Kandidatspeciale

Hvordan krænkes ophavsretten ved brug af indholdsdelingstjenester med særlig fokus på brugerens ansvar og rettighedshavernes håndhævelse

Simon Kviesgaard - studienr. 20156995

AALBORG
UNIVERSITET

Titelblad

Dansk titel:	Hvordan krænkes ophavsretten ved brug af indholdsdelingstjenester med særligt fokus på brugerens ansvar og rettighedshavernes håndhævelse
Engelsk titel:	The users' liability for copyright infringements using filesharing services, and the rights holders access to law enforcement.
Semester:	10. Semester
Forfatter:	Simon Kviesgaard
Fagområde:	Ophavsret
Vejleder:	Lene Wacher Lentz
Universitet:	Aalborg Universitet
Data for aflevering:	2. december 2022

Tegn:

Abstract

The past few years, there's been countless headlines describing the arrival of intimidating letters, sent from lawyers to the Danish citizens, with a demand of payment for watching illegally pirated copyright protected work.

Despite the harsh critic met from a wide variety of the public, the enforcement of the rights holders demands, maintain an important societal function. Each year rights holders and artistic producers are losing monumental amounts of revenue, due to piracy.

The thesis seeks to describe the liability of the user and furthermore the rights holder's access to law enforcement.

This is done by first describing the technical proces facilitating the copyright infringement, followed by a thorough description of national and European law to combine the describing chapter of the thesis.

The initial description is followed by an analysis of the surrounding legislation, and a verbatim analysis of the settlement letter, sent by a representative of the rights holder. Among the surrounding legislation, the thesis focuses on analyzing relevant logging legislation. This is the appropriate target point, as it resembles the primary barrier in place, disabling the rights holders from prosecuting the liable users.

To further illuminate the subject, case law is being analyzed throughout the thesis. As this subject serves as a very dynamic field of law, that rapidly evolves, only using national case law is seldom sufficient. The thesis combines the two, describing the current state of law based on national case law, and the evolution of the field based on European case law.

Historically, the logged information such as name- and address information were loosely passed on to a variety of actors. However, with the recent international focus on data protection, the process of passing on personal data for civil lawsuits are becoming increasingly limited.

Finally, the thesis contains a perspectivation of the logging legislation. This serves as a description of the newly incorporated logging legislation, that arrived as a result of our national duty to comply with European legislation. The perspectivation continues with the help of a summary of existing and newly implemented law, as well as case law, to provide a hypothetical approach on the future options for the rights holders.

Indholdsfortegnelse

Kapitel 1

1.1 Indledning

I mange år har overskrifter som ”Ulovlige downloads: Tusindvis har fået dette dyre brev”[1], ” Downloader du film ulovligt? Nu er du jaget vildt”[2] og ”Anklagerne rammer som spredhagl i PIRATBREVENES ÅRTI”[3] verseret i det danske nyhedsbillede.

Når den almene dansker modtager et brev med en advokatsignatur, modtager det typisk en reaktion. Som overskrifterne antyder, har den været markant over det sidste årti.

Som der kan læses fra artiklerne, modtager rettighedshaverne, som i dette tilfælde ligeledes agerer som de eneste retshåndhævere, en del kritik for fremgangsmåden. Kritikken er også kommet fra officielle instanser, som f.eks. Forbrugerrådet Tænk.

”Selvfølgelig er det ikke i orden at downloade film ulovligt, men brevene har karakter af trusselsbreve. Betal nu, og du slipper for tiltale. Det er absurd, at advokatfirmaerne går efter den enkelte forbruger på den måde – og at nogle føler sig presset til at betale, selvom de måske er uskyldige”[4]

Imens tilgangen til retshåndhævelsen af rettighedshavernes krav måske ikke i alle tilfælde har været lige professionel, så opstår spørgsmålet om nødvendigheden alligevel. Hvis brugerne ikke havde en konsekvens for deres ophavsretlige krænkelser, ville det have markante konsekvenser for rettighedshavernes fortsatte forretning.

Konsekvenserne for producenterne belyses i et citat fra producentforeningen ”
”Ulovlig streaming og download af film og serier har store konsekvenser for den danske filmbranche, ikke mindst for dem, som bruger kræfter og penge på at skabe filmene. Tal viser, at der hvert år ses 4.000.000 danskproducerede film og 6.000.000 danskproducerede serieepisoder ulovligt. Det er vildt høje tal, som direkte betyder at der mangler indtægter og det skader hele produktionskæden – lige fra idegenerering, til produktion og talentudvikling. …”[5] *– Jørgen Ramskov - Direktør*

Denne afhandling belyser brugerens ansvar for fildelingstjenester til at opnå uretmæssig adgang til ophavsbeskyttet indhold, og de forskellige aktørers mulighed for retshåndhævelse af krænkelsen.

Indledningsvist belyses hvordan brugerne ulovligt tilgår ophavsretligt beskyttet materiale. En forklaring på de tekniske foranstaltninger som danner rammerne afhandlingens emne.

Heraf massekrav og hvordan dette retfærdiggøres fra deres side. Efterfulgt af en ordlyds gennemgang af de fremsendte breve til offentligheden. Forud for denne fremsendelse, har rettighedshaverne som er repræsenteret af NJORD Law Firm, indhentet oplysninger ved

[1] https://ekstrabladet.dk/forbrug/Teknologi/ulovlige-downloads-tusindvis-har-faaet-dette-dyre-brev/6485619
[2] https://ekstrabladet.dk/forbrug/Teknologi/downloader-du-film-ulovligt-nu-er-du-jaget-vildt/6439939
[3] https://www.k-news.dk/nyheder/piratbrevenes-aarti.-anklagerne-rammer-som-spredhagl
[4] https://finans.dk/erhverv/ECE9018989/danskere-faar-breve-om-ulovlig-download-af-film-nu-bliver-firmaet-bag-brevene-gransket/

hjælp af en speciel monitorerings software, kaldet MaverickEye, og derigennem opfanget krænkernes IP-adresser.

IP-adresserne som rettighedshaverne i domsanalysen havde på lister, kan ikke identificere personerne bag krænkelsen. Det er derfor en forudsætning for afsendelse af brevene, at rettighedshaverne modtager navne- og adresseoplysninger fra internetudbyderne. Videregivelsen af disse oplysninger, er den eneste retshåndhævelsesmulighed rettighedshaverne har for at forfølge deres krav.

Rettighedshaverne kan komme i besiddelse af de fornødne oplysninger på to måder. Hvis teleudbyderne videregiver oplysningerne frivilligt, eller hvis teleudbyderne pålægges at videregive oplysninger af retten, ved edition. Rettighedshavernes grundlag for denne videregivelse møder en stigende mængde begrænsninger, samtidig med at persondataretten yder en stigende beskyttelse for borgerne.

Det er et ømtåleligt emne, da der tegnes et billede af NJORD Law Firm som svindlere og bedragere, i hvert fald hvis man skal opfatte ovenstående artikler som sandhed. Men hvis man ser bort fra udførelsen, så udfører de fundamentalt en vigtig samfundsfunktion. Såfremt dette område forbliver overset af lovgiverne, og rettighedshavernes eneste tilgang til retshåndhævelse er igennem strafferetlige logningsdatabaser, vil indtjeningsgrundlaget for film, musik, spil, kunst og meget andet som kan tilgås ulovligt, blive udtyndet.

I en undersøgelse fra Dansk Erhverv, fandt de, at 12% af danskerne indenfor 12 måneder har downloadet eller streamet ulovligt indhold på internettet. Det er ca. 560.000 personer.[6] Kun 35% af danskerne i alderen 18-29 fraholder sig fra at tilgå disse tjenester i frygt for bødestraf.

I afhandlingen tilstræbes det at belyse et billede af den nugældende retstilstand, med indførelsen af det nye persondataretlige lovgrundlag, samt udvikling i retspraksis, hvordan rettighedshaverne kan forfølge deres legitime interesse.

[6] https://www.danskerhverv.dk/siteassets/mediafolder/dokumenter/01-analyser/analysenotater-2020/ulovlig-streaming-og-download-i-danmark-i-2020.pdf

1.2 Metodeafsnit

I nærværende afhandling, vil den retsdogmatiske metode anvendes. Metoden karakteriseres ved at der beskrives, systematiseres og analyseres den gældende ret indenfor området. I samme forbindelse skal retskilder og fortolkningsprincipper anvendes.[7]

Fortolkningsprincipperne tjener som hjælpemidler til forståelsen af retsreglerne som anvendes.[8] Til udarbejdelsen af forestående afhandling, anvendes følgende fortolkningsprincipper: ordlydsfortolkning, formålsfortolkning, indskrænkende fortolkning samt direktivkonform fortolkning.

Hvad angår ordlydsfortolkningen, indebærer dette at den almindelige forståelse af ordlyden lægges til grund for en udredning af forståelsens helhed. Ordlydsfortolkningen vil danne grundlag for afhandlingen, og udgør dermed det klare udgangspunkt af fortolkningsprincipperne.[9] En formålsfortolkning afgør formålet med en given lovgivning, hvad lovgiver gerne vil opnå med en pågældende bestemmelse. En formålsfortolkning kan imidlertid både være objektiv og subjektiv.

Den objektive formålsfortolkning angår lovens indhold, og har dermed en tæt tilknytning til ordlydsfortolkningen.

Ved en subjektiv formålsfortolkning anvendes udelukkende den mening forarbejderne havde med udarbejdelsen af loven.[10]

Den indskrænkende fortolkning anvendes flere steder. Bl.a. i redegørelsen for EU-direktiverne, hvor man ser en indskrænkende fortolkning fra de nationale myndigheder, som hjemlet i direktivets artikel 6. Den indskrænkende fortolkning er kendetegnet ved, at anvendelsesområdet for en given retsregel indskrænkes.[11] Dette fortolkningsprincip vil især være gældende, når retsreglerne omhandler en indskrænkning af en borgers rettigheder.[12]

Slutteligt anvendes den direktivkonforme fortolkning i forbindelse med de inddragede EU-direktiver, og deres samspil med gældende national ret. De nationale retsregler, skal fortolkes i overensstemmelse med de EU-retlige direktiver.[13]

Afhandlingen vil anvende lovgivning fra både EU og Danmark. Lande som tilmelder sig EU, afgiver en del af deres suverænitet, for at føje samarbejdet med de mellemfolkelige myndigheder. I Danmarks tilfælde, er dette med hjemmel i Grundlovens §20, stk. 1.De danske lovgivere samarbejder med de EU-retlige lovgivere for at danne et fælles lovgrundlag, som tilsammen udgør det danske retsgrundlag.[14] Dette interne forhold mellem retsregler, er fastlagt af Den Europæiske Unions Domstol (herefter EU-domstolen), hvor EU-retten opnår en forrang i det retlige hierarki.[15] Den EU-retlige del af lovgivning baseres på traktater og

[7] Munk-Hansen, Carsten, 2012, s. 202-203.
[8] Evald, Jens, 2000, s. 52.
[9] Munk-Hansen, Carsten, 2012, s. 281
[10] Evald, Jens, 2000 s. 57-58
[11] Munk-Hansen, Carsten, 2012, s. 278
[12] Munk-Hansen, Carsten, 2012, s. 292.
[13] Munk-Hansen, Carsten, 2012, s. 251.
[14] Munk-Hansen, Carsten, 2012, s. 258-259
[15] Munk-Hansen, Carsten, 2012, s. 264

direktiver. Med dette udgangspunkt, bliver retsakter udstedt, heriblandt forordninger.[16] En EU-retlig forordning har en direkte bindende virkning i medlemsstaterne, og skal således ikke implementeres i national ret, modsat et direktiv, som først skal implementeres før den opnår bindende virkning,[17] jf. jf. Traktat om Den Europæiske Unions Funktionsområde (herefter TEUF) artikel 288.

Retskilderne inddeles i fire hovedgrupper, som udtænkt i dansk retskildeteori. Grupperne inddeles som henholdsvis lovgivning, retspraksis, sædvaner og forholdets natur. Hierarkiet herimellem kan være en flydende rangorden, og afhænge af sagens natur. Der er imidlertid i den danske retskildeteori en enighed om, at en rangorden, grupperne imellem, ikke er fastlagt.[18] Den generelle forståelse fastholder dog, at lovgivningen har forrang før de øvrige retskildegrupper.[19] Denne generelle forståelse er styrket af, at lovgivningen i Danmark altid vil være demokratisk i sin opbygning, da folketingets demokratiske karakter fastsætter reglerne. Herudover øges retssikkerheden ved denne forrang, da det skaber et moment af forudsigelighed.[20]

Retspraksis indgår som en fundamental retskilde i både national og supranational ret. Udgangspunktet for retspraksis og afsagte domme, er at de udelukkende er bindende for sagens parter, men resultat af effektivitets- og retssikkerhedshensyn, nedbrydes retsautoriteten, såfremt afgørelsen ændres ved senere afgørelser.[21] Retspraksis opnår derfor en markant rolle for anvendelsen og forståelsen af gældende ret.

Til denne afhandling, anvendes retskildegrupperne lovgivning, og retspraksis.

Lovgivningen anvendt til afhandlingen består indledningsvist af både national ret og EU-ret, heriblandt ophavsretsloven og den EU-retlige pendant i direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet.

Til opfølgning af dette, inddrages den relevante lovgivning vedrørende teleudbydernes logning af personoplysninger. I denne forbindelse anvendes samtlige direktiver, som tilsammen har dannet et grundlag for den danske regulering af teleudbydernes logning. Af de EU-retlige direktiver er der i afhandlingen anvendt "Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation)" (herefter e-databeskyttelsesdirektivet). E-databeskyttelsesdirektivet suppleres af "Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF" (herefter logningsdirektivet). Som ovenfor nævnt, er dette grundlaget for den danske regulering af logningsfeltet. Denne regulering er "Bekendtgørelse 2006-09-28 nr. 988 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)".

[16] Munk-Hansen, Carsten, 2012, s. 258-259
[17] Munk-Hansen, Carsten, 2012, s. 260
[18] Evald, Jens, 2000, s. 7.
[19] Evald, Jens, 2000, s. 16.
[20] Evald, Jens, 2000, s. 11.
[21] Evald, Jens, 2019, s. 43

Logningen af brugernes internetaktiviteter udgør bevisgrundlaget for de eventuelle ophavsretlige krænkelser, hvorfor ovenstående finder anvendelse i nærværende afhandling.

I tilknytning til ovenstående anvendes "Lovbekendtgørelse 2019-09-10 nr. 938 om rettens pleje" (herefter retsplejeloven). Der sker primært anvendelse af reglerne om tredjemandsedition og isoleret bevisoptagelse i forbindelse med de civile søgsmål.

I afhandlingen analyseres der både domme og kendelser af dansk retspraksis. Disse anvendes som fortolkningsbidrag til at kortlægge hvornår en teleudbyder videregiver navne- og adresseoplysningerne på krænkerne. Dette er relevant, for at fastslå hvordan håndhævelsen af de ophavsretlige krænkelser kan imødekommes.

I denne forbindelse indgår både betragtninger fra by- og landsretten. Det skal her anføres, at præjudikatværdien er højere ved landsretten, end ved byretten.[22] Højesteret er den sidste instans, og dens afsigelser af højeste præjudikatværdi. Højesteret har imidlertid ikke taget stilling til afhandlingens problemstilling.

For at belyse hvorvidt der kan ske videregivelse uden editionskendelse, inddrages administrativ praksis fra Datatilsynet. De har afsagt samtlige afgørelser på feltet, dog efter den daværende persondatalovgivning. De dagældende hensyn er dog i det væsentligste videreført i persondataforordningen, hvorfor afgørelserne fortsat fastholder relevans.[23]

Slutteligt anvendes der i mindre grad, juridisk litteratur. Retslitteratur indgår ikke som en af de fire retskilder, og mangler derfor legitimitet til at binde domstolene. Retslitteraturen anvendes som supplement af de eksisterende retskilder,[24] og anvendes til at forebygge forståelsen af gældende ret.

I kapitlet om perspektivering, anvendes analogiske slutninger når det gælder anvendelsen af de lagrede data. Der eksisterer begrænsede mængde af materiale når det gælder håndhævelsen af civile søgsmål, hvorfor der dannes paralleller til de offentligretlige. Da disse anvender samme lovgrundlag for retshåndhævelse, retfærdiggøres analogien.

[22] Munk-Hansen, Carsten, 2012, s. 305.
[23] Betænkning nr. 1565, s. 15.
[24] Munk-Hansen, Carsten, 2012, s 346.

1.3 Afgrænsning

Emnet for afhandlingen angår brugerens ansvar inden for det ophavsretlige område, og dertil de forskellige instansers retshåndhævelse.

Ansvaret for mellemmandens ophavsretskrænkelser eller ansvar i øvrigt undersøges derfor kun i kontekst, og beskrives kun kort i afsnittet om DSM direktivets artikel 17.

Relevansen af en dybdegående beskrivelse af BitTorrent, vil vise sig nyttig, når der i afhandlingen analyseres hvilke bestemmelser som overtrædes i denne proces. Dette er inddraget for at give læseren en teknisk forståelse af hvilken proces der anvendes, for at tilgå det beskyttede indhold.

Afhandlingen har ikke til formål at beskæftige sig med for meget persondataret, hvorfor samtlige afsnit som belyste afvejningen mellem almindelige og følsomme persondata er uddraget. Som udgangspunkt er navne- og adresseoplysninger almindelige personoplysninger. Hvis der dertil i det videregivne medfølger en form for materiale, kan det overgå til følsomme personoplysninger. Behandlingen af følsomme personoplysninger afgøres efter et andet lovgrundlag, men har ikke bevist sig som skælsættende i forhold til de barrierer som i forvejen begrænsede rettighedshavernes muligheder. Den persondataretlige redegørelse finder dog sin relevans i nærværende afhandling da det udgør bevisgrundlaget i de civilesøgsmål fra NJORD Law Firm og de øvrige aktører.

Indledningsvist beskrives de tekniske foranstaltninger nødvendige for at foretage krænkelserne. En kort historisk beskrivelse af området som helhed, samt de forskellige aktører på området. Her beskrives titlerne Seeders, Peers og Leechers, som alle tilgår den tjeneste som Trackerne udbyder af ophavsretligt beskyttet materiale. Redegørelsen er bevaret kort, men fastholder sin nødvendighed da området kan forekomme omfattende i sin teknisk forståelse.

Både dansk såvel som det EU-retlige lovgrundlag beskrives redegørende. Danmark er underlagt en EU-konform fortolkning, og den nyeste praksis på området er afsagt af de europæiske domstole (herefter EUD).

Teleudbydernes pligter, omtales kun i logningsbekendtgørelsens forstand. Regler omkring vidnefritagelse og tavshedspligt findes uden betydning for afhandlingens område.

Der foretages endvidere ikke en videregående analyse af databeskyttelsesforordningen. Dette er begrundet i, at der i den udvalgte praksis, udelukkende henvises til logningsbekendtgørelsen som hjemler en særegen lovgivning ift. den i afhandlingen beskrevne problemstilling. Regelsættene omhandler udelukkende de retshåndhævendes myndigheders behandling af personoplysningerne.

Ved en overtrædelse af ophavsretsloven, hjemler straffeloven ligeledes en strafpålæggelse. Dette omtales kort i den inddragne sag om overtrædelse af §299b, for at belyse et billede af den fornødne grovhed før myndighederne retshåndhæver dette. Det er primært når der sker en fortjeneste ved de ophavsretlige krænkelser, hvorfor det ikke er relevant for den enkelte bruger. Dette afgrænser ligeledes afhandlingen fra at foretage en dybdegående analyse af

teleudbydernes videregivelse af oplysninger til straffesager. Afhandlingen beskæftiger sig med rettighedshavernes civile krav, på baggrund af forligsbrevet som NJORD Law Firm udsendte. Modtagerne af brevene havde i mange tilfælde ikke nærmet sig den grovhed som straffeloven og retspraksis udviser, er fornøden til strafferetlig efterforskning.

Der haves ikke forudgående fordomme mod NJORD og afhandlingen er beskrevet objektivt. Denne specifikke aktør inddrages ved navn, da de har været førende indenfor håndhævelse af rettighedshavers krav. Mange sagsanlæg og praksis fra NJORD har bidraget til at fastslå retstilstanden som den pt. eksisterer.

1.4 Struktur

Afhandlingen består af 7 kapitler. Kapitlerne består af følgende:

Kapitel 1 redegør for den opgavetekniske del, heraf en præsentation af afhandlingen, en afgrænsning, metoden og strukturen.

Kapitel 2 redegør for den indledende tekniske del. En grundviden omkring de tekniske foranstaltninger som ligger til grund for de ophavsretlige krænkelser findes nødvendig. En redegørelse for de anvendte fagtermer samt systemer redegøres for, i både et nutidigt og historisk øjemed.

Kapitel 3 beskriver de grundlæggende juridiske begreber og lovgivning, som senere anvendes og analyseres i afhandlingen. Herunder både den danske og europæiske lovgivning, for at belyse grundlaget for brugerens ansvar.

Kapitel 4 analyseres teleudbydernes forpligtelser, samt den relevante øvrige lovgivning som faciliterer rettighedshavers adgang til bevismateriale. Samspillet mellem ophavsretten og strafferetten i forbindelse med logningsbekendtgørelsen belyses, samt en ordlydsanalyse af brevet fra NJORD Law Firm.

Kapitel 5 analyseres retspraksis som er udvalgt ud fra deres respektive forandringer af retstilstanden. Denne udvælgelse er baseret på deres præjudicielle værdi, og skælsættende ændringer af den daværende retstilstand.

Kapitel 6 perspektiverer de fælles aspekter mellem strafferetten og ophavsretten. En beskrivelse af den nye logningsbekendtgørelse, og hvordan denne ændrer retstilstanden betragteligt. De oplysninger som rettighedshaverne har brug for til retsforfølgelse, er i stigende grad beskyttede af både finalité princippet, samt persondataretten, hvorfor de to felter ligeledes i fremtiden, følges ad i udvikling.

Kapitel 7 besvarer de spørgsmål problemstillingen lægger op til i en samlet konklusion.

Kapitel 2

2.1 Begrebet Torrenting

I sin essens, er BitTorrent netværk[25] egentlig blot det man kalder et ”peer-to-peer” netværk. Altså en indholdsdelingstjeneste, brugere imellem.

Den engelske oversættelse af torrent hentyder typisk til en ’strøm af noget’. I dette tilfælde, er det data. Datastrømmens retning, er rettet mod den bruger som vælger at downloade filen, men hvorimod afsenderen af filen typisk er en central server, er det ved BitTorrent, mange andre brugere. Man omtaler dette som ”Seeders” og ”Peers”. Seeders værende dem som kontinuerligt oploader data, som Peers i hele verden kan downloade.

En tredje kategori eksisterer, som omtales Leechers. Hvis man anvender et program som det populære PopCornTime, kan man efter man har set sin film, vælge at fortsætte upload af den film man lige har downloadet, for at øge båndbredden for øvrige Peers. Dette undlader de såkaldte Leechers. De lukker blot programmet, og har anvendt ydelsen ’egoistisk’, om man vil.

Et uddrag fra sag C-597-19 om Leechers:

”… peer-to-peer-netværkenes funktion er baseret på en delingsmekanisme, dvs. at enhver downloading skal modsvares af en uploading. Hvis antallet af brugere i nettet, der uploader, er for lille, fungerer netværket dårligt, fordi downloadinghastigheden bliver for langsom. Når der ikke længere er nogen seeder, ophører netværket helt med at fungere, og torrentfilen er »død«. Derfor straffer trackers de brugere, som ikke uploader (leechers), ved at sænke downloadinghastigheden, eller endog helt blokere adgangen. Strategien med at downloade uden at uploade kan kun fungere for lejlighedsvise anvendelser af peer-to-peer-netværket, og leechers udgør pr. definition et mindre fænomen på disse netværk.[26]

Som tydeliggjort i ovenstående, fungerer dette koncept kun hvis der kollektivt uploades fra Seeders for at holde filerne ’i live’, så øvrige peers kan downloade, og derved udbrede det yderligere.

[25] https://da.wikipedia.org/wiki/BitTorrent – Beskrivelse af torrent netværket - tilgået d. 5. september
[26] Sag c-597/19, præmis 52.

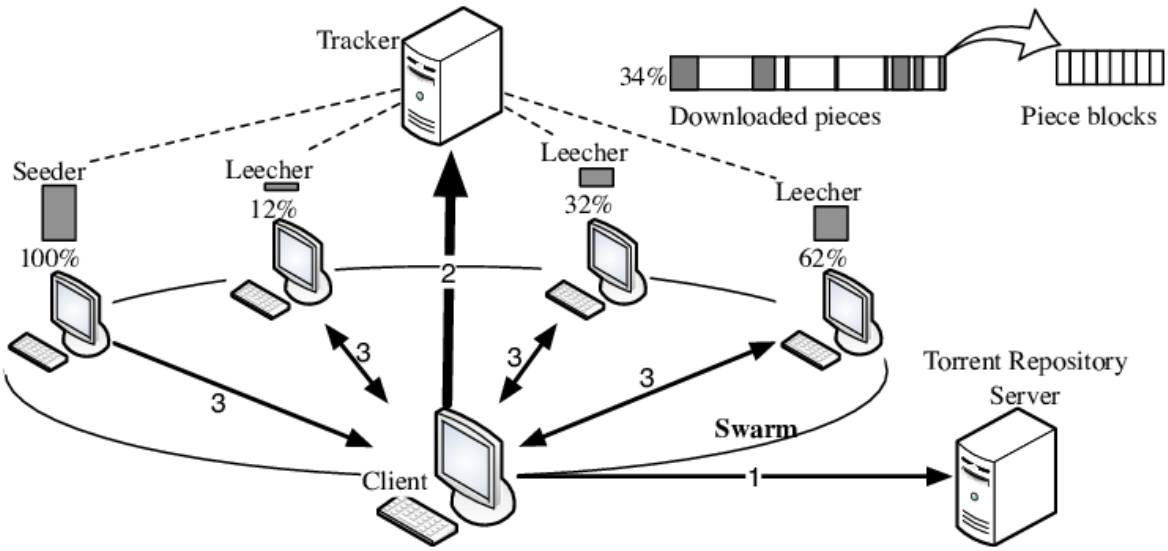

Illustration 1: Systematikken i BitTorrent konceptet

Som det ses på illustrationen I venstre side, findes der en oprindelig seeder, som tilgængeliggør et medie for almenheden, via upload til en Tracker (f.eks. PopCornTime el. ThePirateBay). Omkring Trackeren beligger Leecherne sig, som udelukkende tilgår indholdet, men ikke uploader til videredistribution.

Nederst i illustrationen er slutbrugeren, som anvender den båndbredde til mediet som Seederne og potentielt de øvrige Peers opretholder. Denne afgørelse er afhængig af individets indstillinger, som beskrevet i analysen, altså hvorvidt der sker download samtidig med upload.
Dette kredsløb kaldes for en "Swarm", og indeholder alle de deltagende aktører på tidspunktet for transporten af data. Begrebet Swarm har en stigende betydning efter afgørelsen i sag 597-19, som beskrevet nedenfor.

Øverst til højre i illustrationen ses en bjælke som symboliserer filens fuldstændighed. Såfremt den var fyldt ud, var filen 100% samlet. Men filen downloades som nævnt i fragmenter, som er uanvendelige som individuel enhed.

2.1.1 Lovligheden af BitTorrent

Der eksisterer utvivlsomt en stigmatisering af BitTorrent som værende udelukkende til illegale aktiviteter.[27] Det er dog imidlertid blot et værktøj. Et værktøj som brugeren selv kan vælge hvad de vil bruge til. BitTorrenting er faktisk blot en internetprotokol, ligesom der kendes fra webbrowserens HTTP koncept. Det anskues, at 40% af al internettrafik flyttes over BitTorrent netværk.

Det er dog ikke udelukkende ulovlige ydelser som udbydes over et BitTorrent netværk, det er faktisk en meget lille del af det i nutiden. Dette har dog ikke altid været tilfældet, eftersom teknologien i sin tidlige alder, hurtigt blev omfavnet af "piraterne".

Softwarevirksomheder bruger også denne type af udbredelse. Fordelene ved dette er bl.a. at man ikke behøver en central server som brugerne skal download fra, men derimod med det

[27] https://marketbusinessnews.com/torrents-benefit-businesses/242437/ - Om BitTorrent – Tilgået d. 20. okt.

samme en bruger downloader 1% af filen, begynder den enkelte ligeledes at uploade så båndbredden øges, og downloaden bliver hurtigere for alle. Det er dog kun en selvfølgelighed i legale downloads. Det kan være en fordel såfremt man anvender BitTorrent programmer til at tilgå ophavsbeskyttet materiale, at slå denne indstilling fra, så man egentlig tilgår indholdet som Leecher. Denne variation beskrives nedenfor i afsnit 5.4.

Samtlige store softwarefirmaer har tilsluttet sig denne form for udbredelse af produkter. Når en bruger downloader en fil fra et torrenting netværk fremfor at den downloades fra en central server, så sker der en betydelig mindre belastning af udbyderens netværk. Det kan derfor være en fordel i økonomiske henseende, da der ikke skal opgraderes server kapacitet som udelukkende har henblik på at understøtte en strøm af brugere som vil tilgå et produkt samtidigt. Et eksempel på fordelene ved torrenting kan opstilles således:

Produktet der skal tilgås, er et spil på 50GB. Den gennemsnitlige internethastighed i Danmark er 50 mbit/s.[28] Det vil anslå en download tid på ca. 133 minutter.[29] Det vil i praksis betyde, at en udbyder som f.eks. Blizzard Entertainment som producerer nogle af de største spil på markedet, skal have en server til at uploade i 133 minutter til en enkelt bruger. Det er enorme investeringer i kapacitet der er påkrævet for en udgivelse som denne, som potentielt har millioner af brugere. Dette var en nødvendighed og en praksis for rigtig mange produktioner af software igennem 00'erne.

Blizzard har ligeledes skiftet over til en BitTorrenting tilgang for udbredelse, f.eks. her til spillet Starcraft.[30]

Illustration 2: Blizzards download klient.

[28] https://www.version2.dk/artikel/den-gennemsnitlige-internethastighed-stiger-alligevel-glider-danmark-ned-ad-international - Internethastighed i Danmark – tilgået d. 20. okt.
[29] https://www.omnicalculator.com/other/download-time - Udregningen - tilgået d. 20. okt.
[30] https://www.makeuseof.com/tag/8-legal-uses-for-bittorrent-youd-be-surprised/ - Om Blizzards brug af torrenting – tilgået d. 20. okt.

Slutbrugeren får derved ingen information om at downloaden faktisk foregår ved BitTorrenting, og øvrige brugere som uploader til båndbredden. Det er netop her, hvor sag C-597/19 kan blive problematisk, da det er Swarmen som udgør udmålingen for vederlaget af tabet. En del af Swarmen kan altså være i gang med at tilgå et lovligt produkt, mens dele af den tilgår et ulovligt produkt. Mere om denne variation nedenfor i analysen.

Denne konstellation med et peer-to-peer netværk fremfor en central server, sparer Blizzard enorme mængder af kapacitetsomkostninger. Den skaber ligeledes flere tilfredse kunder, da en stigende mængde af brugere blot vil øge båndbredden, fremfor at deles om båndbredden fra en central server.

2.1.2 Trackerne

Som ovenfor beskrevet, eksisterer der 3 kategorier, som slutbrugeren kan identificere sig. Tillige vil det være nødvendigt at beskrive mellemmanden, som kort nævnt ovenfor. Disse kaldes trackere. En tracker kan for eksempel være siden ThePirateBay, som "tracker", altså sporer disse adgange, til ulovlige torrents. At mellemmanden omtales som tracker, illustrer ligeledes hvordan netværket er opbygget af de enkelte brugere, da ThePirateBay egentlig blot afholder register over de mulige adgange til det indhold, som brugerne deler indbyrdes, og ligeledes downloader kollektivt.

Senere i afhandlingen, vil der udarbejdes en gennemgående analyse af NJORD Law Firms procedure og generelle tilgang de masskrav som den danske befolkning blev mødt af. Mange af de krav som blev udsendt, blev udsendt ved brug af trackeren, PopCornTime. Det er et program der minder om NetFlix, men som anvender BitTorrenting netværk, til at lade brugere stream enhver film der stadigvæk holdes i live af de Seeders som opretholder båndbredden.[31]

2.2 VPN-software

Følgelig af beskrivelsen om BitTorrent, vil en beskrivelse af et virtuelt privat netværk (herefter VPN-software) ligeledes være fornøden. Dette er en type software som varetager det beskyttende element for brugerens aktiviteter på internettet.

Der er ikke i sig selv noget ulovligt ved en VPN,[32] eftersom softwaren egentlig blot sender brugerens internetaktivitet omkring en ekstern server, før IP-adresser el.lign. udgives til offentligheden.

Det er imidlertid ikke udelukkende værten for internetadressen der besøges, men tilmed internetudbyderen som IP-adresser er skjult overfor.

Det vil derfor resultere i at internetudbyderne ikke kan opfylde deres forpligtelse til at logge trafikken i medfør af logningsbekendtgørelsen §1, eller i hvert fald vil logningen være misvisende, da IP-adressen er omdirigeret til anden geografi eller identitet.

[31] https://en.wikipedia.org/wiki/Popcorn_Time - - tilgået d. 11. september 2022
[32] https://www.netkablet.dk/hvad-er-vpn/ - tilgået d. 7. september 2022

En VPN kan bruges i mange henseende. Det kan være en hjemmearbejdsplads som bruger en VPN til at deltage i intranettet ved virksomheden, en studerende som anvender VPN for at tilgå AAU's Karnov adgang, eller tusinde andre formål.

I det ovenstående er dermed statueret de legitime årsager til brugen, men der findes lige så mange ulovlige.

De ulovlige distancerer sig betragteligt fra aktiviteter som ovenstående, og helt til bestilling af narkotika på offentlig tilgængelige sider. Disse sider kendes også som "The Dark Web", og tilgås fra en såkaldt Tor-Browser.[33]

Logoet for Tor-Browser er et løg, som symboliserer det lag af kryptering, forbindelsen gennemgår inden det når frem til udbyderen af siden, eller til internetudbyderen selv.

Ovenstående er inkluderet i afhandlingen, for at statuere mængden af kryptering som er offentligt tilgængeligt for en almen bruger. I denne afhandling, vil dog tages udgangspunkt i en standard kryptering som f.eks. NordNet bruger, altså en 256-bit kryptering.[34]

For at sætte dette i perspektiv, bruges der 256 forskellige "nøgler" eller lag som skal løses eller gennembrydes, før man når frem til den rigtige IP-adresse. Det er den samme mængde som den amerikanske regering bruger til hemmelige dokumenter. Den samme mængde af beskyttelse er altså tilgængelig for ganske almindelige brugere af internettet.

Man kan dermed argumentere for at der eksisterer en mulighed for brugerne til at tilgå ulovlige aktiviteter på internettet, uden nogle sanktionsmuligheder, hverken fra internetudbyderen til at logge, eller politiets efterforskning.

2.2.1 Geoblocking med VPN

Anonymitet er ikke det eneste en VPN kan bruges til. Hvis man ser på fagtermen Geoblocking, er det en måde at beskrive en tilgang til websteder som har geografiske begrænsninger. Et håndterbart eksempel på dette er Danmarks Radio (Herefter DR). Hvis man forsøger at tilgå enhver service fra DR, vil anmodningen blive afvist med en besked om at man skal befinde sig i Danmark for at tilgå indholdet. Det er naturligvis således, da der betales medielicens på dansk territorie, og er derved forbeholdt for de betalende brugere.

Såfremt man køber et domæne, er det først efterfølgende der tages stilling til hvorvidt enkelte lande skal blokeres fra pågældende domæne.[35]

Årsagerne til at geoblocke kan være mangfoldige, såsom f.eks. politiske årsager. Dette er tilfældet i øjeblikket i et lidt omvendt format. I stedet for at afholde andre lande fra at tilgå, afholder Rusland deres eget territorie fra sociale medier.[36] Motiverne for at censurere egne borgere kan ofte være politisk, men ligeledes af lovmæssige årsager. Hertil kan f.eks. nævnes

[33] https://nordvpn.com/da/blog/dark-web/ - tilgået d. 7. september 2022
[34] https://www.avxperten.dk/blog/hvad-er-vpn/ - tilgået d. 7. september 2022
[35] https://vpnservice.dk/geo-blocking-saadan-tilgaar-du-et-website-der-er-blokeret-i-danmark/ - geoblocking – tilgået d. 10. Okt.
[36] https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law - Om Ruslands geoblocking – tilgået d. 21. okt.

Storbritanniens regulering af hjemmesider med pornografi. Brugeren der ønsker at tilgå disse hjemmesiders utraditionelle udbud, skal bekræfte deres alder med noget lignende NemID.[37]

Geografiske begrænsninger findes ligeledes ved f.eks. BBC, Vice TV og Netflix. Deres geografiske blokeringer har til formål at indskrænke udbredelsen af ophavsbeskyttede værker til de lande hvor der er givet samtykke til tilgængeliggørelsen. Til illustration, anvendes eksemplet om DR igen. Såfremt en bruger ikke pålagt licens-betaling, med bopæl uden for dansk territorie, som tilgår DR's tjenester ved brug af en VPN, vil denne handling resultere i en ophavsretlig krænkelse.

Kapitel 3

3.1 Den danske immaterialret

Indledningsvist skal det nævnes at der kan der være en forskel på skaberen og rettighedshaveren. I medieindustrien eksisterer der ofte en type af bindeled som f.eks. udbreder produktet indenfor en angiven geografi, og er dermed rettighedshaver af den krænkede ophavsret, indenfor den pågældende jurisdiktion.

Immaterialrettens helhed, er en fælles betegnelse for den retsbeskyttelse som kunstnere, skabere og diverse andre ophavsmænd, erhverver i forhold til national ret. Ophavsretten beskytter intellektuelle værkers frembringelse, af enhver form. Dog i denne fremstilling, navnlig den kreative del ift. filmindustrien.[38]

3.1.1 Den danske ophavsret

Konkret set, beskytter ophavsretten værker mod at blive kopieret, videreudbredt og brugt i det offentlige rum uden samtykke. Ophavsretten udgør dermed et naturligt centralt beskyttelsesideal i den generelle indholdsdeling af litterære og kunstneriske kreative værker. Dette omfavner derved alt i kategorien, altså både artikler, bøger, musik, videnskabelig litteratur, tv-programmer, og ikke mindst film. Yderligere har kulturministeriet tilmed udgivet en rapport angående emnet om pirateri. Nærmere betegnet, at en eneret til et ophav krænkes på internettet når det gøres tilgængeligt på internettet, uden tilladelse herom. [39]

3.1.2 Ophavsretten §1

Som kort nævnt ovenfor, beskyttes et værk som kan betegnes som litterært eller kunstnerisk jf. Ophavsretsloven §1. Denne beskyttelse er gældende uanset om værket *"fremtræder som en i skrift eller tale udtrykt skønlitterær eller faglitterær fremstilling, som musikværk eller sceneværk, som filmværk eller fotografisk værk… "* jf. Ophavsretsloven §1, stk. 1. Det er dog endvidere et krav at det omtalte værk kan betegnes som havende originalitet.[40] Hvilket selvsagt vil gælde for de fleste film.

---

[37] https://www.theguardian.com/culture/2016/nov/25/what-how-and-why-the-uks-new-online-porn-restrictions-explained - Om Englands geoblocking – tilgået d. 21. okt.
[38] Schovsbo, Jens, m.fl. 2013, s. 23.
[39] https://kum.dk/kulturomraader/ophavsret/ophavsret-paa-internettet
[40] Schovsbo, Jens, m.fl. 2013, s. 74.

3.1.3 Ophavsretten §2

I denne paragraf sikres det der populært kaldes enerettighederne. Den hjemler en form for balance mellem brugerne og ophavsmanden, så ikke alle har adgang til eksemplarfremstilling på lovlig vis. Dette kan imidlertid udføres på to måder, enten ved adgangen til at fremstille eksemplarer af værket, men også til at gøre værket tilgængeligt for almenheden.[41] Disse momenter kan være sammenfaldende, men ikke nødvendigvis, og beskrives derfor særskilt nedenfor.

Download og deling af ophavsretligt beskyttet materiale er ikke lovligt, såfremt handlingen foretages uden rettighedshaverens samtykke, jf. ophavsretslovens § 2. Både hvad angår digital kopiering (som det ses fra Seeders i ovenstående partsbeskrivelse) eller ved download.

3.1.4 Eksemplarfremstilling

I forlængelsen af beskrivelsen om eneretten, følger dernæst eksemplarfremstillingen. Det er primært dette, som eneretten tjener at beskytte. Hvad der nærmere ligger i "eksemplarfremstilling" kan der søges vejledning i ved at kigge på ophavsretslovens § 2, stk. 2. Herefter anses som eksemplarfremstilling *" […] enhver direkte eller indirekte, midlertidig eller permanent og hel eller delvis eksemplarfremstilling på en hvilken som helst måde og i en hvilken som helst form. Som fremstilling af eksemplarer anses også det forhold, at værket overføres på indretninger, som kan gengive det".* Det følger heraf, at eksemplarfremstilling i enhver form, på ethvert medie vil være i strid med princippet om eneretten.

Dette gælder også for midlertidige kopier. I fagsprog, kan man også kalde dette for hvad der opbevares i en computers RAM, ej at forveksle med harddisken. RAM opbevarer en midlertidig kopi, som computeren bruger i samarbejde med computerens processor, til at skabe et billede på skærmen. Pointen her er at, selv det fragment af en midlertidig kopi på en RAM, vil udgøre eksemplarfremstilling.[42]

Den primære forseelse ift. eksemplar fremstilling i denne emnekategori, vil dog fortsat være den forsætlige spredning. Altså en upload af værket til internettet eller upload som torrent-fil. Dette udgør en eksemplarfremstilling efter ophavsrettens §2, stk. 1. idet værket kopieres til netværk operatørens server.[43] I tilfælde af torrenting, vil der derimod bliver fremstillet kopier i form af fragmenter, på alle de tilstødende internationale Peers, med interesse i værket.

Efter § 12, stk. 4, nr. 2, er det ikke tilladt at benytte fremmed medhjælp til eksemplarfremstilling af filmværker, og ulovlig deling af filer i et fildelingsnetværk er således omfattet heraf.

Hvis et værk uden ophavsmandens samtykke uploades til internettet, vil dette resultere i en krænkelse af ophavsmandens eneret til eksemplarfremstilling såvel som hans eneret til offentlig fremførelse.

[41] Schovsbo, Jens, m.fl. 2013, s. 149.
[42] Udsen, Henrik, 2013, s. 44 og s. 82
[43] Schovsbo, Jens, m.fl. 2013, s. 241.

3.1.5 Tilgængeliggørelse for almenheden

Som videre anført i ophavsretslovens §2 stk. 1, besidder ophavsmanden eneretten til at tilgængeliggøre et værk for almenheden. Beskrivelsen af en tilgængeliggørelse fremgår af stk. 3 og kan ske på 3 forskellige måder,

1) eksemplarer af værket udbydes til salg, udlejning eller udlån eller på anden måde spredes til almenheden,

2) eksemplarer af værket vises offentligt, eller

3) værket fremføres offentligt.

Fællesnævneren for disse tre metoder er dog fortsat at det kræver ophavsmandens samtykke.[44]

3.1.6 Spredning

Ifølge ophavsretslovens § 2, stk. 3, nr. 1, har ophavsmanden eneret til at sprede værket til almenheden. Dette suppleres af eksemplarfremstillingsretten, på den måde at når et værk er spredt, ved givet samtykke, mistes der kontrol over det pågældende eksemplars videre gang, jf. konsumptionsreglen i ophavsretsloven § 19. Dette giver dog kun en ret til f.eks. at sælge filmen i dens DVD-kasse, altså at det digitale medie følger det analoge medium, og ved salg, skal den oprindelige ejer miste sin tilgang til varen. Dette er dog omdiskuteret i teorien,[45] men er den slutning der vil lægges til grund for denne afhandling.

3.1.7 Offentlig fremførelse

Ophavsretslovens § 2, stk. 3, nr. 3 samt stk. 4 giver ophavsmanden en eneret til offentlig fremførelse. Selve begrebet "fremførelse" forudsætter, at der i selve handlingen indgår en aktiv proces, der gør modtageren i stand til at tilegne sig værket. Når et værk afvikles, f.eks. når en film afspilles på en computer, foreligger der en aktiv proces i computeren, der gør det til fremførelse i ophavsretslovens forstand.[46]

Ophavsretslovens §2, stk. 3. nr. 3, omhandler dog oftest en direkte offentlig fremførelse. Altså den situation hvor den offentlig fremførelse 'udgår' samme sted som publikum befinder sig, f.eks. en teaterforestilling.[47] Det der gør sig særligt relevant for denne afhandling derimod, er fundet i ophavsrettens §2, stk. 4, det der normalt betegnes som "*overføring til almenheden*". Ifølge denne bestemmelse

"trådbunden eller trådløs overføring af værker til almenheden, herunder udsendelse i radio eller fjernsyn og **tilrådighedsstillelse** af værker på en sådan måde, at almenheden får adgang til dem på et **individuelt valgt sted og tidspunkt**"

[44] Udsen, Henrik, 2013, s. 64
[45] Ibid. s. 68
[46] Ibid. s. 72.
[47] Schovsbo, Jens, m.fl. 2013, s. 163f.

Denne krænkelse er altså karakteriseret ved modtagerens valg af sted og tidspunkt, via internettet. Altså on-demand eller blot modtagerens beslutningstagen om at tilgå et værk ved at trykke på download/play.[48]

De i denne afhandling nævnte fremførelser som PopCornTime, PirateBay, Geoblocking etc. Udgør altså derfor en offentlig fremførelse i strid med ophavsretten, da en modtager kan på sit valgte sted og tidspunkt, tilgå en fremførelse uden ophavsmandens samtykke.

3.1.8 Enerettens undtagelser

Den omtalte eneret, som udgør fundamentet for hele beskyttelsessfæren af ophavsretten, har dog stadig undtagelser. Disse fremgår af kapitel 2, navnlig §11a om midlertidige eksemplarfremstillinger, og §19 om konsumptionsreglen. Endvidere kan fremhæves §12, som omhandler eksemplarfremstilling til privat brug. Alle disse indskrænkninger i princippet om eneret, kræver at der eksisterer et **lovligt forlæg,** jf. 11, stk. 3

3.1.9 Lovligt forlæg

Indskrænkningerne i ophavsretslovens kap. 2 finder alene anvendelse, såfremt der eksisterer et lovligt forlæg. Begrebet lovligt forlæg kan være et lovligt eksemplar af et værk, men kan ligeledes være en lovlig gengivelse af et værk. Et eksemplar eller en gengivelse er lovlig, såfremt ophavsmanden har givet samtykke til en given udnyttelse af værket eller hvis denne udnyttelse er omfattet af en af ophavsretslovens undtagelsesbestemmelser.[49] Jf. kap. 2.

Lovligt forlæg har især betydning ift. Samme lovs §12 om kopiering til personlig brug. Dette indebærer selvsagt, at en kopiering til privat brug ikke er lovlig, såfremt der ikke er grundlag for det lovlige forlæg, som eksempelvis er tilfældet ved fildelingstjenester.

Sammenfattende vil der ikke kunne eksistere et lovligt forlæg, når det gælder anvendelse af fildelingstjenester. Tilgangen vil dermed ikke være omfattet af undtagelseskapitlerne, og eksisterer fortsat som en krænkelse af eneretten, og dermed ligeledes ophavsretten.

3.1.10 Midlertidig eksemplarfremstilling

En midlertidig eksemplarfremstilling er et koncept som fremgår af ophavsretslovens §11a, der eksisterer som en undtagelse til ophavsretsloven §2. Konceptet er et resultat af den EU-konforme fortolkning, og er en implementering[50] af Infosoc-direktivets[51] art. 5, stk. 1. Bestemmelsen indeholder fire kumulative betingelser for om en midlertidig eksemplarfremstilling kan blive lovlig: Eksemplarerne skal være flygtige eller tilfældige, jf. OPHL § 11a, stk. 1, nr. 1, eksemplarerne skal udgøre en integreret og væsentlig del af en teknisk proces, jf. OPHL § 11a, stk. 1, nr. 2, udelukkende have til formål at muliggøre enten en mellemmands transmission af værket i et netværk mellem tredjemænd eller lovlig brug af værket, jf. OPHL § 11a, stk. 1, nr. 3. Slutteligt er den sidste betingelse at, eksemplarerne ikke har selvstændig økonomisk værdi, jf. OPHL § 11a, stk. 1, nr. 4.

[48] ibid. s. 164.
[49] Trzaskowski, Jan, 2017, s. 58.
[50] Udsen, Henrik, 2013, s. 69.
[51] Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet

Bestemmelserne om midlertidig eksemplarfremstilling er for at undgå ovennævnte scenarie vedrørende ophavsretlige krænkelser som sker ved eksemplarfremstilling af et værk i en caching, eller RAM hukommelse.[52] Det vil derfor, som resultat af denne undtagelse om midlertidig eksemplarfremstilling, ikke kræve samtykke fra rettighedshaveren at fremstille et midlertidigt eksemplar.

3.1.11 Sanktioner

Når en bruger foretager en ophavsretskrænkelse, er det ophavsmanden som har sanktionsmulighederne. Disse vil ofte være transporteret til en advokat eller brancheforening el.lign. men i udgangspunktet vil det være ophavsmanden. I denne afhandling, har rettighedshaverne i praksis har transporteret deres krav mod krænkerne ved at lade sig repræsentere af NJORD Law Firm f.eks.

Sanktionsmulighederne fremgår af ophavsretslovens kapitel 7. Ansvarsgrundlaget er forsætlige eller groft uagtsomme krænkelser af ophavsretten, og sanktioneres efter reglerne i §§76-80. Herunder hører straf, erstatning, vederlag og godtgørelse.

Den mest relevante bestemmelse i kapitel 7 er for denne afhandling §76. Ifølge § 76, stk. 1, kan den, der forsætligt eller groft uagtsomt krænker ophavsmandens rettigheder, straffes med bøde. Derimod bestemmer § 76, stk. 2, at hvis krænkelsen er begået forsætligt og under skærpende omstændigheder, kan straffen stige til fængsel i op til 1 år og 6 måneder. De skærpede omstændigheder kan bestå i omfanget af spredningen, såvel som hvis værkerne er tilgængeliggjort på en sådan måde, at almenheden får adgang til dem på et individuelt valgt sted eller tidspunkt. Jf. §2, stk. 4. jf. §76, stk. 2, 2. pkt.

Det vil tydeliggøres i domsanalysen, at frihedsstraf for denne forseelse dog tilhører sjældenhederne, og overføres imidlertid til straffelovens §299b. Dette er historisk kun blevet anvendt mod bagmænd, som har en markant vinding ved den ophavsretlige krænkelse, som nævnt i afsnit 4.5. Derimod er den økonomiske kompensation i forligskrav meget hyppigt. Dette beskrives i afsnit 5.1.

Det interessante heri, er dog, at loven foreskriver at ophavsmanden kan kræve et rimeligt vederlag, der størrelsesmæssigt svarer til det, han ville have haft krav på, såfremt krænkeren havde haft tilladelse til værksudnyttelsen. Jf. §83, stk. 1, nr. 1.[53] I tillæg til dette, vil ophavsmanden kunne kræve erstatning for det tab som han har lidt, jf. §83, stk. 1, nr. 2. Samlet set, vil ophavsmanden altså kunne kræve erstatning for den uberettigede brug, samt det tab han har lidt.

Opgørelse af ophavsmandens tab fremstår i loven som særdeles ukonkret. Ifølge §83, stk. 2 og stk. 3, fastsættes erstatningen ud fra samtlige faktorer som afsætningstab, interne kontroludgifter og i nogle tilfælde markedsforstyrrelser, idet kopierne ødelægger originalproduktets renommé og goodwill.[54] Endvidere kan der i stk. 3. fastsættes en godtgørelse til ophavsmanden for ikke-økonomisk skade. Det kan f.eks. være rettigheder som i §3, hvor ophavsmanden har krav på at blive navngivet på sine værker.

[52] Udsen, Henrik, 2013, s. 85.
[53] Trzaskowski, Jan, 2017, s. 93f.
[54] Ibid. ff.

Slutteligt fremgår det af §84, at retten ved dom kan bestemme at eksemplarer som krænker retten til værker eller frembringelse, kan tilintetgøres. Det er tillige en betingelse at krænkelsen er sket ved overtrædelse af §§ 2-3 og 65-71. Dette vil dog i praksis ikke medføre at ophavsmanden kan kræve at få udleveret og tilintetgjort computeren, men derimod blot kræve at få eksemplarerne slettet.[55]

3.2 Den europæiske immaterialret

Det er samtidig relevant at inddrage den europæiske retstilstand, da den udformer sig i en mere dynamisk facon, end den danske. Et felt som dette, hvor retstilstanden ændrer sig årligt grundet nye afgørelser, vil europæisk ret have et mere retvisende billede af retstilstanden. Dette er også det nugældende tilfælde, med den nyere sag C-597/19 som bidrager med ny praksis på området.

3.2.1 Ophavsretsdirektivet

Det nye ophavsretlige direktiv har haft en turbulent modtagelse i Danmark, med samtlige anklager for at det skulle indskrænke ytringsfriheden.[56] Det har ligeledes været en del forsinket, grundet corona krisen i Danmark.[57]

Ophavsretten er i et internationalt perspektiv bundet af EU harmonisering. Hensynet for dette er, som med alle andre EU harmoniserede felter; at skabe et fælles lovgrundlag i EU. Værker som er beskyttet i Danmark, skal være underlagt den samme beskyttelse som de øvrige europæiske lande mht. deres ophavsretlige lovgivning,

Europa-Parlamentets og rådets direktiv 2001/29/EF af 22. maj 2001, var den gamle version af den supplerende 2019/790. Og regerer som den tilsvarende EU-retlige pendant til vores danske ophavsretslovgivning. Direktivet er implementeret i Danmark.

Der skeles ligeledes til det gamle ophavsretlige direktiv, for at beskrive nogle af de fundamentale ophavsretlige principper. Variationen og tilføjelser i den nye ophavsretlige lovgivning vil slutteligt belyses i bunden af kapitlet.

Udelukkende de direkte relevante artikler er udvalgt til redegørelsen.

3.2.2 Direktivet 2001/29/EF artikel 1 –

Direktivets artikel 1 vedrører direktivets anvendelsesområde. Beskyttelsen omfatter en generel retlig beskyttelse af ophavsretten og dermed også beslægtede rettigheder inden for rammerne af det indre marked. Den EU retlige lovgivning har til formål at yderligere harmonisere EU-retten. Det indeholder også regler om undtagelser fra og indskrænkninger af ophavsretten. Direktivet har henblik på at sikre en velfungerende markedsplads for udnyttelsen af værker og andre frembringelser.

---

[55] Udsen, Henrik, 2013, s. 118.
[56] https://www.bechbruun.com/da/nyheder/2019/nyt-eu-direktiv-om-ophavsret-i-det-digitale-indre-marked - om det nye ophavsretsdirektiv – tilgået d. 1. nov.
[57] https://kum.dk/aktuelt/nyheder/todelt-tidsplan-for-implementering-af-ophavsretsdirektiver - om det nye ophavsretsdirektiv – tilgået d. 1. november 2022.

3.2.3 Direktivets 2001/29/EF artikel 2 –

Medlemsstaterne har en markant selvbestemmelse når det kommer til hvad eneretten omfatter. Kompetencen er derfor overladt til selv at indføre bestemmelserne angående et totalforbud mod reproduktion, f.eks.

I Danmark er det som bekendt, temmelig restriktivt, jf. ophavsretsloven §2.

"a) for ophavsmænd for så vidt angår deres værker
b) for udøvende kunstnere for så vidt angår optagelser af deres fremførelser
c) for fremstillere af fonogrammer for så vidt angår deres fonogrammer
d) for producenter af den første filmoptagelse for så vidt angår den originale film eller eksemplarer heraf, og
e)for radio-og fjernsynsforetagende for så vidt angår optagelser af deres udsendelser, hvad enten der er tale om tråd- bunden eller trådløs transmission, herunder via kabel eller satellit."

Nærliggende for afhandlingen, kan der tages udgangspunkt i flere af ovenstående litra. Mere om dette nedenfor.

3.2.4 Direktivet 2001/29/EF artikel 3 –

Direktivets artikel 3 redegør for overførelsen af værker til almenheden, og derudover retten til tilrådighedsstillelsen til almenheden. Retten til overføring tillægges af medlemsstaten, som etablerer eneretten. Rettighedshaveren med eneretten kan tillade eller forbyde trådbunden eller trådløs overføring til almenheden. Direktivet anvender ligeledes ordlyden om "almenheden får adgang til værket på et individuelt valgt sted og tidspunkt" jf. art. 3.1. Altså en regulering af ikke bare internettets tilgang, men internettets tilgang til on-demand tjenester. Denne formulering er ligeledes kendt fra den danske lovtekst fra eksemplarfremstilling, tilrådighedsstillelse mm.

Dette er som bekendt implementeret i ophavsretten §3.

Begrebet om eneret bliver uddybet i art. 3.2 med de samme kategorier som ovenfor nævnt i artikel 2.

Det er hermed overladt til den enkelte indehaver af eneretten, at beslutte hvor, hvornår, og hvordan et værk skal overføres til almenheden.

3.2.5 Direktivet 2001/29/EF artikel 4 –

Direktivets artikel 4 omhandler retten til spredning. Medlemsstaterne tillægger rettighedshaverne eneret til at tillade eller forbyde spredningen af værket. Den nærmere definition af spredning beskrives i den nationale pendant i afsnit 3.2.9. Det gælder heraf både ved salg eller på anden måde at sprede originalværket.

3.2.6 Direktivet 2001/29/EF artikel 5 –

Direktivets artikel 5 omhandler undtagelserne til eneretten. Disse uddybes i artikel 5.1. Dette er implementeret i ophavsrettens kapitel 2.

"Midlertidige reproduktionshandlinger efter artikel 2, som er flygtige eller tilfældige, som udgør en integrerende og væsentlig del af en teknisk proces, og som udelukkende har til formål at muliggøre

a) en mellemmands transmission i et netværk mellem tredjemænd, eller

b) en lovlig brug

af et værk eller en anden frembringelse, og som ikke har selvstændig økonomisk værdi, er undtaget fra den i artikel 2 nævnte ret til reproduktion."

Det er hermed en overladt ret til medlemsstaterne at indføre undtagelserne og indskrænkninger til den nationale ophavsret efter denne artikel jf. artikel 2.

Særligt relevant ses dog artikel 5, stk. 2, litra b, som er implementeret i ophavsretslovens §12.

"reproduktioner på ethvert medium foretaget af en fysisk person til privat brug og til formål, der hverken direkte eller indirekte er kommercielle, forudsat at rettighedshaverne modtager en rimelig kompensation, i forbindelse med hvilken der tages hensyn til anvendelse eller ikke-anvendelse af de i artikel 6 nævnte tekniske foranstaltninger på det pågældende værk eller den pågældende frembringelse"

Den danske ophavsretslov havde allerede en lignende bestemmelse før implementeringen af direktivet. Den oprindelige bestemmelse omhandlede ligeledes reproduktion til privatbrug og et krav om en kompensation til rettighedshaver, såfremt der skete kopiering af værket. Der skete derfor kun en mindre ændring af denne bestemmelse da Danmark implementerede direktiv 2001/29/EF.[58] Den eneste ændring var privat kopiering hvis det skete med et kommercielt formål.

Såfremt en slutbruger foretager en privatkopiering af et beskyttet værk, skal pågældende bruger i princippet anses for at være skyldner for den i art. 5, stk. 2, litra b, omhandlede rimelig kompensation.[59] Dette taler ligeledes for ovennævnte afsnit om kompensation for rettigshaverne. Det taler ligeledes for en EU konform fortolkning at denne kompensation imødekommes ved national ret, da det er medlemsstatens ansvar at sikre, at rettighedshaver faktisk modtager den rimelige kompensation. Jf. princippet i sag c-462/09 Stichting de Thuiskopie

3.2.7 Direktivet 2001/29/EF artikel 8 –

Direktivets artikel 8 omhandler sanktioner og retsmidler.

En yderligere komplikation når det kommer til håndhævelsesinteressen, blev belyst i sag C-149/17, Bastei Lübbe, hvor en fortolkning af art. 8 stk. 1, sammenholdt med EP/Rdir

[58] Brigitte Lindner & Ted Shapiro, Copyright in the Information Society, 2011, s. 165.
[59] sag C-462/09, Stichting de Thuiskopie, Saml 2011 I-05331 – notat 25.

2004/48, art. 3, stk. 1 og 2, fremkom således at bestemmelserne er til hinder for national lovgivning med henblik på håndhævelse af fildeling.

"Medlemsstaterne indfører passende sanktioner og retsmidler over for krænkelser af de rettigheder og forpligtelser, der er fastsat i dette direktiv, og de træffer de foranstaltninger, der er nødvendige for at sikre, at sanktionerne og retsmidlerne finder anvendelse. Sanktionerne skal være effektive, stå i et rimeligt forhold til krænkelsen og være afskrækkende"

Erstatningsansvaret for indehaveren af en internetforbindelse hvor en ophavsretlig krænkelse er begået, ikke ifaldes, såfremt abonnenten nævner mindst ét familiemedlem som ligeledes havde adgang til forbindelse, uden at have meddelt nærmere detaljer vedrørende tidspunkt eller arten for familiemedlemmets brug af internettet.

Relevant til denne artikel blev der i sag C-275/06, Promusicae udtalt fra EU-domstolen at kravet om en effektiv beskyttelse af ophavsretten, som udtrykt i artikel 8, ikke pålægger medlemsstaterne en pligt til at videregive personoplysninger. Art. 8, stk. 2. hermed:

"Hver medlemsstat træffer de foranstaltninger, der er nødvendige for at sikre, at rettighedshavere, hvis interesser påvirkes af en krænkelse på dens område, kan anlægge erstatningssøgsmål og/eller kræve nedlagt forbud og i givet fald kræve beslaglæggelse af det materiale, der ligger til grund for krænkelsen, samt de i artikel 6, stk. 2, nævnte anordninger, produkter eller komponenter."

En ordlydsanalyse ville sandsynligvis fremkomme med et andet resultat, men der eksisterer således ikke en mulighed i EU-praksis for at opnå de fra rettighedshaverne ønskede oplysninger jf. Promusicae.

Rettighedshaverne vil fortsat have svært ved at håndhæve krav i civile retssager, da beskyttelsen af personoplysninger går forud for beskyttelsen af ophavsret, jf. art 9. Som vedrører *" Dette direktiv berører ikke bestemmelser vedrørende især… beskyttelse af nationale skatte, pligtaflevering, lovgivning om restriktiv praksis og illoyal konkurrence, forretningshemmeligheder, sikkerhed, klassificerede oplysninger, databeskyttelse og privatlivets fred" (egen understregning).*

Samtidig med at der foreligger en håndhævelsespligt for medlemsstaterne, fremhæves altså ligeledes den samme afvejning som blev fremhævet i den øvrige praksis indeholdt i afhandlingen. Intentionen om håndhævelse vil altid indgå i en afvejning, og i dette tilfælde, med sin pendant i form af borgerens fundamentale rettigheder.

3.2.8 Digital single Market direktivet (DSM)

DSM-direktivet kaldes også for copyrights direktivet. Dette er hjemlen for flere forskellige felter af regulering indenfor ophavsretten. Både hvad vedrører onlineplatformes ansvar (mellemmand) men også f.eks. vederlag til rettighedshaverne.[60] Som det også kan læses nedenfor i C-sag 597-19, er direktivets formål at harmonisere ophavsretten i EU, for at opnå en fælles retstilstand i det indre marked. Det er også dette direktiv, som regulerer ulovlig tilgang af beskyttet indhold, og som skeles til i nedenstående EU-afgørelse.

[60] Schønning, Peter, 2019, s. 256.

DSM-direktivet er ikke fuldt implementeret i dansk ret endnu, men dele af det er. Den ophavsretlige del mangler endnu, og forventes først gennemført i dansk ret d. 1. juli 2023.[61] De resterende, endnu ikke implementerede bestemmelser, omhandler primært bestemmelser om ophavsmænd og udøvende kunstnere skal sikres et passende og forholdsmæssigt rettighedsvederlag, samt mulighed for justering af vederlag.

Dette direktivs artikel 17 var dog en del af den første implementering, og er særlig interessant. Den omhandler placering af ansvar for onlineindholdsdelingstjenester. Implementeringen indeholder en pligt for "større" platforme som udbyder individuelt uploadet indhold til almenheden.

Her kan det antages at Facebook, Instagram mm. naturligvis er omfattet, men tvivlen består hvorvidt direktivet nogensinde vil påvirke sortbørs tjenester som PopCornTime el.lign.

Artikel 17 omhandler platformens pligt til at opsøge en tilladelse for det uploadede materiale. I teorien kan man sige at processen vendes om, på den måde at det faktisk bliver platformen (eller værten for upload) som bliver ansvarlig for den ophavsretlige krænkelse, frem for den egentlig bruger som uploader.

Artikel 17 (1) Medlemsstaterne fastsætter, at en udbyder af onlineindholdsdelingstjenester foretager en overføring til almenheden eller tilrådighedsstillelse for almenheden med henblik på dette direktiv, når den pågældende giver offentlig adgang til ophavsretligt beskyttede værker eller andre beskyttede frembringelser, der uploades af brugerne.

Det angives fra RettighedsAlliancen,[62] at hele 30 og 22 procent af danske pirater benytter hhv. Youtube og Facebook til ulovligt at tilgå beskyttet indhold. Endvidere skulle der være en stigende tendens til at anvende ellers lovlige platforme, til at begå ophavsretlige krænkelser.

Med implementeringen af artikel 17, er det RettighedsAlliancens forventning, at det vil blive lettere at håndhæve de sociale onlineplatforme.

Der kan derfor eksistere et grundlag for, at piraterne er begyndt at anvende lovlige tjenester, for at tilgå ulovligt indhold. Såfremt tendensen fortsætter, vil håndhævelsen på området muligvis også imødegå en ny tendens. Dette er imidlertid blot spekulation.

3.3 Delkonklusion

Sammenfattende kan det konkluderes at brugerens handlinger utvivlsomt er en krænkelse af ophavsretten. Dette stadfæstes ligeså i den udvalgte retspraksis. Som det helt klare udgangspunkt hjemler ophavsretten at en eneret til et ophav krænkes på internettet når det gøres tilgængeligt på internettet, uden tilladelse herom.

I sag C-597/19 fastlægges det, at en tilgængeliggørelse af et delelement, ligeledes udgør en ophavsretlig krænkelse.

---

[61] https://jurainfo.dk/artikel/status-implementering-af-de-resterende-bestemmelser-i-dsm-direktivet-om-ophavsrettigheder - Implementering af DSM – tilgået d. 19. okt.
[62] https://rettighedsalliancen.dk/rettighedsalliancens-hoeringssvar-om-implementering-af-ophavsretsdirektivet-fokuserer-paa-haandhaevelsesmuligheder/ - om pirat indhold på ellers lovlige medier – tilgået d. 1. nov.

I ovenstående kapitel 3, er derfor redegjort for brugerens ansvar, og i det følgende kapitel 4, hvordan rettighedshaverne kan håndhæve dette, og de etablerede begrænsninger for samme.

Kapitel 4

4.1 Internetudbyderens forpligtelser

Internetudbyderens forpligtelser har et tæt samspil med rettighedshavernes adgang til retshåndhævelse. I gældende retspraksis, og formentlig også den fremtidige retspraksis, jf. perspektiveringen i kapitel 6, udgør adgangen til oplysningerne den primære begrænsning for retshåndhævelsen.

Hvorvidt internetudbyderne kan forpligtes til videregivelse af oplysningerne, sker på et afvejningshensyn, af hhv. hensynet til retshåndhævelse og beskyttelse af borgerens grundlæggende rettigheder. De grundlæggende rettigheder er imidlertid underlagt varig udvidelse, hvortil persondataretten blokerer for retshåndhævelsen. Dette gennemgås i det følgende kapitel 4, bekræftes i kapitel 5 og endeligt perspektiveres i kapitel 6.

4.1.1 Logningsbekendtgørelsen

Logningsbekendtgørelsen optager en meget central del af nærværende afhandling. I sager som disse angående ophavsretlige krænkelser, vil oplysningerne som udbyderne opbevarer udgøre bevisgrundlaget mod den pågældende krænker. Logningsbekendtgørelsen opbevarer informationer om f.eks. navne- og adresseforhold til abonnenternes IP-adresser.

Logningsbekendtgørelsen er udstedt med hjemmel i retsplejelovens § 786, stk. 4, hvorefter Justitsministeren fastsætter nærmere regler om registrering og opbevaring af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Der fremgår følgende af logningsbekendtgørelsens §1,

Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i udbyderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold.

Logningsbekendtgørelsen fastsætter dermed en pligt for internetudbydere at logge, registrere og opbevare aktivitet fra danske borgere, såfremt det skulle vise sig at skulle bruges i efterforskningsøjemed. Dette er imidlertid den interessante modifikation, da der samtlige gange i logningsbekendtgørelsen understreges at oplysningers formål er efterforskningsmæssige som led i retsforfølgning af strafbare forhold. Hvordan kan en rettighedshaver pålægge internetudbyderen at udlevere data som udelukkende bør anvendes til strafferetlig retsforfølgning? Dette spørgsmål undersøges nedenfor i analysen.

4.2 Opbevaring efter logningsbekendtgørelsen

Internetudbydere er i medfør af logningsbekendtgørelsens § 5, stk. 2, forpligtet til at registrere følgende oplysninger om en brugers adgang til internettet:

1) den tildelte brugeridentitet,

2) den brugeridentitet og det telefonnummer, som er tildelt kommunikationer, der indgår i et offentligt elektronisk kommunikationsnet,

3) navn og adresse på den abonnent eller registrerede bruger, til hvem en internetprotokol-adresse, en brugeridentitet eller et telefonnummer var tildelt på kommunikationstidspunktet og

4) tidspunktet for kommunikationens start og afslutning.

Det er på denne baggrund, at internetudbyderne opbevarer oplysninger om abonnenters internetaktivitet. Et nærværende spørgsmål er imidlertid om disse oplysninger udelukkende er opbevaret som et resultat af opbevaringspligten, eller om teleudbyderne opbevarer for egen drift. Der findes ligeledes et princip om dataminimering i dataforordningens artikel 5, stk. 1, litra c. Opbevaringen skal udelukkende være tilstrækkelig men også begrænset til hvad der er nødvendigt i opbevaringspligten.

Spørgsmålet er relevant, da logningsbekendtgørelsen hjemler en form for beskyttelse af disse oplysninger. Såfremt de udelukkende er opbevaret af årsager indeholdt i logningsbekendtgørelsen, vil samme lovs hensigt til opbevaring tale for, at udbyderne udelukkende er forpligtet til udlevering i overensstemmelse med hensigten.

Der findes samtlige udtalelser i U.2019.2019 fra Telenor, Telia og endda TDC som omtaler deres infrastruktur for behandling og opbevaring af loggede data. De omtaler at til deres egne formål, gemmer de IP-adresser i op til 30 dage, af hensyn til driften. Hertil henvises til deres daglige drift som f.eks. kundeservice og rettelse af fejl til abonnentens fordel.

"Telenor og Telia anslår at have brug for data om logning af ip-adresser med henblik på fejlretning i henholdsvis 30 dage og 3 uger, at Telenor og Telia herefter alene har gemt de krævede data om logning af ip-adresser med henblik på at opfylde logningsbekendtgørelsen." og ydermere at *"tilsvarende gør sig gældende for TDC…"*

I samme afgørelse omtales, at efter de 30 dage overføres disse oplysninger til et "politirapporteringssystem" som er etableret i overensstemmelse med logningsbekendtgørelsen. Opbevaringspligten i logningsbekendtgørelsen forpligter udbyderne til at opbevare oplysningerne i 1 år, jf. logningsbekendtgørelsen §9. Herefter indgår et krav om at teleudbyderne sletter eller anonymiserer oplysningerne, således at abonnenterne ikke kan identificeres.[63]

Sammenfattende kan udledes, at udbyderne ikke ville være i besiddelse af oplysningerne såfremt de ikke var forpligtet hertil jf. logningsbekendtgørelsen. Dette var ligeledes slutningen i U.2019.2019, da landsretten fastslog:

"… alene fortsat er i teleudbydernes besiddelse, fordi teleudbyderne ifølge logningsbekendtgørelsen … 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…"

[63] Datatilsynets vejledning om databeskyttelsesforordningen, 2017, s. 11.

Det kan dermed konkluderes, at oplysningerne omfavnes af beskyttelsen i logningsbekendtgørelsen når de overføres til politirapporteringssystemet, og de efter 30 dage, efter lovens angivelser, udelukkende bør udleveres til efterforskningsøjemed med henblik på strafferetlig forfølgelse. Spørgsmålet er ikke i detaljer omtalt, men der kan argumenteres for at rettighedshaverne kan have en mindre restriktiv adgang til oplysningerne før de overføres til politirapporteringssystemet.

4.2.1 E-Databeskyttelsesdirektivet (direktiv 2002/58/EF)

Formålet med e-databeskyttelsesdirektivet defineres i artikel 1, stk. 1, som *"tager sigte på en harmonisering af medlemsstaternes bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig privatlivets fred i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor…"*

For at opnå et ensartet niveau i beskyttelsen, og sikre medlemsstaternes beskyttelse af de grundlæggende rettigheder, supplerer og specificerer e-databeskyttelsesdirektivet bestemmelserne i persondatadirektivet, jf. e-databeskyttelsesdirektivets artikel 1, stk. 2.

Anvendelsesområdet for e-databeskyttelsesdirektivet blev fremhævet i GD-dommen (sag C-140/20) hvor det overordnede formål med direktivet netop er *"… at beskytte brugerne af elektroniske kommunikationstjenester mod de risikomomenter for deres personoplysninger og privatliv, der følger af anvendelsen af ny teknologi, og navnlig den øgede mulighed for at foretage automatiseret opbevaring og behandling af oplysninger"*

De aktører som benævnes i citatet, er teleudbyderne. Medlemsstaterne skal altså beskytte brugerne mod ovennævnte.

I dette direktiv vil der for nærværende afhandling ligeledes redegøres for artikel 6 og artikel 15.

Et direktivs funktion er som velkendt den harmoniserende effekt, hvorfor enkelte elementer vil gentages i logningsbekendtgørelsen.

Det fremgår i artikel 6 i direktiv 2002/58/EF at *trafikdata vedrørende abonnenter og brugere, som behandles og lagres af udbyderen af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste, skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2, 3 og 5, samt artikel 15, stk. 1.*

Direktivet er imidlertid ikke totalharmoniseret, hvorfor artikel 6 kan modificeres som anført i artikel 15, Indskrænkningerne som medlemsstaterne kan fastsætte, skal være "… passende og forholdsmæssig[e] i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem...", jf. e-databeskyttelsesdirektivets artikel 15, stk. 1.

Sammenfattende kan det konkluderes ud fra direktivet, at de nationale myndigheder har myndighed til at indskrænke eller udvide reglerne.

I relation til problemstillingen, og videre i analysen, vil det blive relevant at have skabt et overblik over hvordan, hvornår og hvilke data som logges af udbyderne. Det er netop denne data der tjener som eneste bevismiddel i en sag om en ophavsretlig krænkelse.

4.3 Samspillet med strafferetten

4.3.1 Adgang til informationen

Eksistensen af bevisgrundlaget, er som belyst i afhandlingen, internetudbydernes opfyldelse af opbevaringspligten i logningsbekendtgørelsens §1, oplysningerne *"... anvendes som led i efterforskning og retsforfølgning af strafbare forhold."* jf. logningsbekendtgørelsens § 1.

Hertil kan det udledes af ordlyden, at oplysningerne udelukkende eksisterer med henblik på at de ved editionskendelse kan udleveres til politiet til brug for forfølgelse af strafbare forhold. Dette er ligeledes et standpunkt som ikke modificeres af retspraksis, og er stadig en stående betingelse for anvendelse.

Informationen som er logget og opbevaret som resultat af pligten i denne bestemmelse udgør det eneste bevisgrundlag for rettighedshavernes forfølgelse af ophavsretlige krænkelser. Det bliver derfor relevant at belyse hvad der forstås ved et strafbart forhold, og om videregivelse alene bør ske til forfølgelse af offentligt påtaleberettigede forhold.

I dansk ret forstås et strafbart forhold som de handlinger hvor der idømmes straffe ift. straffeloven. I straffelovens §31, udgør de almindelige straffe både bøde og fængsel. Straf kan kun idømmes hvis legalitetsprincippet er opfyldt, altså at strafbarheden er hjemlet ved lov, jf. straffelovens §1.

Ud fra ovenstående ordlydsanalyse, er det udfaldsgivende at oplysningerne skal anvendes med henblik på en efterforskning. Som udgangspunkt er det politiet som kan iværksætte en efterforskning jf. retsplejelovens §742, stk. 2. Retsplejeloven udelukker derimod ikke at andre aktører end politiet kan iværksætte en efterforskning. Politiet har imidlertid en eneret til at iværksætte efterforskningsskridt i retsplejelovens forstand. Der kan gives en tilladelse for andre aktører til efterforskning, men som udgangspunkt associeres en efterforskning med en politivirksomhed.[64]

Til opklaring af spørgsmålet om hvorvidt videregivelse udelukkende kan ske til politi og evt. anklagemyndigheden, kan der henvises til U.2019.2019, hvor landsretten anførte følgende i deres afvejning "*...at de efter retskendelse skal kunne udleveres til politiet som led i efterforskning og retsforfølgning af strafbare forhold."* I efterforskningsøjemed, er det således indikeret, at der kan ske udlevering til politiet.

NJORD Law Firm eller øvrige rettighedshavere vil altså ikke have beføjelse til at modtage oplysningerne i et efterforskningsøjemed, i hvert fald ikke efter oplysningerne er overgået til et politirapporterings system som belyst i afsnit 4.2. Oplysningerne er indsamlet til et andet formål, end blot civile søgsmål, og bør efter retslige principper udelukkende anvendes til det hjemlede i loven. jf. finalité princippet.

[64] https://denstoredanske.lex.dk/efterforskning - tilgået d. 28. okt.

Slutteligt bør det belyses hvordan oplysningerne løseligt blev videregivet forud for U.2019.2019, til brug for civile søgsmål, sammenlignet med politiets noget mere restriktive adgang til samme.

I afsnittet om gennemgangen af U.2019.2019, blev det beskrevet hvordan rettighedshavere fik udleveret navne- og adresseoplysninger tilknyttet en liste på IP-adresser samtlige gange, forud for afgørelsen.

For at sammenligne dette med politiets adgang til at retsforfølge brugeren af ophavsretlig krænkende tjenester, skal henvises til Tele2/Watson dommen.

I Tele2/Watson dommen, konkluderes det hvilke typer af kriminalitet politiet kan pålægge udbyderne at videregive oplysninger om. Her blev det fastlagt, at videregivelse kan ske til efterforskning af grov kriminalitet. I dommen, omtaler EU-domstolen, at organiseret kriminalitet og terrorisme under alle omstændigheder er omfattet. Jf. præmis 103. Der uddybes ikke i detaljer, hvilke øvrige kriminalitetsformer der er omfattet af ordlyden, men det må antages, at kriminalitet med en sammenlignelig strafferamme ligeledes må være opfyldende.

For en yderligere belysning af dette begreb, kan henvises til artiklen "Logning af teledata i lyset af Tele2-dommen" af Lene Wacher Lentz. Dette er ligeledes en sammenfatning af fortolkningsbidrag fra en række EU-retsakter og praksis fra Den Europæiske Menneskeretsdomstol (EMD). Forfatteren argumenterer for at følgende kriminalitetstyper ligeledes må omfattes af begrebet om grov kriminalitet, *"... terrorisme, menneskehandel og seksuel udnyttelse af kvinder og børn, ulovlig narkotikahandel, ulovlig våbenhandel, hvidvaskning af penge, korruption, forfalskning af betalingsmidler, edb-kriminalitet og organiseret kriminalitet."* jf. TEUF-artikel 83, stk. 1

Denne sondring mellem offentligretlig og civilretlig håndhævelse af kriminalitet belyses yderligere i afsnittet om perspektivering nedenfor.

Slutteligt kan dog udledes, at det ikke er enhver efterforskning eller retsforfølgning der giver adgang til videregivelse af loggede data. Det er en forudsætning, at dette sker til bekæmpelse af grov kriminalitet jf. Tele-2 dommen nedenfor.

Endvidere er det relevant at notere, at logningsbekendtgørelsen er udstedt med hjemmel i retsplejelovens §786, stk. 4. Dette kapitel af retsplejeloven omhandler indgreb i meddelelseshemmeligheden, observation, dataaflæsning, forstyrrelse eller afbrydelse af radio og telekommunikation og blokering af hjemmesider. Dette tydeliggør lovgivers intention om at formålet med logningsbekendtgørelsen er bekæmpelse af kriminalitet, og til brug for efterforskningsmyndigheder. Denne betragtning indgår ligeledes i kendelsen fra U.2019.2019 hvor det ligeledes blev fremhævet, at logningsbekendtgørelsen var udstedt efter retsplejelovens regler.

4.4 De forenede sager Tele 2/Watson (C-203/15 og C-698/15)

Afgørelserne omhandler de ovenstående to sager som blev behandlet i forening af EU-domstolen. Sagerne opstod i kølvandet på at logningsdirektivet blev erklæret ugyldigt.

Afgørelserne omhandler omfanget af opbevaringspligten for teleudbyderne til logning af data, samt efterforskningsmyndighedernes tilgang af disse data.

Tvisten i C-203/15 vedrører Tele2 Sverige AB over for Post- och telestyrelsen. Tele2 var som resultat af national lovgivning blevet forpligtet til at logge og opbevare sine abonnenters trafikdata. Som resultat af logningsdirektivets ugyldighed, nægtede Tele2 at imødekomme opbevaringsforpligtelsen, og som følge af samme, slettede den allerede lagrede data.

I samme sammenhæng, nægtede Tele2 at videregive data. Denne tvist blev herefter forelagt EU-domstolen, med det præjudicielle spørgsmål værende hvorvidt *"... en generel forpligtelse til at lagre trafikdata, som omfatter alle personer, alle elektroniske kommunikationsmidler og alle trafikdata uden forskel, begrænsninger eller undtagelser med henblik på at bekæmpe strafbare lovovertrædelser […], [er] forenelig med artikel 15, stk. 1, i direktiv 2002/58 [e-databeskyttelsesdirektivet], henset til chartrets artikel 7, artikel 8 og artikel 52, stk. 1"*

Den anden tvist i C-698/15 vedrører parterne Tom Watson, Peter Brice og Geoffrey Lewis over for Secretary of State for the Home Department. Sagen blev forelagt som prøvelse af den eksisterende nationale lovgivning vedrørende teleselskabers lagring og adgang til data ved enhver posttjeneste eller enhver telekommunikationstjeneste. Den nationale lovgivning hjemlede logning og videregivelse uden forudgående tilladelse fra en domstol eller uafhængig administrativ myndighed, jf. præmis 53 og 55.

EU-domstolen afgjorde de to sagers præjudicielle spørgsmål om logning og opbevaring med en samlet udtalelse.

For så vidt angår teleudbydernes pligt til logning og opbevaring fandt EU-domstolen; "…at bestemmelsen [i artikel 15, stk. 1 i e-databeskyttelsesdirektivet sammenholdt med charterets artikel 7, artikel 8 og artikel 52, stk. 1] er til hinder for en national lovgivning, [...] der fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere…".
Angående myndighedernes adgang til oplysningerne, fandt EU-domstolen, at adgangen til disse data alene kunne tillades ved grov kriminalitet, og at adgang kun bør gives ved forudgående kontrol af en domstol, eller anden administrativ myndighed.

EU-domstolen tager i disse afgørelser stilling til de nationale myndigheders muligheder for at foretage indskrænkninger med hjemmel i e-databeskyttelsesdirektivets (direktiv 2002/58) artikel 15.

4.5 Politiets håndhævelse af krænkelserne

Der eksisterer samtlige overtrædelser i dette retsområde som er underlagt offentlig påtale. Politiet beskriver ofte de sager som de involverer sig i som "ophavsretskrænkelser af særligt grov karakter". Her vil det typisk være en efterforskning på baggrund af en anmeldelse, hvor SØIK bliver assisteret af IT-specialister fra Rigspolitiets Nationale Cyber Crime Center (NC3).

Der vil være et forskelligartet ansvar for hvorvidt man distribuerer indhold, eller om man blot tilgår det. Her menes den klassiske forstand af distribution, altså uploader til en seedbox, og evt. opnår uberettiget vinding, som set i denne sag.[65]

"En seedbox er en privat dedikeret server, der gør det muligt hurtigt at uploade og downloade digitale filer - ofte ved brug af BitTorrent-teknologien – således at en bruger slipper for at al trafikken går gennem dennes egen computer, ligesom der opnås en vis form for anonymitet."

Ligeledes har en seedbox sin egen IP-adresse, som adskiller sig fra brugerens. Det fungerer derved lidt som en VPN, at man anvender sin normale computer til at tilgå trackeren, men det er egentlig seedboxen som downloader indholdet, fremfor den almindelige tilknyttede internetforbindelse.

Der skal lægges mærke til at en seedbox beskrives som en **privat** server, altså ulig BitTorrent netværkets klassiske opstilling om offentlig tilgang. En seedbox har typisk et element af berigelse tilknyttet, f.eks. en månedlig betaling.

På baggrund af denne forretning, blev bagmændene bag seedboxen anholdt, og sigtet for ophavsretskrænkelser af særlig grov karakter.

Årsagen til at dette er relevant for nærværende afhandling, er det efterfølgende citat fra Michael Lichtenstein, fungerende politiinspektør, SØIK. *"Det er meget tilfredsstillende, at vi på baggrund af en grundig efterforskning kan stille de seks anholdte, som vi mener er de ansvarlige bagmænd eller centralt placerede staff medlemmer, til regnskab for deres ulovlige drift af fildelingstjenesterne. På baggrund af denne effektive indsats skal vi have gennemgået det beslaglagte materiale – og i den forbindelse kan det ikke udelukkes, at også brugere kan stilles til regnskab for at benytte sig at de ulovlige fildelingstjenester,"*

Her åbnes altså for muligheden for et potentielt strafferetligt ansvar for brugerne som blot har tilgået tjenesten.

Der er tale om en sigtelse for 299b, stk. 1, nr. 1. Dette kan formentlig kun ifalde bagmænd, eftersom der endnu ikke er set en §299b sigtelse af en bruger. Dette på trods af, at brugerne egentlig også kunne ifalde ansvar under en ordlydsfortolkning. Retspraksis fortæller dog, at der formentlig skal en form for berigelseshensigt til for at falde under §299b.

Det er ikke utænkeligt, at fremtiden for håndhævelse af området bliver tillagt politiet. Med den nye logningslovgivning, samt vores pligt til EU-konform fortolkning, er oplysninger som navne- og adresseoplysninger tillagt så stor en værdi for borgernes grundrettigheder, at det er utænkeligt de kan udleveres til civile søgsmål. Mere om dette i kapitel 6.

[65] https://anklagemyndigheden.dk/da/seks-personer-anholdt-ulovlige-fildelingstjenester

4.6 NJORD Law Firm og indstævningerne

NJORD Law Firm repræsenterer jf. deres hjemmeside en lang række rettighedsindehavere. Heriblandt Nu Image, Voltage Pictures LLC og Zentropa.[66] Deriblandt også film som The Expendables 3, Olympus has Fallen og Flaskepost fra P. Såfremt man kender til film, har de alle været på hitlister og biografer rundt om i verden.

I bilag 1 er der inkluderet et billede af det pågældende brev som udsendes. Det bliver her for analyses skyld citeret:

"Fildeling og download af filmen "The Cobbler"

På vegne af filmproducenten Cobbler Nevada LLC kontakter vi dig, da filmen "The Cobbler" er blevet fildelt/downloaded via IP-adressen … den … uden samtykke fra Cobbler Nevada LLC.

Dit teleselskab har oplyst at du var indehaver af IP-adressen på det daværende tidspunkt. Dit teleselskab har intet med disse undersøgelser at gøre, men er blevet pålagt ved en domstol at udlevere dit navn og din adresse.

Cobbler Nevada LLC benytter MaverickEye UG, der overvåger og identificerer datatrafik, herunder IP-adresser- Filmen kan være set via eksempelvis Popcorn Time eller lignende hjemmesider samt ved hjælp af fildelingsprogrammer som BitTorrent.

Det er ifølge ophavsretsloven ikke tilladt af dele eller downloade film på denne måde og vi håber, at du vil besvare vores spørgsmål i en e-mail til os på ip@njordlaw.com

1. *Har husstanden en trådløs internetforbindelse og har denne et password?*
2. *Har en eller flere i husstanden set eller forsøgt at se filmen "The Cobbler" på det pågældende tidspunkt?*

Har du eller andre personer med adgang til IP-adressen, det kan være hjemmeboende børn downloadet, set og/eller delt filmen på det pågældende tidspunkt, kan sagen afsluttes endelig ved, at der indbetales i alt kr. 1500 til konto nr. …

Cobbler Nevada LLCs tilbud om at lukke sagen på oplysninger og betaling er gældende 14 dage fra modtagelsen af dette brev, og har det formål at kukke sagen én gang for alle. Vi opfordrer til, at dette brev besvares med en mail til ip@njordlaw.com, og ønsker at undgå videre undersøgelser af sagen og iværksættelse af retssag.

Rådgivning om ophavsret bør søges hos én, der kender og har erfaring med området. Hjælp os med at sikre en fremtid for skabelse af film.

Med venlig hilsen
Jeppe Brogaard Clausen
Advokat (H)

[66] https://www.njordlaw.com/da/fildeling-og-download-af-film/spoergsmaal-og-svar-vedroerende-ulovlig-fildeling-og-download – om Njord Law firm - tilgået d. 6. september 2022

4.6.1 Andre i husstanden end ejeren af IP-adressen

Ejeren af abonnementet af internetforbindelsen har utvivlsomt ansvaret for sine hjemmeboende børns handlinger såfremt de er under 15 år gamle. jf. lov om hæftelse for børns erstatningsansvar §1, stk. 1.

Der findes dog en undtagelse om handlingens beskaffenhed. Dette er typisk gældende når handlingen indeholder en mængde af kompleksitet, så barnet ikke kan udregne forbundne risici eller lovlighed.[67]

Der kan argumenteres for at krænkende streamingtjenester er så udbredt, at en simpel google søgning på en film kan frembringe rettighedskrænkende resultater, hvilket kan besværliggøre erstatningssagens proces mod krænkeren.

4.6.2 Ubeskyttet internetforbindelse

Årsagen til punktet om hvorvidt internetforbindelsen har været beskyttet, er at præcisere ansvaret for krænkelsen til indstævntes internetforbindelse. Dette udpensles ikke i brevet, men kan læses i øvrige domme hvor de gør lignende anbringende gældende. F.eks. i U2021.4710, hvor Copyright Management Services gør følgende gældende:

"… når, der er kode på et WiFi, er der en formodning for, at den skete krænkelse er foretaget af abonnenten, og at abonnenten er ansvarlig for krænkelsen"

Det er altså en metode for rettighedshaverne at fastlægge skylden for krænkelsen på den pågældende abonnent for internettjenesten.

Men hvordan forholder skyldsspørgsmålet sig på et åbent netværk?

De fleste routere i dag anvender en meget pædagogisk opsætningsproces så selv de mest IT-usagkyndige kan følge med.[68] De fleste routere anvender det der hedder en WPA2-sikkerhed for at beskytte adgangen til netværket. Dette indebærer at hver ny enhed på netværket, skal indsende en adgangskode for at oprette forbindelse.

Ældre routere, eller routere hvor dette ikke har været en standardindstilling, har dog stadigvæk en mulighed for at have en åben internetforbindelse, som enhver kan tilkoble sig.

Dette scenarie er omtalt af IT-advokat Peter Lind Nielsen fra Bender von Haller Dragsted.[69] Han udtaler til ComputerWorld, at der vil være tale om brugstyveri såfremt man anvender naboens ulåste internetforbindelse. Dette på trods af, at der ikke brydes en kryptering. Der er imidlertid ingen domme på området. Det forholder sig således, da man anvender en andens IT-anlæg.

---

[67] https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/civilret/Pjece%20boern.pdf – om handlingens beskaffenhed – tilgået d. 23. okt.
[68] https://tweak.dk/netv%C3%A6rk/s%C3%A5dan-sikres-din-wi-fi-router- - om routere – tilgået d. 25. okt.
[69] https://www.computerworld.dk/art/115166/derfor-er-det-ulovligt-at-laane-naboens-wifi - om brugstyveri af wifi – tilgået d. 25. okt.

Så mens det faktisk er strafbart at tilgå en ubeskyttet internetforbindelse, er det ikke strafbart at eje en ubeskyttet internetforbindelse.

Det nærværende spørgsmål i denne afhandling bliver således hvordan skyld kan præciseres til abonnenten såfremt man har en åben internetforbindelse? Er der nogle former for sporingsteknologi til abonnentens eget IT-udstyr?

Retspraksis har ikke endegyldigt svaret på spørgsmålene, men på trods af dette, er de inddraget i afhandlingen da det kan forekomme som endnu en barriere for rettighedshavernes forfølgelse af civilretlige krav.

4.7 Teleudbyderens videregivelse med editionskendelse

Såfremt teleudbydere pålægges at videregive navne- og adresseoplysninger som følge af en editionskendelse, er teleudbyderen retligt forpligtet hertil. Det retlige grundlag følger af databeskyttelsesforordningen artikel 6, stk. 1, litra c, hvorefter behandlingen kun er lovlig fordi den hviler på en retlig forpligtelse. I denne forbindelse findes den retlige forpligtelse i retsplejelovens § 299, stk. 1, angående tredjemandsedition. Ifølge denne bestemmelse kan retten pålægge en part, herunder en teleudbyder, at udlevere eller videregive dokumenter af betydning til brug for civilretlig forfølgelse.

Således findes en hjemmel til videregivelse i retsplejeloven. En særlig relevant problemstilling forbundet med dette er, at teleudbyderne opbevarer de loggede oplysninger som følge af opbevaringsforpligtelsen i logningsbekendtgørelsen, som beskrevet ovenfor.

Problemstillingen beror imidlertid på, at de opbevarede oplysninger jf. logningsbekendtgørelsen, aldrig har haft til formål at blive videregivet ved editionskendelse til civile erstatningssøgsmål.

4.8 Teleudbyderens videregivelse uden editionskendelse

I de tilfælde der ikke foreligger en editionskendelse, vil det være relevant at belyse, på hvilket grundlag en videregivelse kan pålægges en teleudbyder.

En central afgørelse til fortolkning af dette er fra 20. november 2003. (journalnr. 2002-219-0135) hvor Datatilsynet udtalte sig om hvilke persondataretlige hjemler som kunne anvendes i forbindelse med videregivelse af personoplysninger i sager uden editionskendelse. Dette er imidlertid en afgørelse som er afsagt inden dataforordningens implementering.

I afgørelsen blev Antipiratgruppen pålagt at udarbejde en redegørelse om deres indhentelse af personoplysninger fra teleudbydere uden editionskendelse. Antipiratgruppen adspurgte i den forbindelse at Datatilsynet tog stilling til, hvorvidt videregivelse af navne- og adresseoplysninger var i strid med persondataretten på tidspunktet, når det skete uden kendelse.

Datatilsynets udtalelse blev at videregivelsen i første omgang skal ske på baggrund af en vurdering fra den dataansvarlige. Den nationale hjemmel for dette er persondatalovens § 6, stk. 1, nr. 1-7. Denne hjemmel svarede på tidspunktet for afgørelsen til den nuværende artikel

6 i persondataforordningen, som ret beset indeholder det retlige grundlag for behandling af almindelige personoplysninger.[70]

Datatilsynet ligger til grund, at det må antages at persondatalovens §6, stk. 1, nr. 1, om videregivelse ved samtykke må afkræftes i et tilfælde hvor abonnenten er indstævnt. I øvrigt må det ligges til grund at persondatalovens § 6, stk. 1, nr. 1, i det væsentligste svarer til forordningens artikel 6, stk. 1, litra a.[71] Blot fordi der ikke eksisterer et samtykke i afgørelsen, betyder dog ikke at en situation ikke kan forefindes, hvor et samtykke til videregivelse er afgivet.

Efterfølgende tager Datatilsynet stilling til hvorvidt der foreligger en retlig forpligtelse til videregivelse. I tilfælde af logningsbekendtgørelsen er dette allerede i det henseende, afvist ovenfor. Ligeledes, udtaler Datatilsynet at der ikke synes at foreligge en pligt for teleudbyderne at videregive personoplysningerne jf. persondatalovens § 6, stk. 1, nr. 3, som svarer til den nugældende artikel 6, stk. 1, litra c i forordningen.[72] Der foreligger derved ikke en umiddelbart retlig pligt til videregivelse uden kendelse. Dette er ligeledes i overensstemmelse med EU-retlig praksis i Promusicae (C-275/06). Domstolen konkluderede at e-databeskyttelsesdirektivet ikke udelukker at medlemsstaterne kan fastsætte en pligt til videregivelse. Medlemsstaterne er imidlertid ikke på forhånd pålagt, og ej heller tvunget til at fastsætte en sådan pligt, jf. præmis 54-55. Dette synspunkt er ligeledes tiltrådt i den danske afgørelse i Østre Landsrets kendelse af den 7. maj 2018 som behandles nedenfor.

Samlet set afgør Datatilsynet, at der ikke findes et retligt grundlag for videregivelse af personoplysningerne på baggrund af interesseafvejningen, idet hensynene i afvejningen er opgjort af et fundamental beskyttelseshensyn til borgeren. I en sådan grad at de bør forelægges en domstol. Det er på baggrund af anførte, Datatilsynets vurdering, at der ikke bør ske videregivelse af personoplysninger uden en retskendelse.
Denne konklusion er primært baseret på at sammenhængen mellem IP-adresserne og det ulovligt downloadede materiale, potentielt kan udgøre personoplysninger vedrørende strafbare forhold.

Netop når det gælder strafbare forhold, kan her perspektiveres til ovenstående afsnit om politiets proces for udlevering af lignende oplysninger. Politiet har ingen muligheder for at få udleveret disse oplysninger uden en retskendelse.

Kapitel 5

5.1 Retstilstanden

Når der sker en ophavsretlig krænkelse på internettet, har påtaleberettiget behov for oplysninger fra teleudbyderne som er opbevaret jf. logningsbekendtgørelsen. Der har været samtlige domme og kendelser på dette område, og retstilstanden er derfor nødvendig at opridse.

Retten på Frederiksberg har behandlet samtlige af disse kendelser, bl.a. kendelsen afsagt af Retten på Frederiksberg den 3. november 2017 (sag nr. BS A-1417/2017), kendelsen afsagt af

[70] Betænkning nr. 1565, s. 15.
[71] Betænkning nr. 1565, s. 126
[72] Betænkning nr. 1565, s. 129

Retten på Frederiksberg den 16. august 2017 (sag nr. BS K-741/2017), kendelsen afsagt af Retten på Frederiksberg den 10. november 2015 (sag nr. BS E-1984/2015), med videre.

NJORD Law Firm beskriver en særdeles tilfredshed historisk med disse afgørelser. Dette var lige indtil Dan Bjerrings ankomst til Retten i Frederiksberg. Lars Lokdam udtaler følgende *"Det er et langt sammenhængende forløb. Retten på Frederiksberg har dømt til fordel for vores klienter i en lang periode, inden Dan Bjerring kommer til. Og så kommer Bjerring til og laver om på den praksis på flere måder. Det er ham, der begynder at dømme modsat retten på Frederiksberg og modsat de andre danske byretter."*

Siden 2019 var Bjerring dommer i samtlige sager som NJORD havde anlagt som repræsentant for rettighedshaverne. Samtlige af disse gik dem og deres klienter imod. Det var også i 2019 at Bjerring sendte en sag direkte til førstebehandling i Østre Landsret. Endvidere udgiver byretten en såkaldt "vejledning"[73], som ikke længere kan tilgås. Vejledningen indeholdt blandt andet en rimelig direkte opfordring til modtagerne af piratbrevene om ikke at betale kravet. I vejledningen fremgik følgende *"Retten har […] fundet anledning til ved retsbøgerne at vejlede de sagsøgte om, at det står enhver frit for at indgå et forlig i en sag – men også om, at et sådant forlig, hvis det indebærer, at sagsøgte påtager sig at betale et beløb, vil kunne medføre et unødigt økonomisk tab for sagsøgte af tilsvarende størrelse"*[74]

Det var dette der "fik bægeret til at flyde over"[75] for Lars Lokdam.

NJORD Law Firm indgiver en klage over dommeren og hans retspræsident til Den Særlige Klageret.

Den nyeste skelsættende kendelse på området er afsagt af Østre Landsret i U.2019.2019. Denne vil blive behandlet nedenfor i detaljer. I byretten blev parterne Telenor og Telia pålagt at udlevere navne- og adresseoplysninger på de internetabonnenter som rettighedshaverne igennem MaverickEye havde givet ledetråde på, havde begået en ophavsretlig krænkelse. Telenor og Telia kærede denne afgørelse til landsretten. Østre landsret udtalte følgende. *"[s]elv 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 [repræsentant for rettighedshaverne] 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."*

Landsretten foretager altså en interesseafvejning af hensynene til retsforfølgning kontra brugerens rettigheder. Logningsdata som disse, må utvivlsomt betegnes som personoplysninger, og brugeren har dermed et ønske om hemmeligholdelse, uagtet om der er sket en krænkelse eller ej. Østre Landsret vurderede at brugerens rettigheder vægtede højere end videregivelsen af oplysninger, og kendelsen statuerer dermed en skærpet adgang til forfølgning af ophavsretlige krænkelser.

[73] https://www.k-news.dk/nyheder/usaedvanlig-vejledning-om-piratbreve-sendt-til-alle-byretter
[74] https://www.k-news.dk/nyheder/byretsdommeren-vs.-advokatfirmaet
[75] ibid

Retstilstanden på området er altså i øjeblikket, som uddraget fra dommen nedenfor anfører, at Zentropa (og NJORD) udelukkende kan få udleveret personoplysninger hvis afvejningen til de retsforfølgende interesser vægter højere end interessen for hemmeligholdelse.

5.2 U.2019.2019 Ø

Den seneste relevante danske afgørelse på området er ovennævnte. Østre Landsrets kendelse af d. 7. maj 2018, og har været særlig relevant i udviklingen af retsområdet.

5.2.1 Sagens parter

Parterne i sagen er hhv. Telenor og Telia vs. Copyright Management Services (CMS). CMS repræsenterer en række rettighedshavere, heriblandt ovennævnte, Zentropa. Kendelsen blev anket på baggrund af byrettens afgørelse om udlevering af navne- og adresseoplysninger. Begge selskaber blev pålagt at videregive denne information til CMS, som led i deres forfølgelse af ophavsretlige krænkelser i form af deling af beskyttede filer. Byretten pålagde Telenor og Telia at videregive deres logningsdata i medfør af retsplejelovens regler om tredjemandsedition i §299 og isoleret bevisoptagelse i §343.

5.2.2 Sagsfremstilling

Sagsfremstillingen drejer sig om udlevering af 4011 IP-adresser som CMS har oplyst er blevet anvendt ved krænkelse af CMS' rettigheder. Det fremgår fra domsnotatet at det er ubestridt, at Telenor og Telia er i besiddelse af disse oplysninger. CMS var kommet i besiddelse af IP-adresserne igennem en software som hedder MaverickEye. Disse lister med ip-adresser som har krænket CMS' rettigheder er efter det oplyste i dommen indhentet ved brug af et program kaldet MaverickMonitor, udviklet af en tysk softwareleverandør, MaverickEye. *"Programmet skal have »fodret« et fildelingsnetværk med film, som de af CMS repræsenterede rettighedshavere har ophavsret til, hvorefter programmet har »foregivet« at ville downloade en film. Programmet har derefter registeret visse brugeres ageren med programmet, ikke brugeres ageren med andre brugere"*

Det er med andre ord, en form for parasitisk software som agerer trojansk hest i kernen af filen, uden brugerens kendskab. Det bliver endvidere analyseret af Dr. Simone Richter, som bekræfter programmets præcision og integritet til formålet.

Dette er imidlertid i mange af sagerne kritiseret af modparterne. F.eks. i U2021.4710, hvor det fremhæves at udtalelsen fra Dr. Simone Richter er en ensidigt indhentet erklæring, og dermed vægtet, og ligesådan med de øvrige syns og skønsrapporter som er indhentet til at støtte brugen af MaverickEye.

CMS var i sagen repræsenteret af NJORD Law Firm, som tidligere havde repræsenteret klienter i lignende sager, hvor videregivelse af navne- og adresseoplysninger var udleveret. Udleveringen var sket på samme lovgrundlag, altså tredjemandsedition og isoleret bevisoptagelse. Denne videregivne information, blev derefter anvendt i den berygtede masseudsendelse af forligsbreve.

5.2.3 Anbringender

I kendelsen modsatte sagsøgte (Telia og Telenor) at videregive de omtalte navne- og adresseoplysninger. Sagsøgte gjorde anbringende om at typen af oplysninger som var påbudt udleveret, ikke lovligt kunne videregives til forfølgelse af civilretlige krav. Internetudbydere er som beskrevet ovenfor påkrævet at logge og opbevare data som denne jf. logningsbekendtgørelsen. Personoplysningerne er altså alene opbevaret som følge af opbevaringsforpligtelsen.

I denne sammenhæng gjorde Telia og Telenor endvidere gældende at videregivelsen ville være i strid med persondatarettens finalité princip, altså princippet om formålsbestemthed. Logningsbekendtgørelsens indsamling af oplysninger indsamles til udtrykkeligt angivne og saglige formål, og behandlingen må ikke være uforenelig med de oprindelige formål. Jf. persondatalovens §5, stk. 2. Forfølgelse af civilretlige krav er ikke angivet som formålet for logningsbekendtgørelsen. En sådan videregivelse kan kun forefindes i et omfang som fremmer efterforskning eller retsforfølgning af straffelovsovertrædelser.

Som altovervejende præcedens derimod, blev det anført at i sager som disse, skulle der foretages en proportionalitetsafvejning mellem CMS's interesser og borgerens grundlæggende rettigheder, herunder retten til privatliv og beskyttelse af personoplysninger. Tillige gjorde Telia og Telenor gældende at de skulle varetage en lovhjemlet pligt om hemmeligholdelse af logningsoplysningerne.

Slutteligt gjorde Telia og Telenor gældende at retsplejelovens regler om isoleret bevisoptagelse og edition ikke var gældende da videregivelsen ikke skulle bruges som anlæg til en retssag, men derimod blot tilbud om forlig.

Modparten gjorde gældende overfor ovenstående, at der hverken i logningsbekendtgørelsen eller forarbejderne fremgår at der ikke kan ske udlevering til forfølgelse af civilretlige krav. Tillige anbragte CMS at forfølgelse af disse krav ikke var muligt uden videregivelsen af logningsdata. Endvidere fremførte CMS at der hverken i ordlyden i §343 om isoleret bevisoptagelse eller §299 om edition indgår et krav om at det skal ske som anlæg til en retssag. Slutteligt nævner CMS at danske domstole tidligere har behandlet begæringer om edition og pålagt udbyderne at videregive personoplysningerne tilknyttet IP-adresserne.

5.2.4 Rettens afgørelse

Retten foretog først en vurdering af hvorvidt den isolerede bevisoptagelse var retmæssig. I sagen handler det initialt for CMS om at kortlægge hvem krænkerne egentlig er, på meget sparsom information. Spørgsmålene til §343, verserer derved om, hvorvidt sagsøger supplerer nok information eller om det ligeledes fremstår som en "fisketur".

Endvidere udtaler retten til §343, "*En begæring om bevisoptagelse, som alene skal tjene til vejledning for, om en sag overhovedet skal anlægges, skal afvises. Undtagelsen hertil er, hvis rekvirenten kan godtgøre, at bevisoptagelsen er nødvendig for at afklare, hvem der er rette sagsøgte. Det forudsætter imidlertid stadig, at rekvirenten har en intention om at indlede retssag.*"

MaverickEye supplerer i tilfælde kun meget begrænset information, og ej heller om forbrydelsen er fuldbyrdet. En situation kan tænkes hvor der trykkes "play" men computeren lukkes derefter. Her, vil bevisoptagelsen fra den pågældende bruger være en vejledning for hvorvidt en sag kan anlægges, i modsætning til hvorvidt han var rette sagsøgte.

Østre Landsret fastlægger endvidere at isoleret bevisoptagelse kun kan foretages med intention om at indlede en retssag.

Retten udtaler følgende om §299, "*På baggrund af CMS' forretningsmodel - og den foreliggende editionsbegæring - fremstår editionsbegæringen som en »fisketur«, der ikke tillades efter gældende ret, jf. eksempelvis princippet i U.1968.608H*". Retten udtaler i sagen at CMS har ikke sandsynliggjort, at materialet har betydning for de kendsgerninger, der skal bevises, jf. hertil retsplejelovens §341.

Slutteligt foretages en kumulation af afvejninger. Først blev det fastslået at informationerne som Telenor og Telia opbevarer utvivlsomt er nødvendige for at afklare rette sagsøgte, og dermed af betydning for sagen. Dernæst tog retten stilling til vidnepligten, og heraf pligten til hemmeligholdelse af abonnenternes personfølsomme oplysninger.

Vidende om at rettighedshaverne ikke kunne forfølge deres krav, vægtede Østre Landsret hensynet til hemmeligholdelsen højere, end CMS' interesse i civilretlig forfølgelse af kravene. Slutteligt, i denne forbindelse, lagde retten også vægt på at de opbevarede oplysninger som indfanget jf. logningsbekendtgørelsen skal anvendes og behandles med udgangspunkt i strafferetsplejen.

5.2.5 Andre kommentarer

Hvad angår ansvarsgrundlaget, og om hvorvidt forseelsen kan være sket uagtsomt, anføres af en sagkyndig i sagen *"Users need to take active steps to set up and install software to enable participation in the P2P Network. These steps cannot be »accidently« or inadvertently undertaken by a user. Any user wishing to participate in file sharing needs to install or actively start specialised software known as a BitTorrent client (BitTorrent Client). In order to do so, a user will need to download a BitTorrent Client from a website that distributes BitTorrent clients. As part of the installation process, a user may configure the BitTorrent Client in accordance with his or her preferences or adopt standard settings. A BitTorrent Client enables users to access a given P2P Network, such as eDonkey or BitTorrent. Some examples of BitTorrent Clients for the BitTorrent network include Azureus, BitComet and UT"*

Det er altså hermed fastlagt, at deltagelsen i et BitTorrent netværk, kræver for mange aktive tiltag, til nogensinde at kunne kategorisere som uagtsomhed.

5.2.6 Konklusion

Denne sag er skelsættende da det er den første gang videregivelsen blev nægtet i landsretten. Dette på trods af der har været en historik for at pålægge teleudbyderne at videregive.

Østre landsret ændrer byrettens afgørelse og leder retspraksis i en anden retning end hidtil. Det vil dog formentlig ikke betyde at videregivelse vil være umulig fremadrettet. Et stort tab for CMS' anbringender var, at deres bevisoptagelse ikke skulle bruges til sagsanlæg, som

retten fastslog var et krav. En stor del af sagen centrerede sig om ordlyden for edition og bevisoptagelse, hvilket de sandsynligvis kan rette op på ved blot at anlægge sagerne, eller i hvert fald skabe omtale om at de anlægger sagerne.

Den næste fremtrædende præcedens fra dommen er henvisningen til logningsbekendtgørelsen. De opbevarede oplysninger skal overholde finalité-princippet, og udelukkende bruges i forbindelse med strafferetsplejen.

Slutteligt, hensynet til rettigheder og afvejningen af parternes interesser. Eftersom sagen angik 4011 IP-adresser, må retsgrundlaget siges at være ret generelt i denne dom. Retten vægter altså hemmeligholdelsen højere, end interessen for civilretlig forfølgelse.

Det skal nævnes, at både begrundelse og resultat blev genspejlet i en senere dom, afsagt af Retten på Frederiksberg d. 22. maj 2019. (BS-31445/2018-FRB)

5.3 Sag C-597/19 (BitTorrent)

NJORD Law Firm omtaler denne dom[76] på deres hjemmeside, som en revolutionerende ændring i retspraksis.

"Afgørelsen er meget konkret og har beskæftiget sig med mange aspekter af fildelingssagerne. På baggrund af EU-domstolens klare afgørelse kan det konkluderes, at de civile søgsmål er og stedse har været i fuld overensstemmelse med EU-retten og dansk ret." - Lars Lokdam

Og endvidere:

"Vi håber, at EU-domstolens klare budskab bliver læst og kommunikeret, og at vi igen kan få fokus på, at pirateri af film ikke er lovligt og at advokater, der bistår rettighedshavere, sammen med politi og andre myndigheder varetager en vigtig samfundsfunktion." - Lars Lokdam

5.3.1 Sagens parter

Sagsøger i hovedsagen er M.I.C.M. Mircom International Content Management & Consulting Limited (herefter Mircom). Mens sagsøgte i sagen er Telenet BVBA. Altså en rettighedshaver mod en internetudbyder, som også set i U.2019.2019.

Mircom nedlægger påstand om at Telenet fremlægger navne- og adresseoplysninger for tusindvis af sine abonnenter, hvilket Telenet har afvist. Ifølge sagsøger har de pågældende abonnenter ved brug af BitTorrent-teknologi uploadet film hvoraf de er rettighedshavere, hvilket ifølge Mircom er en ulovlig overføring af dets film til almenheden.

5.3.2 De præjudicielle spørgsmål

Første spørgsmål i sagen omhandler hvorvidt download via peer-to-peer netværk, (med det som EU-retten kalder "pieces", altså de ovenfor nævnte fragmenter af en fil), med henblik på

[76] https://www.njordlaw.com/da/eu-domstolen-giver-njords-klient-ret-i-fildelingssagerne - NJORD udtaler sig om dommen – tilgået d. 18-10-2022

at uploade til tilrådighedsstillelse (Seeders) betragtes som en overføring til almenheden. Dette på trods af at disse individuelle fragmenter i sig selv er uanvendelige. Dette spørgsmål blev delt op i to:

- Findes der en bagatelgrænse for, hvornår seeding af disse fragmenter udgør en overførsel til almenheden?
- Er det en relevant omstændighed at seeding kan ske automatisk, og således uden brugerens viden (som nævnt ovenfor, kan upload af fragmenterne ske automatisk efter en film er set).

Kan en person som har fået transporteret ophavsrettigheder ifølge aftale, men som ikke selv udnytter disse rettigheder i anden forstand end blot at kræve skadeserstatning af mistænkte krænkere af ophavsretten, og hvis indtjening således afhænger af piratvirksomheders fortsatte krænkelse af ophavsretten, nyde de samme rettigheder som tilkommer licenshavere som udnytter rettighederne på 'normal' vis?

Det tredje spørgsmål er det samme som i U.2019.2019 dommen. Afvejningen mellem håndhævelsen af de intellektuelle rettigheder, og på den anden side individets grundlæggende rettigheder jf. grundrettighedscharteret, såsom beskyttelse af privatlivet og personoplysningerne.

Er den systematiske registrering og behandling af IP-adresserne på ophavsrets krænkerne lovlig, på trods af de sker af en hel "Swarm".

En Swarm er de øvrige peers man forbinder til, når man skal downloade de øvrige fragmenter af filen. Der vil derfor sandsynligvis være en bifangst af IP-adresser, når man ser på den totale monitorerede mængde. Den bifangst har muligvis ikke begået samme forseelse som de øvrige, hvilket kan gøre retshåndhævelsen svær, da rettighedshaverne egentlig kan ende med at registrere og behandle uskyldige IP-adresser.

5.3.3 Udtalelse fra Generaladvokaten

I forhold til det første spørgsmål, udtaler generaladvokaten at den omstændighed, at delelementer af en fil, der indeholder et beskyttet værk, stilles til rådighed for download via et peer-to-peer-netværk stadigvæk udgør en tilgængeliggørelse for almenheden. Dette på trods af, hvorvidt den pågældende bruger selv havde downloadet hele filen eller havde fuldt kendskab til omstændighederne om hvorvidt han uploadede (seedede) selv.

Sekundært behandler generaladvokaten hvorvidt virksomheder som har fået overført deres rettigheder (NJORD) f.eks. skal stilles ift. de oprindelige rettighedshavere. Det er situationen hvor rettighederne udelukkende er overført med den intention at retsforfølge i form af erstatningskrav. Generaladvokaten udtaler at under de foreliggende omstændigheder i direktiv 2004/48/EF, vil sådanne virksomheder ikke have mulighed for at gøre brug af de i samme direktivs kapitel II nævnte foranstaltninger, såsom lettere tilgang til procedure og retsmidler generelt. Direktivet er dog ikke til hinder for, at en medlemsstat vælger at give en erhverver af rettigheder (eller fordringer i dette tilfælde) muligheden for at retshåndhæve krænkelserne. jf. Kapitel II i direktiv 2004/48/EF.

Ydermere indeholder udtalelsen en beskrivelse om anvendelsen af direktivet 2004/48/EF artikel 8,

Artikel 8: Medlemsstaterne sikrer, at de kompetente retslige myndigheder i forbindelse med sager om krænkelse af en intellektuel ejendomsrettighed og som svar på en velbegrundet og forholdsmæssig afpasset begæring fra rekvirenten, **kan pålægge den krænkende part og/eller enhver anden person at give oplysninger** om oprindelsen af og distributionskanalerne for de varer eller tjenesteydelser, **der krænker en intellektuel ejendomsrettighed**, såfremt den pågældende:

a), er fundet i besiddelse af de omtvistede varer i kommerciel målestok
b), er fundet i færd med at anvende de omtvistede tjenesteydelser i kommerciel målestok
c), er fundet i færd med at yde tjenester, der anvendes i de omtvistede aktiviteter, i kommerciel målestok,

eller

d) er blevet identificeret af den i litra a), b) eller c) omhandlede person som indblandet i produktion, fremstilling eller distribution af sådanne varer eller levering af sådanne tjenesteydelser.

Altså en bestemmelse om at man kan være tvunget til selvinkriminering eller kan rekvirenten pålægge internetudbyderen at videregive pågældende information.

Generaladvokaten udtaler at national ret bør nægte denne adgang, hvis den under hensyn til sagens omstændigheder finder den uretmæssig. Altså en gengivelse af afvejningsprincippet.

Slutteligt omtaler generaladvokaten beskyttelsen af personoplysninger og om fri udveksling af samme. Registrering og behandling af IP-adresser i dette øjemed, skal fortolkes således at såfremt de er blevet brugt til deling af værker via peer-to-peer netværk, udgør det en lovlig behandling af personoplysninger. Det er imidlertid et krav, at denne registrering (fra f.eks. MaverickEye) skal ske med henblik på forfølgelse af en legitim interesse, navnlig med henblik på at indgive den i artikel 8 nævnte begrundede anmodning om udlevering af navne- og adresseoplysninger.

5.3.4 Rettens afgørelse

Afgørelsen i sagen følger delvist generaladvokatens, men ikke helt.

I henhold til det første spørgsmål, afgør retten at den omtalte upload vil udgøre en tilrådighedsstillelse for almenheden, på trods af disse delelementer kun er anvendelige i sig selv, når en vis andel er downloadet. Ligeledes er det uden betydning, hvorvidt upload sker automatisk som følge af BitTorrent-softwarens indstillinger. De nævner dog at ovenstående er gældende hvis upload sker til en software hvortil der er tegnet abonnement. Hvorvidt dette skal tælle som en modificering, må forblive usikkert, dog er det nærliggende at pointere.

Sekundært, fastlægger retten at en afvejning af hensyn er afgørende for hvorvidt begæringen som rekvirenten indsender til den dataansvarlige skal imødekommes eller ej. Hertil nævnes, og gentages fra generaladvokaten, at begæringen skal være velbegrundet og forholdsmæssigt afpasset. Den forelæggende ret er ansvarlig for denne efterprøvelse.

Slutteligt omtaler retten hvorvidt registrering og behandling af IP-adresserne fra de krænkende er systematisk indfanget. Retten fastlægger at der ikke findes harmoniseret lovgivning til hinder for denne proces, hverken for indehaveren eller tredjemand. Det er dog et krav, at internetforbindelsen er blevet brugt til krænkende aktiviteter, og at det sker med henblik på at anlægge et erstatningssøgsmål ved en civil domstol vedrørende de tab som brugeren har forvoldt.

5.3.5 Konklusion

NJORD Law Firm beskriver som ovenfor nævnt denne dom som en sejr for retstilstanden.

Det kan dog umiddelbart være svært at se hvor meget der går i deres retning, udover den lovlige registrering og behandling af IP-adresser. En begæring efter artikel 8, er stadig begrænset af de samme omstændigheder som ses i den danske version om isoleret bevisoptagelse og editionsreglerne.

NJORD Law Firm opstiller selv 5 uddrag fra sagen:

"at MIRCOM som outsourcing virksomhed har påtaleret til at føre sager (søgsmålskompetence), Præmis 61, 62, 68, 69, 76, 77, 79, 80, 82, 83, 84, 95 og 96.

at outsourcing virksomhed (som MIRCOM og CMS) ikke efter EU-retten skal behandles mindre gunstigt end filmproducenternes egen håndhævelse, Præmis 77.

at opgørelsen af vederlaget foretages ud fra den brugergruppe, der befinder sig i SWARM under delingen, Præmis 32, 44 og 53.

at tilgængeliggørelse af et delelement, som bevist i loggen, er en ophavsretskrænkelse, Præmis 32, 42, 43, 45 og 57.

at opbevaring og behandling af personoplysninger i disse sager er forenelig med GDPR-reglerne, Præmis 97, 106, 109 og 110."

Punkt 1 kan ikke anses for en fornyelse af retstilstanden. Det var allerede fastslået at de havde søgsmålskompetence.

Punkt 2 om en mindre gunstig behandling behandlede den danske landsretssag også. Denne antog i forvejen at de havde samme rettigheder som filmproducenten.

Punkt 3 kan være en modifikation, eftersom vederlaget kan blive højere jo større den pågældende SWARM i øjeblikket beligger sig i.

Punkt 4 om delelementer afspejles også i dansk praksis. U.2019.2019 kom ligeledes frem til at tilgængeliggørelse af et delelement som bevist i loggen, udgør er en ophavsretskrænkelse. Dette kan derfor ikke udledes som en ændring af den i forvejen gældende praksis.

Punkt 5 om opbevaring og behandling af personoplysninger værende forenelig med GDPR-reglerne kan imidlertid anses som en sejr for rettighedshaverne. Forud for denne afgørelse, blev der for rettighedshavernes synspunkt, henvist til en afgørelse fra Datatilsynet. Afgørelsen (journalnr. 2016-217-1119) blev publiceret d. 12. juli 2017. Afgørelsen

omhandler advokaters behandling af personoplysninger, når de anvendes til civilretlig forfølgning af ophavsretlige krænkelser. Det præjudicielle i afgørelsen angik, hvorvidt opbevaring og behandling var i overensstemmelse med den dagældende persondatalov.

Datatilsynet fandt, at såfremt behandling og opbevaring af advokatfirmaet (som repræsenterer rettighedshaver) sker til et legitimt formål, og ligeledes er nødvendig for advokaten til at forfølge denne legitime interesse, kan det tillades. Afgørelsen nævner dog, at nødvendigheden for at varetage det legitime formål, klart skal overstige hensynet til abonnentens privatliv.

Sammenfattende har dette imidlertid formentlig ikke ændret retstilstanden på baggrund af denne præmis. Det har dog valideret det retlige grundlag for opbevaring og behandling, da afgørelsen nu, er afsagt af en højere instans.

NJORD Law Firms hidtidige forretningsmodel om forligsbreve, vil derfor ej heller være forenelig med retspraksis ifølge denne afgørelse. Med denne afgørelse bliver U.2019.2019 dommen ligeledes valideret i højere instans, da afgørelsen er enig på de forenelige fakta. Navnlig at editionsreglerne skal anvendes med henblik på sagsanlæg, og ikke blot forligsbreve.

5.4 Tilgang uden tilgængeliggørelse

De ovennævnte domme omtaler begge scenariet hvor der sker en tilgang nogenlunde samtidig med at der ligeledes tilgængeliggøres for almenheden. Hvordan forholder loven og gældende praksis sig til Leecher situationen, hvor der udelukkende tilgås, men ikke distribueres, altså download af ophavsbeskyttet materiale, men uden der uploades.

Situationen hvor der hverken sker upload samtidig med eller efter download, er som ovennævnt beskrevet som Leechers. Nogle BitTorrent klienter tillader en konfiguration, som blokerer muligheden for andre brugere at downloade delelementerne fra deres computer. Denne situation medfører derfor ikke en krænkelse af eneretten.

Dette er imidlertid stadigvæk en forseelse, det er bare ikke en krænkelse specifikt af eneretten. Der sker stadigvæk en krænkelse af retten til reproduktion, som er beskyttet i artikel 2 om retten til reproduktion i direktiv 2001/29.

Artikel 2: Medlemsstaterne indfører en eneret til at tillade eller forbyde direkte eller indirekte, midlertidig eller permanent reproduktion på en hvilken som helst måde og i en hvilken som helst form, helt eller delvis:

a) for ophavsmænd for så vidt angår deres værker

Når det beskyttede værk downloades fra en ulovlig kilde, på trods af den anvendes til private formål, fremgår det af fast EU-retspraksis,[77] at en reproduktion ikke er omfattet af undtagelsen om privatkopiering i direktivets artikel 5, stk. 2, litra b. Dette vil netop være tilfældet for download af et værk hvortil kilden er fra et peer-to-peer netværk. Kilden er ulovlig da ophavsmanden ikke har givet samtykke til en tilgængeliggørelse på netværket.

[77] Præmis 51 – Sag C597-19 – Tilgået d. 22. okt.

Der er dog ikke i hverken sag U.2019.2019 eller sag C-597-19 lavet en subsidiær påtale for en krænkelse af retten til reproduktion. Såfremt retten kom frem til at der ikke fandtes en krænkelse af eneretten af tiltalte, eftersom pågældende eventuelt kun var en Leecher, havde sagen så været tabt grundet anklageskriftet?

Kapitel 6

6.1 Perspektivering af logningsbekendtgørelsen

Som beskrevet ovenfor, er logningsbekendtgørelsen unægtelig knyttet til strafferetten. Oprindelsen, ordlyden og forarbejderne tegner et billede af at indsamlingen af data er ment til efterforskning af kriminalitet. Hjemlen for den nye logningsregulering kan tilmed findes i retsplejelovens §786, litra a-j.

Det sammenfaldende moment er imidlertid, at det er disse lagrede data, som ligeledes anvendes til retshåndhævelsen af ophavsretlige krænkelser. Dette taler for, at anvendelsen af disse data, både nu, men også på sigt, vil følges ad i sin udvikling. For analyse af denne udvikling, og hvordan retshåndhævelsen af ophavsretlige krænkelser vil håndteres i nu- og fremtid, vil en belysning af samspillet være relevant for afhandlingen. Til denne tages udgangspunkt i retsudviklingen,[78] for at skabe et helhedsbillede af afvejningen mellem retshåndhævelse og hensynet til borgerens rettigheder.

Danmark har siden 2007 pålagt alle internetudbydere at logge deres abonnenters data om telekommunikation. Denne forpligtelse for teleudbyderne var vidtrækkende, i en grad som inkluderede hvem der ringede til hvem, hvornår, og ved brug af hvilken telemast opkaldet var foretaget. Forpligtelsen indeholdt ligeledes en opbevaringspligt, til at gemme disse data i ét år, så politiet kunne få adgang til disse, i tilfælde af efterforskningen af et strafbart forhold.

En tilsvarende logningsforpligtelse har været gældende i mange medlemsstater, navnlig som resultat af logningsdirektivet fra 2006, hvor EU forsøgte at harmonisere logningen af teledata.[79] Lovligheden af det daværende logningsdirektiv blev fundet i strid med EU-retten, først i Digital Rights dommen i 2014, da direktivet indebar et indgreb i de grundlæggende rettigheder.

Dette var blot startskuddet til en række afgørelser hvor EUD har forholdt sig til de logningsforpligtelser som medlemsstaterne påtvinger teleudbyderne. Præjudicielle afgørelser blev ligeledes afsagt i Tele2-dommen fra 2016, La Quadrature du Net-dommen[80] (herefter LQDN) fra 2020 og senest G.D dommen[81] fra 2022.

Uddrag fra disse tre domme, vil anvendes i løbet af perspektiveringen, for at danne et grundlag for den nugældende retstilstand, men også den fremtidige. Det tegner ligeledes et

[78] Lentz, Wacher, Lene og Christensen, Kammersgaard, Tanja. "Logning af teledata – balancen mellem hensynet til kriminalitets bekæmpelse og borgerens privatliv", Juristen nr. 4 og 5, 2022
[79] Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15/3-2006 (logningsdirektivet).
[80] EUD-dom af 6/10-2020 i de forenede sager vedr. La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18).
[81] EUD-dom af 5/4-2022 G.D. (C-140/20).

billede af, at medlemsstaternes beføjelser ift. at pålægge logningspligten på teleudbyderne, er stærkt svækket. Medlemsstaterne er utvivlsomt sat på en vanskelig opgave med at konstruere en national logningsregulering som finder balancen mellem hensynet til håndhævelse overfor hensynet til den enkelte borgers rettigheder. Hvorvidt medlemsstaterne finder denne balance, vil skulle stå overfor en prøvelse ved EUD.

6.1.1 Lovændringen og udfasning af den gamle logningsmetode

Afvejningen som beskrevet ovenfor har der i dansk kontekst særligt været varetaget hensynet til håndhævelsen.[82] Efter en revision af logningsreglerne, fremkom justitsministeriet med et lovforslag d. 24/3-2021. Denne blev sendt til udkast og høring den 27/9-2021, fremsat d. 18/11-2021 og vedtaget d. 3/3-2022.

Formålet med denne nye logningsregulering er at sikre overensstemmelsen med EUD's praksis, især den seneste afgørelse i G.D dommen.

Før denne lovændring, blev teleudbyderne pålagt en pligt til generelt og udifferentieret at logge abonnenternes teledata. Dette udgangspunkt er modificeret, så denne form for logning udelukkende kan foretages ved brug af den nye bestemmelse i retsplejelovens §786, e, stk. 1. Justitsministeren kan efter forhandling med Erhvervsministeren *" fastsætte regler, der pålægger udbydere at foretage generel og udifferentieret registrering og opbevaring af trafikdata, når der foreligger tilstrækkeligt konkrete omstændigheder, der giver anledning til at antage, at Danmarkstår over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig"*

I tillæg til dette, kræves der en domstolsprøvelse efter Grundlovens §63, for at kunne iværksætte en lov som forpligter internetudbyderne til at igangsætte en general og udifferentieret logning.

6.1.2 Anvendelsen af data

Hvad angår proceduren for anvendelsen af den loggede data, skal efter EMD retspraksis ligeledes være beskrevet i loven. Disse hensyn består typisk i, at der skal eksistere et klart og forudsigeligt lovgrundlag for borgeren. I tillæg til dette, skal adgangene til den loggede data, være betinget af godkendelse fra enten en uafhængig myndighed (hvilket vi ikke har i Danmark) eller en domstol.[83]

Anvendelsen af data skal fortsætte som hidtil, hvor det skal ske efter reglerne om retskendelse, og proportionaliteten skal ligeledes være opfyldt. Jf. §§ 783 og 782 i retsplejeloven.

I det nye lovforslag, er det endvidere nedskrevet i lov, at adgangen til de indsamlede data, og dermed indgreb i meddelelseshemmeligheden, alene skal tillades i sager der angår *grov* kriminalitet.

[82] Juristen nr. 4 og 5, 2022, s. 175
[83] Tele2 dommen, præmis 120.

Der ses dog en forskel i typen af de loggede data. Der eksisterer en variation af hvorvidt de loggede data er indsamlet ud fra en målrettet metode, eller en generel og udifferentieret metode.

Justitsministeriet vurderede at der eksisterede en væsentlig procesrisiko[84] forbundet hermed, da det var uvist hvilke data myndighederne kunne anvende til hvilke givne formål. Således fremgår det af LQDN pr. 166 at *"... der under ingen omstændigheder kan gives adgang til ... data med henblik på at retsforfølge og straffe en almindelig strafbar handling, når lagringen heraf er begrundet i formålet om bekæmpelse af grov kriminalitet eller a fortiori i formålet om beskyttelse af den nationale sikkerhed. I overensstemmelse med proportionalitetsprincippet, (...) kan en adgang til data, der er lagret med henblik på bekæmpelse af grov kriminalitet, under forudsætning af, at de i den foregående præmis nævnte materielle og proceduremæssige betingelser, der gælder for at opnå en sådan adgang, overholdes, til gengæld begrundes i formålet om beskyttelse af den nationale sikkerhed.*

Og endvidere fra EUD "*Når disse data undtagelsesvis er blevet lagret generelt og udifferentieret med henblik på at beskytte den nationale sikkerhed mod en trussel, som må anses for at være reel og aktuel eller forudsigelig (---), kan de kompetente nationale myndigheder på området for strafferetlig efterforskning ikke få adgang til disse data i forbindelse med strafferetlig forfølgning, idet forbuddet mod at foretage en sådan lagring med henblik på bekæmpelse af grov kriminalitet (---) herved vil blive berøvet sin effektive virkning.*[85]*"*

Sammenfattende kan det fastlægges, at en general og udifferentieret logning, er den mest vidtgående. Denne metode kan udelukkende pålægges teleudbyderne når logningen skal anvendes til beskyttelse af den nationale sikkerhed. Anvendelsen af disse, er også underlagt et strengt krav om udelukkende at blive anvendt til dette formål.

Det skal noteres, at der i øjeblikket fra justitsministeriet, er pålagt en generel og udifferentieret logning, og at dette tager udgangspunkt i vurderingen fra CTA's (Center for Terroranalyse) årlige trusselsvurdering, der har vurderet terrortruslen mod Danmark som alvorlig siden 2014. Om dette er en dansk omgåelse af G.D.-dommen må være op til læseren, men følgende tager udgangspunkt i at fortolke retstilstanden fastlagt i G.D.-dommen, frem for øjebliksbilledet Danmark forholder sig i.

Modsat, kan den mindre vidtgående logningsmetode, den målrettede, anvendes til bekæmpelse af både grov kriminalitet, men også trusler mod den nationale sikkerhed.

Dette er et eksempel på en klassisk proportionalitetsafvejning, at der ikke må anvendes mere indgribende foranstaltninger, hvis mindre indgribende foranstaltninger er tilstrækkelige, og at indgrebet skal stå i rimeligt forhold til målet.

[84] L 93 Forslag til lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester, s. 70

[85] G.D-dommen, præmis. 100

6.1.3 Den nye logningsmetode

Det er relevant for afhandlingen at belyse den mindre indgribende logningsmetode, nemlig den målrettede logning.

Som ovenfor nævnt, kan der efter e-databeskyttelsesdirektivets art. 5, stk. 1, art. 15, stk. 1, samt EUD-retspraksis, anvendes en målrettet logning som alternativ til den generelle og udifferentierede. Den vidtgående kan som benævnt udelukkende anvendes til nationale trusler, hvorfor den mindre indgribende, målrettede, bliver den relevante ift. igangværende problemstilling.

Det er et krav at den målrettede logning skal være begrænset til det strengt nødvendige, hvad angår kategorierne af teledata som lagres, det skal endvidere begrænses til de berørte personer, og skal have en fastsat varighed.[86]

Dette krav er ligeledes opstillet i retsplejeloven, hvor logningsmetoden skal være personbestemt eller geografisk afgrænset. Jf. retsplejelovens §§ 786 b og 786 c.

6.1.4 Delkonklusion

Når parallellen mellem hensynet til retshåndhævelse og borgerens privatliv, bliver optegnet som problematisk når det gælder håndhævelsen af kriminalitet, fremstår det som yderligere problematisk at håndhæve de i mange tilfælde, mindre grove krænkelser af ophavsretlig natur.

Den logning der førhen ligeledes har indeholdt oplysninger som aktører f.eks. NJORD Law Firm har anvendt til at udsende forligsbreve, er ifølge den nye logningsbekendtgørelse ulovlig at foretage. Dette har i mange tilfælde, undtaget de tilfælde hvor politiet i forvejen har haft en mistanke, været foretaget ved en generel og udifferentieret logning, som nu udelukkende er en metode som kan anvendes til trusler mod den nationale sikkerhed. Den målrettede logning er en mindre indgribende metode, og kan anvendes ved grov kriminalitet.

Såfremt der ikke kan henvises til en alvorlig trussel mod den nationale sikkerhed eller til bekæmpelse af grov kriminalitet, vil internetudbyderne ifølge ny lovgivning, ikke have logget den nødvendige information som de retshåndhævende aktører har brug for til forfølgning af de civile krav.

Hvordan efterlader dette håndhævelsen af ophavsretlige krænkelser?

6.1.5 Håndhævelse af ophavsretlige krænkelser fremadrettet

Relevansen for ovenstående med den nærværende afhandling, er som benævnt at oplysningerne til civilretlig retshåndhævelse, er de samme som til håndhævelse af kriminalitet.

Den civile retshåndhævelse er utvivlsomt svækket ift. den daværende metode, hvor navne- og adresseoplysninger løseligt blev udgivet på baggrund af en liste over IP-adresser.

[86] LQDN pr. 147.

Det er dog efter den nye lovgivning, formentlig ikke umuligt at retsforfølge kravene. En generel og udifferentieret logning som hidtil har været anvendt, kan bruges til efterforskning af kriminalitet af samme grovhed som begrundede logningen, jf. princippet i G.D.-dommen. Derimod, kan der eksistere et grundlag for en målrettet logning.

Som et fortolkningsbidrag til problemstillingen, kan inddrages TEUF art. 83, stk. 1. som angiver minimumsregler som Europa-Parlamentet og rådet fastsætter for, hvad der anses som strafbare handlinger. Hertil også hvad der kan kategoriseres som grov kriminalitet, hvilket udgør kravet for en målrettet logning. Følgende områder nævnes som værende omfattet af grov kriminalitet *"Terrorisme, menneskehandel og seksuel udnyttelse af kvinder og børn, ulovlig narkotikahandel, ulovlig våbenhandel, hvidvaskning af penge, korruption, forfalskning af betalingsmidler,* ***edb-kriminalitet*** *og organiseret kriminalitet."*

Ifølge retsplejelovens §§ 786 b, stk. 1, og 786 c, stk. 1, som begrunder målrettet logning, angår metoden de forbrydelser der kan straffes med fængsel i 3 år eller derover. Hertil nævnes §299b, som ovennævnte sag i afsnit 4.1. Bestemmelsen angår ophavsretlige krænkelser af særligt grov karakter, den har imidlertid en strafferamme på 6 år.

Processen skulle imidlertid være markant anderledes, i den forstand, at rettighedshaverne har deres liste over de krænkende IP-adresser, som vil udgøre persongruppen den målrettede logning skulle rettes mod. Den målrettede logning skulle derefter godkendes af en domstol om at blive foretaget. Når den loggede data derefter er indsamlet fra internetudbyderen, vil disse formentlig skulle godkendes til anvendelse af enten domstol eller en uafhængig myndighed.

Der kan i den forbindelse argumenteres for, at processen er langt mere kontrolleret, end den historisk har været. Ifølge ovenstående proces vil der både skulle kræves godkendelse fra domstol ved logningen, men samtidig for behandlingen. Det fremstår imidlertid som en passende foranstaltning, taget i betragtning at U.2019.2019 omhandlede en forespørgsel på persondata på over 4.000 IP-adresser.

Der findes imidlertid et alternativ til den generelle og udifferentierede, og den målrettede. Dette omtales som **hastesikring**.

Denne metode gør brug af den data som teleudbyderne anvender til deres egne formål, som beskrevet ovenfor i afsnit 4.2, er det den data de skal bruge til fejlretning, debitering af abonnenter og afregning af samtrafik.[87]

Metoden om hastesikring kan bruges, ifølge justitsministeren, når politi og anklagemyndighed støder på et procesproblem. Procesproblemet værende, at myndighederne ikke har hjemmel til at indhente fornødne teledata til bevisbyrden.

Ifølge denne metode, må der logges i en kortere periode, på eksempelvis 14 dage. Denne type af loggede oplysninger, vil politiet have mulighed for at hastesikre, såfremt lovovertrædelse angår kriminalitet med strafferamme på over 3 år. Jf. retsplejelovens §786, litra a.

[87] Bekg. nr. 1882 af 4/12-2020 Persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester, § 10.

Som alternativ til den strikse EU-konforme fortolkning, kan der argumenteres for, som gentaget ovenfor, at disse oplysninger ikke tjener formålet i logningsbekendtgørelsen mens de stadigvæk udelukkende er til eget brug for teleudbyderne. Såfremt denne hypotese bekræftes, kan rettighedshaverne potentielt have en kortere vej til videregivelse af navne- og adresseoplysninger, såfremt der ansøges om en hastesikring uden at motivet er hjemlet i logningsbekendtgørelsen.

Sammenfattende kan det ikke endegyldigt konkluderes at logningen kan anvendes til retsforfølgning af civilretlige krav, men der er dog indikatorer på at muligheden kunne eksistere.

Kapitel 7

7.1 Konklusion

Afhandlingen har til formål at belyse brugernes ansvar for ophavsretlige krænkelser, og rettighedshavernes retshåndhævelses muligheder. I udarbejdelsen af afhandlingen, fremstod de problematiske forhindringer sig tydeligt, navnlig i forhold til navne- og adresseoplysningernes videregivelse.

I det redegørende afsnit, bliver de forskellige former for P2P-networking belyst. I datiden var denne type af download ofte associeret med ophavsretlige krænkelser, da ikke kun var anonymiseret, men ligeledes ikke krævede en central server. Disse faktorer besværliggjorde retshåndhævelsen, og gør det stadig, især ved hjælp af de beskrevne VPN-services. P2P-networking er imidlertid blevet langt mere anerkendt, som en fungerende business-model for diverse software udviklere. I afhandlingen nævnes f.eks. Blizzard Entertainment, som udbyder download af deres spil mm. igennem torrenting. Dette har mangfoldige fordele, som f.eks. højere download hastigheder, samt færre kapacitetsomkostninger til centrale servere osv.

Der foretages en analyse af forligsbrevet, som blev udsendt fra NJORD Law Firm til abonnenterne. I brevet fremgår der spørgsmål til hvorvidt der findes andre brugere af forbindelse, og ligeledes om forbindelsen er beskyttet af password. Dette er to momenter, som kan besværliggøre søgsmålsprocessen. Det etableres i afsnittet, at tilgangen til ulovlige streamingtjenester er så udbredt, at når en simpel google søgning kan være tilstrækkelig, at et barn ikke vil have forståelse for at dette var en ulovlig handling. Tilsvarende har retspraksis anvendt password beskyttede forbindelser som en måde at præcisere ansvar på, hvilket efterlader et åbent spørgsmål om hvorvidt ansvaret kan præciseres på en åben forbindelse. Retspraksis har ikke taget stilling til dette, formentlig fordi mange forbindelser har standard indstillinger til dette.

Der har i samtiden været et øget fokus på lovgivning når det vedrører persondata. Udgangspunktet er, at IP-adresser udgør almindelige personoplysninger, disse er imidlertid blevet godkendt for behandling af EU-retten, i BitTorrent sagen (sag C-597/19). Dette beskrev NJORD Law Firm som en sejr, da anvendelsen af MaverickEye softwaren, tidligere havde været kritiseret, og ligeledes en del af modpartens anbringender.

Det viste sig i udarbejdelsen, at teleudbydernes forpligtelser var forskelligartede. Opbevaringen starter som en opbevaring til brug for deres egen drift, men overgår efter en periode, til et politirapporteringssystem, som opfylder deres forpligtelser i forhold til

logningsbekendtgørelsen. Denne forpligtelse til opbevaring, medfører at den loggede data skal eksistere i systemet i 1 år. Dette går ud over standard samtykket som abonnenten giver, hvilket bekræfter den påstand som opstillet af Telia og Telenor i U.2019.2019 sagen. Påstanden angik hvorvidt de opbevarede oplysninger udelukkende var et resultat af opbevaringspligten i logningsbekendtgørelsen, hvilket ville besværliggøre videregivelsesprocessen for rettighedshaverne.

Udfaldet af U.2019.2019 blev, at oplysningerne udelukkende var opbevaret for de opstillede kriterier i logningsbekendtgørelsen, og at de ellers ville have været slettet fra databasen. Dette medfører, at videregivelse kun kan ske såfremt formålet med oplysningerne opfyldes, hvilket i logningsbekendtgørelsen, er efterforskning af strafbare forhold. Rettighedshaverne udgør ikke, i retsplejelovens forstand, en efterforsknings myndighed, da de udelukkende vil anvende oplysningerne til civilretlige søgsmål. Endvidere blev der afsagt dom i Tele2 sagen, som afgjorde spørgsmålet om hvilke typer af kriminalitet der kunne ske videregivelse af oplysningerne til. Retspraksis efter denne afgørelse indikerer, at videregivelse kun kan ske til myndigheder, som har kompetence til at foretage efterforskning, og at efterforskningen skulle angå grov kriminalitet.

Når brugerens ansvar skulle præciseres, har det ligeledes været et omtalt spørgsmål hvorvidt tilgængeliggørelsen var en ophavsretlig krænkelse, når dette kun var et fragment af en fil. Det udslagsgivende var, at fragmentet i sig selv, uden helheden, ikke kunne anvendes. Dette spørgsmål blev besvaret i afgørelsen fra EUD, hvor på trods af at tilgængeliggørelsen udelukkende omfattede et delelement, ville dette stadig udgøre en ophavsretlig krænkelse.

Ligeledes blev det fastlagt, at det ligeledes ikke var diskulperende, at brugeren ikke var vidende om, at softwaren uploadede af sig selv. Dette udgjorde ikke en uagtsomheds betragtning, og var stadig en ophavsretlig krænkelse.

Samtlige af disse punkter blev ligeledes bekræftet i den inddragne EU-praksis, hvor det endvidere blev etableret, at videregivelse kun forekomme til efterforskning af grov kriminalitet, jf. Tele2 dommen. I BitTorrent dommen blev det ligeledes fastslået, at NJORD Law Firm og øvrige rettighedshavers behandling af IP-adresser var tilladelig, såfremt det anvendtes til forfølgelse af en lovlig interesse.

Slutteligt foretages en perspektivering af helheden for logningsbekendtgørelsen. Eftersom det er denne bestemmelse som gentagne gange sætter dagsordenen for hvorvidt der sker videregivelse, vil dette ultimativt også blive fremtiden for feltet for retshåndhævelse af disse civile søgsmål. Det må antages at grundlaget for den generelle og udifferentierede logning er passerende, og dermed vil Danmark vende tilbage til en logningstilstand som tiltænkt af lovgiver. I den forbindelse kan der potentielt findes et grundlag for at foretage en målrettet logning, eller en hastesikring af de fornødne oplysninger til brug for forfølgelsen. Retstilstanden er fortsat uklar på området.

Bibliografi

Litteratur

Evald, Jens, ”Retskilderne og den juridiske metode”, 2. udgave, Jurist- og Økonomforbundets Forlag, 2000. (Forkortes: Evald, Jens, 2000)

Lidner, Brigitte, Shapiro, Ted, ”Copyright in The Information Society”, Edward Elgar Publishing Ltd, 2011.

Munk-Hansen, Carsten, “Retsvidenskabsteori”, 1. udgave, Jurist- og Økonomforbundets Forlag, 2014. (Forkortes: Munk-Hansen, Carsten, 2014)

Schovsbo, Jens & Rosenmeier, Morten, & medvirken af Petersen, Clemens, 2013, ”Immaterialret”, Jurist-og Økonomforbundets Forlag og forfatterne.
(Forkortes: Schovsbo, Jens, m.fl. 2013)

Schønning, Peter: ”EU-direktiverne om ophavsret” 2. udgave, Djøf forlag, 2019.
(Forkortes: Schønning, Peter, 2019)

Trzaskowski, Jan, m.fl., ”Internetretten”, 3. udgave, Ex Tutu Publishing A/S, 2017.
(Forkortes: Trzaskowski, Jan, 2017)

Udsen, Henrik: ”IT-RET” 1. udgave, 1. oplag, Ex Tuto Publishing A/S, 2013.
(Forkortes: Udsen, Henrik, 2013)

Lovreferencer

Bekendtgørelse 2006-09-28 nr. 988 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) (Forkortes: Logningsbekendtgørelsen)

Konsolideret udgave af Traktaten om Den Europæikse Unions Funktionsområde (2016/C 202/01) (Forkortes: TEUF)

Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (Forkortes: E-databeskyttelsesdirektivet)

Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Forkortes: Persondatadirektivet)

Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (Forkortes: Logningsdirektivet)

Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (Forkortes: Forordningen)

Lov 2000-05-31 nr. 429 om behandling af personoplysninger (Forkortes: Persondataloven)

Lov 2018-05-23 nr. 502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) (Forkortes: Databeskyttelsesloven)

Lovbekendtgørelse 15/09/2021 nr. 1835 om rettens pleje (Forkortes: Retsplejeloven)

Lovbekendtgørelse 28/09-2022 nr. 1350, Straffeloven (Forkortes: Straffeloven)

Lovbekendtgørelse 2014-10-23 nr. 1144, Ophavsretsloven (Forkortes: Ophavsretsloven)

Lov 1953-06-05 nr. 169 om Danmarks Riges Grundlov (Forkortes: Grundloven)

Bekg. nr. 1882 af 4/12-2020 Persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester

Lov 08/03/2022 nr. 291 om om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester (forkortes:

Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet

Europa-Parlamentets og rådets direktiv 2004/48/EF af 29 april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder

Forarbejder

Betænkning nr. 1565 om databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning, Justitsministeriet, del I, bind 1 (Forkortes: Betænkning nr. 1565)

Tidsskriftartikler

Lentz, Wacher, Lene, ”Logning af teledata i lyset af Tele2-dommen", Juristen nr. 5, Jurist- og Økonomforbundets Forlag, 2017.

Lentz, Wacher, Lene og Christensen, Kammersgaard, Tanja. ”Logning af teledata – balancen mellem hensynet til kriminalitets bekæmpelse og borgerens privatliv”, Juristen nr 4 og 5. Jurist- og Økonomforbundets Forlag, 2022

Dansk retspraksis

U.2019.2019 Ø

EU-retspraksis

C-597-19
C-462/09
C-511/18
C-512/18
C-520/18
C-140/20
C-149/17
C-275/06
C-203/15
C-698/15

Administrativ praksis

Journalnr. 2002-219-0135, "Antipiratgruppens behandling af personoplysninger", Datatilsynet, den 20. november 2003.

Journalnr. 2016-217-1119, "Behandling af oplysninger om bl.a. ophavsretlige krænkelser", Datatilsynet, den 12. juli 2017

Vejledninger

Datatilsynet, "Databeskyttelsesforordningen (En introduktion til de kommende, nye regler om beskyttelse af personoplysninger)", Justitsministeriet, oktober 2017. (Forkortes: Datatilsynets vejledning: databeskyttelsesforordningen, 2017)

Justitsministeriet, "Børns erstatningsansvar"
https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/civilret/Pjece%20boern.pdf

Internetkilder

Ekstra bladet, ”Ulovlige downloads: Tusindvis har fået dette dyre brev” (Tilgået d. 17-11-2022)
https://ekstrabladet.dk/forbrug/Teknologi/ulovlige-downloads-tusindvis-har-faaet-dette-dyre-brev/6485619

Ekstra bladet, ”Downloader du film ulovligt? Nu er du jaget vildt”” (Tilgået d. 17-11-2022)
https://ekstrabladet.dk/forbrug/Teknologi/downloader-du-film-ulovligt-nu-er-du-jaget-vildt/6439939

Karnov News, ”Piratbrevenes Årti – Anklagerne rammer som spredhagl” (Tilgået d. 17-11-2022)
https://www.k-news.dk/nyheder/piratbrevenes-aarti.-anklagerne-rammer-som-spredhagl

Finans, ”Danskere får breve om ulovlig download af film – nu bliver firmaet bag brevene gransket” (besøgt d. 17-11-2022)
https://finans.dk/erhverv/ECE9018989/danskere-faar-breve-om-ulovlig-download-af-film-nu-bliver-firmaet-bag-brevene-gransket/

Dansk erhverv, ”Ulovlig streaming og download i Danmark i 2020” (Tilgået d. 15-11-2022)
https://www.danskerhverv.dk/siteassets/mediafolder/dokumenter/01-analyser/analysenotater-2020/ulovlig-streaming-og-download-i-danmark-i-2020.pdf

Wikipedia, ”BitTorrent” (Tilgået d. 05-09-2022)
https://da.wikipedia.org/wiki/BitTorrent

Market business news, “BitTorrent” (Tilgået d. 20-10-2022)
https://marketbusinessnews.com/torrents-benefit-businesses/242437/

Version 2, “Gennemsnitlig dansk internethastighed” (Tilgået d. 20-10-2022)
https://www.version2.dk/artikel/den-gennemsnitlige-internethastighed-stiger-alligevel-glider-danmark-ned-ad-international

Omnicalculator, ”Udregningen af internethastighed” (Tilgået d. 20-10-2022)
https://www.omnicalculator.com/other/download-time

Makeuseof, ”Blizzards brug af torrenting” (Tilgået d. 20-10-2022)
https://www.makeuseof.com/tag/8-legal-uses-for-bittorrent-youd-be-surprised/

Wikipedia, ”PopCornTime”, (Tilgået d. 11-09-2022)
https://en.wikipedia.org/wiki/Popcorn_Time

Netkablet, ”VPN”, (Tilgået d. 07-09-2022)
https://www.netkablet.dk/hvad-er-vpn/

NordVPN, ”Dark web”, (tilgået d. 07-09-2022)
https://nordvpn.com/da/blog/dark-web/

AVXperten, ”Hvad er VPN”, (Tilgået d. 07-09-2022)
https://www.avxperten.dk/blog/hvad-er-vpn/

VPNService, ”Geoblocking”, (Tilgået d. 10-10-2022)
https://vpnservice.dk/geo-blocking-saadan-tilgaar-du-et-website-der-er-blokeret-i-danmark/

The Guardian, “Ruslands Geoblocking”, (Tilgået d. 21-10-2022)
https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law

The Guardian, “Englands Geoblocking”, (Tilgået d. 21-10-2022
https://www.theguardian.com/culture/2016/nov/25/what-how-and-why-the-uks-new-online-porn-restrictions-explained

Kultur ministeriet, ”Ophavsret på internettet”, (Tilgået d. 18-09-2022)
https://kum.dk/kulturomraader/ophavsret/ophavsret-paa-internettet
Kultur ministeriet, ”Tidsplan for ny direktiv”, (Tilgået d. 01-11-2022)
https://kum.dk/aktuelt/nyheder/todelt-tidsplan-for-implementering-af-ophavsretsdirektiver

Bech-Bruun, ”Det nye ophavsretsdirektiv”, (Tilgået d. 01-11-2022)
https://www.bechbruun.com/da/nyheder/2019/nyt-eu-direktiv-om-ophavsret-i-det-digitale-indre-marked

Jurainfo, ”Implementering af DSM”, (Tilgået d. 19-10-2022)
https://jurainfo.dk/artikel/status-implementering-af-de-resterende-bestemmelser-i-dsm-direktivet-om-ophavsrettigheder

Rettighedsalliancen, ”Pirat indhold på lovlige medier”, (Tilgået d. 01-11-2022)
https://rettighedsalliancen.dk/rettighedsalliancens-hoeringssvar-om-implementering-af-ophavsretsdirektivet-fokuserer-paa-haandhaevelsesmuligheder/

Denstoredanske, ”Efterforskning”, (Tilgået d. 28-10-2022)
https://denstoredanske.lex.dk/efterforskning

Anklagemyndigheden, ”Seks personer anholdt for ulovlig fildelingstjenester”, (Tilgået d. 29-10-2022)
https://anklagemyndigheden.dk/da/seks-personer-anholdt-ulovlige-fildelingstjenester

NJORD Law Firm, ”Q&A”, (Tilgået d. 06-09-2022)
https://www.njordlaw.com/da/fildeling-og-download-af-film/spoergsmaal-og-svar-vedroerende-ulovlig-fildeling-og-download

Tweak, ”Routere”, (Tilgået d. 25-10-2022)
https://tweak.dk/netv%C3%A6rk/s%C3%A5dan-sikres-din-wi-fi-router-

ComputerWorld, “Brugstyveri af Wifi”, (Tilgået d. 25-10-2022)
https://www.computerworld.dk/art/115166/derfor-er-det-ulovligt-at-laane-naboens-wifi

Karnov News, ”Vejledning til byretter” (Tilgået d. 10-11-2022)
https://www.k-news.dk/nyheder/usaedvanlig-vejledning-om-piratbreve-sendt-til-alle-byretter

Karnov News, ”Byretsdommeren vs. Advokatfirmaet” (Tilgået d. 11-11-2022)
https://www.k-news.dk/nyheder/byretsdommeren-vs.-advokatfirmaet

NJORD Law Firm, ”NJORDs udtalelse”, (Tilgået d. 18-10-2022)
https://www.njordlaw.com/da/eu-domstolen-giver-njords-klient-ret-i-fildelingssagerne