

UDSKRIFT
AF
ØSTRE LANDSRETS DOMBOG

K E N D E L S E

Afsagt den 7. maj 2018 af Østre Landsrets 20. afdeling
(landsdommerne Ib Hounsgaard Trabjerg, Henrik Bitsch og Kristine Kjellerup Hansen
(kst.)).

20. afd. nr. B-2451-17:

Telenor A/S

(advokat Michael Hopp)

mod

Copyright Management Services Ltd.

(advokat Jeppe Brogaard Clausen)

og

20. afd. nr. B-2458-17:

Telia Danmark

Filial af Telia Nättjänster Norden A/B, Sverige

(advokat Anette Moll Berg)

mod

Copyright Management Services Ltd.

(advokat Jeppe Brogaard Clausen)

Telenor A/S og Telia Danmark, Filial af Telia Nättjänster Norden A/B, Sverige, har begge
kæret kendelse afsagt den 24. oktober 2017 af Retten på Frederiksberg (BS A-678/2017 og
BS A-711/2017), hvorefter selskaberne blev pålagt til Copyright Management Services

Ltd. (Copyright Collection Ltd.) at udlevere navne og adresser på de af deres abonnenter, der havde fået tildelt ip-adresserne på de pågældende tidspunkter opregnet i bilag til editionsbegæringerne.

Telenor A/S (herefter Telenor) og Telia Danmark, Filial af Telia Nättjänster Norden A/B, Sverige (herefter Telia), har nedlagt påstand om, at Copyright Management Services Ltd.'s anmodning om isoleret bevisoptagelse og editionspålæg nægtes fremme.

Copyright Management Services Ltd. (herefter CMS) har påstået stadfæstelse.

Kæremålet er behandlet mundtligt.

Sagsfremstilling

Sagen drejer sig om udlevering af navne og adresser på de af Telenor og Telias abonnenter, der på et givent tidspunkt var tildelt de i alt 4.011 ip-adresser, som CMS har oplyst er blevet anvendt ved krænkelse af CMS' rettigheder i forbindelse med deling af ophavsretligt beskyttede filer på internettet.

Det er ubestridt, at Telenor og Telia er i besiddelse af de oplysninger, som CMS kræver udleveret.

Ved brug af internettet anvendes en internetprotokol-adresse (ip-adresse), hvorved en brugers router identificeres på netværket. Ip-adressen kan efter det oplyste enten være fast og tildelt en enkelt abonnent (statisk) eller ændre sig og dermed løbende være tildelt forskellige abonnenter (dynamisk).

De under denne sag omhandlede delinger af ophavsretligt beskyttede filer på internettet skal være sket gennem et fildelingsnetværk ved anvendelse af en BitTorrent-client, som brugerne af netværket hver især havde installeret. Hver af disse BitTorrent-clients kommunikerer automatisk med hinanden og sørger for, at der kan deles materiale fra brugerne, således at der typisk hentes materiale til brug for download af f.eks. en film fra flere forskellige brugere. Derved forudsætter fildelingen ikke en hurtig upload-hastighed fra de øvrige brugere.

Listerne med de angivne ip-adresser er efter det oplyste indhentet ved brug af et program kaldet *MaverikMonitor*, udviklet af en tysk softwareleverandør, *Maverickeye UG*. 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 registreret visse brugeres ageren med programmet, ikke brugeres ageren med andre brugere.

I sagen er der fremlagt en udtalelse af 2. april 2014 udarbejdet af dr. Simone Richter om "Evaluation of the System *MaverikMonitor*." Udtalelsens pkt. 5 indeholder følgende "Summary of Findings":

"5.1. In my examination of the System, I found that:

- (a) it is capable of monitoring traffic on the BitTorrent network;
- (b) it identifies the IP addresses of users and records the time of the data transfer accurately. This information enables ISPs to identify the Subscriber whose internet connection was used to conduct the alleged copyright infringement;
- (c) The System implements mechanisms to ensure that no erroneous IP addresses are collected by the System.
- (d) The System establishes connections with remote computers and receives and stores pieces of data from those computers which make content available across the BitTorrent network.
- (e) The received pieces of data are compared to a control copy using hash value comparison. If the hash value of the piece of data downloaded from the source is the same as the control copy, then the received pieces of data and the control copy are considered to be identical.
- (f) Dynamic IP addresses have no influence on the accuracy of the System logging and recording IP addresses and associated time stamp of infringement.
- (g) If the source computer's IP address changes during capture of a data transfer, no data is saved by the System, and therefore not used by *Maverickeye UG*."

I den del af udtalelsen, der omhandler den anvendte terminologi, anføres om BitTorrent bl.a. følgende:

"6.4. Users need to take active steps to set up and install software to enable participation in the P2P Network. These steps cannot be 'accidentally' 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”.

Njord Law Firm har på vegne af klienter i en række tidligere tilfælde i medfør af retsplejelovens regler om isoleret bevisoptagelse og tredjemandsedition, jf. retsplejelovens § 343 og § 299, fået udleveret navne og adresser på abonnenter, der angiveligt har downloadet ophavsretligt beskyttede film som angivet ovenfor, og oplysningerne er blevet anvendt til at fremsende breve til de pågældende abonnenter. I sagen er der fremlagt et eksempel på et sådant brev med følgende ordlyd:

”På vegne af filmproducenten kontakter vi dig, da filmen ”Fasandræberne” er blevet fildelt/downloadet via IP-adressen --- den --- uden samtykke fra filmproducenten.

Dit teleselskab er af en domstol blevet pålagt at oplyse, hvem der var abonnent på IP-adressen på daværende tidspunkt, og dit teleselskab har udleveret dit navn og din adresse. Det er vores opfattelse, at du som abonnent har den nærmeste adgang til bidrage til belysningen af sagen.

Filmproducenten benytter MaverickEYE UG, der overvåger og identificerer datatrafik, herunder IP adresser. Filmen kan være set via eksempelvis Popcorn Time eller lignende hjemmesider af dig eller andre.

Det er ifølge ophavsretsloven ikke tilladt, at 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 du kendskab til at én eller flere i husstanden har set eller forsøgt at se filmen ”Fasandræberne” på det pågældende tidspunkt?

Har du eller andre personer med adgang til IP-adressen, det kan være hjemmeboende børn, set eller forsøgt at se filmen på det pågældende tidspunkt, kan sagen afsluttes endeligt ved, at der indbetales i alt kr. 2.100 til konto ---, med oplysning om sagsnummer ---. Beløbet kan også indbetales via MobilePay på tlf. ---. Husk angivelse af sagsnummer også ved denne form for betaling ---.

Vi ser frem til at høre fra dig indenfor 14 dage fra modtagelsen af dette brev. Fremkomst af oplysninger på mail til ip@njordlaw.com kan suspendere fristen. Vi ønsker at undgå videre undersøgelser af sagen og iværksættelse af retssag, og ser frem til at høre fra dig. Husk at oplyse sagsnummer ---.

Rådgivning om ophavsret bør søges hos én, der kender og har erfaring med området. Du kan læse meget mere på vores hjemmeside www.njordlaw.com/da/fildeling. Hjælp os med at sikre en fremtid for skabelse af film.”

Efter afsigelsen af byrettens kendelse af 24. oktober 2017 i denne sag har CMS dokumenteret at have anlagt en række civile retssager ved byretterne mod abonnenter på grundlag af oplysninger modtaget i henhold til tidligere afsagte editionskendelser. En del af sagerne er blevet forligt, ligesom der i nogle tilfælde er blevet afsagt udeblivelsesdom. Andre sager verserer fortsat.

Forklaringer

Der er for landsretten afgivet forklaring af Flemming Pedersen, Lasse Andersen, Bastian Rankløve og Ronnie Fridthjof.

Flemming Pedersen har forklaret, at han har været ansat i Telenor i 26 år. Før det var han ansat i TDC. Han har gennemført forskellige uddannelsesforløb inden for tekniske forhold. De i sagen omhandlede ip-adresser er både statiske og dynamiske. Telenor bruger oplysninger om ip-adresser til afregning og gemmer dataene, fordi de er forpligtet til det i henhold til logningsbekendtgørelsen. Telenor gemmer ikke ip-adresser til brug for andet end opfyldelse af de krav, der følger af logningsbekendtgørelsen. Ip-adresserne er i det almindelige system gemt i op til 30 dage af hensyn til driften, så de kan foretage fejlretninger. Efter de 30 dage slettes dataene i det almindelige system og ligger derefter i Telenors ”politirapporteringssystem”. Systemet hedder sådan, fordi det er politiet, der har brug for de historiske teleoplysninger. Han kan som tekniker ikke få adgang til data i politirapporteringssystemet. Dataene bruges ikke til andet end politirapportering. Politiet har en dommerkendelse, når de skal have udleveret oplysninger.

Telenor gemmer trafikdata til brug for fakturering i 1 år. De gemmer ikke trafikdata til brug for markedsføring, bortset fra nogle data i anonymiseret form. Han ved ikke hvor længe. Henvendelsesgruppen i Telenor består af fem til syv mennesker, og det er dem, der håndterer henvendelserne fra politiet. Han kan ikke sige, hvor længe det tager at svare på en henvendelse vedrørende 5.000 ip-adresser. Man kan søge i politirapporteringssystemet, men nogle ting tager længere tid at finde. Der skal parres en masse data, hvilket kan være ret omstændeligt, da politiet skal have den reelle ip-adresse, der ligger bag.

Lasse Andersen har forklaret, at han er ansat som advokat i Telia og er ansvarlig for Public Affairs, hvilket også omfatter loggede data. Han har været hos Telia i 13 år. I november 2016 modtog Telia første gang et editionspålæg på grundlag af en begæring fra Njord Law Firm. I 2017 modtog Telia to begæringer. Telia har opfyldt alle tre begæringer og har ud-

leveret oplysninger på omkring 1.000 abonnenter bag ip-adresserne. Telia er forpligtet til at gemme ip-adresser med henblik på udlevering til politiet. Det er de oplysninger, der er brugt til at opfylde begæringerne. Telia har ikke brug for ip-adresser til at generere regninger. Teknikerne kan bruge ip-adresser til fejlsøgning og fejlretning. De har et system, hvor de gemmer de data, der er logget til brug for politiet. Hvis Telia ikke havde pligt til at logge, ville de formentlig have behov for oplysningerne til fejlretning i tre uger. Telia har en ”politiafdeling” med to medarbejdere, som sidder for sig selv i organisationen. Afdelingen tager sig af alle henvendelse fra politiet og matcher manuelt ip-adresser med et tidspunkt. De to personer i afdelingen er sikkerhedsgodkendt af politiet og sidder i et aflåst rum. Telia har udleveret oplysninger til politiet 72 gange. I de 72 henvendelser fra politiet var der som hovedregel kun tale om udlevering af abonnentsoplysninger for én kunde. Han har aldrig set en begæring, der omhandlede mere end én kunde. Telia har protesteret over for editonsbegæringerne i denne sag, da der skulle udleveres så mange oplysninger. Fra Njord Law Firms side var der lagt op til, at der også fremover skulle udleveres mange oplysninger, hvorfor man fra advokatfirmaets side gerne ville have sat det i proces. Njord Law Firm var indstillet på at medfinansiere en teknisk mulighed for at fremfinde oplysningerne med henblik på udlevering. Telia havde derfor brug for en principiel afgørelse.

Telia medvirker til blokering af hjemmesider. Der er blandt teleselskaber en såkaldt ”code of conduct”, der betyder, at hvis ét teleskab skal blokere en hjemmeside, spærrer alle de andre teleselskaber også den samme hjemmeside. Det er et resultat af et samarbejde med Rettighedsalliancen. Der kommer typisk en sag om spærring af en hjemmeside hver tredje eller fjerde måned. Telia opbevarer data til brug for fakturering i fem år. De opbevarer de loggede data i op til tre uger.

Han har talt med tre abonnenter, der har modtaget breve fra Njord Law Firm, men ikke fra nogen, der er blevet stævnet.

Bastian Rankløve har forklaret, at han har været ansat som advokat hos TDC i 10 år og er chef for erhvervsretsgruppen, som bl.a. beskæftiger sig med persondataskyttelse og ophavsretskrænkelser. Udlevering af ip-adresser hører under hans afdeling. TDC har i mange år fået anmodninger om udlevering af ip-adresser. I 2015 fik de en henvendelse fra et advokatfirma, som ville have udleveret rigtig mange ip-adresser og gerne ville indgå i en dialog omkring det praktiske i den forbindelse. I 2016 og 2017 modtog TDC henvendelser fra politiet vedrørende i alt 10.000 ip-adresser. I samme periode har TDC udleveret oplys-

ninger vedrørende 167.000 ip-adresser til advokater. I november 2017 stillede TDC sagerne om udlevering i bero på grund af den stigning, der var sket i antallet af henvendelser.

TDC har en afdeling, der kaldes ”politigruppen”, som tager sig af henvendelser fra politiet. Der er fem medarbejdere i politigruppen. Denne gruppe har også håndteret anmodningerne om udlevering af oplysningerne til advokatfirmaet.

De specifikke oplysninger ender i ”logningssystemet”, som bruges til at varetage opfyldelse af forpligtelserne til logning i henhold til logningsbekendtgørelsen. Hvis der ikke var en forpligtelse til at logge, ville TDC ikke gemme ip-adresserne, men kun have dem i under en måned. TDC bruger ikke oplysningerne til andet end udlevering efter logningsreglerne, og de er ikke nødvendige for at foretage afregninger.

TDC har tilsluttet sig protesten mod udleveringen, fordi udformningen af logningsreglerne for tiden er under overvejelse, og der derfor er tvivl om, hvorvidt udlevering kan ske. TDC vil gerne sikre sig, at udleveringen er i orden, også under hensyn til det store antal anmodninger. Nogle kunder har fået den opfattelse, at det er TDC, der overvåger dem, hvilket skaber et uønsket modsætningsforhold. TDC ønsker at være neutrale, men vil ikke lægge hindringer i vejen for rettighedshavere, der vil beskytte deres rettigheder.

Den aftalte ”code of conduct” betyder, at de andre teleselskaber følger trop, hvis der i forhold til et teleselskab er afsagt en dom om, at en hjemmeside skal lukkes. Hvis hjemmesiden placeres på en ny adresse, accepterer man også at blokere den nye adresse.

Som vidnet husker det, opbevarer TDC data med henblik på at opfylde bogføringsloven i 400 dage. Det er for at håndtere klager fra kunder. TDC har ikke behov for at opbevare ip-adresser til fejlretning. TDC har som et gammelt selskab mange forskellige systemer, men har siden 2017 forsøgt at håndtere henvendelser om udlevering bedre. Data i logningssystemet bruges ikke til andet end udlevering. Det er kun politigruppen, der har adgang til systemet.

Ronnie Fridthjof har forklaret, at han ejer filmselskabet Fridthjof Film A/S. Selskabet startede i 2000 og har 40-50 fastansatte og op mod 200 freelanceansatte, når de er i gang med en produktion. Selskabet står bl.a. bag filmene ”Blå Mænd”, ”Armadillo”, ”The War Show” samt ”Alle for én”, ”Alle for to” og ”Alle for tre”, der er nogle af de mest sete film i

Danmark. "Alle for én" omsatte for 20,3 mio.kr. ved det fysiske salg, mens "Alle for tre" kun omsatte for 16 mio. kr. De håbede, at denne nedgang i omsætningen ville blive erstattet af en øget omsætning ved det digitale salg, men det skete ikke. Det digitale salg var stort set det samme for begge film. Markedet er ved at finde sit niveau for det digitale salg.

Fridthjof Film A/S er medlem af Producentforeningen, som bl.a. er med i Rettighedsalliancen. Selskabet har ved rettighedskrænkelser på nettet prøvet at samarbejde med politiet og med Njord Law Firm. Rettighedskrænkelser var et problem allerede i 2008, hvor selskabet politianmeldte nogle forhold, men fik at vide, at selskabet selv skulle forfølge krænkelserne civilretligt. Rettighedsalliancen har en strategi om at gå efter bagmændene. De har konstateret mere end 18.000 ulovlige fildelinger af filmen Alle for tre. Han vil tro, at det reelle tal nok nærmere er 50.000. Vidnet havde den 13. juni 2017 et møde med SØIK, hvor det blev konkluderet, at SØIK ikke kunne hjælpe. SØIK henviste endnu engang til, at selskabet selv civilretligt måtte forfølge krænkelserne, da SØIK ikke ville banke på og beslaglægge alle computere i et hjem. Alternativt skulle selskabet komme med beviser for en omfattende deling. På et møde i fredags forklarede vidnet også justitsministeren om situationen. Vidnet tror på den direkte kontakt med brugeren, så man kan ændre brugerens adfærd, ikke på at gå efter bagmændene. Hvis selskabet ikke kan få adgang til ip-adresser civilretligt, kan selskabet ikke gøre noget.

Anbringender

Telenor har i processkrift af 28. marts 2018 bl.a. anført følgende:

"2 INDLEDNING

Telenor mener, at ophavsrettigheder skal respekteres, og søger generelt at medvirke til modarbejdelsen af ophavsretskrænkelser. Telenor mener dog, at retsmidlerne til forfølgelse af krænkelser skal være proportionale og forenelige med internetabonnenters grundlæggende menneskerettigheder, hvilket ikke er tilfældet i denne sag.

Den tidligere byretspraksis fremlagt af Copyright Management Services Ltd. ("CMS") har været uden grundig prøvelse af det juridiske grundlag, herunder den udvidede argumentation fremført i denne sag. Særligt anbringenderne om fortroligheden af logningsdata er nye og er blevet relevante efter EU-Domstolens afgørelse i C-203/15 og C-698/15 (Tele2-dommen).

CMS henviser desuden til visse afgørelser fra Datatilsynet, Forbrugerombudsmanden og Advokatsamfundet. Gengivelsen af disse afgørelser er unøjagtig, da afgørelserne alene siger, at data kan behandles af CMS efter udlevering, hvis domstolene har afvejet og godkendt udleveringen forinden.

Østre Landsrets afgørelse bør derfor træffes uafhængigt af den tidligere fremlagte danske praksis og på grundlag af anbringenderne i de 3 hovedspørgsmål i sagen, der gennemgås enkeltvist nedenfor.

Det bemærkes, at Telenor og Telia for at undgå gentagelser har "fordelt" sagen således, at Telenor særligt fokuserer på de EU-retlige og persondataretlige element, mens Telia fokuserer på de civilprocessuelle forhold. Telenor påberåber sig således også det af Telia anførte.

3 DEN SÆRLIGE BESKYTTELSE AF LOGNINGSDATA

3.1 Indledningsvist om de grundlæggende rettigheder

Den EU-retlige ramme for denne sag udgøres af EU-chartret om grundlæggende rettigheder, herunder art. 17 om ejendomsret og art. 47 om effektive retsmidler på den ene side, og art. 7 om privatlivets fred, art. 8 om beskyttelsen af personoplysninger og art. 11 om ytringsfriheden på den anden side. Dette suppleres af retten til privatliv og familieliv i art. 8 i den Europæiske Menneskerettighedskonvention (EMRK).

Rettighederne skal ses i lyset af Chartrets art. 52, hvorefter rettigheder kun kan begrænses under respekt af rettighedernes væsentligste indhold og under iagttagelse af proportionalitetsprincippet med mere, samt af art. 51, hvorefter Unionens institutioner og organer, samt medlemsstaterne, skal respektere bestemmelserne i Chartret, når de gennemfører EU-retten.

Der skal i den foreliggende sag derfor foretages en afvejning mellem CMS' ophavsretlige interesser overfor abonnenternes ret til privatliv og beskyttelse af personoplysninger - og om CMS' interesser kan begrunde en fravigelse af Telenors tavshedspligt i medfør af udbudsbekendtgørelsen (Bkg. 715/2011), som implementerer tavshedspligten i E-databeskyttelsesdirektivet (2002/58/EF).

Denne sag udspringer dermed af fællesskabslovgivning.

Afvejningen af disse rettigheder blev oprindeligt behandlet i den principielle dom, C-275/06 Promusicae, hvor EU-domstolen afgjorde, at de nationale domstole skal foretage en afvejning af de nævnte grundlæggende rettigheder med hensyntagen til fællesskabsretlige principper, herunder proportionalitet.

EU-Domstolen konkluderede desuden, med henvisning til E-databeskyttelsesdirektivet, direktiv 2000/31/EF (e-handelsdirektivet), direktiv 2001/29/EF (InfoSoc-direktivet), og direktiv 2004/48/EF (Retshåndhævelsesdirektivet), at der ikke af EU-retten følger en almindeligt pligt for internetudbydere til at videregive oplysninger til brug for beskyttelsen af ophavsretten under en civil retssag. Der er dog intet til hinder for, at medlemsstaterne indfører en sådan regel under respekt af de almindelige regler.

Efterfølgende har EU-domstolen i den svenske præjudicielle afgørelse kendt som "Tele2-dommen" fundet, at indsamlingen af logningsdata på måde, som den finder sted i Sverige - som svarer til de danske forhold - er disproportional og derfor i strid med charteret. De svenske (og danske) logningsregler skal derfor ændres, hvilket imidlertid endnu ikke er sket i Danmark.

3.2 E-databeskyttelsesdirektivet og den danske implementering

E-databeskyttelsesdirektivets art. 5 fastlægger teleselskabernes tavshedspligt og fortrolighed, der også vedrører trafikdata. Trafikdata reguleres desuden i art. 6, hvoraf fremgår at sådanne data skal slettes, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog bl.a. art. 15, stk. 1.

Art. 15 vedrører anvendelsesområdet for visse bestemmelser i direktiv 95/46/EF (Persondatadirektivet), og det følger heraf, at der kan gøres indskrænkning i rækkevidden af rettighederne i bl.a. E-databeskyttelsesdirektivets art. 5 og 6. Artikel 15 er den eneste bestemmelse, der giver mulighed for at fravige direktivets øvrige bestemmelser, f.eks. gennem logging.

En indskrænkning, der er vedtaget med hjemmel i denne bestemmelse, skal derfor være begrundet i et af de oplyste hensyn i bestemmelsen, hvilket også gælder for de danske logningsregler. Retsforfølgning af civile krav er ikke et af de oplyste hensyn i art. 15, og allerede derfor er indskrænkning i teleselskabernes tavshedspligt af hensyn til forfølgning af et civilretligt krav ikke muligt.

I Danmark er art. 15 i E-databeskyttelsesdirektivet udmøntet i teleloven, samt i bekendtgørelse nr. 715 af 23. juni 2011 (udbudsbekendtgørelsen). Bekendtgørelsen regulerer trafikdata, herunder hvornår teleselskaberne må behandle trafikdata i § 23, stk. 1, med henvisning til bl.a. retsplejelovens § 786, stk. 4 om telelogning.

Reglerne om logning af data fremgår af bekendtgørelse nr. 988 af 28. september 2006 (logningsbekendtgørelsen), der er udstedt med hjemmel i teleloven, og følger af art. 15 i E-databeskyttelsesdirektivet. Oplysningerne, der begæres af CMS i denne sag, er disse loggede teledata.

Logningsbekendtgørelsens § 1 beskriver formålet med logning som værende til brug for "efterforskning og retsforfølgning af strafbare forhold.". Ligesom E-databeskyttelsesdirektivet er der intet i logningsbekendtgørelsens ordlyd, der indikerer, at logningsdata kan anvendes til forfølgning af civile krav.

Dette er særligt væsentligt i forhold til persondatareguleringen, da det følger af "Finalité-princippet" i persondatalovens § 5, stk. 2 og persondatadirektivets art. 6, stk. 1, litra b, at behandlingen af persondata alene må ske til udtrykkeligt angivne og saglige formål, og ikke senere må viderebehandles til hermed uforenelige formål. Formålet med dette princip er, at de registrerede skal kunne vide hvilke formål deres oplysninger anvendes til, og vide at oplysningerne ikke behandles til andre uforenelige formål, se i den forbindelse U.2017.1092Ø.

Idet logningsreglerne ikke nævner udlevering af logningsdata til civiles forfølgelse af ophavsretlige krænkelse som et formål, og dette må betragtes som uforeneligt med formålet for logningsdata - at der kan ske udlevering til politiet ved alvorlig forbrydelse - vil udlevering derfor være i strid med Finalité-princippet.

3.3 EU-dommene - Tele 2 og Digital Rights Ireland

Det europæiske logningsdirektiv blev kendt ugyldigt af EU-domstolen i Digital Rights Ireland dommen (C-293/12). Som konsekvens af dette er medlemsstaternes logningsregler nu baseret på hjemlen i E-databeskyttelsesdirektivets art. 15, hvilket også er tilfældet for den danske logningsbekendtgørelse.

Grænsen for anvendelsen af logningsdata blev optrukket yderligere i Tele2/Watson-dommen (C-203/15 og C-698/15), hvor EU-domstolen afgjorde, at de svenske logningsregler ikke levede op til kravene i Chartret, da logningen var for bred og udifferentieret, præmis 110-112. Domstolen behandlede herefter myndighedernes adgang til logningsdata i præmis 114-119, og konkluderede, at myndighedernes adgang skal være begrænset til det strengt nødvendige. Det er endvidere et absolut krav, at

"Hvad angår de mål, som kan begrunde en national lovgivning, der fraviger princippet om fortrolighed i forbindelse med elektronisk kommunikation, bemærkes, at for så vidt som opregningen af de mål, der er fastsat i artikel 15, stk. 1, første punktum, i direktiv 2002/58, er udtømmende, således som det er blevet fastslået i denne doms præmis 90 og 102, skal adgangen til de lagrede data faktisk og præcist opfylde et af disse mål. For så vidt som det mål, der forfølges med den pågældende lovgivning, skal stå i forhold til alvoren af det ind-

greb i de grundlæggende rettigheder, som denne adgang indebærer, følger det desuden heraf, at det på området for forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser alene er bekæmpelse af grov kriminalitet, der kan begrunde en sådan adgang til de lagrede data." (Præmis 115)

I forlængelse heraf fortsatte EU-domstolen, at foranstaltninger skal "... fastsætte klare og præcise regler, der angiver, under hvilke omstændigheder og på hvilke betingelser udbyderne af elektroniske kommunikationstjenester skal give de kompetente nationale myndigheder adgang til de pågældende data", præmis 116.

De begærede oplysninger i denne sag er logningsdata, der alene er opbevaret af teleselskaberne til bestemte vigtige hensyn, der ikke omfatter forfølgelsen af civile krav. Der er ingen klare og præcise regler i dansk ret om, at logningsdata kan udleveres til private til at forfølge civile krav, og CMS' baserer sin begæring på de generelle editionsregler. Udlevering af logningsdata til CMS' forfølgelse af civile krav, på baggrund af editionsreglerne, er derfor uforeneligt med Tele2/Watson-dommen.

Dette bekræftes af Europaudvalget, der i 2017 skrev, at "De danske logningsregler går videre end det nu ugyldige EU-logningsdirektiv. Men de danske regler indeholder samtidig en del betingelser, som den nye dom forudsætter for logning og for politiets adgang til logningsdata. Disse betingelser er oplyst i retsplejelovens § 781 - § 784: - det er alene politiet, der må få telelogningsdata udleveret..."

Selv hvis udlevering kunne ske til forfølgelse af civile retssager, ville det være betænkeligt, hvis private virksomheder havde nemmere ved at få udleveret logningsdata end politiet og myndighederne. Udlevering til civile bør derfor alligevel kun ske i tilfælde, der er sammenlignelige med grov kriminalitet. CMS' eget vidne udtalte til hovedforhandlingen i 1. instans, at ophavsretskrænkelserne i denne sag ikke er alvorlig kriminalitet, men skal ses som tyveri af tyggegummi og parkeringsbøder.

Det er dermed klart, at denne sag ikke kan sammenlignes med grov kriminalitet, og begæringen bør afvises på samme vis, som hvis en kommune begærede oplysningerne udleveret til brug for inddrivelse af p-bøder. CMS kan således alene få adgang til de begærede logningsdata, såfremt retten finder, at CMS skulle have en videre adgang til logningsdata end politiet har.

Tele2/Watson-dommen nævner ingen undtagelser i tilfælde af, at oplysningerne er nødvendige for opklaring af mindre forbrydelser. Kravet om "grov kriminalitet" er absolut og også af denne grund, er det derfor uvedkommende, at oplysningerne måtte være nødvendige for CMS' retsforfølgning.

Overordnet gør Telenor derfor gældende, at udlevering af logningsdata til brug for forfølgelse af et civilretligt krav strider imod den samlede regulering af logningsdata og vil være i direkte strid med EU's charter om grundlæggende rettigheder, som det fortolkes af EU-domstolen i Tele2-dommen.

3.4 Retshåndhævelsesdirektivet

Som anført af CMS, følger det af retshåndhævelsesdirektivet, at medlemsstaterne skal fastsætte foranstaltninger og retsmidler, der er nødvendige for at sikre håndhævelsen af intellektuelle rettigheder og står "i et rimeligt forhold til krænkelsen". I art. 6 uddybes det, at der på baggrund af "et rimeligt tilgængeligt bevismateriale, der er tilstrækkeligt til at understøtte hans påstand", kan pålægges at udlevere oplysninger "under forudsætning af at fortrolige oplysninger beskyttes".

Retshåndhævelsesdirektivet anerkender dermed en grænse for de anvendelige retsmidler, herunder når det er uforholdsmæssigt, når bevisførelsen er usikker, samt for at beskytte fortrolige oplysninger, såsom logningsdata. Rettighedshavere har dermed alene en begrænset adgang til retsmidler, der er forholdsmæssige - desuagtet, at der ikke er alternative retsmidler.

Det er derfor Telenors opfattelse, at retshåndhævelsesdirektivet er i overensstemmelse med retsstillingen efter Tele2-dommen, og ikke kan føre til et andet resultat. Eftersom der er tale om særligt fortrolige logningsoplysninger, og CMS i øvrigt ikke har fremlagt tilstrækkeligt bevis for den enkelte krænkelses omfang, må udlevering af data betragtes som et uforholdsmæssigt retsmiddel.

3.5 Domstolen er forpligtet til EU-konform fortolkning

Danske domstole skal tage E-databeskyttelsesdirektivet, Chartret og EU-domstolens praksis i betragtning, når de behandler denne sag, herunder når de foretager proportionalitetsvurderingen, jf. Chartrets art. 51 og 52.

Domstolene er derfor forpligtet til at fortolke dansk ret på en måde, der er forenelig med EU-reguleringen på området, og som ikke kommer i konflikt med de grundlæggende rettigheder eller almindelige EU-retlige principper, såsom proportionalitetsprincippet, jf. C-461/10 (Bonnier).

De danske regler i retsplejelovens § 299 og § 344 er formuleret åbent, og det er muligt - uden at kollidere med ordlyden af bestemmelserne - at fortolke EU-konformt ved anvendelse af de almindelige fortolkningsmetoder, der er anerkendt i dansk ret. Både de persondatarelige regler og retsplejelovens regler om edition indeholder "skøn", idet edition pålægges, når retten finder det "hensigtsmæssigt", og udleveringen af persondata kan ske, hvis domstolen finder det proportionalt.

Da den ene fortolkningsmåde vil bringe dansk ret i strid med EU-retten, må pligten til EU-konform fortolkning medføre, at logningsdata ikke kan udleveres til forfølgelse af civile krav med hjemmel i retsplejelovens editionsregler. Manglende inddragelse af EU-retten i landsrettens afgørelse ville være i strid med Chartrets art. 51.

4 ADGANGEN TIL BEVISOPTAGELSE EFTER RETSPLEJELOVEN

4.1 Udgangspunktet er hemmeligholdelse

Ifølge CMS bør udlevering af logningsdata være muligt til civile formål, idet der ikke udtrykkeligt fremgår et forbud herom i hverken logningsreglerne eller retsplejeloven.

Dette er ikke korrekt fortolket.

Et specifikt forbud er ikke nødvendigt, når udgangspunktet for logningsdata er, at disse skal hemmeligholdes, jf. udbudsbekendtgørelsen (Bkg. 715/2011), medmindre en undtagelse er specifikt hjemlet. Da det fremgår af både logningsbekendtgørelsen og vejledningen hertil, at logning alene sker til "efterforskning og retsforfølgning af strafbare forhold", er udlevering til forfølgelse af civile krav som udgangspunkt udelukket.

Der er tale om anvendelse til et nyt formål, som strider mod det oprindelige formål, set i lyset af at teledata er fortrolige og alene må behandles - både tidsmæssigt og indholdsmæssigt - til at levere teletjenesten til brugeren. Dette udgangspunkt gennemskydes af logningsreglerne for at sikre tilstedeværelsen af fortrolige oplysninger til brug for "efterforskning og retsforfølgning af strafbare forhold" - men ikke til andre formål. Som nævnt ovenfor, medfører "Finalité-princippet" i persondatalovens § 5, stk. 2, således, at der ikke kan ske udle-

vering til civil forfølgelse af ophavsretlige krænkelse, når dette ikke er angivet som formålet med logningsdata i lovgivningen.

En generel bestemmelse om edition bør desuden ikke kunne gennembyrde bestemmelser om fortrolighed i særlovgivning uden udtrykkelig hjemmel, jf. princippet om *lex specialis*. Hvis lovgiver ønskede, at logningsdata skal kunne udleveres til civile sager om ophavsret, bør dette fremgå af loven eller forarbejderne hertil, jf. i denne retning EU-Domstolens afgørelse i C-275/06 (*Pro-musicae*). Selv hvis de generelle editionsregler kunne bryde fortroligheden, vil reglerne dog fortsat ikke kunne anvendes til at få udleveret data i denne sag, jf. straks nedenfor.

4.2 Editionsreglerne forudsætter en vis hensigt om at anlægge retssag

Det følger af forarbejderne til retsplejelovens § 343, at retten undtagelsesvis kan bestemme, at bevisførelse eller en del af denne skal ske inden hovedforhandlingen, når retten finder det hensigtsmæssigt. Det følger desuden, at bevisoptagelse, som alene skal tjene til vejledning for, om en sag overhovedet skal anlægges, ikke kan tillades - hvilket må betyde, at § 343 alene finder anvendelse, når parten allerede har besluttet, at en sag skal anlægges.

Kulturministeriet har udtalt, at Retsplejeloven giver mulighed for at anvende domsstolssystemet til at få udleveret abonnentoplysninger til brug for en verserende retssag. Dog uddybes det, at Retsplejelovens regler næppe kan anvendes i de situationer, hvor personoplysninger alene ønskes udleveret for at udsende "informationsbreve". Det er således ikke hensigten med reglerne, at rettighedshavere skal anvende oplysningerne til andre formål uden for domstolene (såsom udsendelse af breve med bøde i), men alene til verserende retssager.

Selvom et udtrykkeligt krav om anlæggelse af retssag ikke fremgår af editionsreglerne, må dette udledes af ordlyden "inden retssag anlægges", samt af at bevisoptagelse ikke kan ske "til vejledning for, om sag overhovedet skal anlægges". Dette bestyrkes desuden af ordlyden af retsplejelovens § 340, der har en nær forbindelse til §343, hvorefter "Når omstændighederne taler derfor, kan retten dog bestemme, at bevisførelsen eller en del af denne skal ske inden hovedforhandlingen". Det er dermed forudsat, at bevisoptagelse skal ske for at tilvejebringe bevis til en retssag - og CMS skal derfor have til hensigt at anlægge retssager i alle tilfælde, hvor der ikke der indgås forlig.

4.3 CMS har overordnet ingen hensigt om anlæggelse af retssager

Som altovervejende hovedregel bliver der ikke anlagt retssager om disse krænkelse, når forlig ikke indgås. Tidligere udleveringer af oplysninger til Njord Law Firm har primært været anvendt til udsendelse af såkaldte "trusselsbreve" til internetabonnenterne, jf. Telias bilag A, B og R. Brevene indeholder en "opfordring til forlig", og det fremgår, at videre undersøgelser og retssager gerne vil undgås, jf. også bilag B. Under hovedforhandlingen i 1. instans redgjorde advokat Jeppe Brogaard Clausen også for, at alle de tidligere udleverede oplysninger alene havde ført til en meget begrænset antal retssager.

I CMS' nye bilag 53 vises en række retssager, der næsten udelukkende er blevet anlagt og ført efter hovedforhandlingen i 1. instans. Dette supplerer med en uspecificeret liste af sager, der umiddelbart tilsvarende er anlagt for nyligt, bilag 53.1. Denne pludselige og uforklarlige ændring af Njords praksis er utroværdig og må alene ses som et forsøg på at forbedre CMS' retsstilling i denne sag. Retten bør vurdere Njords tidligere normale praksis, samt det faktum at der fortsat alene er anlagt retssager for en forsvindende lille brøkdelen af de abonnenter, som Njord har fået udleveret oplysninger om.

For langt størstedelen af de krænkelser, som CMS ønsker oplysninger udleveret om, ligger det derfor allerede på nuværende tidspunkt helt fast, at CMS aldrig vil komme til at anlægge en retssag - enten fordi CMS ikke har viljen til det, fordi rette sagsøgte ikke kan findes, fordi krænkelsen ikke vil kunne bevises, eller fordi forlig indgås uden om domstolene.

Da CMS overordnet ikke har intention om at anlægge en retssag, og dermed ikke kan sandsynliggøre at bevisoptagelsen sker til brug for en retssag, er betingelserne for at udlevere oplysningerne på baggrund af retsplejelovens regler om edition efter § 299 og 343 ikke opfyldt.

4.4 Udlevering af oplysninger vil være uhensigtsmæssigt

I henhold til retsplejelovens § 343, kan retten undtagelsesvis bestemme, at bevisførelse eller en del af denne skal ske inden hovedforhandlingen, når retten finder det hensigtsmæssigt. Selv når bevisoptagelsen sker til brug for en retssag, har retten således et vidt skøn i forhold til, om udlevering vil være hensigtsmæssigt.

I visse tilfælde vil udgangspunktet om, at det er eftertragtellesværdigt, at sager afsluttes uden rettens involvering, skulle modificeres. I denne sag udgør abonnenterne en svagere part, hvis retssikkerhed bygger på domstolsprøvelsen af, om CMS kan løfte bevisbyrden for, at en krænkelser er begået af en abonnent. Udsendelsen af "trusselsbrevene" fra Njord presser abonnenterne til at indgå forlig i disse sager, uagtet om abonnenten er skyldig, og om CMS kan løfte bevisbyrden ved en retssag. Abonnenterne kan vælge at betale for at undgå besværet og udgifterne ved at bevise deres uskyld i en retssag, eller fordi abonnenten fejlagtigt tror, at retten allerede har forholdt sig til vedkommendes ansvar, da retten traf afgørelse om udleveringen af oplysninger.

CMS søger at opkræve penge fra abonnenterne uden prøvelse af ophavsretskrænkelsen, og udleveringen af data muliggør denne problematiske forretningsmodel. At forretningsmodellen er uønsket, bekræftes desuden af Forbrugerrådet Tænk (Talias bilag c), samt af at regeringen i 2012 afviste en brevmodel, bl.a. på baggrund af Rettighedsalliancens udtalelser om, at breve fører til flere uønskede konsekvenser, ikke er formålstjenstlig og ikke er egnet til at imødegå ophavsretskrænkelser (Talias bilag D). Brevene er ifølge Rettigheds-Alliancens mest af alt egnet til at skade advokatstandens omdømme, og brevene giver ikke nogle særlige indtægter, udover hos advokaten selv.

På baggrund af dette bør udlevering af de begærede oplysninger betragtes som uhensigtsmæssigt, da det fører til en omgåelse af formålet med retsplejelovens regler for isoleret bevisoptagelse og en svækkelse af abonnenternes retssikkerhed. Retten bør beskytte borgere mod en sådan krænkelser af deres retssikkerhed og bør på den baggrund afvise CMS' begæring.

Selv hvis retten mener, at udleveringen vil være hensigtsmæssig efter Retsplejelovens regler, skal der foretages en proportionalitetsafvejning i medfør af EU-retten, persondataretten og de grundlæggende rettigheder, der samlet fører til, at begæringen må afvises, som uddybet nedenfor.

5 PROPORTIONALITETSAFVEJNINGEN

5.1 Persondataretten

Ud over at være logningsdata, er de begærede oplysninger personoplysninger omfattet af persondataloven. Det følger af det grundlæggende persondatarelige princip i persondatalovens § 5, stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål som oplysningerne behandles til. Andet led i denne be-

stemmelse fastlægger, at behandlingen af oplysninger er undergivet et proportionalitetsprincip, hvorefter man skal afveje det saglige hensyn, som behandlingen sker til varetagelse af, med de berørte personers ret til beskyttelse af deres persondata.

Som udgangspunkt vil navn, adresse, emailadresse og lignende være almindelige personoplysninger. Udleveringen af data vil dog også kunne medføre behandling af andre typer oplysninger, herunder særligt når en abonnents navn sættes i forbindelse med en strafbar handling (ophavsretskrænkelser), samt efter omstændighederne i tilfælde, hvor den registrerede sættes i forbindelse med film indeholdende følsomme elementer (porno, politiske eller religiøse budskaber, info om sygdomme mv.), se f.eks. bilag E-I.

Denne sag vedrører ikke umiddelbart film med følsomme elementer for så vidt angår Telenors abonnenter. De begærede oplysninger bliver dog sammenkoblet med følsomme oplysninger om strafbare forhold, og er derfor beskyttet mod videregivelse i overensstemmelse med persondatalovens § 8, stk. 2. Typen af personoplysninger, der behandles, skal således inddrages i proportionalitetsvurderingen.

Udlevering af navn og kontaktoplysninger på abonnenter, til brug for retslig forfølgelse eller udsendelse af indkrævninger, er af indgribende karakter for abonnenterne, jf. den udvidede beskyttelse af teledata i E-databeskyttelsesdirektivet. Dette skærper kravene til den bevisførelse, som CMS skal føre for at sandsynliggøre, at den, om hvem oplysningerne begæres udleveret, har foretaget den påståede krænkelse, samt at de begærede oplysninger er egnede, nødvendige og proportionale ift. CMS' interesser.

Fordelingen af private- og erhvervsabonnementer i denne sag vides ikke, men der vil som udgangspunkt være tale om behandling af personoplysninger, uanset om der er tale om erhvervsabonnenter eller private abonnenter, da et erhvervsabonnement ofte kan henføres til bestemte personer i virksomheden. Udleveringen af data ift. et erhvervsabonnement kan være særligt alvorligt, idet CMS' efterfølgende udsendelse af breve kan afsløre oplysninger om den ansatte over for arbejdsgiveren, der kan få alvorlige konsekvenser for vedkommende.

Kontakten til en internetabonnent ved brev eller stævning, når denne ikke er den ansvarlige for krænkelsen, vil i praksis medføre en videregivelse af følsomme oplysninger til tredjemand. En sådan videregivelse forudsætter efter persondatadirektivet og EMRK art. 8, at der for hver enkelt udlevering skal ske en forudgående prøvelse af nødvendighed og proportionalitet. Ved afvejningen bør der derfor lægges særligt vægt på, at videregivelsen af oplysningen om ophavsretskrænkelser kan være af indgribende karakter, da afsløringen kan bringe krænkeren i unåde hos bl.a. abonnenten.

5.2 Kumulativ eller individuel vurdering af krænkelse

Landsrettens proportionalitetsafvejningen skal foretages i forhold til den enkelte krænkelse, begået af det enkelte individ - idet persondataretten, herunder Chartrets art. 8, netop søger at beskytte det enkelte individ. Det er derfor forkert at foretage vurderingen på baggrund af en samlet kumulativ vurdering af alle de oplistede krænkelse i sagen, ligesom det er retssikkerhedsmæssigt betænkeligt at begrænse et individs grundlæggende rettigheder på baggrund af et kollektivt ansvar for andre individers handlinger. Retten på Frederiksbergs lægger derfor vægt et usagligt kriterie, når det anførtes, "... at krænkelse samlet set har et betydeligt omfang".

Det bør ikke være afgørende for parternes retsstilling, hvorvidt krænkelse behandles samlet eller hver for sig, og CMS bør ikke opnå en forbedret retsstilling ved at samle en liste af urelaterede krænkelse. En sådan retsstilling ville medføre, at rettighedshavers evne til at håndhæve sine rettigheder afhang af mængden af værker, denne har rettigheder til. Hverken i dansk ophavsret eller i EU-retten er der hjemmel til, at rettighedshaveres adgang til retsmidler skal afhænge af akkumuleringen af rettigheder og krænkelse, eller til at foretage "kollektive tvangsindgreb".

Landsretten bør derimod vurdere krænkelse på samme vis, som den Norske Høyesterett gjorde i afgørelsen fremlagt i bilag A, hvor retten nåede frem til, at der skal foretages en konkret afvejning, og at der kun kan ske udlevering, hvis den enkelte krænkelse er af et vist omfang.

Som nævnt forklarede CMS' eget vidne, at den enkelte krænkelse i denne sag ikke er en hårdet kriminel, og at den enkelte krænkelse kan sammenlignes med en p-bøde eller at stjæle et tyggegummi. Det er i denne sag tydeligt disproportionalt at tillade et tvangsindgreb i den enkeltes menneskerettigheder på baggrund af en krænkelse, der skal sammenlignes med en p-bøde, og hvis omfang ikke er bevist.

5.3 CMS har alene bevist provokerede krænkelse af meget begrænset omfang
CMS har hverken gjort gældende eller ført bevis for, at nogen konkret abonnent hos Telenor individuelt har begået en krænkelse, som går ud over et begrænset omfang. Værdierne i bilag 1, 44, 46 og 47, viser derimod kun meget begrænsede informationer:

1. Swarm size - "det antal brugere, der deler og downloader en film i et BitTorrent-netværk i løbet af enhver aktuelt dag". Dette er alene generel information om, at der på verdensplan begås krænkelse af et ubestemt omfang. Oplysningen bekræfter desuden, at den enkelte krænkelse er ubetydelig i det samlede billede og for de samlede bestræbelser på at stoppe ophavsretskrænkelse. "Audience size" er tilsvarende generel information, og uden konkret betydning for den enkelte krænkelse.
2. Client - "hvilken BitTorrent-klient, der er blevet brugt til at downloade og dele en fil". BitTorrent-klienter er computersoftware og kan normalt anvendes til både lovlige og ulovlige formål. Besiddelse af en bitTorrent-klient er ikke i sig selv en krænkelse, og er derfor irrelevant ift. vurderingen af en krænkelse.
3. Hashes - "... repræsenterer, hvor mange forskellige hovedfiler en bruger har delt med MaverikMonitor". Captures/Title - "hvor mange gange en bruger har delt det aktuelle værk med Maverik-monitor" Captures - "samtlige "captures" for samtlige værk, som Maverickeye UG har aftale om at afdække fildeling for".

Værdierne relaterer sig alene til, hvor mange gange Maverick-monitor har igangsat en provokeret deling, og viser kun, at det har været muligt at igangsætte en overførsel. Værdierne i Captures/Title og Captures er indholdsløse, da MaverickMonitor hurtigt selv kan fremprovokere et hvilket som helst antal captures, imens antal reelle delinger med andre er ukendt og kan være nul. Værdien i "Captures" er endvidere betydningsløs for denne sag, da det er en værdi for samtlige værker, som Maverickeye UG afdækker fildeling for, og ikke kun de værker som CMS har rettigheder til at påtale krænkelse for.

4. Xref - "... Maverickeye UG har ingen konkrete data, der viser, at en bruger har downloadet det fuldstændige værk eller delt værket for alle de filtitler

XRef-værdierne omfatter". Værdien relaterer sig til tilknytningen af swarms, der som nævnt blot er en generel uspecifik angivelse af alle deltagere, der potentielt kunne have deltaget i delingen af et værk på verdensplan. Det er uklart om værdien overhovedet er begrænset til værker som CMS' har rettigheder til.

Det påhviler CMS at løfte bevisbyrden for den enkelte krænkelse, hvilket retten må vurdere, om CMS har gjort. Telenor kan alene konstatere, at de fremlagte lister blot beviser tilstedeværelsen af en andel af en fil på en bestemt IP-adresse, men ingen egentlige detaljer om de enkelte krænkelsers omfang.

Der er intet oplyst om, hvor mange filen er delt med eller hvor meget af filen var tilgængelig på IP-adressen. Der kan derfor reelt være tale om et ubrugeligt lille stykke af filen, som kun var tilgængelig kortvarigt og aldrig blev delt i øvrigt, f.eks. pga. sletning, flytning eller hvis computeren stod slukket.

Sondringen mellem at have hentet et filmværk ned og at tilgængeliggøre samt distribuere dette filmværk til andre er i øvrigt ikke skarpt opdelt inden for peer-to-peer fildeling, da mange "clients" er forudindstillet til at viderelede. Brugeren er ikke nødvendigvis bekendt med, at denne bidrager til videredelingen, og det vil ofte kræve en aktiv målrettet handling at slå dette fra. Det bør derfor inddrages i proportionalitetsafvejningen, at der ikke er tale om bevidste, kommercielle eller grove overtrædelser.

De registrerede IP-adresser viser alene hen til den router, som forbinder enhederne på et netværk til internettet. Andre både inden for og uden for en abonnents hjem kan forbinde til et trådløst netværk, hvis netværket er usikret, eller ved brug af adgangskode eller hacking. Dette kan dermed ske uden internetabonnentens viden eller samtykke, og krænkelseerne kan derfor være begået af enhver person med adgang til routeren.

Det er endvidere normalt og tilladt for en abonnent at give andre i husstanden adgang til routeren, herunder også gæster. Abonnenter er ikke objektivt ansvarlige for, hvad deres internetforbindelse bliver brugt til, selv i tilfælde hvor forbindelsen er usikret. Det er således heller ikke sandsynliggjort, at krænkeren også er abonnenten, som CMS ønsker oplysninger udleveret om.

CMS' rettigheder går ikke forud for, og berettiger ikke en krænkelse af, en uskyldig persons rettigheder. Formodningen for abonnenternes uskyld og den uberettigede krænkelse af abonnenternes rettigheder bør tillægges særlig vægt ved rettens vurdering. Proportionalitetsafvejningen bør derfor ikke falde ud til fordel for CMS, når CMS ikke kan sandsynliggøre, at abonnenterne er de ansvarlige for krænkelseerne.

Telenor mener i lyset af ovenstående, at et indgreb i abonnenternes rettigheder ikke kan eller bør godkendes på så spinkelt et bevismæssigt grundlag, særligt ikke når de beviste krænkelse er provokerede og af begrænset omfang. På den modsatte side, er der tale om alvorlige brud på potentielt uskyldige abonnenters grundlæggende rettigheder og et tvangsindgreb i de særligt beskyttede logningsoplysninger. At CMS har svært ved at forfølge krænkelseerne ellers, bør ikke føre til et andet resultat.

På baggrund af alle de ovenstående betragtninger gør Telenor overordnet gældende, at landsrettens proportionalitetsafvejning tydeligt bør falde ud til fordel for Telenor, således at CMS' begæring afvises.

6 NY NORDISK RETSPRAKSIS

Som CMS har bemærket, kan der være forskelle i de nationale lovgivninger, der gør at udenlandsk retspraksis kun har begrænset betydning for den foreliggende vurdering.

Det afgørende ved den nordiske praksis, der fremlægges af Telenor i denne sag, er ikke de nationale retsregler, men derimod at flere nordiske højesteretsdomstole har begrænset en tidligere lempelig praksis for udlevering af logningsdata efter Tele2-dommen.

Den finske Højesteret afsagde således dom den 8. december 2017 i sag KKO:2017:85, der vedrørte udlevering af logningsdata til brug for CMS' forfølgelse af ophavsretskrænkelser. I dommen afgjorde Højesteret, at teleselskabet kun kunne udlevere almindelige data, som teleselskabet havde til egne behov, men kunne ikke pålægges at udlevere de oplysninger, som alene opbevares som logningsdata pga. en retlig forpligtelse. Dette til trods for, at der i sagen var tale om et betydeligt antal filmværker og krænkelser, og uanset at oplysningerne måtte betragtes som uundværlige for at kunne afklare ophavsretlighedskrænkelserne og præcisere kravene.

Den Norske Høyesterett traf tilsvarende en kendelse den 26. april 2017 (bilag A), hvor en begæring om udlevering af oplysninger på abonnenter med tilknytning til bestemte IP-adresser blev afvist. Høyesterett udtalte, at det fulgte af forarbejderne til den norske åndsverkslov, at der i den enkelte sag måtte foretages en konkret afvejning af retten til privatliv over for rettighedshaverens interesser. For at en begæring kunne tages til følge, måtte hensynene, som talte for udlevering af oplysningerne, veje tungere end hensynet til tavshedspligten, og vurderingen skulle tage udgangspunkt i krænkelsens grovhed, omfang og skadevirkning. Oplysninger kunne ifølge retten kun udleveres, hvis retten var af et vis omfang.

Ligesom i denne sag, erkendte rekvirenten, at det ikke var muligt at sandsynliggøre det præcise omfang af krænkelserne, og retten fandt, at de fremlagte beviser reelt ikke svarede på, om der var sket deling af materialet med andre end det anvendte "efterforskningsprogram". Retten nåede på den baggrund frem til, at retten til privatliv måtte vægte højest, og at oplysningerne ikke skulle udleveres.

Østre Landsret bør i denne sag tilsvarende genoverveje den lempelige danske praksis i lyset af Tele2-dommen, og retten bør foretage den samme afvejning som den Norske Høyesterett som følge af C-275/06 Promusicae dommen. Tilsvarende den norske Høyesterettssag har CMS i den foreliggende sag ikke ført bevis for grovheden af den enkelte IP-adresses potentielle krænkelse, hvilket må komme abonnenterne til gode i proportionalitetsafvejningen.

6.1 Norsk tingsretspraksis

CMS har i bilag 52 fremlagt en norsk tingretts kendelse afsagt efter ovennævnte Høyesteretts dom. Det bør indledningsvist bemærkes, at dommen har begrænset betydning, da der alene er tale om en tingretts sag, og sagen er desuden blevet kærret. I sagen havde CMS oprindeligt begæret udlevering af oplysninger på 23.375 IP-adresser, og efter Høyesteretts dom frafaldt CMS sin begæring for hele 19.711 af IP-adresserne, da de ikke opfyldte den tærskel som Høyesterett opstillede.

Måden CMS udlægger dommen på, er ikke retvisende. Den norske tingrett godkendte udlevering af oplysninger, men byggede dette på en konkret vurdering af yderligere omfattende og detaljeret dokumentation om krænkelserne (sammenlagt ca. 3000 sider i sagen). Krænkelserne var i sagen desuden blevet inddelt i kategorier baseret på forskellige parametre. Retten lagde specifik vægt på, at beviserne i denne sag gav langt bedre mulighed for at vurdere omfanget af hver enkelt krænkelse, end der havde været i Høyesterettssagen.

Ifølge CMS, er der i den foreliggende sag fremlagt "... eksempler, som de skærbilleder af fildelingsprogrammer, der var fremlagt for Oslo tingrett". Det bør dog bemærkes, at der alene er fremlagt et enkelt eksempel for en enkelt IP-adresse i den foreliggende sag. Der er derfor ikke sket den samme specificering af krænkelsernes alvor i denne sag, som der skete i sagen for den norske tingrett.

Det må på den baggrund slås fast, at det eneste pt. sikre er, at den Norske Høyesterettsdom fik en klar begrænsende virkning for, hvornår der kan ske udlevering af oplysninger. Sagen bekræfter indtil videre, at der fremover vil blive stillet betydeligt skærpede krav til bevisførelsen, og at udlevering forudsætter, at krænkelserne har et vist omfang - hvilket også bør være tilfældet for dansk ret.

7 OPSUMMERING AF ANBRINGENDER

Til støtte for påstanden om, at editionsbegæringen skal nægtes fremme, gøres det sammenfattende gældende, at logningsdata ikke lovligt kan udleveres til privates forfølgelse af ophavsretskrænkelser, at CMS ikke kan anvende retsplejelovens regler om edition som hjemmel til udleveringen, samt at en samlet proportionalitetsafvejning falder ud til fordel for Telenor og abonnenterne. Der skal i sagen foretages en proportionalitetsafvejning mellem CMS' og abonnenternes grundlæggende rettigheder og interesser samt Telenors hemmeligholdelsespligt for logningsdata i medfør af Bkg. 715/2011 (udbudsbekendtgørelsen) og E-databeskyttelsesdirektivet (2002/58/EF). Hemmeligholdelsen kan kun indskrænkes på baggrund af et af de oplyste hensyn i E-databeskyttelsesdirektivets art. 15, hvor civile søgsmål ikke er nævnt.

EU-domstolen slog i C-203/15 og C-698/15 (Tele2/Watson) fast, at myndighedernes adgang til logningsdata skal være begrænset til det strengt nødvendige. Det er et absolut krav, at det på området for forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser alene er bekæmpelse af grov kriminalitet, der kan begrunde adgang til de lagrede data. Udlevering kan desuden alene ske på baggrund af klare og præcise regler for, under hvilke omstændigheder og på hvilke betingelser de kompetente nationale myndigheder kan gives adgang.

Det persondataretlige "Finalité-princip" i persondatalovens § 5, stk. 2 betyder, at der ikke kan ske udlevering af data til brug for civil håndhævelse af ophavsrettigheder, når ikke dette er angivet som et formål med logningen af teledata, jf. også U.2017.1092Ø.

Telenor gør gældende, at Tele2-dommen skal forstås således, at udlevering kan endvidere alene ske, når der er klare og præcise regler, hvilket der ikke er i Danmark for udlevering til private. Selv såfremt der var, bør udlevering være begrænset til tilfælde, der kan sammenlignes med grov kriminalitet, da der ellers vil være en videre adgang til oplysningerne, end politiet og myndighederne har. Der er i denne sag tydeligvis ikke tale om krænkelser, der kan sammenlignes med grov kriminalitet, og begæringen bør derfor afvises.

Østre Landsret skal inddrage ovenstående i vurderingen af denne sag, da dansk ret skal søges fortolket på en EU-konform måde, som ikke kommer i konflikt med de grundlæggende rettigheder, herunder proportionalitetsprincippet, jf. Chartrets art. 51 og 52 samt C-461/10 (Bonnier). Dette kan ske uden at komme i konflikt med bestemmelsernes ordlyd, idet editionsreglerne i Retsplejelovens §§ 229 og 344 giver retten et skøn til at pålægge edition, når det er hensigtsmæssigt, ligesom EU-retten og persondataretten indebærer et skøn i den konkrete proportionalitetsafvejning.

Bevisoptagelse efter retsplejelovens regler om edition

Det gøres gældende, at udgangspunktet for logningsdata er hemmeligholdelse, og at der ikke i dansk ret eksisterer en klar og specifik hjemmel til at udlevere til private, jf. C-275/06 (Promusicae) og Tele2-dommen. CMS kan ikke basere sin begæring på retsplejelovens generelle editionsregler, og Danmark er ikke forpligtet til at sikre udlevering af logningsdata, jf. retshåndhævelsesdirektivets art. 6 og 8, idet udlevering forudsætter, at dette er forholdsmæssigt, at fortrolige oplysninger beskyttes, og at CMS har fremført et rimeligt tilgængeligt bevismateriale, der er tilstrækkeligt til at understøtte sin påstand.

Det følger af lovforarbejderne til retsplejelovens § 343, at CMS skal have til hensigt at anlægge retssager, for at reglerne om edition kan finde anvendelse. Tidligere praksis viser tydeligt, at Njord og CMS alene udsender "bødebreve", jf. Telias bilag A, B og R, og kun rent undtagelsesvist anlægger retssager mod nogle få af de utallige abonnenter, som oplysninger udleveres om.

Da det ikke kan sandsynliggøres, at bevisoptagelse sker til brug for en retssag, er betingelserne for edition efter retsplejelovens §§ 299 og 343 ikke opfyldt. Selv hvis betingelserne var opfyldt, bør udlevering betragtes som u hensigtsmæssigt af retten, idet Njords og CMS' brevmodel (i) er en trussel for abonnenternes retssikkerhed, (ii) omgår formålet med retsplejelovens regler om isoleret bevisoptagelse, og (iii) generelt er uønskelig for samfundet, jf. Telias bilag C og D.

Proportionalitet

De begærede oplysninger er persondata omfattet af persondataloven, herunder §§ 5, 6 og 8. Udleveringen af data er af indgribende karakter for abonnenterne, jf. den særlige beskyttelse af logningsdata, hvilket skærper kravet til bevisførelsen for, at det individ, om hvem oplysningerne begæres udleveret, har foretaget den påståede krænkelse, samt at de begærede oplysninger er egnede, nødvendige og proportionale i forhold til CMS' interesser.

Landsrettens proportionalitetsafvejning skal foretages i forhold til den enkelte krænkelse begået af det enkelte individ, idet persondataretten, herunder Chartrets art. 8, søger at beskytte det enkelte individ. Det er forkert og retssikkerhedsmæssigt betænkeligt at foretage en kumulativ vurdering af krænkelse i sagen samt at begrænse abonnenternes rettigheder på baggrund af et kollektivt ansvar. Landsretten bør, ligesom den Norske Høyesterett (bilag A), afgøre, at der skal foretages en konkret afvejning, og at der kun kan ske udlevering, hvis hver enkelt krænkelse er af et vist omfang.

CMS har ikke ført tilstrækkeligt bevis for den enkelte krænkelses omfang, og krænkelse skal sammenlignes med en p-bøde eller at stjæle tyggegummi. De få konkrete beviser, der er blevet fremlagt, er provokerede krænkelse, som MaverickMonitor selv har iværksat. Omfanget af krænkelse er i øvrigt ren spekulation, og der er ingen beviser for, at abonnenterne er dem, der har foretaget krænkelse. Enhver tvivl om krænkelse bør komme abonnenterne til gode i afvejning, og det er derfor disproportionalt at tillade tvangsindgreb på den baggrund.

Telenor mener i lyset af ovenstående, at et indgreb i abonnenternes rettigheder ikke kan eller bør godkendes på så spinkelt et bevismæssigt grundlag, ligesom indgrebet vil ramme helt uskyldige personer, der intet ansvar har for krænkelse. En samlet proportionalitetsafvejning af CMS' spinkle bevisgrundlag over for det voldsomme indgreb i Telenors hemmeligholdelsespligt og abonnenternes grundlæggende rettigheder bør derfor klart føre til en afvisning af CMS' begæring."

Telia har i processkrift af 27. marts 2018 bl.a. anført følgende:

”ANBRINGENDER

Telia gør følgende overordnede anbringender gældende:

Udlevering af personoplysninger, der er logget i medfør af logningsbekendtgørelsen, kan kun finde sted i forbindelse med politiets efterforskning af strafbare forhold.

Retsplejelovens betingelser for isoleret bevisoptagelse og editionspålæg er ikke opfyldt, da udlevering af de efterspurgte personoplysninger ikke sker til brug for anlæg af retssag.

Hensynet til håndhævelsen af immaterielle rettigheder må efter en proportionalitetsafvejning vige for beskyttelsen af persondata.

Nærmere om anvendelse og udlevering af personoplysninger logget i medfør af logningsreglerne

Hjemlen til logning af datatrafik

Det er en forudsætning for CMS’s anmodning om udlevering af personoplysninger, at teleselskaberne foretager logning af abonnenternes IP-adresser efter logningsreglerne. Derved bruger CMS logningsreglerne som løftestang for privat retsforfølgelse (”trusselsbreve”) af immaterialretskrænkelser. Uden logningsreglerne ville teleselskaberne kun være berettiget til at opbevare data om tildelte IP-adressers forbindelse til abonnenter i ganske kort tid og ville dermed ikke være i stand til at efterkomme editionsbegæringer som den foreliggende. Der henvises til persondatalovens § 23.

Logningspligten er hjemlet i retsplejelovens § 786, stk. 4, hvoraf det fremgår, at teleselskaberne er forpligtede til at foretage registrering og opbevaring i ét år af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold.

Logningsbekendtgørelsen indeholder nærmere regler om logningen og angiver blandt andet i § 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.”

Det fremgår med andre ord både af hjemmelsgrundlaget og af bekendtgørelsen, at oplysningerne skal registreres og opbevares til brug for efterforskning og retsforfølgelse af strafbare forhold.

Logningsreglerne er en fravigelse fra hovedreglen i artikel 5 i E-databeskyttelsesdirektivet, som pålægger medlemsstaterne at sikre kommunikationshemmeligheden. Kommunikationshemmeligheden er også hjemlet i EU’s Charter om grundlæggende rettigheder, jf. artikel 7, 8 og 11.

Fortolkning af logningsreglernes anvendelsesområde

Da logningsreglerne er en fravigelse fra hovedreglen om beskyttelse af persondata generelt og om meddelelshemmeligheden specifikt, gøres det gældende, at logningsreglerne skal fortolkes indskrænkende, således at loggede oplysninger kun må bruges til de udtrykkeligt angivne formål, altså politiets efterforskning og retsforfølgning af strafbare forhold, og under iagttagelse af de retssik-

kerhedsgarantier, som er indeholdt i retsplejelovens kapitel 71 og kapitel 74, herunder §§ 806 og 781, jf. § 801, stk. 3.

Den danske hjemmel i retsplejelovens § 786 er placeret i retsplejelovens kapitel 71 om indgreb i meddelelshemmeligheden mv. Det følger af § 781, at indgreb kun må finde sted, når det sker som led i efterforskning af en lovovertrædelse, som efter loven kan straffes med fængsel i seks år eller derover, en forsætlig overtrædelse af en række opregnede bestemmelser i straffeloven eller en overtrædelse af udlændingeloven.

Selvom selve udleveringen af abonnentoplysninger, der kæder personoplysninger sammen med en IP-adresse, ikke nødvendigvis er indgreb i meddelelshemmeligheden, så følger det af retsplejelovens § 801, stk. 3, at betingelserne i § 781 skal være opfyldt for udlevering af lagrede teleoplysninger.

Til støtte for Telias fortolkning af logningsreglernes anvendelsesområde taler også forarbejderne til den ændring i den dagældende telelov, som blev indført samtidig med vedtagelsen af logningsbekendtgørelsen i 2006. Der henvises til lovforslag nr. 63 af 3/11 2006, hvormed der blev fremsat forslag om indføjeelse af en bestemmelse i telelovens § 15, stk. 1, nr. 1, hvorefter:

”... det tekniske udstyr og de tekniske systemer, udbyderen anvender, er indrettet således, at politiet kan få adgang til oplysninger om teletrafik samt til at foretage indgreb i meddelelshemmeligheden i form af historisk teleoplysning og udvidet teleoplysning, jf. lov om rettens pleje kapitel 71 og 74.”

En tilsvarende forpligtelse findes i den nugældende telelov § 10.

Lovforslaget blev i 2006 blandt andet ledsaget af følgende bemærkninger:

”De i lovforslaget indeholdte ændringer af regler om udbydernes udstyr og systemer skal alene muliggøre adgang for politiet i henhold til retsplejeloven. Ændringerne vil således ikke medføre, at det bliver lettere for andre - herunder for personer, der er ansat hos eller udfører arbejde for udbyderne - at få adgang til oplysninger, som er dem uvedkommende.”

Til støtte for Telias fortolkning af anvendelsesområdet taler også EU-Domstolens dom af 21. december 2016 i sag C-203/15 og C-698/15 (Tele2/Watson). Domstolen udtalte, at logningshjernen i artikel 15 i E-databeskyttelsesdirektivet generelt skal anvendes og fortolkes med forsigtighed. Domstolen udtalte, at hjemlen til, at medlemslandene kan vedtage indskrænkninger i kommunikationshemmeligheden, ikke kan begrunde en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata.

Domstolens præmis 112 er sålydende:

”Artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.”

Domstolen udtalte videre, at national lovgivning skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af lagrede data og skal sikre, at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der

gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Præmis 109 om hjemlen i direktivets artikel 15 er sålydende:

”For at opfylde de krav, der er anført i denne doms foregående præmis, skal en sådan national lovgivning for det første fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af en sådan foranstaltning om lagring af data, og som opstiller en række mindstekrav, således at de personer, hvis data er blevet lagret, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug...”

Den danske logningsbekendtgørelse og reglerne om adgang til de loggede data er i tråd hermed afgrænset til politiets efterforskning af grove strafbare forhold med de retssikkerhedsmæssige garantier, der er gengivet ovenfor, jf. herved Retsplejelovens §§ 781 og 801.

Krænkelser af ophavsrettigheder er i intet tilfælde undergivet en straf ramme på mere end seks års fængsel. Indkærede har i øvrigt ikke anmodet om udlevering af oplysningerne til brug for en strafferetlig påtale af de påståede krænkelser. Der er derfor ikke hjemmel i dansk lovgivning til at udlevere og anvende de loggede oplysninger som ønsket af rekvirenten.

Telia er kun i besiddelse af de ønskede oplysninger til opfyldelse af en pligt til under ganske strenge betingelser at udlevere disse til brug for politiets efterforskning af grov kriminalitet. Dette faktum bør naturligvis ikke kunne udnyttes af private aktører, der som led i en præventiv kampagne mod ulovlig fildeling ønsker at rette henvendelse til teleabonnenter, fra hvis netværk en angivelig ulovlig fildeling har fundet sted.

CMS synes med henvisning til Promusicae- og Bonnier-dommene at argumentere for, at data, der er lovligt logget, lovligt kan anvendes til civilretlig forfølgelse af ophavsretlige krænkelser.

Promusicae-dommen tager stilling til medlemsstaternes ret (min understregning) til at vedtage indskrænkninger i kommunikationshæmmeligheden i overensstemmelse med artikel 15 i E-databeskyttelsesdirektivet. Det fremgår klart af præmis 55, at artikel 15 ikke indeholder nogen pligt (min understregning) for staterne til at give adgang til at anvende trafikdata til civilretlig forfølgelse. Dommen udtaler videre i præmis 57, at selvom de tre forelagte direktiver i dommen – E-handelsdirektivet, Infosoc-direktivet og Retshåndhævelsesdirektivet – alle sigter mod at sikre effektiv beskyttelse af immaterielle rettigheder, så følger det af de pågældende direktiver, at persondatabeskyttelsen går forud for beskyttelse af immaterielle rettigheder efter de samme direktiver. Bonnier-dommen udtalte på linje hermed, at det nu ophævede logningsdirektiv ikke hindrede nationale bestemmelser indført til implementering af artikel 8 i retshåndhævelsesdirektivet, som giver mulighed for at pålægge en internetudbyder at give abonnentoplysninger om bestemte IP-adresser, forudsat at den domstol, der anmodes om at give et sådant påbud, skal afveje de modstående interesser mod hinanden.

Bonnier-dommen var resultatet af en præjudiciel forelæggelse fra den svenske Højesteret. I Sverige er der til implementering af artikel 8 i retshåndhævelsesdirektivet indført en særlig hjemmel i den svenske ophavsretslovs § 60a til at kræve udlevering af de efterspurgte personoplysninger.

I Danmark er artikel 8 implementeret ved vedtagelsen af lov nr. 279 af 5. april 2006 om indførelse af kapitel 29a i retsplejeloven om oplysningspligt ved krænkelser af immaterialrettigheder mv.

Dette kapitel indeholder imidlertid kun hjemmel til at pålægge parter og tredjemænd at fremlægge beviser, oplysninger eller andet under en verserende retssag (min understregning).

Det var ifølge forarbejderne Justitsministeriets opfattelse, at der ikke som følge af retshåndhævelsesdirektivet var behov for at ændre de danske regler om tredjemandsedition, men at reglerne om partsedition ikke fuldt ud levede op til kravet i retshåndhævelsesdirektivets artikel 8.

Det må dermed lægges til grund, at den danske implementering af retshåndhævelsesdirektivet ikke giver hjemmel til informationspålæg til tredjemænd, fx internetudbydere, der går videre, end hvad der allerede er hjemlet i retsplejelovens § 343, og at hverken artikel 8 i retshåndhævelsesdirektivet eller artikel 15 i e-databeskyttelsesdirektivet pålægger Danmark at indføre regler svarende til fx de svenske regler.

Nærmere om retsplejelovens regler om isoleret bevisoptagelse og edition

For det tilfælde, at Østre Landsret ikke måtte finde, at logningsbekendtgørelsen og hjemmelsgrundlaget udelukker pålæg om udlevering af de efterspurgte abonnentoplysninger i den foreliggende sag, gøres det gældende, at retsplejelovens almindelige betingelser for isoleret bevisoptagelse og edition i den civile retspleje ikke er opfyldt.

Isoleret bevisoptagelse

Retsplejelovens § 343, stk. 1, er sålydende:

”Retten kan tillade, at der optages bevis, selv om dette ikke sker til brug for en verserende retssag. Anmodning om bevisførelse indgives til retten på det sted, hvor vidnet bor eller opholder sig, eller for så vidt angår syn og skøn til retten på det sted, hvor genstanden for forretningen findes. Anmodning om optagelse af bevis i udlandet indgives til retten på det sted, hvor sagen eventuelt skal anlægges her i landet.”

Bestemmelsen i § 343 har en nær sammenhæng med § 340, hvorefter der:

”Når omstændighederne taler derfor, kan retten dog bestemme, at bevisførelsen eller en del af denne skal ske inden hovedforhandlingen.”

Det er altså en forudsætning for anvendelsen af § 343, at bevisoptagelsen sker med henblik på tilvejebringelse af bevis til en retssag.

Denne fortolkning støttes af forarbejderne til bestemmelsen, hvoraf fremgår:

”Isoleret bevisoptagelse forudsætter således, at parterne eller en af dem har en særlig interesse i, at bevisoptagelsen finder sted, inden retssag anlægges, og dette må sandsynliggøres over for retten, inden denne kan give tilladelse til bevisoptagelse.” (min understregning)

Rekvirenten skal derfor sandsynliggøre, at den isolerede bevisoptagelse sker til brug for en efterfølgende retssag.

Det fremgår videre:

”En bevisoptagelse, som alene skal tjene til vejledning for, om sag overhovedet skal anlægges, kan heller ikke tillades, men derimod efter omstændighederne

nok, hvis bevisoptagelsen er nødvendig for, at »parten« kan finde ud af, hvem han skal sagsøge.”

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.

Telia gør gældende, at oplysningerne ikke er begæret udleveret med henblik på anlæg af retssag. Telia har i alle processkrifter både for byretten og for Landsretten opfordret CMS til at dokumentere, at der er anlagt retssager mod nogen af de abonnenter, om hvem der er udleveret personoplysninger i kraft af tidligere editionspålæg over for Telia eller over for andre teleselskaber. Der henvises til svarskrift af 20. juni 2017, punkt 13, samordnet svarskrift af 19. juli 2017, punkt 38, duplik af 14. august, punkt 17, kæreskrift af 6. november 2017, punkt 62, kære-replik af 28. december 2017, punkt 8, samt Telias processkrift af 18. januar 2018.

Indtil indkæredes processkrift II for Landsretten af den 4. marts 2018 har der ikke foreligget oplysninger om mere end en enkelt retssag, som blev afgjort ved Retten i Glostrup den 13. oktober 2016, jf. bilag 23, med afsigelse af udeblivelsesdom.

At der ikke tidligere har været anlagt andre sager, ligger i tråd med direktør Anders Kjærhauges forklaring i byretten. Det fremgik heraf, at CMS og de retlighedshavere, som CMS repræsenterer generelt, ikke har intention om at indlede retssag, hvis ikke de opkrævede bøder bliver betalt. Anders Kjærhauge sammenlignede bødekravet i brevene med en P-bøde.

Der henvises endvidere til bilag R, print fra Producentforeningens hjemmeside, som indeholder et opslag fra den 12. oktober 2016.

Her præsenteres en abonnementsordning, som Producentforeningen har etableret sammen med advokatfirmaet Njord, som også repræsenterer indkærede Copyright Management Services Ltd. i denne sag. Ordningen giver medlemmerne mulighed for at få sendt individuelle breve til danske brugere, fra hvis IP-adresse der kan konstateres ulovlig download/fildeling. Brevene vil ifølge opslaget indeholde et tilbud om, at sagen kan afsluttes mod betaling af kr. 1.500 til fuld og endelig afslutning af sagen.

Det fremgår, at Njord vil foretage løbende rapportering og årlig afregning til medlemmerne af indbetalte forligsbeløb fra brevmodtagere fratrukket alle omkostninger til administration af ordningen, og at man på baggrund af tidligere erfaringer forventer, at tilmeldte medlemmer vil modtage positiv afregning fra Njord.

Det er ikke beskrevet, hvad der skal ske med de abonnenter, som ikke foretager indbetaling af det tilbudte forligsbeløb, endsige omtalt muligheden for at føre retssager mod de brevmodtagere, som modsætter sig det fremsatte godtgørelseskrav eller i hvert fald undlader at betale.

Anders Kjærhauge forklarede i byretten, at 60 % af de abonnenter, der har modtaget breve fra CMS om påstået fildeling, reagerer på brevene. Heraf må udledes, at 40 % af modtagerne ikke har reageret, endsige betalt den opkrævede kompensation/bøde. Når henses til, at der på tidspunktet for Frederiksberg Rets kendelse var udleveret oplysninger om mere end 100.000 IP-adresser, jf. Jakob Willers forklaring, svarer det altså til, at ca. 40.000 brevmodtagere ikke har reageret på de fremsendte breve.

Indkærede har nu med processkrift II til meget begrænset opfyldelse af Telias gentagne opfordringer fremlagt oplysninger om nogle få anlagte retssager. Oplysningerne i bilag 53 er meget ufuldstændige, men det lader sig dog udlede, at der er anlagt i alt 19 retssager mod teleselskabsabonnenter. Trods Telias opfordring er det ikke oplyst, hvornår sagerne er anlagt. De fleste af sagerne er tilsyneladende anlagt i november og december 2017, og afgørelserne hhv. retsforligene er dateret i januar, februar og marts 2018.

Det fremgår desuden, at alle de sager, der er dokumenteret anlagt med undtagelse af en enkelt, er anlagt efter at Retten på Frederiksberg afsagde kendelse i nærværende sag den 29. oktober 2017. Sagsanlæg, der har fundet sted, efter at den afgørelse som Landsretten skal tage stilling til, er truffet, kan naturligvis ikke tillægges betydning ved Landsrettens afgørelse af sagen.

Den meget begrænsede opfyldelse af provokationerne betyder, at Landsretten må lægge til grund, at mindre end én promise af de abonnenter, der ikke har reageret på trusselsbrevene, efterfølgende er blevet sagsøgt af CMS. Telia er opmærksom på, at ikke alle abonnent-oplysninger er udleveret til CMS eller til CMS's advokat, og at andelen af sagsanlæg i forhold til det samlede antal udsendte breve kan være lidt højere. Det ændrer dog ikke det generelle indtryk. Den usikkerhed, der fortsat råder trods Telia og Telenors gentagne provokationer til CMS om at oplyse, i) hvor mange breve der er sendt ud, ii) brevenes nærmere indhold, iii) modtagernes reaktioner og iiiii) antallet af anlagte retssager, må udelukkende komme CMS til skade. CMS har både interesse i og mulighed for at opfylde provokationerne i langt højere grad, end det er sket. Landsretten må derfor lægge til grund, at det kun er én promise eller mindre af de mange abonnentoplysninger, der er udleveret, der har ført til sagsanlæg. Det må følgelig forsat lægges til grund, at CMS generelt ikke ønsker abonnentoplysninger udleveret for at anlægge og føre retssager om abonnenternes mulige hæftelse for ophavsretskrænkelser, men at oplysningerne i langt overvejende grad bruges til at udsende bødebrev, som ikke følges op med sagsanlæg, hvis modtagerne ikke betaler den opkrævede erstatning. Der er derfor heller ikke tale om, at CMS udsender brevene for at afsøge muligheden for forlig forud for sagsanlæg, som foreskrevet i retsplejelovens § 336.

Allerede af denne grund skal anmodningen om bevisoptagelse afvises.

Dertil kommer, at CMS ikke opnår tilstrækkeligt bevis for sit krav med den foreliggende anmodning om isoleret bevisoptagelse.

Ved Østre Landsrets dom af 5. september 2008 i sag B-19-08 (utrykt) afviste Landsretten, at en sammenstilling af en IP-adresse og kundedata udgjorde et nødvendigt bevis for en immaterialretlig krænkelse. Det kan derfor ikke forventes, at CMS ved bevisoptagelsen opnår det nødvendige bevis for sit eventuelle krav. Dette er formentlig baggrunden for, at CMS hidtil har været meget tilbageholdende med at anlægge sager mod abonnenter, der ikke umiddelbart har anerkendt de fremsatte bødekrav. Man har ikke udsigt til at få medhold i en påstand om krænkelse.

Editionspålæg

Det gøres endvidere gældende, at betingelserne i retsplejelovens regler om edition ikke er opfyldt.

Retsplejelovens § 299, stk. 1, er sålydende:

”Retten kan efter begæring af en part pålægge tredjemand at forevise eller udlevere dokumenter, der er undergivet hans rådighed, og som har betydning for

sagen, medmindre der derved vil fremkomme oplysning om forhold, som han ville være udelukket fra eller fritaget for at afgive forklaring om som vidne, jf. §§ 169-172.”

CMS har ikke sandsynliggjort, at materialet har betydning for de kendsgerninger, der skal bevises, jf. hertil retsplejelovens § 341.

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.

Dertil kommer, at den administrative byrde for Telia med at identificere kunderne ikke står i rimeligt forhold til betydningen af, at bevismidlet kommer frem, jf. princippet i retsplejelovens § 171, stk. 2, nr. 3. Bemærk her, at kun 60 % af de breve, der udsendes, medfører en reaktion fra modtagerne, og at det er uoplyst, i hvor mange tilfælde udsendelsen af breve fører til betaling af de opkrævede bøder.

Nærmere om proportionalitetsafvejningen mellem immaterialretten og persondataretten

Telia gør gældende, at hensynet til håndhævelsen af immaterielle rettigheder efter omstændighederne og i den konkrete situation må vige for beskyttelsen af persondata og af privatliv i mere overordnet betydning.

Telia er som udbyder af telekommunikationstjenester underlagt persondataretens regler om behandling af persondata og skal sikre, at der sker en forsvarlig behandling af kundedata.

Det vil efter Telias opfattelse udgøre en tilsidesættelse af persondataretten, hvis bevisoptagelsen fremmes.

Hjemlen til afvejning

Som omtalt ovenfor under punkt 26-28 udtalte EU-Domstolen i Promusicaedommen, præmis 54, at E-databeskyttelsesdirektivet ikke indeholder et egentligt forbud mod, at medlemsstater pålægger en teleudbyder at fremlægge kundedata til brug for civile retssager. Domstolen udtalte videre i præmis 57, at selvom de tre forelagte direktiver alle har til formål at sikre beskyttelse af intellektuelle ejendomsrettigheder, herunder ophavsret, så følger det af direktiverne, at de ikke går forud for bestemmelser om blandt andet beskyttelse af personoplysninger.

Det følger videre af præmis 70, at de nationale myndigheder og domstole ved anvendelse af de tre direktiver til sikring af ejendomsret til intellektuelle rettigheder skal sikre, at de grundlæggende rettigheder (herunder ejendomsret, ret til personlige data og privatlivets fred) og proportionalitetsprincippet respekteres.

Der henvises desuden i præmis 69 til, at artikel 15 i E-databeskyttelsesdirektivet udtrykkelig henviser til EU-traktatens artikel 6, stk. 1 og 2, om EU-Chartret og den europæiske menneskerettighedskonvention. Dette understreger, at der ved anvendelse af logningshjemlen og de loggede data skal ske afvejning af de immaterialretlige interesser over for persondataretten, og at der skal lægges særlig vægt på den grundlæggende respekt for personoplysninger og privatlivets fred.

Tilsvarende udtales det i Bonnier-dommen, præmis 56, at de nationale myndigheder og domstole skal sikre, at der lægges en fortolkning til grund, der både respekterer de grundlæggende rettigheder og proportionalitetsprincippet.

Disproportionalitet mellem krænkelse og de efterspurgte persondata

Ved afvejningen af de hensyn, som immaterialretten varetager over for hensynet til persondatasikkerheden, bør der ske inddragelse af den disproportionalitet, der består mellem den bagatelagtige karakter af hver enkelt ophavsretskrænkelser og fraværet af retslige skridt på den ene side, over for antallet af kunder, der må tåle at få delt deres personfølsomme oplysninger, på den anden side.

De påståede krænkelse skal vurderes enkeltvis over for udleveringen af den enkelte internetabonnents oplysninger. Rekvirenten har ikke i tilstrækkelig grad dokumenteret omfanget eller grovheden af krænkelse.

Det fastholdes, at hver enkelt af de ophavsretskrænkelser, som hævdes at være foretaget fra en given abonnents internet, har en bagatelagtig karakter. Dette afspejles i den trods alt beskedne compensation, som kræves i rekvirentens breve, jf. bilag B i størrelsesordenen kr. 2.100 og de med bilag 53 fremlagte retsbogsudskrifter, hvoraf det fremgår, at der i de fleste tilfælde er krævet kr. 5.000 i erstatning.

Det blev også bekræftet af Anders Kjærhauge, der nok udtalte, at han var provokeret over, at man omtalte ulovlig fildeling som bagatelagtig, men som samtidig anførte, at den enkelte krænker ikke er en hårdet kriminel, og at de kan sammenlignes med dem, der får en P-bøde.

Til støtte for Telias synspunkt om, at de påståede krænkelse i afvejningen med persondataretten må anses for mindre betydende, taler også baggrunden for Retshåndhævelsesdirektivet. Det følger således af betragtning 14, at direktivet, der blandt andet er baggrund for indførelsen af Retsplejelovens kap 29a, primært er vedtaget for at give bedre redskaber til bekæmpelse af immaterialretskrænkelser af kommercielt tilsnit. CMS har ikke sandsynliggjort, endsi dokumenteret, at de krænkelse, som påstås at have fundet sted, jf. bilag 44 og 45, har et sådant kommercielt tilsnit. Selvom listerne i bilag 44 og 45 samlet viser mange tilfælde af fildeling, så skal proportionalitetsafvejningen forsat ske abonnent for abonnent. I den afvejning må hensynet til den enkelte persons krav på beskyttelse af sine data vejer tungere end en ganske beskedne ophavsretlig krænkelse som angivet i bilag 44 og 45.

CMS har i et supplerende processkrift II i kæresagen anvendt en norsk byretsdømme til at argumentere for, at de krænkelse, der er vist i bilag 44 og 45 har en karakter og et omfang, der kan begrunde, at beskyttelse af de efterspurgte personoplysninger skal vige for beskyttelse af den ophavsret, der angiveligt var krænkelse. Det følger af dommen, at den norske lovgivning indeholder et krav om, at der skal foreligge en krænkelse af "et visst omfang", for at der kan ske udlevering af personoplysninger. Den norske domstol har fundet, at der i den forelagte sag var dokumenteret krænkelse af "et visst omfang".

Hertil bemærkes, at en norsk domstols vurdering på baggrund af norske lovforarbejder af, om et kriterie indeholdt i en norsk lov, som ikke er baseret på et EU-direktiv, er overholdt, naturligvis ikke er anvendeligt, endsi bindende for en dansk domstol.

Ikke bevist sammenfald mellem krænker og indehaver af persondata

I proportionalitetsafvejningen skal også indgå, at rekvirenten ikke har sandsynliggjort, at de påståede krænkelse er foretaget af den, der har tegnet internetabonnementet hos Telia, og om hvilke der ønskes oplysninger. Flere domme, blandt andet U.2009.280V, har bekræftet, at det er rettighedshaveren, der har bevisbyrden for, hvem der har foretaget en given krænkelse. Der er ikke hjem-

mel til nogen form for objektivt ansvar eller ansvar med omvendt bevisbyrde for krænkelse, der foregår via en given internetforbindelse.

Risiko for særligt personfølsomme oplysninger

Det fremgår af de lister, der er fremlagt som bilag 45, at titlerne på de film, der hævdes delt ulovligt, i en række tilfælde indikerer, at der er tale om pornofilm. Det kan ikke udelukkes, at andre titler dækker over film med et særligt religiøst eller politisk budskab. Allerede oplysningen til rettighedshaveren om, at en given person er indehaver af en netforbindelse, hvorfra der er delt film med et sådant indhold, indebærer behandling af særligt følsomme personoplysninger, jf. persondatalovens § 7, med de særlige krav til behandlingen, der følger heraf. Hertil kommer, at et efterfølgende brev til abonnenten med oplysning om, at en person med eller uden samtykke har anvendt abonnentens internetforbindelse til at fildele film med et sådant følsomt indhold, kan indebære krænkelse af denne persons personfølsomme oplysninger.

Lovgivers holdning

Endelig bør det indgå i afvejningen, at lovgiver i årene 2008 til 2012 forhandlede med en række interesseorganisationer om mulige tiltag mod digitale krænkelse af ophavsrettigheder på internettet. Der henvises til bilag 18, Kulturministeriets rapport fra 2011. Man drøftede blandt andet at indføre lovhjælp til en brevmodel, der havde visse træk til fælles med de bødebrev, som rekvirenten udsender. I 2012 blev modellen endeligt opgivet politisk.

Fra politisk hold har man altså overvejet og forkastet en såkaldt brevmodel. Dette bør indgå i proportionalitetsafvejningen til skade for rettighedshaverne. På denne baggrund og under hensyn til karakteren af CMS' forretningsmodel gør Telia gældende, at hensynet til persondataretten og retten til privatlivets fred må veje tungere end hensynet til immaterialretten, og at begæringen om udlevering af oplysninger derfor må nægtes fremme.

Særlige bemærkninger til CMS' processkrift II

CMS opregner i processkriftet på ny en række punkter, som parterne under sagen skulle være enige om.

Til punkt 1 og 2 bemærkes på ny, at Telia kun kan tiltræde, at der har fundet fildeling sted, uden at der heri ligger nogen mere principiel anerkendelse af bevisværdien af listerne baseret på Maverick Monitor-værktøjet.

Til punkt 3 bemærkes, at Telia kun er i besiddelse af oplysningerne, når IP-adresserne er tildelt et bredbåndsabonnement. Abonnenterne bag IP-adresser tildelt via mobilnetværket kan ikke oplyses.

Til punkt 6 bemærkes, at Telia ikke har oplyst, at man opbevarer koblingen mellem IP-adresse og abonnent i mindst tre uger, men at man ikke har brug for oplysningerne i mere end tre uger.

Til afsnit 2.2 om omfanget af fildelingen, bemærkes, at CMS må bære risikoen for, at krænkelse har et påstået større omfang, end hvad der fremgår af listerne. Dette har betydning ved den proportionalitetsafvejning, som skal foretages.

Det bestrides, at der skulle være særlige holdepunkter for at antage, at en person, som ifølge listerne har anvendt en given IP-adresse til deling af en mindre del af en film, har set og delt hele filmen. Der er formentlig mange situationer, hvor der kun deles/downloades en lille del af en film, hvorefter personen fortryder enten på grund af manglende interesse eller af frygt for at foretage sig noget ulovligt.

Endelig bestrides det, som anført på side 8, at der eksisterer en mangeårig praksis for at give editionsoplæg i sager som den forelagte. Retten på Frederiksberg udtalte i den påkærede afgørelse, at teleudbydere efter dansk retspraksis var blevet pålagt at udlevere abonnentoplysninger. Baggrunden herfor er dog primært, at de danske teleselskaber tidligere ikke udtalte sig imod at udlevere de efterspurgte oplysninger.

I takt med det meget store antal personoplysninger, der er udleveret de seneste år, sammenholdt med EU-Domstolens kritiske holdning til logning af teletrafik-data (Tele2/Watson-dommen mv.), og i erkendelse af, at de udleverede abonnentoplysninger stort set ikke har ført til sagsanlæg, men kun til udsendelse af bødebreve, har teleselskaberne dog nu ønsket at få en mere principiel prøvelse af, om man er forpligtet til at efterkomme ønsket om udlevering af persondata som begæret i denne sag. Det bemærkes herved, at også andre teleselskaber ud over Telia og Telenor har udtrykt ønske om en afklaring. Der henvises til bilag S og T, erklæringer fra TDC A/S og Stofa A/S.”

CMS har i processkrift af 28. marts 2018 bl.a. anført følgende:

”2. *Parternes tilskæring af sagen*

CMS gør gældende, at følgende forhold kan lægges til grund ved behandlingen ved Østre Landsret:

- 2.1. Registreringer foretaget via MaverikMonitor er tilstrækkeligt bevis for, at fildeling kan knyttes til bestemte IP-adresser på bestemte angivne tidspunkter. De fremlagte registreringer viser, at en andel af en fil var tilgængelig på en IP-adresse på et givent tidspunkt.
- 2.2. Der har på de anførte tidspunkter fundet én eller flere krænkelse af CMS’ ophavsret sted, som kan relateres til de anførte IP-adresser.
- 2.3. Telenor og Telia er i besiddelse af navne og adresser på abonnenterne til de anførte IP-adresser.
- 2.4. De anmodede navne og adresser knyttet til de anførte IP-adresser kan ikke tilvejebringes CMS på anden måde eller fra andre end Telenor og Telia.
- 2.5. CMS kan først efter sikring og udlevering af navne og adresser fra Telenor og Telia konstatere, om krænkelsen af ophavsretten på den enkelte IP-adresse omfatter flere værker, konstatere længden af den periode krænkelsen eller krænkelse er foregået i, og om der er gentagne forhold også for abonnenter, fra hvis IP-adresse CMS tidligere har konstateret ophavsretlige krænkelse.
- 2.6. Telenor og Telia opbevarer navne og adresser på abonnenter i ét år pga. forpligtelse i logningsbekendtgørelsen, men også i en periode til internt brug og abonnementsbehandling (Telia efter det oplyste i mindst 3 uger og Telenor efter det oplyste i 30 dage).

...

3.1. *Kan persondata, der er logget i medfør af retsplejelovens § 786 og den udstedte logningsbekendtgørelse, lovligt udleveres og anvendes til civilretlig retsforfølgning af ophavs- retskrænkelser?*

CMS gør gældende:

E-databeskyttelsesdirektivets art. 6 – trafikdata

at parterne er enige om, at de data, som anmodes udleveret, lagres af Telenor og Telia med hjemmel i e-databeskyttelsesdirektivets art. 6 om trafikdata for en periode med henblik på debitering af abonnenten og afregning for samtrafik, og at en sådan behandling er tilladt indtil udløbet af den lovbe-

stemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger,

- at Telenor og Telia med hjemmel i e-databeskyttelsesdirektivets art. 6, med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af tillægs-tjenester, må behandle oplysningerne i det omfang og tidsrum, som sådanne tjenester eller markedsføring kræver, hvis den abonnent eller bruger, som oplysningerne vedrører, har givet sit samtykke hertil,
- at debitering og markedsføring er begrundet i civilretlige formål helt på linje med civilretlig håndhævelse af ophavsrettigheder, hvorfor CMS' adgang til data og muligheder for håndhævelse ikke bør være ringere end teleudbydernes muligheder for debitering og markedsføring,

Logningsbekendtgørelsen

- at parterne er enige om, at strafferetsplejens bestemmelser i retsplejelovens kapitel 71 og den i medfør af retsplejelovens § 786, stk. 4, udstedte logningsbekendtgørelse vedrører straffeplejen og de aktører, der agerer inden for straffeplejen,
- at parterne er enige om, at nærværende sag vedrører den civilretlige del af retsplejeloven, herunder retsplejelovens bestemmelser om edition efter retsplejelovens §§ 299 og 343,
- at udbydere af elektroniske kommunikationsnet eller -tjenester (Telenor og Telia) ifølge logningsbekendtgørelsen skal registrere en større mængde oplysninger opregnet i bekendtgørelsens §§ 4-6, herunder som en mindre del koblingen mellem IP-adresser og abonnenter, der skal opbevares i 1 år, jf. bekendtgørelsens § 9,
- at der ikke af bekendtgørelsens ordlyd, vejledning eller efter retspraksis kan sluttes, at oplysningerne ikke kan anvendes til efterforskning og retsforfølgning af civile forhold eller alene kan udleveres til forfølgning af strafbare forhold,
- at der ikke i retsplejelovens regler for strafferetspleje er bestemmelser, der i deres ordlyd eller forarbejder udelukker udlevering af navne og adresser på abonnenter i civile sager,
- at danske domstole civilretligt i mere end 10 år har behandlet lignende begæringer, og at rettighedshavere i alle sager har fået medhold i udleveringen af beviserne, så længe de anmodede beviser har været til stede hos rekvisitus,
- at det danske teleselskab, TDC, i januar 2012 bekræftede ovennævnte praksis ved at meddele at ville efterkomme begæringer om edition uden indsigelse, jf. efterfølgende kendelse fra retten på Frederiksberg 14. maj 2012,

EU-retten

- at artikel 8 i retshåndhævelsesdirektivet er implementeret i retsplejelovens kap. 29 a vedrørende oplysningspligt ved krænkelse af immaterialrettigheder og i de almindelige regler om edition i retsplejelovens §§ 343 og 299,
- at en anmodning om isoleret bevisoptagelse henhører under anvendelsesområdet for retshåndhævelsesdirektivet, jf. Bonnier-sagens præmis 54,
- at e-databeskyttelsesdirektivet ikke udelukker, at de begærede oplysninger kan udleveres til brug for beskyttelsen af andres rettigheder og frihedsrettigheder, herunder rettighedshaveres håndhævelse af deres ophavsrettigheder, jf. bl.a. Tele2/Watson-sagens præmis 115 og 90 med henvisning til Promusicae-sagens præmis 53,
- at hverken e-databeskyttelsesdirektivet eller logningsdirektivet udelukker nationale bestemmelser, som er implementeret i medfør af artikel 8 i retshånd-

- dhævelsesdirektivet, og som fastsætter en forpligtelse til overførsel af personoplysninger til privatpersoner med henblik på at retsforfølge krænkelse af ophavsretten ved civile domstole, jf. Bonnier-sagens præmis 55 og 61,
- at EU-Domstolen i Digital Rights sagen fandt, at logningsdirektivet ikke overholdt proportionalitetsprincippet og derfor var ugyldigt,
- at parterne er enige om, at Østre Landsret i denne sag ikke skal tage stilling til, hvorvidt de danske logningsregler er i overensstemmelse med EU-retten, og at der pågår politisk arbejde i Danmark med reglerne,
- at EU-Domstolen i Tele2/Watson-sagen fortolkede de rammer, der blev sat i Digital Rights sagen for bl.a. de svenske regler,
- at EU-Domstolen i Tele2/Watson-sagen ikke udelukkede udlevering af de begærede oplysninger til brug for retsforfølgelse af ophavsretlige krænkelse ved civile domstole,
- at der i Sverige er fremsat lovforslag om nye logningsregler med ikrafttrædelse i 2018, hvorefter der fortsat i Sverige skal registreres IP-adresser og abonnenterne tilknyttet disse, og at opbevaringen af nævnte oplysninger i Sverige er blevet foreslået fastsat til 10 måneder,
- at EU-retten ikke er til hinder for Telenor og Telias udlevering af data til brug for CMS' håndhævelse af deres ophavsrettigheder, og at Østre Landsret derfor i lighed med retten på Frederiksberg kan pålægge Telenor og Telia at udlevere de begærede oplysninger, såfremt retten finder det hensigtsmæssigt og proportionelt,

Norsk og finsk højesteretspraksis

- at den norske Høyesterett ikke har besluttet, at logningsdata ikke kan udleveres til forfølgelse af civile krav,
- at Oslo tingrett i afgørelsen fra januar 2018 har fortolket afgørelsen fra den norske Høyesterett derhen, at den i sagen indgivne anmodning om udlevering af oplysninger om abonnenter, baseret på samme bevismateriale som i nærværende sag, må tages til følge, og at de anmodede oplysninger herefter skal udleveres,
- at den finske Højesteret alene har udtalt sig om de finske logningsregler, der i Finland er implementeret forskelligt fra i Danmark og derfor leder til forskellige resultater,
- at den finske og danske lovgivning er grundlæggende forskellige, idet der i den finske Information Society Code er klare bestemmelser for at gemme og udlevere data til private virksomheder og/eller myndigheders brug,
- at hjemlen til udlevering i Finland findes i den finske ophavsretslovs artikel 60 a, der refererer til den finske Information Society Code, herunder artiklerne 137, 157 og 322, hvorefter den finske Højesteret alene præciserede, at de i sagen begærede informationer alene kan udleveres efter artikel 137 i den finske Information Society Code, der giver en hjemmel til at gemme for og udlevere til private virksomheder,
- at den finske Højesteret alene har præciseret, at det udtrykkeligt fremgår af artikel 157 i den finske Information Society Code, at oplysninger udelukkende må bruges til brug for efterforskning af kriminalitet,
- at hjemlen i retsplejelovens § 299, jf. § 343, ikke er begrænset på samme måde som reglerne i den finske Information Society Code, og at en sammenligning af de straffeprocessretlige regler i retsplejeloven med de finske regler efter Information Society Code Artikel 157, for derefter at udelukke udlevering af data gemt i medfør af de danske logningsregler, er forkert,

at en sådan sammenligning og en begrænsning til, at udleveringen alene skulle omfatte oplysninger, som teleselskaberne gemmer til eget brug, gør udleveringen af data vilkårlig eftersom teleselskaber kan have forskellig politik, måder at håndtere på m.v., hvilket ikke vil være proportionelt med CMS muligheder for at undersøge ophavsretskrænkelser samt de samfundsmæssige hensyn i at sikre både ophavsretten og retsfølelsen,

3.2. Er retsplejelovens betingelser for isoleret bevisoptagelse og editionspålæg, jf. retsplejelovens §§ 299 og 343, opfyldt?

CMS gør gældende:

Krav efter retsplejeloven

at Der i retsplejeloven findes flere regler om sikring og udlevering af beviser i forbindelse med immaterielle krænkelser, og at der med hjemmel i retsplejelovens § 343, stk. 1, med rettens tilladelse kan optages bevis, selv om dette ikke sker til brug for en verserende retssag, og at retten med hjemmel i retsplejelovens § 299, stk. 1, kan pålægge Telenor og Telia at udlevere dette bevis,

at beviset, som er omfattet af begæringen, er begrænset til navne og adresser på abonnenter, som har fået tildelt IP-adresserne på de tidspunkter, som er angivet i de omhandlede lister, og at de ønskede oplysninger er undergivet Telenor og Telias rådighed, jf. retsplejelovens §§ 299, stk. 1, og 300, stk. 1, at retsplejelovens § 340, stk. 2, om underretning af Telenor og Telia om bevisførelse inden hovedforhandlingen med en uges varsel, er iagttaget,

Retshåndhævelsesdirektivet

at retsplejelovens regler om edition i civile sager skal fortolkes i lyset af retshåndhævelsesdirektivet,

at følgende fremgår af retshåndhævelsesdirektivets præambel (21): ”Da beviser er af altafgørende betydning for at fastslå en krænkelse af intellektuelle ejendomsrettigheder, bør det sikres, at der reelt er mulighed for at optage, fremlægge og sikre beviser. Procedurene bør tage hensyn til forsvarets rettigheder og sikre de nødvendige garantier, herunder beskyttelse af fortrolige oplysninger. Hvad angår krænkelser i kommerciel målestok er det også vigtigt, at domstolene i givet fald kan kræve finansielle og kommercielle dokumenter, herunder bankdokumenter, som er under den formodede krænkende parts kontrol, fremlagt.”,

at følgende fremgår af retshåndhævelsesdirektivets præambel (23): ”Rettighedshaverne bør, uden at dette berører andre tilgængelige foranstaltninger, procedurer eller retsmidler, have mulighed for at anmode om, at der udstedes påbud over for mellemmand, hvis tjenesteydelser anvendes af tredje mand til at krænke rettighedshaverens industrielle ejendomsret. Betingelser og procedurer for sådanne påbud bør fastsættes i medlemsstaternes nationale lovgivning. For så vidt angår krænkelser af ophavsret og beslægtede rettigheder er der allerede i direktiv 2001/29/EF indført en udstrakt grad af harmonisering. Artikel 8, stk. 3, i direktiv 2001/29/EF bør derfor ikke berøres af dette direktiv.”,

at det følger af retshåndhævelsesdirektivets artikel 3, at medlemsstaterne skal fastsætte foranstaltninger og retsmidler, der er nødvendige for at sikre håndhævelsen af intellektuelle ejendomsrettigheder, og at foranstaltningerne og retsmidlerne ligeledes skal være effektive, stå i et rimeligt forhold til krænkelsen og have afskrækkende virkning,

- at det følger af retshåndhævelsesdirektivets artikel 6, at medlemsstaterne skal sikre, at de kompetente retslige myndigheder, på begæring af en part der har fremført et rimeligt tilgængeligt bevismateriale, der er tilstrækkeligt til at understøtte hans påstande, og som til støtte for sine påstande har angivet bevismateriale, som modparten har kontrol over, kan pålægge modparten at fremlægge det pågældende bevismateriale, under forudsætning af at fortrolige oplysninger beskyttes,
- at parterne er enige om, at både de persondatarelige regler og retsplejelovens regler indeholder et ”skøn”, hvorefter der kan optages bevis, når retten finder det hensigtsmæssigt, og at udlevering af persondata kan ske, hvis retten finder det proportionelt,

Krav om anlæggelse af retssager og bevisernes egnethed

- at Telenor og Telia anerkender, at et udtrykkeligt krav om efterfølgende anlæggelse af retssag ikke fremgår af editionsreglerne,
- at der ikke kan udledes et krav af bestemmelserne i retsplejelovens § 343, stk. 1, og § 299, stk. 1, om at CMS efterfølgende skal anlægge retssag, hverken af bestemmelsernes ordlyd, forarbejder eller retspraksis,
- at retsplejeloven har været revideret mange gange siden tilblivelsen af retsplejelovens §§ 299 og 343, og at såfremt lovgiver ønskede et krav om anlæggelse af retssag, ligesom efter eksempelvis reglerne i retsplejelovens kapitel 57 a, herunder § 653 c, kunne lovgiver have benyttet de mange revisioner til at præcisere dette,
- at CMS’ udenretlige forligsbestræbelser er i overensstemmelse med forpligtelsen i retsplejelovens krav om undersøgelser af muligheden for forlig forud for sagsanlæg, og at tilsidesættelse af denne pligt kan få konsekvenser for CMS, jf. retsplejelovens §§ 336 a og 318, stk. 2,
- at som følge af CMS’ bestræbelser på at opnå udenretlige forligsløsninger er der i de fleste sager ikke behov for anlæggelse af en retssag,
- at CMS’ udenretlige forligsbestræbelser er i overensstemmelse med udviklingen i retsplejeloven, ligesom både Datatilsynets, Advokatnævnets og Forbrugerombudsmandens undersøgelser, behandling og konklusioner om ”brevmodellen” ikke har fundet anledning til kritik,
- at culpaansvaret i forbindelse med ophavsretskrænkelser og en abonnents IP-adresse er både belyst og prøvet for landsretterne og Højesteret, og at CMS, henset til den teknologiske udvikling, herunder brugen af Internettet, er opmærksom på nye typer af ophavsretskrænkelser og nye former for beviser, og derfor løbende indleder prøvesager for domstolene for fortsat at belyse culpaansvaret,
- at CMS allerede under forberedelsen af sagen for retten på Frederiksberg oplyste, at beviserne efterfølgende bliver anvendt i retssager, og at CMS i forbindelse med forberedelsen til sagens behandling i Østre Landsret har oplyst og dokumenteret kendskab til, at der har været anlagt over 75 individuelle retssager i 2017 og 2018 i Danmark mod abonnenter efter udlevering af navne og adresser fra teleselskaber på baggrund af editionskendelser,
- at navn og adresse på en abonnent ikke i sig selv altid identificerer rette sagsøgte for ophavsretskrænkelserne, men at abonnenten er nøglen til de yderligere undersøgelser, som CMS efterfølgende foretager, herunder ved kontakt til abonnenten med spørgsmål og efterfølgende kommunikation med abonnenten eller tredjemand,
- at undersøgelserne, som CMS foretager i forlængelse af teleselskabernes udlevering af oplysninger om abonnenter, hvis IP-adresser er blevet benyttet til

- ulovlig fildeling, leder til forskellige udfald afhængigt af undersøgelsesresultater og kommunikationen med abonnenten og/eller tredjemand, som illustreret i de for Østre Landsret fremlagte retsforlig,
- at det først er på tidspunktet for udlevering af navne og adresser, at CMS kan fastslå om a) der er tale om den samme abonnent med forskellige IP-adresser (dynamiske IP-adresser), b) om den enkelte abonnent har foretaget flere krænkelse af samme eller flere værker, c) om abonnenten tidligere har foretaget krænkelse af de rettigheder, som CMS bistår med at håndhæve, d) om abonnenten er en juridisk person, og e) om IP-adressen er knyttet til en VPN-tjeneste, så navn og adresse ikke lader sig identificere,
- at Producentforeningens medlemstilbud ikke kan tages som udtryk for, at der ikke anlægges retssager mod abonnenter, hvilket også fremgår af forklaringerne fra Producentforeningen og Zentropa for retten på Frederiksberg, der begge bakker op om retssager, der belyser culpaansvaret i forbindelse med ophavsretskrænkelser tilknyttet IP-adresser,
- at Telenor tidligere har anført, at CMS grundlæggende ikke anvender udleverede oplysningerne til at retsforfølge krænkelse, men alene til at udsende ”trusselsbreve”, ligesom vidnet Jakob Willer fra Teleindustrien forklarede, at ”det er usympatisk at sende skræmmebreve ud. Truslen er ikke reel”,
- at ”truslen” om retssag skal ses i lyset af de mere end 75 retssager i 2017-2018,
- at det er dokumenteret, at de udleverede oplysninger både kan og faktisk bruges til retsforfølgelse af ophavsretlige krænkelse, og at eksemplerne på domme og retsforlig illustrerer, at de udleverede oplysninger er egnede til den videre retsforfølgelse af ophavsretslige krænkelse.

3.3.Hvordan skal den proportionalitetsafvejning, der skal ske mellem hensynet til håndhævelsen af immaterielle rettigheder og hensynet til beskyttelsen af persondata, falde ud?

CMS gør gældende:

Almindelige og personfølsomme oplysninger

- at der er tale om ikke-personfølsomme oplysninger, idet det udelukkende er abonnenters navne og adresser, der begæres udleveret,
- at erhvervsabonnenter (juridiske personer), som også er omfattet af anmodningerne, ikke er omfattet af persondataloven, og at navne og adresser på de juridiske personer ikke skal tillægges særlig beskyttelsesinteresse,
- at der i denne sag er tale om udlevering af oplysninger til civil håndhævelse af ophavsrettigheder, og at der kan ske behandling af de pågældende personoplysninger, når det som her er nødvendigt til varetagelse af en berettiget interesse og interessen klart overstiger hensynet til den registrerede,
- at Datatilsynet konkluderede, at selv om der kan være tale om en følsom oplysning om et strafbart forhold, kan der alligevel i medfør af persondatalovens § 7, stk. 2, nr. 4, jf. § 8, stk. 6, § 8, stk. 4, og § 6, stk. 1, nr. 7, ske behandling af de pågældende personoplysninger, hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede,

Samlet eller individuel vurdering af krænkelse

- at der i denne sag er tale om et større antal registrerede ophavsretskrænkelser, hvilket samlet set har et betydeligt omfang, og at det samlede omfang skal indgå i vurderingen af proportionalitetshensynet,

- at CMS først på tidspunktet efter udlevering af navne og adresser kan foretage en individuel vurdering af krænkelse, herunder a) om der er tale om samme abonnent med forskellige IP-adresser (dynamiske IP-adresser), b) om den enkelte abonnent har foretaget flere krænkelse af samme eller flere værker, c) om abonnenten tidligere har foretaget krænkelse af de rettigheder, som CMS bistår med at håndhæve, d) om abonnenten er en juridisk person, og e) om IP-adressen er knyttet til en VPN-tjeneste, så navn og adresse ikke lader sig identificere,
- at Østre Landsret må inddrage disse realhensyn i sin vurdering og ligesom retten på Frederiksberg konkludere, at det er det samlede omfang, der skal indgå i vurderingen af proportionalitetshensynet,
- at der ikke efter dansk ret kan opstilles noget krav om, at CMS skal kunne sandsynliggøre individuelle ophavsretlige krænkelse hos én eller flere abonnenter af et "vist omfang" for at få udleveret navn og adresse på en abonnent,
- at ophavsretsloven og de processuelle regler om håndhævelse af ophavsrettigheder ikke indeholder en "bagatelgrænse" for ophavsrettigheder, der kan beskyttes og håndhæves,
- at ophavsretsloven er funderet på et krav om værkshøjde og ikke en "bagatelgrænse", og at Telenor og Telia har ikke bestridt, at de pågældende film og/eller tv-serier omfattet af begæringen har værkshøjde eller at der er foregået en ophavsretskrænke,
- at CMS har belyst de enkelte krænkelse omfang og ved eksempler belyst krænkelse naturen og sandsynlige hændelsesforløb, uden at Telenor eller Telia har redegjort nærmere for, hvad Telenor eller Telia forstår konkret ved den introducerede bagatelgrænse,
- at skadevirkningen for rettighedshavere er større med et større antal krænkelse,
- at hver enkelt brugers deltagelse i et fildelingsnetværk er en forudsætning for fildelingsnetværkets eksistens, og at proportionalitetshensynet derfor må ses i den sammenhæng,
- at vurderingen af det samlede omfang er i overensstemmelse med svensk ret, herunder de svenske lovforarbejder til den svenske ophavsretslov og den faste svenske retspraksis på området,
- at det ikke, hverken af den norske Høyesterettsdom (Scanbox-sagen) eller af norsk lovgivning, udtrykkeligt fremgår, at proportionalitetsafvejningen mellem rettighedshavere og abonnenter, hvis IP-adresser er blevet benyttet til ulovlig fildeling, udelukkende skal baseres på en vurdering af hver enkeltstående krænkelse for sig,
- at Oslo tingrett netop inddrog det samlede omfang i interesseafvejningen i den første afgørelse efter den norske Høyesteretts afgørelse,
- at Østre Landsret i overensstemmelse med hidtidig dansk retspraksis, svensk retspraksis og norsk retspraksis bør inddrage det samlede omfang i interesseafvejningen,

Telenor og Telias abonnenter

- at routere i dag er udstyret med en kode, og at abonnenter har pligt til at sikre deres internet med kode mod uretmæssig brug og kan – afhængigt af omstændighederne – komme i misligholdelse af deres abonnement ved misbrug af IP-adressen,

- at anvendelse af abonnementet til formidling af trafik for andre end abonnenten, dennes husstand, eller en eventuelt registreret bruger, udgør en misligholdelse af abonnementsaftalen,¹⁷
- at teleselskaberne ikke har et eget kontrolorgan og ikke overvåger abonnenternes internettrafik,
- at abonnenten er den nærmeste til at afklare omstændighederne om den eller de konstaterede ophavsretskrænkelser(r) på abonnentens egen IP-adresse, og at CMS uden oplysninger om abonnentens identitet de facto vil være afskåret fra at identificere rette sagsøgte,

Sagens bevismateriale

- at CMS beskriver de registrerede krænkelser ved et antal øjeblikbilleder, der er knyttet til de anførte IP-adresser, og at CMS derigennem beviser en del af omfanget af den fildeling, der er sket fra en abonnents IP-adresse,
- at fildeling af en del af et filmværk/tv-værk, herunder et øjebliksbillede, i sig selv udgør en ophavsretlig krænkelser, idet dele af filmværk/tv-værk udgør ophavsretligt beskyttede værker,
- at fildeling af pornografiske værker også udgør ophavsretskrænkelser, der bør kunne håndhæves, hvorfor der ikke skal sondres mellem de enkelte værker i proportionalitetsvurderingen,
- at en undtagelse vedrørende pornografiske værker vil skabe en retstilstand, der vil umuliggøre retsforfølgning af disse værker, hvilket vil være i modstrid med ophævelsen af forbuddet mod billedpornografi i Danmark af 1. juli 1969 og ligestillingen af disse værker med andre ophavsbeskyttede værker,
- at der hverken efter svensk eller finsk retspraksis skal sondres mellem pornografiske værker og andre værker,

MaverikMonitors pålidelighed og nøjagtighed

- at ekspertundersøgelser foretaget i forbindelse med forberedelsen for retten på Frederiksberg konkluderede, at MaverikMonitor på en sikker, pålidelig og nøjagtig måde er egnet til at afdække krænkelser af ophavsrettigheder,
- at Oslo tingrett efter den norske højesteretsafgørelse (Scanbox-sagen) har behandlet anmodninger om udlevering af navne og adresser knyttet til fildeling af film og tv-serier konstateret på IP-adresser i Norge (bilag 52),
- at CMS og Telenor begge er parter i sagen, som sideløbende med denne sag er blevet behandlet af Oslo tingrett,
- at Oslo tingrett har vurderet, at det er sandsynliggjort, at MaverikMonitor på en sikker, pålidelig og nøjagtig måde er egnet til at afdække ophavsrettigheder, og at det samme eller tilsvarende bevismateriale er blevet fremlagt i nærværende sag,
- at Oslo tingrett har fundet det sandsynliggjort, at informationen om de konkrete beviser (værdier) for de registrerede krænkelser omfang er information, som faktisk stammer fra MaverikMonitor og er korrekt gengivet,
- at der ikke efter dansk ret kan opstilles et krav om sandsynliggørelse af krænkelser af "et visst omfang", når der er konstateret en ophavsretlig krænkelser, uanset om den, som beskrevet af Telenor og Telia, må fremstå som "bagatelagtig",
- at Oslo tingrett fandt, baseret på tilsvarende bevismateriale, som er fremlagt i nærværende sag, at der var fremlagt beviser, der sandsynliggjorde krænkelser af "et visst omfang", og at oplysninger tilknyttet de registrerede krænkelser derfor skulle udleveres,

- at CMS ved de dokumenterede øjebliksbilleder og eksempler har sandsynliggjort, at de i denne sag registrerede fildelinger omfatter hele filmværker,
- at Oslo tingrett, baseret på tilsvarende bevismateriale som i denne sag, har vurderet, at det er højst usandsynligt, at brugerne omfattet af sagen kun har delt med MaverikMonitor,
- at CMS i denne sag har sandsynliggjort, at der fra de registrerede IP-adresser er blevet delt ophavsretligt beskyttet materiale med andre brugere og således ikke kun med MaverikMonitor,

Abonnenters reaktioner på breve

- at CMS' kommunikation med finske abonnenter i Finland har været enslydende med CMS' kommunikation med danske abonnenter i Danmark, og at kommunikationen i Finland og Danmark er sket i samme periode,
- at den finske Rettighedsalliance, TEKIJÄNOIKEUDEN TIEDOTUS- JA VALVONTAKESKUS RY, i efteråret 2017 foranledigede en større spørgeundersøgelse i Finland,
- at det fremgår af den finske spørgeundersøgelse, at fire ud af ti af de adspurgte har kendskab til advokatfirmaer eller rettighedshavere, der sender breve vedrørende op-havsretskrænkelser²³, og at det har formodningen for sig, at de samme tal gør sig gældende i Danmark,
- at 13 % af finnerne i undersøgelsen svarede, at de var holdt op med ulovlig fildeling på grund af brevene, og at over 50 % fandt at brevene udgør en effektiv måde at bekæmpe ulovlig fildeling på, og at det har formodningen for sig, at de samme tal gør sig gældende i Danmark,
- at det har formodningen for sig, at en undersøgelse i Danmark vil have samme konklusioner som i Finland, hvor undersøgelser og håndhævelse er foregået på samme måde og over samme tid,
- at en større del af Telenor og Telias bevismateriale er bygget på avisartikler med overskrifter som "Bøder for ulovlig download af film får kritik: Det minder om trusselsbreve" og "Advokatfirma afkræver Søren penge for piratkopiering: Som en Bandidos-rocker der stikker mig en dummebøde" og således ikke faktiske undersøgelser i Danmark eller andre nordiske lande,
- at avisartikler med fangende overskrifter har en meget begrænset bevisværdi og bør tillægges meget lidt eller ingen betydning, ligesom Telenor og Telias sprogbrug må opfattes som af mere personlig og politisk karakter,
- at tingretten i Oslo konkluderede (bilag 52), at et indlæg fra det norske forbrugerråd og teleorganisationen IKT-Norge, angående rettighedshaveres ansvar i forbindelse med tilbud af bedre løsninger, fremstod som både politiske og mere personlige,
- at direktøren for IKT-Norge, Torgeir Waterhouse, i februar 2018, efter afgørelsen fra Oslo tingrett fra januar 2018, opfordrede det norske Storting til at forbyde udsendelse af breve i Norge, hvilket illustrerer den personlige og politisk motiverede bevæggrund,
- at Oslo tingrett er uenig i, at de norske breve, der tilsvarende de danske breve er blevet sendt til norske abonnenter, fremstår som "trusselbrev", der konstaterer skyld og udgør et ubetinget pengekrav,

"Forretningsmodellen" – brevmodellen

- at CMS med henvisning til Maria Fredenslunds vidneforklaring for retten på Frederiksberg bestrider, at lovgiver har afvist CMS' "forretningsmodel" eller "brevmodel",

- at en arbejdsgruppe under det finske kultur- og undervisningsministerium, med deltagelse af interessenter fra musik- og filmindustrien, teleselskaber og brevmodtagere, som var repræsenteret af Electronic Frontier Finland – EFFI ry, har udarbejdet en rapport fra januar 2018 med anbefalinger til ”bedste praksis” for overvågning af ophavsretskrænkelser og breve sendt til privatpersoner,
- at arbejdsgruppen konkluderede, at brevmodellen har haft afgørende indflydelse på faldet i brugen af ulovlige fildelingstjenester i Finland, hvorfor CMS på denne baggrund gør gældende, at brevmodellen er et effektivt middel til at bekæmpe ulovlig fildeling på også i Danmark,
- at arbejdsgruppen på baggrund af undersøgelserne udarbejdede 15 anbefalinger for bedste praksis til indholdet af brevene samt til begæringer om udlevering af oplysninger om abonnenter, og at CMS med henvisning til bl.a. det danske Advokatnævns kendelser, Forbrugerombudsmandens pressemeddelelse og Datatilsynets udtalelse lever op til bedste praksis for brevmodellen i Danmark.”

Retsgrundlag

EU-retten

Den Europæiske Unions Charter om grundlæggende rettigheder (EU’s charter) indeholder en række bestemmelser af betydning for beskyttelse af persondata. Chartrets artikel 7 fastslår, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation. Artikel 8 om beskyttelse af personoplysninger fastslår i stk. 1, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende. Disse oplysninger skal ifølge stk. 2 behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har desuden ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf. Af stk. 3 fremgår det, at overholdelsen af reglerne skal være underlagt en uafhængig myndigheds kontrol. Af chartrets artikel 52, stk. 1, følger det, at enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved chartret, skal være fastlagt i lovgivningen og skal respektere disse rettigheders og friheders væsentligste indhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder. Artikel 52, stk. 3, fastslår, at i det omfang charteret indeholder rettigheder svarende til dem, der er sikret ved Den Europæiske Menneskerettighedskonvention, har rettighederne samme betydning og omfang som i konventionen, dog således at EU-retten kan yde en mere omfattende beskyttelse.

I 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 (persondatadirektivet) er der fastsat generelle regler om persondataskyttelse. Direktivet er gennemført i dansk ret ved persondataloven. Persondatadirektivet afløses af Europa-Parlamentets og Rådets forordning 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 (persondataforordningen), der træder i kraft den 25. maj 2018.

Ved Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 med senere ændringer om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet) er der fastsat særregler for telesektoren. Direktivet afløste Europa-Parlamentets og Rådets direktiv 97/66 EF. Der er den 10. januar 2017 fremsat forslag til en e-databeskyttelsesforordning (KOM (2017) 10), der skal afløse e-databeskyttelsesdirektivet.

Særreglerne i e-databeskyttelsesdirektivet har bl.a. til formål at sikre kommunikationshemmeligheden, personoplysninger og privatlivets fred, således at kommunikationsdata slettes snarest muligt, og abonnementsoplysninger kun lagres i det omfang, det er nødvendigt med henblik på afregning, og kun i et begrænset tidsrum, jf. nærmere direktivets præambelbetragtning 3, 4, 23 og 26. Dele af direktivet er gennemført i dansk ved lov nr. 450 af 10. juni 2003 om ændring af lov om konkurrence- og forbrugerforhold på telemarkedet med flere love. Direktivets artikel 5 om kommunikationshemmelighed og artikel 6 om trafikdata har følgende ordlyd:

”Art. 5

Stk. 1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf.

Stk. 2. Stk. 1 vedrører ikke lovmedholdelig registrering af kommunikation og de dermed forbundne trafikdata, hvis den foretages som led i lovlig forret-

ningspraksis med henblik på at kunne forelægge bevis for en handelstransaktion eller enhver anden forretningsmæssig kommunikation.

Stk. 3. Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv 95/46/EF at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.

Art. 6

Stk. 1. 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.

Stk. 2. Med henblik på debitering af abonnenten og afregning for samtrafik er det tilladt at behandle trafikdata. En sådan behandling er tilladt indtil udløbet af den lovbestemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger.

Stk. 3. Med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af værdiforøgende tjenester er det tilladt udbyderen af en offentligt tilgængelig elektronisk kommunikationstjeneste at behandle de i stk. 1 omtalte oplysninger i det omfang og tidsrum, som sådanne tjenester eller markedsføringen kræver, hvis den abonnent eller bruger, som oplysningerne vedrører, forudgående har givet sit samtykke hertil. Brugeren eller abonnenten skal på et hvilket som helst tidspunkt have mulighed for at trække sit samtykke til behandling af trafikdata tilbage.

Stk. 4. Tjenesteudbyderen underretter abonnenten eller brugeren om, hvilke typer trafikdata der behandles med henblik på det i stk. 2 omhandlede formål og om behandlingens varighed; ved behandling med henblik på det i stk. 3 omhandlede formål skal underretning ske, inden samtykke indhentes.

Stk. 5. Behandling af trafikdata i henhold til stk. 1, 2, 3 og 4 må kun foretages af personer, som handler efter bemyndigelse fra udbydere af de offentligt tilgængelige kommunikationsnet og -tjenester, og som er beskæftiget med debitering eller trafikstyring, kundeforespørgsler, afsløring af svig, markedsføring af elektroniske kommunikationstjenester eller levering af en tillægstjeneste, og skal begrænses til det for sådanne aktiviteter nødvendige.

Stk. 6. Stk. 1, 2, 3 og 5 berører ikke de kompetente organers mulighed for i overensstemmelse med gældende lovgivning at indhente oplysninger om trafikdata med henblik på bilæggelse af tvister, navnlig vedrørende samtrafik eller debitering.”

Medlemsstaterne kan inden for de rammer, der er fastsat i e-databeskyttelsesdirektivets artikel 15, stk. 1, indskrænke rækkevidden af bl.a. artikel 5 og 6 ved vedtagelse af retsfor skrifter. Artikel 15, stk. 1, har følgende ordlyd:

”Stk. 1. Medlemsstaterne kan vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig 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 efter artikel 13, stk. 1, i direktiv 95/46/EF. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke. Alle i dette stykke omhandlede forskrifter skal være i overensstemmelse med fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.”

Ved 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 (logningsdirektivet) blev medlemsstaterne uanset artikel 5 og 6 i e-databeskyttelsesdirektivet pålagt at sikre, at der blev foretaget lagring af en række kategorier af data i mindst seks måneder og højst to år for datoen for kommunikationen. I henhold til artikel 4 skulle det samtidigt sikres, at de data, der blev lagret i henhold til direktivet, kun blev udleveret til de kompetente myndigheder under nærmere angivne betingelser. Endvidere blev der til e-databeskyttelsesdirektivets artikel 15 tilføjet stk. 1 a, hvorefter artikel 15, stk. 1, ikke fandt anvendelse på data, der krævedes lagret i henhold til logningsdirektivet.

I EU-Domstolens dom af 29. januar 2008 i sag C-275/06 (Promusicae) er det i præmis 57 anført, at Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (e-handelsdirektivet), Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (infosoc-direktivet) og Europa-Parlamentets og Rådets direktiv 2004/48/EF af 29. april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder (retshåndhævelsesdirektivet) sigter på, at medlemsstaterne sikrer den effektiv beskyttelse af intellektuelle ejendomsrettigheder, herunder særlig ophavsretten. I forlængelse heraf er det videre anført, at det følger af bestemmelser i alle tre direktiver, at kravene forbundet med beskyttelse af personoplysninger går forud for en sådan beskyttelse. I præmis 70 er det videre anført, at de anførte direktiver og e-databeskyttelsesdirektivet ikke pålægger medlemsstaterne at fastsætte en pligt til at videregive personlige data vedrørende benyttelse af

internettet med henblik på at sikre den effektive beskyttelse af ophavsretten under en civil retssag, men at der ved gennemførelse af direktiverne skal sikres mulighed for at foretage den rette afvejning af de forskellige grundlæggende rettigheder, bl.a. under iagttagelse af proportionalitetsprincippet.

Ved EU-domstolens dom af 19. april 2012 i sag C-461/10 (Bonnier Audio AB) blev det fastslået, at logningsdirektivet ikke var til hinder for anvendelse af en national lovgivning indført i henhold til artikel 8 i retshåndhævelsesdirektivet, som indebærer, at en internetudbyder med det formål at kunne identificere en internetabonnent eller -bruger kan tilpligtes at give indehaverne af ophavsretten eller den, til hvem retten er overgået, oplysninger om den abonnent, der har fået tildelt en IP-adresse, hvorfra den påståede krænkelse er foretaget, idet en sådan lovgivning ikke omfattes af det materielle anvendelsesområde for logningsdirektivet. Det blev endvidere fastslået, at e-databeskyttelsesdirektivet og retshåndhævelsesdirektivet skal fortolkes således, at de ikke er til hinder for en national lovgivning herom, hvis denne lovgivning gør det muligt for den nationale ret på grundlag af omstændighederne i den konkrete sag og under hensyntagen til de krav, der følger af proportionalitetsprincippet, at afveje de pågældende modstridende interesser mod hinanden, jf. præmis 61.

Logningsdirektivet blev ved EU-Domstolens dom af 8. april 2014 i sag C-293/12 (Digital Rights Ireland Ltd) erklæret ugyldigt, idet det blev fastslået, at EU-lovgiver henset til EU's charter artikel 7 om respekt for privatliv og familieliv, artikel 8 om beskyttelse af personoplysninger og artikel 52, stk. 1 om rækkevidde og fortolkning af rettigheder og principper, ved vedtagelsen af direktivet havde overskredet de grænser, som kræves overholdt af hensyn til proportionalitet, jf. præmis 69. Som begrundelse herfor var bl.a. anført, at der skulle foretages en streng efterprøvelse af, om indgrebet var forholdsmæssigt, idet beskyttelsen af personoplysninger spiller en betydelig rolle i forhold til den grundlæggende ret til privatlivet, jf. præmis 48, at bekæmpelse af grov kriminalitet ikke i sig selv kunne begrunde, at en så omfattende datalagring som indført ved direktivet kunne anses for nødvendig, jf. præmis 51, at undtagelserne fra og beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige, jf. præmis 52, at der derfor skulle fastsættes klare og præcise regler, som regulerer rækkevidden og anvendelsen af foranstaltningen og fastsætter en række mindstekrav, således at den person, som har fået lagret data, råder over tilstrækkelige garantier til effektiv beskyttelse af oplysningerne mod misbrug, ulovlig adgang til og anvendelse heraf, jf. præmis 54, at sådanne regler ikke var fastsat, jf. præmis 59, 60 og 61, og at

der derimod var fastsat regler om lagring af alle trafikdata vedrørende fastnettelefoni, mobiltelefoni, internetadgang samt e-mail og telefoni via internettet, hvilket indebar indgreb i de grundlæggende rettigheder for praktisk talt hele den europæiske befolkning, herunder personer omfattet af tavshedspligt, jf. præmis 56 og 57.

Ved EU-Domstolens dom af 21. december 2016 i de forenede sager C-203/15 og C-698/15 (Tele2 Sverige AB og Watson m.fl.) blev det fastslået, at e-databeskyttelsesdirektivets artikel 15, stk. 1, sammenholdt med EU's charter artikel 7, 8 og 11 samt 52, stk. 1, skal fortolkes sådan, at bestemmelsen er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet foreskriver en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation, jf. præmis 112. Det fremgår endvidere bl.a. af dommen, at opregningen af de formål, der er fastsat i e-databeskyttelsesdirektivets artikel 15, stk. 1, 1. pkt., er udtømmende, og at adgangen til de lagrede data faktisk og præcist skal opfylde et af disse formål, ligesom proportionalitetsprincippet skal iagttages, jf. præmis 115 og 116.

Den Europæiske Menneskerettighedskonvention

Den Europæiske Menneskerettighedskonvention (EMRK) fastslår i artikel 8, stk. 1, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance. Det følger af stk. 2, at ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

Ved Den Europæiske Menneskerettighedsdomstols dom af 4. december 2008 i sag 30562/04 og 30566/04 (S. og Marper mod Storbritannien), der angik fingeraftryk, dna-profiler og celleprøver udtaget i forbindelse med mistanke om strafbart forhold, blev det bl.a. fastslået, at beskyttelsen af personfølsomme oplysninger er af afgørende betydning for en persons ret til respekt for sit privatliv og familieliv i henhold til EMRK artikel 8. Endvidere blev det anført, at der er et særligt behov for beskyttelse af oplysninger, der anvendes til politimæssige formål, jf. præmis 103.

Regler om beskyttelse af personoplysninger i dansk ret

Persondataloven indeholder generelle regler om beskyttelse af personoplysninger.

For kommercielle udbydere af elektroniske kommunikationsnet og -tjenester er der fastsat særregler om beskyttelse af personoplysninger i lov om elektroniske kommunikationsnet og -tjenester (teleloven) og bekendtgørelser udstedt med hjemmel heri.

Det følger af telelovens § 7, stk. 1, i lovens kapitel 3 om grundlæggende slutbrugerrettigheder under overskriften ”Hemmeligholdelse af elektronisk kommunikation, informationsikkerhed, behandling af persondata og bistand til aflytning m.v.”, at udbydere ikke uberettiget må videregive oplysninger om andres brug af nettet. Udbydere skal endvidere træffe de nødvendige foranstaltninger for at sikre, at oplysninger om andres brug af nettet ikke er tilgængelige for uvedkommende.

Efter telelovens § 8, stk. 1, skal Erhvervs- og vækstministeren fastsætte regler for udbydere om minimumskrav til behandling af persondata i elektroniske kommunikationsnet og -tjenester. Efter stk. 3 i samme bestemmelse kan regler efter stk. 1 bl.a. omfatte krav om opbevaring og behandling af trafikdata og lokaliseringsdata i forbindelse med elektronisk kommunikation af hensyn til persondatabeskyttelse.

Bekendtgørelse nr. 715 af 23. juni 2011 om udbud af elektroniske kommunikationsnet og -tjenester (udbudsbekendtgørelsen) er udstedt med hjemmel i bl.a. telelovens § 8, stk. 1. Udbudsbekendtgørelsens § 23, der er placeret i kapitel 4 om ”Hemmeligholdelse og oplysningspligt”, er sålydende:

”§ 23. Udbydere af offentlige elektroniske kommunikationsnet eller -tjenester skal sikre, at trafikdata, jf. § 2, stk. 1, nr. 2, vedrørende abonnenter eller brugere slettes eller anonymiseres, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2-5 og retsplejelovens § 786, stk. 4, eller regler udstedt i medfør heraf.

Stk. 2. Uanset stk. 1 må en udbyder, som nævnt i stk. 1, behandle og opbevare trafikdata med henblik på debitering af abonnenter og afregning for samtrafik. En sådan behandling og opbevaring af data er tilladt indtil udløbet af den lovhjemlede forældelsesfrist for de omhandlede gældsforpligtelser og afregninger.

Stk. 3. Uanset stk. 1 må en udbyder, som nævnt i stk. 1, behandle trafikdata, jf. § 2, stk. 1, nr. 2, vedrørende abonnenter eller brugere med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af tillægstjenester, jf. § 2, stk. 1, nr. 4, forudsat at abonnenten eller brugeren forud for behandlingen har givet sit samtykke hertil. Behandlingen er kun tilladt i det omfang og tidsrum, som tjenesten eller markedsføringen kræver. Abonnenten eller

brugeren skal på et hvilket som helst tidspunkt have mulighed for at trække sit samtykke tilbage.

Stk. 4. Udbydere, som nævnt i stk. 1, skal underrette abonnenten eller brugeren om, hvilke typer af trafikdata der behandles med henblik på de i stk. 2 og 3 omhandlede formål og om behandlingens varighed. Ved behandling med henblik på de i stk. 3 omhandlede formål skal underretning ske, inden samtykke indhentes.

Stk. 5. Udbydere, som nævnt i stk. 1, skal sikre, at behandling af trafikdata som nævnt i stk. 1-4 kun foretages af personer, som er ansat hos eller handler efter bemyndigelse fra udbydere af offentlige elektroniske kommunikationsnet eller -tjenester, og som er beskæftiget med debitering eller trafikstyring, behandling af klager eller andre henvendelser fra abonnenter, opsporing af svig eller med markedsføring af udbyderens egne tjenester eller levering af tillægstjenester. I forbindelse med behandlingen af sådanne konkrete sager skal behandlingen af trafikdata begrænses til alene at vedrøre det, der er nødvendigt for behandlingen af sagen.”

Efter telelovens § 13 skal udbydere på begæring af politiet udlevere oplysninger, der identificerer en slutbrugers adgang til elektroniske kommunikationsnet eller -tjenester. Bestemmelsen betyder, at disse oplysninger kan udleveres til politiet uden en editionskendelse, når der er tale om statiske ip-adresser. Udlevering af dynamiske ip-adresser mv. skal ske i medfør af retsplejelovens regler og forudsætter således en retskendelse, jf. herved det anførte i forarbejderne til bestemmelsen i telelovens § 13 (lovforslag nr. L 59 af 17. november 2010).

Logningsregler udstedt i medfør af retsplejeloven

Efter retsplejelovens § 786, stk. 4, der findes i retsplejelovens fjerde bog om strafferetsplejeloven og er medtaget i kapitel 71 om ”Indgreb i meddelelshemmeligheden, observation, forstyrrelse eller afbrydelse af radio- eller telekommunikation og blokering af hjemmesider”, påhviler det udbydere af telenet eller teletjenester at foretage registrering og opbevaring (logning) i 1 år af oplysninger om teletrafik til brug for efterforskning og retsfulgning af strafbare forhold.

Retsplejelovens § 786, stk. 4, blev indført ved § 2 i lov nr. 378 af 6. juni 2002 om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Gennemførelse af FN-konventionen til bekæmpelse af finansiering af terrorisme, gennemførelse af FN's Sikkerhedsråds resolution nr. 1373 (2001) samt øvrige initiativer til bekæmpelse af terrorisme m.v.) (anti-terrorpakke I). Bestemmelsen trådte i kraft den 15. september 2007.

I forbindelse med indførelsen af retsplejelovens § 786, stk. 4, blev det fastsat, at bestemmelsen senere skulle revideres, jf. ændringslovens § 8. Denne revision er efterfølgende blevet udskudt flere gange, senest ved lov nr. 673 af 8. juni 2017. Udskydelsen af revisionen er i bemærkningerne til lovforslaget hertil (lovforslag nr. L 191 af 26. april 2017) bl.a. begrundet i overvejelser i anledning af EU-Domstolens dom af 21. december 2016 dom i de forenede sager C-203/15 og C-698/15 (Tele2 Sverige AB og Watson m.fl.) om de svenske og britiske logningsreglers forenelighed med EU-retten. Justitsministeren har ved lovforslag nr. L 218 af 11. april 2018 til lov om ændring af lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (Ændring af revisionsbestemmelse) fremsat forslag om, at revisionen på ny udskydes.

Bekendtgørelse nr. 988 af 28. september 2006, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014, om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen) er udstedt med hjemmel i retsplejelovens § 786, stk. 4 og stk. 7, og fastsætter nærmere regler for registreringen af teledata. Reglerne i logningsbekendtgørelsen er opretholdt, indtil den ovenfor nævnte revision af logningsreglerne er gennemført. Det fremgår af en fodnote til den oprindelige logningsbekendtgørelse fra 2006, at bekendtgørelsen indeholder bestemmelser, der gennemfører dele af logningsdirektivet. Fodnoten blev ophævet ved ændringen af bekendtgørelsen i 2014.

Logningsbekendtgørelsens §§ 1, 4, 5, 6 og 9 er sålydende:

”§ 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.

§ 4. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal registrere følgende oplysninger om fastnet- og mobiltelefoni samt SMS-, EMS- og MMS-kommunikation:

- 1) opkaldende nummer (A-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 2) opkaldte nummer (B-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,

- 3) ændring af opkaldte nummer (C-nummer) samt navn og adresse på abonnenten eller den registrerede bruger,
- 4) kvittering for modtagelse af meddelelser,
- 5) identiteten på det benyttede kommunikationsudstyr (IMSI- og IMEI-numre),
- 6) den eller de celler en mobiltelefon er forbundet til ved kommunikationens start og afslutning, samt de tilhørende masters præcise geografiske eller fysiske placering på tidspunktet for kommunikationen,
- 7) tidspunktet for kommunikationens start og afslutning og
- 8) tidspunktet for første aktivering af anonyme tjenester (taletidskort).

§ 5. En udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal 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.

Stk. 2. Udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, der udbyder trådløs adgang til internettet, skal endvidere registrere oplysninger om det lokale netværks præcise geografiske eller fysiske placering samt identiteten på det benyttede kommunikationsudstyr.

§ 6. Udover de i § 5 nævnte oplysninger skal en udbyder af elektroniske kommunikationsnet eller -tjenester til slutbrugere registrere følgende oplysninger om egne e-mail-tjenester:

- 1) afsendende e-mail-adresse og
- 2) modtagende e-mail-adresse.

Stk. 2. For så vidt angår oplysninger om kommunikation foretaget ved brug af udbyderens egne internettelefoni-tjenester, skal de i § 5, stk. 1, nævnte oplysninger registreres.

§ 9. De i medfør af §§ 4 - 6 registrerede oplysninger skal opbevares i 1 år.”

Landsrettens begrundelse og resultat

Det er ubestridt, at Telenor og Telia er i besiddelse af oplysningerne om hvilke abonnenter, der var tildelt de i alt 4.011 anførte ip-adresser på de anførte tidspunkter.

Efter Asbjørn Skov Jensen og Lasse Andersens forklaringer lægger retten til grund, at Telenor og Telia ikke har brug for data om logning af ip-adresser med henblik på at foretage afregning over for deres abonnenter, at 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, at de krævede data om logning af ip-adresser

opbevares i systemer, der er adskilt fra teleudbydernes almindelige system, og at kun få, udvalgte medarbejdere, der håndterer henvendelser om udlevering fra politiet, har adgang til disse systemer. Efter Bastian Rankløves forklaring lægges det til grund, at tilsvarende gør sig gældende for TDC, dog således at data om logning af ip-adresser ikke for TDC er nødvendige med henblik på at foretage fejlretning.

Isoleret bevisoptagelse

Efter ordlyden af retsplejelovens § 343, stk. 1, og bestemmelsens placering i retsplejeloven må det anses for en betingelse for isoleret bevisoptagelse, at den sker med henblik på at tilvejebringe bevis til brug for en retssag eller til brug for overvejelser om, hvem en retssag skal anlægges mod.

Landsretten finder det efter de foreliggende oplysninger tilstrækkeligt sandsynliggjort, at der kan have fundet ophavsretskrænkelser sted, som vil kunne retsforfølges af rettighedshaverne, herunder efter ophavsretslovens § 81.

Henset til oplysningerne om, at der for tiden verserer en række civile sager, hvor stævning er udtaget efter opfyldelse af tidligere editionspålæg, er det i fornødent omfang godtgjort, at beviset ønskes optaget af CMS til brug for eventuelt senere anlæg af en retssag. Det kan ikke føre til en anden vurdering, at de civile sager efter det oplyste først er anlagt efter byrettens kendelse af 24. oktober 2017 i denne sag. Det bemærkes i den forbindelse, at kære kan støttes på nye beviser, jf. retsplejelovens § 393, stk. 5.

Da udlevering af ip-adresserne er nødvendige for at bidrage til afklaring af, hvem der senere kan anlægges sag mod, må optagelsen af et sådant bevis, selv om det ikke sker til brug for en verserende retssag, desuden anses for hensigtsmæssig.

Edition

Som anført er det ubestridt, at Telenor og Telia har rådighed over de ønskede oplysninger om hvilke abonnenter, der var tildelt de anførte ip-adresser på de anførte tidspunkter. Da oplysningerne er nødvendige for at bidrage til afklaring af, hvem der kan anlægges sag mod, må de anses for at være af betydning for sagen. Det ændrer ikke herved, at oplysningerne muligvis ikke i sig selv vil være tilstrækkelige til, at rettighedshaverne kan få medhold i en civil sag om en rettighedskrænkelse.

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

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

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

Det følger endvidere af EU-Domstolens dom af 29. januar 2008 i sag C-275/06 (Promusicae) og dom af 19. april 2012 i sag C-461/10 (Bonnier Audio AB), at bl.a. e-databeskyttelsesdirektivet ikke er til hinder for nationale regler om udlevering af oplysninger om en abonnents ip-adresse i forbindelse med retsforfølgning af krænkelse af ophavsrettigheder, men at der skal være mulighed for at foretage en afvejning af de modstridende interesser i sagen i forbindelse med en sådan udlevering af oplysninger.

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

Disse tungtvejende grunde skal afvejes over for CMS' interesse i at få oplysningerne udle- veret.

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

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

Konklusion og sagsomkostninger

På den ovenfor anførte baggrund ændres byrettens kendelse, således at begæringerne om tredjemandsedition under den isolerede bevisoptagelse ikke tages til følge.

Efter sagernes karakter skal ingen af parterne heller ikke for landsretten betale sagsom- kostninger til en anden part.

T h i b e s t e m m e s:

Byrettens kendelse ændres, således at Copyright Management Services Ltd.'s begæringer om tredjemandsedition under den isolerede bevisoptagelse ikke tages til følge.

Ingen af parterne skal betale sagsomkostninger til en anden part.

Kærefgiften i begge sager tilbagebetales.

(Sign.)

— — —

Udskriftens rigtighed bekræftes. Østre Landsret, den