads across Europe."
>
> …
>
> Maverick Eye believes in the protection of creative works and trademarks against piracy in the digital world. The company provides court-tested reliable data and support for rights holders. With its recent association with Hatton & Berkeley, Maverick Eye will further expand its notable efforts to support enforcement and passionate advocacy in "the UK's largest anti-piracy campaign ever".
>
> …
>
> Patrick Achache, cofounder and consultant for Maverick Eye, said:
>
> "We look forward to supporting Hatton and Berkeley in their program in the UK. Hatton and Berkeley understands the needs of their clients. They understand the big picture. Working with Robert (Croucher), we will be able to provide them with the support they need for efficiently and effectively dealing with the problems of piracy."

Ifølge hjemmesiden opencorporates.com var selskabet H & B Administration LLP, der angiveligt ledes af Robert Croucher, tidligere i partnerskab med bl.a. Hatton & Berkeley Management Ltd. og CMS, og selskabets angivelige"ultimate beneficial owners" er bl.a. Patrick Achache og Lubesly Tellidua.

Britiske medier har også bragt flere artikler om Robert Croucher og Hatton & Berkeleys indsats for bekæmpelse af ulovlig download af film i England, herunder f.eks. artiklen af 5. marts 2016 på www.expressandstar.com "Family of 83-year-old great grandmother who 'can just about turn the computer on' brand

claims she illegally downloaded film 'laughable'" og artikel af 23. september 2016 i The Times.

Sammenfattende om selskabernes forhold

Retten bemærker, at ingen af de ovennævnte forhold i sig selv bevirker, at det kan udelukkes, at CMS og MIRCOM er reelle foretagender, der har forsøgt at forfølge reelle ophavsretskrænkelser.

Hvis CMS/MIRCOM havde været rette sagsøger i sagerne i sagskomplekset kunne retten imidlertid efter en samlet vurdering af forholdene og bevisets stilling i øvrigt – efter omstændighederne – have været nødsaget til at søge bl.a. de pågældende forhold nærmere belyst under anvendelse af retsplejelovens § 339, stk. 2, henholdsvis § 406, stk. 3, med henblik på at sikre, at der var det fornødne grundlag for nærmere at kunne vurdere ikke blot den sagsøgte borgers pålidelighed og troværdighed, men også sagsøgers pålidelighed og troværdighed.

På det foreliggende grundlag kan retten imidlertid blot konstatere, at selskabernes ovenfor nævnte forhold umiddelbart yderligere understøtter rigtigheden af konklusionen i Østre Landsrets domme af 8. april 2020.

Betydningen af Østre Landsrets kendelse af 7. maj 2018 (U 2019.2019 Ø) og databeskyttelsesforordningen

Retten på Frederiksberg har i sin endelige dom af 22. maj 2019 i sag BS-31445/2018-FRB indirekte berørt spørgsmålet om betydningen af Østre Landsrets kendelse af 7. maj 2018, gengivet i U 2019.2019 Ø.

Af dommens præmisser fremgår bl.a.:

> "Af Østre Landsrets kendelse af 7. maj 2018 i 20. afdelings sag nr. B-2451-17 og sag nr. B-2458-17, der drejer sig om Copyright Management Services Ltd.'s anmodning om editionspålæg til teleselskaber om udlevering af navne og adresser på abonnenter, der er tildelt ip-adresser, på baggrund af antagelser om ulovlig fil-deling fra de pågældende ip-adresser, fremgår bl.a.:
>
> > "Som anført er det ubestridt, at Telenor og Telia har rådighed over de ønskede oplysninger om hvilke abonnenter, der var tildelt de anførte ip-adresser på de anførte tidspunkter. Da oplysningerne er nødvendige for at bidrage til afklaring af, hvem der kan anlægges sag mod, må de anses for at være af betydning for sagen. Det ændrer ikke herved, at oplysningerne muligvis

ikke i sig selv vil være tilstrækkelige til, at rettighedshaverne kan få medhold i en civil sag om en rettighedskrænkelse.

Efter retsplejelovens § 299, stk. 1, kan der ikke meddeles editionspålæg om forhold, som teleudbyderne ville være udelukket fra eller fritaget for at afgive forklaring om som vidne, jf. lovens §§ 169-172. Efter retsplejeloves § 170, stk. 3, kan retten bestemme, at forklaring ikke skal afgives om forhold, med hensyn til hvilke vidnet i medfør af lovgivningen har tavshedspligt, og hvis hemmeligholdelse har væsentlig betydning. Efter bestemmelsens ordlyd er udgangspunktet dog, at der er vidnepligt.

Efter telelovens § 7, stk. 1, har Telenor og Telia pligt til at hemmeligholde oplysninger om deres abonnenters brug af nettet og har således tavshedspligt bl.a. i relation til de oplysninger, som ønskes udleveret. Efter udbudsbekendtgørelsens § 23, stk. 1, har Telenor og Telia endvidere som udgangspunkt pligt til at slette eller anonymisere trafikdata. Trafikdata kan – og skal – imidlertid efter udbudsbekendtgørelsens § 23, stk. 1, opbevares med henblik på udlevering til politiet efter retsplejelovens § 786, stk. 4, hvorefter der skal ske logning som fastsat i logningsbekendtgørelsen.

Disse bestemmelser skal navnlig ses i sammenhæng med e-databeskyttelsesdirektivets artikel 5 og 6 om kommunikationshemmelighed og sletning af trafikdata samt direktivets artikel 15 om adgangen til at foretage indskrænkninger i rækkevidden af bl.a. disse bestemmelser. Endvidere skal bestemmelserne ses i sammenhæng med de hensyn, der skal varetages efter EU's charter artikel 7, 8 og 52, stk. 1, om respekt for privatliv og familieliv, beskyttelse af personoplysninger og proportionalitetshensyn og EMRK's artikel 8 ligeledes om respekt for privatliv og familieliv, jf. herved EU-charter artikel 52, stk. 3, således som disse bestemmelser er fortolket bl.a. af EU-Domstolen i dom af 8. april 2014 i sag C-293/12 (Digital Rights Ireland Ltd), i dom af 21. december 2016 i de forenede sager C-203/15 og C-698-15 (Tele2 Sverige AB og Watson m.fl.) og af Den Europæiske Menneskerettighedsdomstol i dom af 4. december 2008 i sag 30562/04 og 30566/04 (S. og Marper mod Storbritannien).

Det følger endvidere af EU-Domstolens dom af 29. januar 2008 i sag C-275/06 (Promusicae) og dom af 19. april 2012 i sag C-461/10

(Bonnier Audio AB), at bl.a. e-databeskyttelsesdirektivet ikke er til hinder for nationale regler om udlevering af oplysninger om en abonnents ip-adresse i forbindelse med retsforfølgning af krænkelse af ophavsrettigheder, men at der skal være mulighed for at foretage en afvejning af de modstridende interesser i sagen i forbindelse med en sådan udlevering af oplysninger.

Under henvisning til telelovens § 7, stk. 1, og udbudsbekendtgørelsens § 23, stk. 1, og henset til de ovennævnte forhold samt til, at de data, der ønskes udleveret til en privat aktør i medfør af de civilprocessuelle regler i retsplejelovens § 343, jf. § 299, alene fortsat er i teleudbydernes besiddelse, fordi teleudbyderne ifølge logningsbekendtgørelsen udstedt efter reglerne i strafferetsplejen er forpligtet til at opbevare dem med det formål, at de efter retskendelse skal kunne udleveres til politiet som led i efterforskning og retsforfølgning af strafbare forhold, finder landsretten, at der er tungtvejende grunde til hemmeligholdelse af de teledata, der ønskes udleveret.

Disse tungtvejende grunde skal afvejes over for CMS' interesse i at få oplysningerne udleveret.

CMS har sandsynliggjort, at der kan have fundet ophavsretskrænkelser sted, som vil kunne retsforfølges af rettighedshaverne, herunder efter ophavsretslovens § 81. Omfanget af de angivelige krænkelser, der er omfattet af begæringerne under denne sag, må ved en samlet bedømmelse også anses for betydeligt. Det nærmere omfang heraf i relation til den enkelte abonnent er imidlertid ikke nærmere dokumenteret.

Selv om det må antages, at rettighedshaverne ikke uden udlevering af oplysningerne kan forfølge et eventuelt krav direkte over for de abonnenter, hvis internetforbindelse har været anvendt til disse ophavsretskrænkelser, finder landsretten efter en samlet afvejning, at CMS's interesse i at få udleveret oplysningerne over for hensynet til de enkelte abonnenters krav på hemmeligholdelse ikke kan begrunde en udlevering af de under sagen omhandlede oplysninger i medfør af retsplejelovens § 343, jf. § 299."

Ved kendelsen har Østre Landsret således fastslået, at teleselskaber ikke via edition kan pålægges at udlevere oplysninger om navn og adresse på en abonnent, der er tildelt en angiven ip-adresse, og at

> selskaberne heller ikke lovligt kan udlevere disse oplysninger, til brug for en civil sag."

Retten har endvidere i forlængelse heraf i en retsbog af 7. november 2019 i rettens sag BS-30249/2019 bl.a. anført:

> "Det spørgsmål, som kendelsen af 7. maj 2018, gengivet i U 2019.2019 Ø, rejser i forhold til de verserende sager, er […] ikke, om de forudgående kendelser om isoleret bevisoptagelse og edition er retskraftige i den forstand, at de pågældende teleselskaber på daværende tidspunkt har udleveret personoplysningerne om de sidenhen sagsøgte borgere i sagskomplekset med rette.
>
> Spørgsmålet er derimod, om domstolene er forpligtet til på nuværende tidspunkt at rette op på, at de pågældende personers rettigheder, der bl.a. afledes af Den Europæiske Menneskerettighedskonventions artikel 8 og EU's charter, ikke er blevet behørigt beskyttet ved de tidligere byretsafgørelser, når dette i øvrigt stadig er muligt for domstolene, fordi de verserende sager ikke er afgjort.
>
> Spørgsmålet er i den forbindelse også, om det modsatte – at domstolene ikke har en sådan forpligtelse – kan begrundes, herunder også ud fra et almindeligt princip om ligebehandling af borgerne, og herved henset til, at 4.011 personer ved landsrettens kendelse fik deres oplysninger beskyttet bl.a. under henvisning til afvejningen af hensynet til deres menneskerettigheder over for hensynet til CMS' interesse i at kunne forfølge sagerne, og at disse 4.011 personer dermed ikke kunne retsforfølges af CMS, selv om de angiveligt, og på samme grundlag, som de borgere, der nu er stævnet, havde begået tilsvarende ophavsretskrænkelser.
>
> Disse spørgsmål må formentlig endvidere vurderes i lyset af, at de borgere, hvis personoplysninger er blevet udleveret til CMS, ikke var part i de sager om isoleret bevisoptagelse og edition, der ligger til grund for udleveringen af oplysningerne, og at retsgrundlaget var det samme, da de oprindelige editionsafgørelser blev truffet, som da landsretten siden afsagde sin kendelse af 7. maj 2018.
>
> Da de pågældende borgere ikke var part i sagerne, havde de ikke adgang til at påberåbe sig f.eks. deres menneskerettigheder i denne proces, og de havde dermed heller ingen adgang til at kære de afgørelser, der blev truffet i byretten, og som siden – ved landsrettens kendelse af 7. maj 2018 – har vist sig at skulle have haft et andet udfald.

> Da reglerne i retsplejelovens § 340, stk. 2, om advokatbeskikkelse heller ikke var benyttet, var der i øvrigt heller ingen andre til at repræsentere borgerne og eventuelt på deres vegne påberåbe sig deres menneskerettigheder m.v. i denne del af processen."

Hertil må imidlertid også bemærkes, at det fremgår af retsplejelovens § 393, stk. 1, at kære kan iværksættes af enhver, over for hvem kendelsen eller beslutningen indeholder en afgørelse.

Under de ovenfor nævnte omstændigheder modtog de borgere, der viste sig at være de reelle adressater for Retten på Frederiksbergs afgørelser om, at deres personoplysninger skulle udleveres, imidlertid aldrig den for dem relevante afgørelse fra Retten på Frederiksberg.

Der var således heller ikke ingen, der på daværende tidspunkt vejledte de pågældende borgere om deres adgang til at kære den pågældende afgørelse. En sådan kærevejledning er heller ikke givet siden.

Hvis borgerne havde fået meddelelse om afgørelsen og kærevejledning, ville borgerne – og ikke blot teleselskaberne – have haft mulighed for at kære de pågældende kendelser med opsættende virkning med det resultat, at de pågældende oplysninger ikke var blevet udleveret, idet Østre Landsret ville have omgjort Retten på Frederiksbergs kendelser.

Der er herudover heller ingen – herunder heller ikke CMS eller MIRCOM – der efterfølgende har oplyst borgerne om landsrettens kendelse af 7. maj 2018.

Da borgerne endvidere i vidt omfang var uden advokatbistand var der heller ikke nogen til at vejlede borgerne om kendelsens betydning for deres retsstilling, selv hvis de pågældende borgere måtte have været bekendt med afgørelsen via medieomtale af denne.

Under disse omstændigheder kan der rejses spørgsmål om, hvorvidt borgernes kærefrist overhovedet er begyndt at løbe, og hvis den er begyndt at løbe, fra hvornår, dette i givet fald er sket, og om der eventuelt vil være anledning til at meddele borgerne oprejsningsbevilling.

Disse spørgsmål må i øvrigt besvares i lyset af artikel 13 i Den Europæiske Menneskerettighedskonvention, der har følgende ordlyd:

> "Enhver, hvis rettigheder og friheder efter denne konvention er blevet krænket, skal have adgang til effektive retsmidler herimod for en

> national myndighed, uanset om krænkelsen er begået af personer, der handler i embeds medfør."

Det følger i øvrigt af praksis vedrørende bestemmelsen, at et "effektivt retsmiddel" efter omstændighederne kan kræve, at der tillægges opsættende virkning.

Spørgsmålene må endvidere besvares i lyset af artikel 47, stk. 1 og 2, i Den Europæiske Unions Charter om grundlæggende rettigheder, der har følgende ordlyd:

> "Enhver, hvis rettigheder og friheder som sikret af EU-retten er blevet krænket, skal have adgang til effektive retsmidler for en domstol under overholdelse af de betingelser, der er fastsat i denne artikel.
>
> Enhver har ret til en retfærdig og offentlig rettergang inden en rimelig frist for en uafhængig og upartisk domstol, der forudgående er oprettet ved lov. Enhver skal have mulighed for at blive rådgivet, forsvaret og repræsenteret."

Det følger af EU-Domstolens praksis, jf. bl.a. sag C-619/10, Trade Agency, at retten til en retfærdig rettergang efter art. 47 kræver, at enhver retsafgørelse er begrundet, således at det er muligt for sagsøgte dels at forstå, hvorfor han er blevet dømt, dels på nyttig og effektiv vis at tage retslige skridt til prøvelse af en sådan afgørelse.

Det siger sig selv, at en borger ikke gives nogen mulighed for på effektiv vis at tage retslige skridt til prøvelse af en afgørelse, hvis borgeren aldrig får afgørelsen meddelt.

Det følger endvidere af EU-Domstolens praksis, jf. bl.a. sag C-472/11, Banif Plus Bank, at det vil være en krænkelse af den grundlæggende ret til effektiv domstolsbeskyttelse, hvis en retsafgørelse er baseret på faktiske omstændigheder og dokumenter, som parterne, eller en af disse, ikke har kunnet skaffe sig kendskab til, og som de således ikke har kunnet tage stilling til i en kontradiktorisk proces.

Det siger sig selv, at en borger ikke gives nogen mulighed for at tage stilling til en sag, som borgeren ikke får at vide, at borgeren reelt er part i.

Det har i øvrigt formodningen for sig, at EU-Domstolen i sag C-597/19 vil komme frem til et resultat, der understøtter rigtigheden af Østre Landsrets kendelse af 7. maj 2018, og at EU-Domstolen også vil fastslå, at MIRCOM's (og dermed også CMS's) dataindsamling er sket i strid med databeskyttelsesforordningen.

At dataindsamlingen er sket i strid med databeskyttelsesforordningen vil så meget desto mere være tilfældet, når CMS og MIRCOM ikke på tidspunkterne for indsamling af data har haft et (tilstrækkeligt) aftalegrundlag med de eventuelle indehavere af ophavsrettten til de værker, hvis angivelige udbredelse i de pågældende netværk, man har indsamlet data om.

Hvis der herefter skal rådes bod på de skete krænkelser af borgernes rettigheder, og hvis det skal sikres, at domstolene ikke opretholder krænkelserne ved at afsige domme, der hviler på krænkelserne, ses domstolene ikke at have anden mulighed end at afskære CMS og MIRCOM fra at benytte de indsamlede data og udleverede personoplysninger.

Når CMS/MIRCOM endvidere ikke er rette sagsøgere i sagerne i sagskomplekset, var de heller ikke rette sagsøgere i sagerne om edition og isoleret bevisoptagelse.

De personoplysninger om de sagsøgte, som CMS og MIRCOM på denne baggrund med urette er kommet i besiddelse af, er de forpligtede til at slette, jf. databeskyttelsesforordningens artikel 17 og (bl.a.) den af Østre Landsret ved kendelsen af 7. maj 2018 foretagne interesseafvejning.

CMS og MIRCOM kan således heller ikke med rette videregive personoplysningerne til indehavere af ophavsretten af de i sagskomplekset omhandlede film, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra f, sammenholdt (bl.a.) med den af Østre Landsret ved kendelsen af 7. maj 2018 foretagne interesseafvejning.

Konklusion

Af samtlige de ovenfor nævnte grunde ville fortsat behandling af denne sag, og de øvrige for retten verserende sager i sagskomplekset – selv hvis Copyright Management Services Ltd. havde godtgjort retten til at føre sagen i eget navn – stride mod væsentlige hensyn til retsordenen og borgernes retssikkerhed og adgang til en retfærdig rettergang.

Retten afsagde herefter

KENDELSE

Som følge af Østre Landsrets domme af 8. april 2020 i sagerne BS-39423/2019-OLR og BS-41550/2019-OLR skal denne sag afvises fra domstolene.

Retten bemærkede, at L skal anses for at have vundet sagen, og at det skal pålægges CMS at betale fulde sagsomkostninger, jf. retsplejelovens § 314.

Ved fastsættelsen i medfør af retsplejelovens § 316, stk. 1, af det passende beløb til erstatning af udgifter til advokatbistand til L, skal der lægges vægt på sagens værdi, omfang og karakter.

Retten bemærker om sagens omfang og karakter, at den, som følge af CMS's forhold – i forhold til sagens værdi – har haft et betydeligt omfang og en betydelig grad af kompleksitet.

Efter en samlet vurdering kan beløbet til erstatning af udgifter til advokatbistand herefter passende fastsættes til 15.000 kr., inklusiv moms.

Thi bestemmes:

Denne sag afvises fra retten.

Copyright Management Services Ltd. skal inden 14 dage skal betale 15.000,00 kr. i sagsomkostninger til L.

Sagsomkostningerne forrentes efter rentelovens § 8 a.

Sagen sluttet.