

Kandidatspeciale

Teleudbyderes videregivelse af navne- og adresseoplysninger tilknyttet
IP-adresser til civilretlig forfølgelse af ophavsretlige krænkelser

En analyse af om videregivelse er i overensstemmelse med persondataretten



Foto: Shutterstock.com

Pernille Jensen, studienr. 20155415

Louise Korsholm, studienr. 20154098

Nanna Cecilie Bødker, studienr. 20146935



AALBORG UNIVERSITET

Titelblad

Dansk titel:	Teleudbyderes videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser til civilretlig forfølgelse af ophavsretlige krænkelse - En analyse af om videregivelse er i overensstemmelse med persondataretten
Engelsk titel:	Telecommunications providers disclosure of name and address information connected to IP addresses for civil prosecution of copyrights violations - An analysis of whether disclosure is in accordance with the data protection legislation.
Forfattere:	Louise Korsholm, Pernille Jensen og Nanna Cecilie Bødker
Semester:	10. semester
Fagområde:	Persondataret
Vejleder:	Torsten Bjørn Larsen
Universitet:	Aalborg Universitet (AAU)
Dato for aflevering:	19. maj 2020

Abstract

Over the last years telecommunications providers in Denmark have disclosed name and address information connected to IP-addresses to rights holders. These rights holders request the client information connected to IP-addresses in order to pursue copyrights violations.

The following thesis examines whether this disclosure of clients' name and address information connected to IP addresses to the rights holders, with the objective of civil prosecution of copyrights violations, is in accordance with the Danish data protection legislation. The thesis examines the legality of disclosure to the rights owners both with and without a discovery order in which the court orders the telecommunications providers to hand over the requested information.

To examine whether the disclosures of the data is in accordance with the Danish data protection legislation the provisions and principles of the data protection act and the Danish data protection law is being examined and analyzed. Especially interesting for this thesis is the legislation on telecommunications providers logging since this is crucial to the information being in the telecommunications providers possession. Therefore, relevant logging legislation is being analyzed and examined from a personal data legislation perspective. Throughout the thesis relevant case law from the Danish court and the EU Court of Justice, rulings from the Danish supervisory authority and more are applied.

As a result of the analysis it has been concluded that name and address information connected to an IP-address is protected by the data protection legislation as long as a natural person can be identified. Name and address information connected to IP addresses is normally considered to be general personal data. When the information is put in connection with the accessed material it can form sensitive personal data. Similarly, the name and address information connected to IP addresses can form data relating to criminal convictions and offences when connected to the copyright violations.

Furthermore, it has been concluded that storage of the personal data can happen in accordance with the data protection legislation. At the time of storage, the information will be considered general personal data. According to the data protection act the telecommunications providers can store the information to fulfil the contract and on the basis of the Danish act on logging. The Danish act on logging establishes an obligation for the telecommunications providers to store the information for one year.

In regard to the disclosure of the data it has been concluded that the telecommunications providers have legal basis to disclose the data if a discovery order has been issued. When no discovery order is issued the telecommunications providers should not disclose the information due to the essential considerations that are to be weighed. This balancing should be done by the court.

The purpose of the Danish act on logging is to log name and address information to investigate and prosecute criminal offenses. From thorough analysis it has been concluded that civil prosecution is not concluded in or compatible with the purpose of this act. From relevant case law it is made clear that no legislation prevents Danish legislators in making laws for this purpose.

When the Danish act on logging is not applied the disclosure appears to be lawful but, similarly as when the Danish act on logging applies, the disclosure is not in accordance with the principles of the Danish data protection legislation.

In conclusion, it may be said that a telecommunications providers' disclosure of name and address information connected to an IP-address is not in accordance with the Danish data protection legislation when the information is handed over to a rights owner to be used for civil prosecution of copyrights violations. This conclusion applies whether the information is stored in accordance with the Danish act on logging or for the telecommunications providers' own needs.

KAPITEL 1.....	5
1.1 Indledning.....	5
1.2 Emnevalg.....	7
1.3 Afgrænsning af emne.....	8
1.4 Metode og retskilder.....	9
1.5 Struktur.....	12
KAPITEL 2.....	13
2.1 Retten til beskyttelse af personoplysninger.....	13
2.2 Databeskyttelsesforordningen.....	14
2.2.1 Forordningens hensyn og formål.....	14
2.2.2 Forordningens anvendelsesområde.....	15
2.2.3 Persondataretlige definitioner.....	16
2.2.3.1 Personoplysning.....	16
2.2.3.2 Behandling.....	17
2.2.3.3 Dataansvarlig.....	17
2.2.3.4 Databehandler.....	18
2.2.3.5 Tredjemand.....	18
2.2.4 Principper for behandling af personoplysninger.....	19
2.2.4.1 Princippet om lovlighed, rimelighed og gennemsigtighed.....	19
2.2.4.2 Princippet om formålsbegrænsning.....	20
2.2.4.2.1 Viderebehandling.....	21
2.2.4.2.2 Forenelighedstesten.....	21
2.2.4.3 Princippet om dataminimering.....	22
2.2.4.4 Princippet om rigtighed.....	22
2.2.4.5 Princippet om opbevaringsbegrænsning.....	23
2.2.4.6 Princippet om integritet og fortrolighed.....	23
2.2.5 Behandling af personoplysninger.....	23
2.2.5.1 Behandling af almindelige personoplysninger.....	24
2.2.5.1.1 Forordningens artikel 6, stk. 1, litra a – samtykke.....	24
2.2.5.1.2 Forordningens artikel 6, stk. 1, litra b – opfyldelse af en kontrakt.....	25
2.2.5.1.3 Forordningens artikel 6, stk. 1, litra c – retlig forpligtelse.....	25
2.2.5.1.4 Forordningens artikel 6, stk. 1, litra f – interesseafvejningsreglen.....	25
2.2.5.2 Behandling af følsomme personoplysninger.....	26
2.2.5.2.1 Forordningens artikel 9, stk. 2, litra a - udtrykkeligt samtykke.....	26
2.2.5.2.2 Forordningens artikel 9, stk. 2, litra f - retskrav.....	26
2.2.5.2.3 Forordningens artikel 9, stk. 2, litra g - væsentlige samfundsinteresser.....	27
2.2.5.3 Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser.....	27
2.3 Øvrig relevant lovgivning.....	28
2.3.1 Retsplejeloven.....	28
2.3.2 Logningsbekendtgørelsen.....	29
2.3.2.1 Logningsdirektivet (direktiv 2006/24/EF).....	29
2.3.2.2 E-databeskyttelsesdirektivet (direktiv 2002/58/EF).....	30
KAPITEL 3.....	31
3.1. Den nuværende retstilstand.....	31
3.2 Retspraksis.....	32

3.2.1 Østre Landsrets kendelse af den 7. maj 2018 (U.2019.2019 Ø).....	32
3.2.2 Tele2/Watson-dommen (C-203/15 og C-698/15).....	34
3.2.3 Promusicae (C-275/06).....	35
3.3 Forordningens genstand og formål	36
3.3.1 Personoplysning.....	36
3.3.1.1 IP-adresser som personoplysning	37
3.3.2 Fysisk person	38
3.4 Forordningens anvendelsesområde.....	38
3.5 Kategorier af personoplysninger.....	39
3.6 Behandling af personoplysninger	40
3.6.1 Behandling af almindelige personoplysninger.....	41
3.6.1.1 Teleudbyderes opbevaring af personoplysninger.....	41
3.6.1.2 Teleudbyderes videregivelse af personoplysninger.....	42
3.6.1.2.1 Videregivelse ved editionskendelse	42
3.6.1.2.2 Videregivelse uden editionskendelse	43
3.6.2 Behandling af følsomme personoplysninger	45
3.6.2.1 Videregivelse ved editionskendelse	45
3.6.2.2 Videregivelse uden editionskendelse	46
3.6.3 Behandling af oplysninger om strafbare forhold	46
3.6.4 Rettighedshaveres behandling af personoplysninger.....	47
3.7 Teleudbyderes forpligtelser efter logningsbekendtgørelsen	49
3.7.1 Opbevaring efter logningsbekendtgørelsen	49
3.7.2 Videregivelse efter logningsbekendtgørelsen.....	51
3.7.2.1 Videregivelse til forfølgelse af civilretlige krav.....	52
3.7.2.2 Videregivelse til forfølgelse af strafferetlige krav.....	54
3.7.2.3 Rækkevidden af logningsbekendtgørelsens formål.....	57
3.7.2.3.1 Forenelighedstesten.....	59
3.8 Teleudbyderes videregivelse uden for logningsbekendtgørelsens anvendelsesområde.....	62
3.8.1 Behandling af personoplysninger	62
KAPITEL 4.....	64
4.1 Konklusion	64
KAPITEL 5.....	67
5.1 Perspektivering til nordiske lande.....	67
5.1.1 Finsk Højesteretsafgørelse af den 8. december 2017 (KKO:2017:85).....	68
5.1.2 Norsk Højesteretsafgørelse af 26. april 2017 (HR-2017-833-A).....	69
5.1.3 Sammenfattende om nordisk retspraksis	69
Litteraturliste	70
Bilagsoversigt.....	76

Kapitel 1

1.1 Indledning

*“Uskyldige internetbrugere stævnes for ulovlig download”*¹, *“Anklagerne rammer som spredhagl”*² og *“It-jurist: Advokater skræmmer folk med tynde bøder for ulovlig download af film”*³ er blot en række af de overskrifter, som præger det danske nyhedsbillede. Disse artikler omhandler forfølgelse af en række ophavsretlige krænkelse vedrørende ulovlig download og deling af film på internettet. Rettighedshaveres forfølgelse af disse ophavsretlige krænkelse har medført, at tusindvis af danskere har fået tilsendt et såkaldt forligsbrev.⁴ Advokat hos NJORD Law Firm, Jeppe Brogaard Clausen, udtalte i forsommeren 2018, at advokatfirmaet i en årrække inden år 2017 har udsendt omkring 30.000-40.000 forligsbreve. Potentielt kan der være udsendt over 150.000 forligsbreve til danskerne.⁵

Brevene har medført, at der verserer en række lignende sager i landets retskredse vedrørende ulovlig download og deling af film på internettet. Her kan blandt andet nævnes Københavns Byret, hvor der verserer omkring 160 sager samt Retten på Frederiksberg, hvor der verserer omkring 70 sager.⁶ Hertil har retspræsidenten ved Retten på Frederiksberg udtalt, at der mindst verserer 1.000 sager ved landets domstole.⁷ I denne forbindelse har Retten på Frederiksberg fundet det hensigtsmæssigt at udarbejde en generel vejledning til denne type af sager. Vejledningen er udarbejdet til såvel sagens parter, advokater, som landets byretter.⁸ Denne vejledning slår fast, at der ikke er fastlagt en retspraksis på området og at den nuværende byretspraksis ikke kan betragtes som værende ensartet.⁹ Retstilstanden i denne type sager er således uklar.

Rettighedskrænkelserne, der ligger til grund for de fremsendte forligsbreve, består i fysiske personers download og deling af ophavsretligt beskyttede filer. De ophavsretligt beskyttede filer kan eksempelvis være film og musik.

Forud for fremsendelsen af de omtalte forligsbreve har rettighedshaverne, som er repræsenteret ved eksempelvis NJORD Law Firm, indhentet oplysninger om hvilke IP-adresser, der har tilgået det ophavsretligt beskyttede materiale. Rettighedshaverne er kommet i besiddelse af IP-adresserne via deres samarbejde med virksomheden Maverick Eye. Inden forligsbrevene kan fremsendes og en krænkelse kan gøres gældende, er det en forudsætning, at rettighedshaverne kommer i besiddelse af navne- og adresseoplysningerne tilknyttet IP-adresserne. Uden navne-

¹ Petersen, Steen, 2019.

² Poulsen, Dan, del 2, 2020.

³ Stenz, Emil, 2016.

⁴ Poulsen, Dan, del 1, 2020.

⁵ Poulsen, Dan, del 3, 2020.

⁶ Danmarks Domstole, Fildeling, 2020.

⁷ Poulsen, Dan, Nyhed, 10-02-2020.

⁸ Poulsen, Dan, Nyhed, 07-02-2020.

⁹ Retten på Frederiksbergs vejledning af den 5. februar 2020, s. 4.

og adresseoplysningerne kan rettighedshaverne ikke identificere de pågældende personer bag IP-adresserne.

De pågældende navne- og adresseoplysninger tilknyttet IP-adresserne er teleudbyderne i besiddelse af. Rettighedshaverne kan således komme i besiddelse af de nødvendige personoplysninger, hvis teleudbyderne frivilligt videregiver oplysningerne eller hvis teleudbyderne pålægges at videregive oplysninger af retten ved edition. Siden i hvert fald 2012 har teleselskaber, videregivet navne- og adresseoplysninger tilknyttet IP-adresser til advokatfirmaer.¹⁰ Tidligere advokat for TDC, Bastian Rankløve, oplyser, at TDC i perioden fra 2016-2017 har videregivet oplysninger om 167.000 IP-adresser.¹¹ Desuden udtaler Telenors juridiske direktør, at Telenor i 2015 modtog 6.187 henvendelser vedrørende videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser. I 2016 var dette tal steget til 21.163.¹² Henvendelserne til teleudbyderne vedrørende en sådan videregivelse er således steget markant.

Nærværende afhandling vil undersøge, hvorvidt en videregivelse af disse oplysninger fra teleudbydere til rettighedshavere til brug for forfølgelse af ophavsretlige krænkelse er i overensstemmelse med persondataretten. Nærværende afhandling vil alene undersøge, hvorvidt videregivelsen er i overensstemmelse med dansk ret.

Problemstillingen i nærværende afhandling kan tydeliggøres med følgende illustration. Fokus i nærværende afhandling vil være på sidste led i illustrationen og dermed forholdet mellem teleudbyderen og rettighedshaveren.

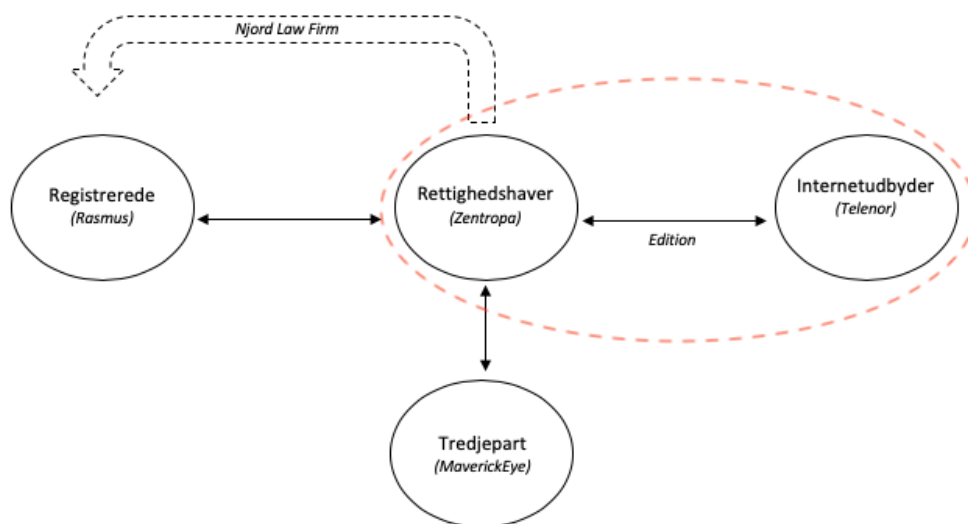


Illustration 1

¹⁰ Se bilag 9.

¹¹ U.2019.2019 Ø.

¹² Breinstrup, Thomas, 2020.

På baggrund af ovenstående illustration kan der opstilles følgende eksempel, som tydeliggør hændelsesforløbet, der ligger til grund for problemstillingen:

Rasmus downloader og deler filmen "Fasandræberne". Denne handling bliver rettighedshaver Zentropa Productions gjort opmærksom på af MaverickEye, som overvåger ulovlig download og fildeling på internettet efter aftale med Zentropa Productions. MaverickEye tilvejebringer IP-adresserne som har tilgået filmen "Fasandræberne" ulovligt. Herunder fremgår Rasmus' IP-adresse. Før end Zentropa Productions kan gøre krænkelsen gældende, er det nødvendigt at kunne identificere personer bag de indsamlede IP-adresser. Denne identifikation kan finde sted ved, at Zentropa Productions indhenter oplysninger om eksempelvis navn og adresse på brugeren af IP-adressen. Disse oplysninger er teleudbyderen, Telenor, i besiddelse af. Telenor ønsker dog ikke at videregive de pågældende oplysninger til Zentropa Productions. Telenor er imidlertid ikke forpligtet til at videregive oplysningerne om deres abonnenter uden retskendelse, hvorfor Zentropa Productions begærer tredjemandsedition. Retten efterkommer editionsbegæringen, hvorefter Zentropa Productions bliver bekendt med Rasmus' identitet. Zentropa Productions antager NJORD Law Firm til forfølgelse af krænkelsen. Rasmus modtager herefter et brev fra NJORD Law Firm. I brevet opfordres Rasmus til at indbetale 2.300 kr., hvorefter sagen kan afsluttes ved forlig. Alternativt vil Rasmus blive stævnet med krav om betaling af 7.500 kr. Rasmus bliver bekendt med, at ovenstående kan være i strid med persondataretten.

Henset til ovenstående vil afhandlingen behandle følgende problemformulering:

Er teleudbyderes videregivelse af en abonnents navne- og adresseoplysninger tilknyttet en IP-adresse i overensstemmelse med persondataretten, når oplysningerne videregives til rettighedshavere, der ønsker at forfølge en ophavsretlig krænkelse civilretligt?

1.2 Emnevalg

Motivationen, for at vælge problemstillingen i nærværende afhandling, er overordnet begrundet i det øgede fokus persondataretten har fået, efter databeskyttelsesforordningen trådte i kraft den 25. maj 2018.

Afhandlingen behandler en højaktuel problemstilling, idet flere tusinde danskere har modtaget forligsbreve vedrørende ulovlig download og fildeling af ophavsretligt beskyttet materiale. Forligsbrevene har været - og er fortsat - meget debatterede, særligt i medierne. Problemstillingen på området er desuden blevet bemærket i retssystemet. Dette blev tydeliggjort ved, at Retten på Frederiksberg den 5. februar 2020 offentliggjorde en vejledning til sager, hvor rettighedshavere har anlagt sag om ulovlig download og fildeling. Vejledningen er udstedt til såvel sagens parter, advokater samt landets byretter.¹³

¹³ Poulsen, Dan, Nyhed, 07-02-2020.

Kombinationen af de to højaktuelle områder forekommer spændende, relevant og konkret. Desuden er det særligt spændende, at sagerne netop nu befinder sig et skelsættende sted, da de afventer stillingtagen fra højere instans. Den specifikke persondataretlige konflikt, som nærværende afhandling udforsker, er desuden forholdsvis uberørt, hvorfor afhandlingen forhåbentlig forekommer brugbar og lærerig.

1.3 Afgrænsning af emne

Hensigten med nærværende afhandling er at belyse, hvorvidt teleudbyderes videregivelse af en abonnents navne- og adresseoplysninger tilknyttet IP-adresser er i overensstemmelse med persondataretten, når oplysningerne videregives til rettighedshavere, der ønsker at forfølge en ophavsretlig krænkelse civilretligt.

For nærmere at belyse denne problemstilling, vil afhandlingen indledningsvist behandle databeskyttelsesforordningens hensyn og formål samt anvendelsesområde. Endvidere vil afhandlingen inddrage relevante definitioner i databeskyttelsesforordningens artikel 4. Derudover vil afhandlingen behandle de generelle principper for behandling af personoplysninger som fastsat i artikel 5. I forlængelse heraf vil afhandlingen tillige behandle artikel 6, 9 og 10, hvoraf det retlige grundlag for behandling af personoplysninger fremgår.

Logningsbekendtgørelsen har betydning for behandlingsgrundlaget, da denne bekendtgørelse fastsætter en række krav og forpligtelser i forhold til behandlingen af en abonnents navne- og adresseoplysninger tilknyttet IP-adresser. I denne tilknytning er det særligt logningsbekendtgørelsens formål som behandles.

Den ophavsretlige krænkelse forfølges civilretligt af rettighedshaverne. Det vil derfor blive behandlet, hvorvidt teleudbydere kan videregive en abonnents navne- og adresseoplysninger tilknyttet IP-adresser, særligt ved anvendelse af retsplejelovens civilretlige regler om tredjemandsedition under isoleret bevisoptagelse.

I forbindelse med rettighedshavernes civilretlige forfølgelse af ophavsretlige krænkelse optræder en række aktører. Afhandlingens problemstilling vedrører alene relationen mellem teleudbydere og rettighedshavere. Problemstillinger i andre relationer end denne, behandles således ikke.

Nærværende afhandling vil ikke beskæftige sig med databeskyttelsesforordningens regulering vedrørende behandling til arkivformål, uanset at dette er omtalt i de for afhandlingen relevante bestemmelser. Behandling til arkivformål findes ikke at være relevant for afhandlingens problemstilling, da denne vedrører videregivelse til forfølgelse af ophavsretlige krænkelse.

Databeskyttelsesforordningen er en del af Europa Kommissionens databeskyttelsespakke. Denne pakke består dels af databeskyttelsesforordningen og dels af retshåndhævelses-

direktivet, som er implementeret i dansk ret ved retshåndhævelsesloven.¹⁴ Til trods for at retshåndhævelsesdirektivet er en del af denne databeskyttelsespakke, behandles beskyttelsen af personoplysninger i forbindelse med retshåndhævelse ikke i afhandlingen. Dette er begrundet i, at disse regelsæt omhandler retshåndhævelsesmyndigheders behandling af personoplysninger, herunder politi, anklagemyndighed samt domstolen.

Udlevering efter retsplejelovens § 299, stk. 1 omhandlende tredjemandsedition, kan ikke ske, hvis tredjemand er udelukket fra eller fritaget for at afgive vidneforklaring. Vidneudelukkelse kan begrundes i den lovbestemte tavshedspligt i telelovens § 7. Afvejningen af, hvorvidt en teleudbyder er udelukket fra at afgive forklaring, som følge af tavshedspligten, findes uden betydning for om en videregivelse er i overensstemmelse med persondataretten. Teleloven vil derfor ikke blive inddraget i afhandlingen. Tilsvarende vil behandlingen i U.2019.2019 Ø vedrørende denne tavshedspligt ikke blive inddraget.

Uanset at afhandlingens problemstilling omhandler videregivelse til civilretlig forfølgelse af ophavsretlige krænkelse, inddrages den ophavsretlige lovgivning ikke i afhandlingen. Dette er begrundet i, at karakteren af den ophavsretlige krænkelse ikke har betydning for, hvorvidt teleudbydernes videregivelse til civilretlig forfølgelse er i overensstemmelse med persondataretten.

Ved overtrædelse af ophavsretsloven er der hjemmel til at pålægge straf. Denne afhandling vedrører imidlertid rettighedshavernes mulighed for civilretligt at opnå økonomisk kompensation for ophavsretlige krænkelse, hvorfor der afgrænses fra teleudbyderens mulighed for at videregive oplysninger til straffesager.

1.4 Metode og retskilder

I nærværende afhandling anvendes den retsdogmatiske metode. Denne metode er karakteriseret ved, at den beskriver, systematiserer og analyserer gældende ret. I denne forbindelse skal retskilder og fortolkningsprincipper anvendes.¹⁵

Fortolkningsprincipper er hjælpemidler til forståelsen af retsregler.¹⁶ De anvendte fortolkningsprincipper i afhandlingen udgør ordlydsfortolkning, formålsfortolkning, indskrænkende fortolkning samt direktivkonform fortolkning.

Ordlydsfortolkning indebærer, at den almindelige forståelse af ordlyden lægges til grund, hvorfor dette fortolkningsprincip er udgangspunktet.¹⁷ Formålsfortolkning vedrører formålet med lovgivningen. En sådan fortolkning kan være objektiv og subjektiv. Objektiv formålsfortolkning vedrører lovens eget indhold og har nær tilknytning til ordlydsfortolkning.

¹⁴ Betænkning nr. 1565, s. 9.

¹⁵ Munk-Hansen, Carsten, 2012, s. 202-203.

¹⁶ Evald, Jens, 2000, s. 52.

¹⁷ Munk-Hansen, Carsten, 2012, s. 281.

Ved subjektiv formålsfortolkning fortolkes alene lovens forarbejder.¹⁸ Ved en indskrænkende fortolkning forstås, at anvendelsesområdet for en retsregel indsnævres.¹⁹ Indskrænkende fortolkning er af særlig relevans, når retsregler indskrænker en borgers rettigheder.²⁰ Direktivkonform fortolkning indebærer, at lovregler baseret på direktiver skal fortolkes i overensstemmelse hermed.²¹

Retskilderne kan efter bred tilslutning i den danske retskildeteori kategoriseres i fire hovedgrupper. Disse grupper er henholdsvis lovgivning, retspraksis, sædvaner og forholdets natur. Den indbyrdes rangorden mellem disse retskilder er ikke fastlagt. I den danske retskildeteori er der imidlertid enighed om, at en sådan rangorden ikke findes.²² Den generelle forståelse er dog, at lovgivningen har forrang i forhold til de øvrige retskildegrupper.²³ Dette er begrundet i, at lovgivningen er demokratisk legitimeret. Desuden øges retssikkerheden herved, da lovgivningen skaber en grad af forudsigelighed.²⁴ I nærværende afhandling anvendes retskildegrupperne lovgivning og retspraksis.

Afhandlingen vil anvende både lovgivning fra Danmark og Den Europæiske Union (herefter EU). Danmark har, som følge af sit medlemskab af EU, afgivet en del af landets suverænitet med hjemmel i Grundlovens § 20, stk. 1. Dette indebærer, at EU-retten skal iagttages og udgør dermed en del af det danske retsgrundlag.²⁵ Forholdet mellem EU-retten og dansk ret er fastslået af Den Europæiske Unions Domstol (herefter EU-domstolen), hvorefter EU-retten har forrang.²⁶ EU-retten er baseret på et traktatretligt grundlag. Med udgangspunkt i disse traktater kan der udstedes retsakter, herunder blandt andet forordninger og direktiver.²⁷ En forordning er direkte bindende i medlemsstaterne og kræver således ikke implementering, hvorimod et direktiv kræver implementering i national ret, jf. Traktat om Den Europæiske Unions Funktionsområde (herefter TEUF) artikel 288.²⁸

Hovedsageligt vil afhandlingen beskæftige sig med “Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)” (herefter forordningen). Danmark har i denne sammenhæng udstedt “Lov 2018-05-23 nr. 502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)”. Denne lov supplerer forordningen, jf. databeskyttelseslovens § 1, stk.

¹⁸ Evald, Jens, 2000, s. 57-58.

¹⁹ Munk-Hansen, Carsten, 2012, s. 278.

²⁰ Munk-Hansen, Carsten, 2012, s. 292.

²¹ Munk-Hansen, Carsten, 2012, s. 251.

²² Evald, Jens, 2000, s. 7.

²³ Evald, Jens, 2000, s. 16.

²⁴ Evald, Jens, 2000, s. 11.

²⁵ Munk-Hansen, Carsten, 2012, s. 258-259.

²⁶ Munk-Hansen, Carsten, 2012, s. 264.

²⁷ Munk-Hansen, Carsten, 2012, s. 258-259.

²⁸ Munk-Hansen, Carsten, 2012, s. 260.

1. Databeskyttelsesloven inddrages i nærværende afhandling, hvor forordningen har overladt den nærmere regulering til medlemsstaterne.

Forordningen afløser det tidligere direktiv ”Europa-Parlamentet 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” (herefter persondatadirektivet). Dette direktiv var i dansk ret implementeret ved ”Lov 2000-05-31 nr. 429 af om behandling af personoplysninger” (herefter persondataloven).²⁹ Hensynene og formålene i persondatadirektivet og persondataloven er i det væsentligste videreført i henholdsvis forordningen og databeskyttelsesloven.³⁰

Endvidere inddrages præambelbetragtningen til forordningen samt betænkning nr. 1565 om databeskyttelsesforordningen (2016/679) udarbejdet af Justitsministeriet. Desuden inddrages ”Lovforslag nr. 68 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)”. Disse inddrages for at belyse hensynene samt formålet med forordningen samt databeskyttelsesloven. Der er uenighed om, hvorvidt lovforarbejder udgør en retskilde. Lovforarbejder anvendes som bidrag til forståelsen af gældende ret, hvorfor disse ikke bør betragtes som en egentlig retskilde.³¹

Herudover inddrages relevant lovgivning vedrørende teleudbyderes logning af personoplysninger. I denne forbindelse anvendes ”Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation)” (herefter e-databeskyttelsesdirektivet). E-databeskyttelsesdirektivet er suppleret af ”Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF” (herefter logningsdirektivet). Disse direktiver danner grundlag for den danske regulering af teleudbyderes logning. I nærværende afhandling er ”Bekendtgørelse 2006-09-28 nr. 988 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)” således relevant. Desuden inddrages § 23 i ”Bekendtgørelse 2011-06-23 nr. 715 vedrørende udbud af elektroniske kommunikationsnet og -tjenester” (herefter udbudsbekendtgørelsen) omhandlende teleudbyderes sletning og anonymisering af trafikdata.

Foruden ovenstående inddrages ”Lovbekendtgørelse 2019-09-10 nr. 938 om rettens pleje” (herefter retsplejeloven). Særligt reglerne om tredjemandsedition og isoleret bevisoptagelse i civile sager er relevante.

²⁹ Betænkning nr. 1565, s. 9.

³⁰ Betænkning nr. 1565, s. 21.

³¹ Munk-Hansen, Carsten, 2012, s. 347.

I afhandlingen inddrages dansk retspraksis i form af domme og kendelser. Disse analyseres og anvendes som fortolkningsbidrag til at fastlægge, hvornår teleudbydere kan videregive en abonnents navne- og adresseoplysninger tilknyttet IP-adresser. Afhandlingen vedrører den danske retstilstand. Dog er en række af retskilderne i afhandlingen baseret på EU-retsakter, hvorfor EU-retspraksis inddrages til at belyse formålet og forståelsen af de danske retskilder.

Dansk retspraksis, som behandles i nærværende afhandling, er afsagt af henholdsvis by- og landsret. I denne tilknytning skal det anføres, at afgørelser afsagt af en landsret har en højere præjudikatværdi end afgørelser afsagt af en byret.³² Højesteretsafgørelser har dog den højeste præjudikatværdi. På nuværende tidspunkt har Højesteret ikke taget stilling til afhandlingens problemstilling.

Endvidere inddrages administrativ praksis afsagt af Datatilsynet. De anvendte afgørelser fra Datatilsynet er primært afsagt efter den dagældende persondatalov. Persondataloven og hensynene bag denne er i det væsentligste videreført i forordningen, hvorfor disse afgørelser fortsat er relevante.³³ Datatilsynets afgørelser anvendes hovedsageligt til at analysere, hvorvidt en behandling af personoplysninger er i overensstemmelse med persondataretten.

Afhandlingen vil endvidere inddrage retslitteratur. I og med retslitteratur mangler legitimitet, udgør dette ikke en retskilde, som kan binde domstolene. Retslitteratur kan imidlertid inddrages som argumentation i kombination med retskilder.³⁴ I nærværende afhandling anvendes retslitteratur til at underbygge forståelsen af retstilstanden.

Nærværende afhandling behandler en specifik og aktuel problemstilling, som endnu ikke er behandlet indgående, hverken i retspraksis eller retslitteraturen. Det er i særdeleshed det persondataretlige aspekt, som ikke ses nærmere undersøgt. Dette har dermed en naturlig indflydelse på omfanget af tilgængelig retspraksis og retslitteratur.

1.5 Struktur

Nærværende afhandling består af 6 kapitler. Kapitlernes indhold gennemgås i det følgende:

Kapitel 1 udgør afhandlingens indledende del. Heraf fremgår en introduktion til afhandlingens emne og problemstilling, baggrunden for emnevalget, afgrænsning af emnet, metode og retskilder.

Kapitel 2 beskriver relevante begreber og regelsæt, som er af betydning for analysen af afhandlingens problemstilling. Herunder behandles den grundlæggende rettighed, privatlivets fred, som danner grundlag for retten til beskyttelse af personoplysninger. Herefter behandles forordningen. I denne sammenhæng redegøres for forordningens hensyn og formål samt

³² Munk-Hansen, Carsten, 2012, s. 305.

³³ Betænkning nr. 1565, s. 15.

³⁴ Munk-Hansen, Carsten, 2012, s. 346.

anvendelsesområde. Dernæst beskrives relevante persondataretlige definitioner. Endvidere behandles de persondataretlige behandlingsprincipper samt det retlige grundlag for behandlingen af personoplysninger. Afslutningsvist redegøres for øvrig relevant lovgivning, herunder logningsbekendtgørelsen samt retsplejeloven.

Kapitel 3 udgør afhandlingens analyse. Indledningsvist beskrives udvalgt retspraksis som anvendes gennemgående i analysen. Herefter analyseres afhandlingens problemstilling ved inddragelse af henholdsvis forordningen, databeskyttelsesloven, logningsbekendtgørelsen og e-databeskyttelsesdirektivet. Desuden inddrages dansk retspraksis, EU-retspraksis samt administrativ praksis som fortolkningsbidrag.

Kapitel 4 besvarer afhandlingens problemstilling med en samlet konklusion.

Kapitel 5 perspektiverer afhandlingens problemstilling til henholdsvis norsk og finsk retspraksis.

Kapitel 2

2.1 Retten til beskyttelse af personoplysninger

Beskyttelse af personoplysninger udgør en del af retten til privatlivets fred.³⁵

Retten til privatlivets fred kan spores tilbage til 1948, hvor FN's generalforsamling vedtog Verdenserklæringen om Menneskerettigheder. I denne erklæring bestemmer artikel 12, at *"[i]ngen må være genstand for vilkårlig indblanding i private forhold, familie, hjem eller korrespondance, ej heller for angreb på ære og omdømme."*

I 1950 vedtog Europarådet Den Europæiske Menneskerettighedskonvention (herefter EMRK). Denne konvention har til formål at beskytte menneskerettigheder og grundlæggende frihedsrettigheder. I konventionens artikel 8 beskyttes privatlivets fred tilsvarende.

I EU beskyttes retten til privatlivets fred tillige i Den Europæiske Unions Charter om Grundlæggende Rettigheder (herefter charteret) artikel 7. Endvidere nyder personoplysninger en særlig beskyttelse i charterets artikel 8, stk. 1, hvorefter *"[e]nhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende"*. Efter charterets artikel 8, stk. 2 skal personoplysninger behandles *"... rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag."* Desuden nyder personoplysninger denne særlige beskyttelse i TEUF artikel 16, stk. 1.

³⁵ Trzaskowski, Jan, 2017, s. 102.

Retten til privatlivs fred er i Danmark lovfæstet i Grundlovens § 72. Denne bestemmelse har været en del af Grundloven siden 1849.³⁶

Formålet med at udstede reglerne vedrørende beskyttelse af personoplysninger bidrager således til at sikre den grundlæggende rettighed til privatlivets fred.³⁷

2.2 Databeskyttelsesforordningen

I januar 2012 fremsatte Europa Kommissionen "Forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)". Forslagets formål var at imødekomme udfordringer i forbindelse med beskyttelse af personoplysninger. Disse udfordringer var opstået i takt med den hurtige teknologiske udvikling, særligt på grund af stigningen i mængden af dataindsamling og -deling.³⁸ Lovforslaget blev vedtaget den 14. april 2016, hvorefter forordningen fandt anvendelse fra den 25. maj 2018.³⁹

I forordningen er der fastsat mulighed for at medlemsstaterne kan vedtage national lovgivning, som supplerer og præciserer forordningens bestemmelser. I Danmark har dette resulteret i vedtagelsen af databeskyttelsesloven. Databeskyttelsesloven er i det væsentligste en gengivelse af forordningens indhold.⁴⁰

2.2.1 Forordningens hensyn og formål

Forordningens formål er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, herunder navnlig retten til beskyttelse af personoplysninger. Endvidere er forordningens hensigt at sikre fri udveksling af personoplysninger i EU, jf. art. 1, stk. 1.

Forordningen *"har til formål at bidrage til skabelsen af et område med frihed, sikkerhed og retfærdighed samt en økonomisk union og til økonomiske og sociale fremskridt, styrkelse af og konvergens mellem økonomierne inden for det indre marked og fysiske personers velfærd."*⁴¹

Det er menneskets rettigheder, som bør være i fokus ved behandling af personoplysninger. Dog er beskyttelse af personoplysninger ikke en absolut ret, men derimod en rettighed, der skal afvejes op imod samfundsinteresser og øvrige grundlæggende rettigheder.⁴²

Den kraftige vækst i den teknologiske udvikling har medført et stigende omfang af indsamling og deling af personoplysninger. Forordningen tager hensyn til denne stigende udvikling og

³⁶ Christensen, Jens Peter, m.fl., 2012, s. 287.

³⁷ Trzaskowski, Jan, 2017, s. 101.

³⁸ Forslag til databeskyttelsesforordningen, 2012, s. 1.

³⁹ Betænkning nr. 1565, s. 9.

⁴⁰ Lovforslag nr. 68, pkt. 1.3.

⁴¹ Forordningen, præambelbetragtning nr. 2.

⁴² Forordningen, præambelbetragtning nr. 4.

anfører, at en sådan udvikling kræver en stærk og sammenhængende databeskyttelsesramme i EU. Dette indebærer et behov for effektiv håndhævelse for at skabe tillid mellem fysiske personer, erhvervsdrivende og offentlige myndigheder.⁴³ For at sikre et ensartet beskyttelsesniveau skal behandling af personoplysninger ske ensartet og konsekvent i EU.⁴⁴ For netop at sikre denne ensartethed og således hindre forskelle er der behov for en forordning, der sikrer retssikkerhed og gennemsigtighed.⁴⁵ Desuden er forordningen udfærdiget teknologineutralt, således at fysiske personer opnår persondataretlig beskyttelse uanset den teknologiske innovation.⁴⁶

De principper, som forordningen bygger på, er oplistet i præambelbetragtningens nr. 39. I forordningens artikel 5, stk. 1, litra a-f er disse principper lovfæstet. Dette tydeliggør vigtigheden af, at de generelle principper skal tages i betragtning i forbindelse med behandling af personoplysninger. Disse principper behandles nærmere i afsnit 2.2.4 i nærværende afhandling.

2.2.2 Forordningens anvendelsesområde

Forordningens materielle anvendelsesområde er fastsat i artikel 2. Forordningen finder anvendelse ved hel eller delvis elektronisk behandling af personoplysninger samt ikke-elektronisk behandling, der indgår i et register.⁴⁷ Anvendelsesområdet begrænses alene af de oplistede undtagelser i artikel 2, stk. 2, litra a-d. Disse undtagelser kan kort oplistes som følgende; aktiviteter uden for EU, aktiviteter vedrørende den fælles udenrigs- og sikkerhedspolitik inden for EU, personlige eller familiemæssige aktiviteter samt kompetente myndigheders behandling af strafbare handlinger med henblik på at beskytte den offentlige sikkerhed.

Forordningens artikel 3 fastsætter det territoriale anvendelsesområde. Det fastsættes i artikel 3, stk.1, at forordningen finder anvendelse på aktiviteter foretaget af en dataansvarlig eller en databehandler, som er etableret inden for EU. Af forordningens artikel 3, stk. 2, litra a og b, fremgår en række tilfælde, hvor det territoriale anvendelsesområde udvides. Udvidelsen omhandler tilfælde, hvor den dataansvarlige eller databehandleren er etableret uden for EU, men hvor den registrerede befinder sig i EU. Litra a bestemmer, at forordningen finder anvendelse, når behandlingen vedrører udbud af varer eller tjenesteydelser til de registrerede, uanset om betaling fra de registrerede er påkrævet. Litra b bestemmer, at forordningen finder anvendelse, hvis der er tale om overvågning af registreredes adfærd, hvis denne adfærd finder sted i EU. Forordningens artikel 3, stk. 2 udtrykker et virkningsprincip. Dette virkningsprincip

⁴³ Forordningen, præambelbetragtning nr. 7.

⁴⁴ Forordningen, præambelbetragtning nr. 10.

⁴⁵ Forordningen, præambelbetragtning nr. 13.

⁴⁶ Forordningen, præambelbetragtning nr. 15.

⁴⁷ Begrebet "elektronisk behandling" skal forstås på samme måde som begrebet "automatisk behandling", Lovforslag nr. 68, pkt. 2.1.2.

medfører, at forordningen skal finde anvendelse på behandling, der vedrører fysiske personer, når disse befinder sig inden for EU.⁴⁸

2.2.3 Persondataretlige definitioner

Forordningens artikel 4 indeholder 26 legaldefinitioner, som er centrale for forståelsen af forordningen.⁴⁹ I det følgende behandles udvalgte legaldefinitioner, som findes at være relevante for nærværende afhandling.

2.2.3.1 Personoplysning

I forordningens artikel 4, nr. 1 defineres en personoplysning, som følger:

”Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet”

Ved en personoplysning forstås således enhver form for information, som kan henføres til én bestemt fysisk person. Der kan dermed ikke opnås ret til databeskyttelse, hvis der alene foreligger oplysninger om en gruppe af personer.⁵⁰ Definitionen af personoplysninger vedrører alene fysiske personer, hvorfor oplysninger om virksomheder ikke betragtes som personoplysninger.⁵¹

For at afgøre hvorvidt en fysisk person er identificerbar, bør alle midler, som med rimelighed kan tænkes anvendt af en dataansvarlig eller andre, tages i betragtning, til at identificere den fysiske person direkte eller indirekte.⁵²

Forordningen sonderer mellem, om en oplysning er en følsom personoplysning eller en ikke-følsom personoplysning. Forordningen opregner i artikel 9 en udtømmende liste over hvilke personoplysninger, der betragtes som værende følsomme oplysninger. De følsomme personoplysninger i henhold til artikel 9 er oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometrisk data med henblik på entydig identifikation, helbredsmæssige oplysninger samt

⁴⁸ Betænkning nr. 1565, s. 36.

⁴⁹ Blume, Peter, 2018, s. 68.

⁵⁰ Blume, Peter, 2018 s. 69.

⁵¹ Trzaskowski, Jan, 2017, s. 112.

⁵² Forordningen, præambelbetragtning nr. 26.

oplysninger om seksuelle forhold eller orientering. Personoplysninger, som ikke er omfattet af forordningens artikel 9, betragtes som ikke-følsomme personoplysninger.⁵³

Sammenligning med eksempel

Sammenholdt med ovenstående eksempel vedrørende Rasmus udgør navne- og adresseoplysningerne, som Telenor pålægges at videregive, personoplysninger.

2.2.3.2 Behandling

Forordningen definerer i artikel 4, nr. 2 behandling, som følger:

”Enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse”

Begrebet behandling er således meget bredt defineret, og dækker over enhver aktivitet, der relaterer sig til behandlingen af personoplysninger.⁵⁴

Sammenligning med eksempel

Med udgangspunktet i eksemplet vedrørende Rasmus udgør Telenors videregivelse af navne- og adresseoplysninger til Zentropa Productions en behandling. Ligeledes udgør det en behandling af personoplysninger, når Telenor og Zentropa Productions opbevarer oplysningerne.

2.2.3.3 Dataansvarlig

Forordningen definerer i artikel 4, nr. 7 en dataansvarlig, som følger:

”En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret”

⁵³ Trzaskowski, Jan, 2017, s. 113.

⁵⁴ Trzaskowski, Jan, 2017, s. 113.

Den dataansvarlige bestemmer, med hvilke formål behandlingen må ske samt hvordan oplysningerne må behandles, herunder hvem der må foretage behandlingen.⁵⁵ Den dataansvarlige har således det umiddelbare ansvar for behandlingen.

Sammenligning med eksempel

I relation til eksemplet vedrørende Rasmus er Telenor dataansvarlig for deres behandling af personoplysninger angående deres abonnenter.

2.3.3.4 Databehandler

Forordningen definerer i artikel 4, nr. 8 en databehandler, som følger:

”En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne”

Forholdet mellem en dataansvarlig og en databehandler er nærmere reguleret i forordningens artikel 28. Det er blandt andet et krav, at der skal foreligge en skriftlig databehandleraftale, jf. forordningens artikel 28, stk. 3. Det følger desuden af forordningens artikel 29, at den dataansvarlige skal udstede en instruks, såfremt andre skal behandle oplysninger på dennes vegne. Hvis en databehandler handler uden for instruks, bliver denne dataansvarlig. En databehandler vil desuden blive betragtet som dataansvarlig, hvis databehandleren selv fastsætter til hvilke formål og med hvilke hjælpemidler en behandling foretages, jf. forordningens definition i artikel 4, nr. 7.

Sammenligning med eksempel

På baggrund af eksemplet vedrørende Rasmus behandler MaverickEye oplysninger på vegne af Zentropa Productions. MaverickEye udgør dermed en databehandler.

2.3.3.5 Tredjemand

Forordningen definerer i artikel 4, nr. 10 en tredjemand, som følger:

”En anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger.”

Forordningens definition på en tredjemand er således i overensstemmelse med den almindelige sproglige forståelse.⁵⁶ En tredjemand forstås dermed som en fysisk eller juridisk person, der

⁵⁵ Datatilsynets vejledning om dataansvarlige og databehandlere, 2017, s. 5.

⁵⁶ Andersen, Mads Bryde, 2014.

hverken er dataansvarlig eller databehandler. Desuden indgår en tredjemand ikke i en relation med disse.

Sammenligning med eksempel

I eksemplet med Rasmus foreligger et samarbejde mellem Zentropa Productions og MaverickEye, hvorfor Telenor i denne sammenhæng er udenforstående og dermed en tredjemand.

2.2.4 Principper for behandling af personoplysninger

I forordningens artikel 5 er de grundlæggende principper for behandling af personoplysninger fastsat.

De grundlæggende principper giver ikke i sig selv hjemmel til behandling af personoplysninger, men indeholder en række krav, som enhver behandling skal være i overensstemmelse med. Samtidig er det en forudsætning, at der findes et retligt behandlingsgrundlag i enten forordningens artikel 6, 9 eller 10.⁵⁷

Forordningens artikel 5, stk. 1, litra a-f angiver de seks grundlæggende principper for behandling af personoplysninger. Disse behandlingsprincipper er omgivet af et overordnet princip om ansvarlighed. Dette overordnede princip indebærer, at det er den dataansvarlige, der har ansvaret og bevisbyrden for, at de grundlæggende principper i forordningens artikel 5, stk. 1 overholdes, jf. forordningens artikel 5, stk. 2.⁵⁸

2.2.4.1 Princippet om lovlighed, rimelighed og gennemsigtighed

Af forordningens artikel 5, stk. 1, litra a fremgår, at personoplysninger skal "*behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede*." Dette princip kræver, at god databehandlingsskik skal iagttages.⁵⁹

Kravet om lovlighed indebærer ikke blot, at behandlingen skal være i overensstemmelse med forordningen, men at denne ligeledes skal efterleve anden EU-lovgivning samt national ret. De persondataretlige regler skal således ses i sammenhæng med det samlede retssystem.⁶⁰

Herudover er der et krav om rimelighed, hvilket indebærer, at det ikke er tilstrækkeligt, at behandlingen er lovlig. Dette krav udtrykker, at behandling af personoplysninger skal være i overensstemmelse med de værdier og interesser, som forordningen bygger på.⁶¹

⁵⁷ Trzaskowski, Jan, 2017, s. 118.

⁵⁸ Trzaskowski, Jan, 2017, s. 119.

⁵⁹ Trzaskowski, Jan, 2017, s. 119, Betænkning nr. 1565, s. 92 og Blume, Peter, 2018, s. 85.

⁶⁰ Blume, Peter, 2018, s. 85.

⁶¹ Blume, Peter, 2018, s. 85.

For så vidt angår kravet om gennemsigtighed, er dette nærmere uddybet i forordningens præambelbetragtning nr. 39. Heraf følger, at behandlingen skal være lettilgængelig og letforståelig og at der tillige skal anvendes et klart og enkelt sprog. Kravet indebærer desuden, at den registrerede som udgangspunkt skal have oplyst, hvem der er ansvarlig for behandlingen af personoplysninger og til hvilke formål denne behandling foretages.⁶²

Princippet om lovlighed, rimelighed og gennemsigtig udgør den ydre ramme, som behandlingen af personoplysninger skal foretages indenfor.⁶³ Dette grundlæggende princip udgør dermed en generalklausul.⁶⁴

2.2.4.2 Princippet om formålsbegrænsning

I forordningens artikel 5, stk. 1, litra b fremgår princippet om formålsbegrænsning også kaldet finalité-princippet. Udgangspunktet er i dette princip, at personoplysninger skal *“indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål...”*⁶⁵

Af forordningens præambelbetragtning nr. 39 følger, at de specifikke formål i forhold til behandlingen af personoplysninger, skal være fastlagt, når disse indsamles. Det fremgår af princippet ordlyd, at formålsbegrænsningen alene relaterer sig til selve indsamlingen af personoplysninger og ikke den videre behandling heraf.⁶⁶ I retslitteraturen anføres imidlertid, at princippet må antages at gælde generelt og derfor vedrører alle dele af behandlingen.⁶⁷

For så vidt angår kravet om udtrykkelighed, indebærer dette, at den dataansvarlige skal fastlægge, til hvilket formål den pågældende behandling skal ske. Det vil sige, at formålet skal være veldefineret og præcist angivet således, at der skabes gennemsigtighed for den registrerede i forhold til behandlingen af personoplysningerne. Det er ikke i strid med forordningens principper at behandle personoplysninger til flere formål. I det omfang, der behandles personoplysninger til flere formål, forudsætter dette en større præcision af formålene. Kravet om udtrykkelighed indebærer endvidere, at en dataansvarlig ikke kan indsamle oplysninger med den begrundelse, at disse muligvis ønskes behandlet i fremtiden.⁶⁸

Forordningen kræver desuden, at indsamlingen sker til legitime formål. Med legitime formål menes, at formålene skal være saglige. Ved bedømmelsen af, hvorvidt indsamlingen er sket til legitime formål, skal dette vurderes i forhold til den konkrete virksomhed, der behandler personoplysningerne. Det er i denne forbindelse afgørende, om behandlingen af personoplysninger ligger inden for den konkrete virksomheds kompetenceområde.⁶⁸

⁶² Datatilsynets vejledning: databeskyttelsesforordningen, 2017, s. 10.

⁶³ Trzaskowski, Jan, 2017, s. 119.

⁶⁴ Blume, Peter, 2018, s. 85.

⁶⁵ Trzaskowski, Jan, 2017, s. 121.

⁶⁶ Blume, Peter, 2018, s. 86.

⁶⁷ Trzaskowski, Jan, 2017, s. 121.

⁶⁸ Trzaskowski, Jan, 2017, s. 122.

Som eksempel herpå kan nævnes, at det vil være et legitimt formål, at en læge behandler oplysninger om en fysisk persons helbred, hvorimod behandlingen heraf ikke vil være legitimt for den lokale købmand.

Det sidste krav i princippet om formålsbegrænsning, er kravet om, at personoplysninger ikke må viderebehandles på en måde, der er uforenelig med det oprindelige formål, jf. forordningens artikel 5, stk. 1, litra b. Dette indebærer, at en dataansvarlig ikke af egen drift kan genbruge, videregive eller på anden måde viderebehandle personoplysninger.

Hvorvidt en behandling er uforenelig med det oprindelige formål, beror på en konkret vurdering. I denne vurdering kan den dataansvarlige inddrage en række hensyn oplistet i forordningens artikel 6, stk. 4.⁶⁹ Denne bestemmelse udgør således et supplement til forordningens artikel 5, stk. 1, litra b.⁷⁰

2.2.4.2.1 Viderebehandling

I henhold til forordningens artikel 6, stk. 4 kan der oplistes tre tilfælde, hvor den dataansvarlige lovligt kan viderebehandle personoplysninger til andre formål end det oprindelige.⁷¹ En viderebehandling kan for det første finde sted på baggrund af den registreredes samtykke. Dernæst kan det følge af regler i EU-retten eller national ret, at viderebehandling kan foretages. Desuden kan viderebehandling ske, såfremt den dataansvarliges vurdering af en række hensyn medfører, at en viderebehandling er forenelig med det oprindelige formål. Disse hensyn fremgår af artikel 6, stk. 4, litra a-e og kaldes forenelighedstesten.⁷² De i bestemmelsen angivne hensyn er ikke udtømmende, hvilket fremgår af ordlyden, hvor begrebet "bl.a." anvendes. Disse hensyn er tillige oplistet i forordningens præambelbetragtning nr. 50, 1. led.

2.2.4.2.2 Forenelighedstesten

I medfør af forordningens artikel 6, stk. 4, litra a, bør den dataansvarlige tage hensyn til *"enhver forbindelse mellem det formål, som oplysningerne er indsamlet til, og formålet med den påtænkte viderebehandling"*. Den dataansvarlige bør, i medfør af forordningens artikel 6, stk. 4, litra b, tage hensyn til *"den sammenhæng, hvori oplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige"*. Derudover bør den dataansvarlige, efter forordningens artikel 6, stk. 1, litra c, tage hensyn til *"personoplysningernes art, navnlig om der er tale om behandling af følsomme oplysninger, eller oplysninger vedrørende straffedomme eller lovovertrædelser"*. Med hjemmel i forordningens artikel 6, stk. 4, litra d, bør den dataansvarlige desuden tage hensyn til *"den påtænkte viderebehandlings mulige konsekvenser for de registrerede"*. Endelig bør den dataansvarlige, på baggrund af forordningens artikel 6, stk. 4, litra e, tage hensyn til *"tilstedeværelsen af fornødne garantier, som kan omfatte kryptering eller pseudonymisering"*.

⁶⁹ Trzaskowski, Jan, 2017, s. 122.

⁷⁰ Betænkning nr. 1565, s. 94.

⁷¹ Betænkning nr. 1565 s. 96.

⁷² Betænkning nr. 1565, s. 94.

Den dataansvarlige bør således tage relevante hensyn i betragtning ved afgørelsen af, om en viderebehandling er forenelig med det oprindelige formål, jf. forordningens artikel 6, stk. 4.

Hvis en dataansvarligs viderebehandling findes at være forenelig med det oprindelige formål, vil behandlingen fortsat kunne foretages i medfør af den oprindelige behandlingshjemmel.⁷³

Forordningens artikel 6, stk. 4 er tillige lovfæstet i den danske databeskyttelseslovs § 5, stk. 2. Ifølge Peter Blume er årsagen hertil, at lovgiver har ønsket at tydeliggøre, at der er tale om et behandlingsprincip og ikke en behandlingshjemmel, uanset at placeringen i forordningen antyder dette.⁷⁴

2.2.4.3 Princippet om dataminimering

Det grundlæggende princip om dataminimering i forordningens artikel 5, stk. 1, litra c indebærer, at personoplysninger skal *“være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.”* Dette princip udgør således et proportionalitetsprincip. Personoplysninger bør derfor alene behandles, i det omfang behandlingens formål ikke kan opnås med mindre indgribende midler.⁷⁵

I relation til kravet om tilstrækkelighed og relevans sigtes mod, at typen af oplysninger skal være i overensstemmelse med de formål, der danner grundlag for behandlingen af personoplysninger. Det vil sige, at der ikke må være flere oplysninger til stede end hvad der kræves til opfyldelse af formålet med behandlingen.⁷⁶ Dette princip er med til at sikre, at unødvendig dataophobning ikke finder sted.⁷⁷

Et eksempel på en situation, hvor princippet om dataminimering ikke blev efterlevet er Datatilsynets afgørelse (journalnr. 2018-31-0070) publiceret den 11. februar 2019. I denne afgørelse opbevarede TDC en større mængde data, end de var forpligtet til efter logningsbekendtgørelsen. Mængden af den opbevarede data skyldtes alene opbygningen af TDC's mobilnet. TDC havde ikke selv et formål med at registrere de overskydende oplysninger. Datatilsynet vurderede i denne forbindelse, at TDC's behandling af personoplysninger ikke levede op til princippet om dataminimering.

2.2.4.4 Princippet om rigtighed

Af forordningens artikel 5, stk. 1, litra d følger princippet om rigtighed. Bestemmelsen angiver, at personoplysninger skal *“være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil*

⁷³ Betænkning nr. 1565, s. 96.

⁷⁴ Blume, Peter, 2018, s. 88.

⁷⁵ Betænkning nr. 1565, s. 97.

⁷⁶ Trzaskowski, Jan, 2017, s. 123.

⁷⁷ Blume, Peter, 2018, s. 91.

de behandles, straks slettes eller berigtiges.” Formålet med dette princip er, at de opbevarede personoplysninger til enhver tid er korrekte og dermed sikrer datakvalitet.⁷⁸

2.2.4.5 Princippet om opbevaringsbegrænsning

I forordningens artikel 5, stk. 1, litra e, fremgår princippet om opbevaringsbegrænsning, hvorefter personoplysninger skal *“opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles...”*.

Princippet indebærer, at den dataansvarlige skal slette eller anonymisere personoplysninger, når personoplysningerne ikke længere er nødvendige til opfyldelse af den dataansvarliges formål.⁷⁹ Dette medfører, at den dataansvarlige bør indføre slettefrister, hvormed det sikres, at oplysningerne ikke opbevares i længere tid end nødvendigt, jf. præambelbetragtning nr. 39.⁸⁰ Formålet med princippet er at sikre, at der ikke sker en unødvendig dataophobning.⁸¹

Dette princip har tæt sammenhæng med behandlingsprincipperne vedrørende dataminimering og formålsbegrænsning.⁸²

2.2.4.6 Princippet om integritet og fortrolighed

Efter forordningens artikel 5, stk. 1, litra f, skal personoplysninger *“behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.”*

Bestemmelsen er således et udtryk for, at der gælder et grundlæggende princip om behandlingssikkerhed.⁸³

2.2.5 Behandling af personoplysninger

De grundlæggende principper, som nævnt i afsnit 2.2.4, giver ikke i sig selv hjemmel til behandling af personoplysninger. Enhver behandling af personoplysninger skal støttes på et retligt behandlingsgrundlag. Den dataansvarlige skal således have hjemmel i forordningen til at behandle de pågældende personoplysninger.⁸⁴ Uanset at der foreligger et behandlingsgrundlag, vil behandlingen fortsat være i strid med forordningen, såfremt de grundlæggende behandlingsprincipper ikke er opfyldt.

⁷⁸ Blume, Peter, 2018, s. 92.

⁷⁹ Datatilsynets vejledning: databeskyttelsesforordningen, 2017, s. 11.

⁸⁰ Betænkning nr. 1565, s. 100.

⁸¹ Trzaskowski, Jan, 2017, s. 126.

⁸² Trzaskowski, Jan, 2017, s. 126.

⁸³ Betænkning nr. 1565, s. 100.

⁸⁴ Trzaskowski, Jan, 2017, s. 127.

I tilknytning til nærværende afhandling er der overordnet to behandlingsgrundlag, som den dataansvarlige skal iagttage, når personoplysninger videregives. For det første skal den datasansvarlige iagttage, at denne har et retligt behandlingsgrundlag. Derudover skal den dataansvarlige iagttage, at den modtagende dataansvarlige tillige har et retligt grundlag til behandling af de pågældende personoplysninger. Personoplysninger skal behandles lovligt i medfør af forordningens artikel 5, stk. 1, litra a. Dette princip forudsætter, at både den videregivende og den modtagende dataansvarlige har et lovligt behandlingsgrundlag. Det er således ikke tilstrækkeligt, at den videregivende dataansvarlige alene iagttager eget retlige grundlag for behandlingen.

Med henvisning til eksemplet vedrørende Rasmus, er den overførende dataansvarlige Telenor og den modtagende dataansvarlige er Zentropa Productions.

Det retlige grundlag for behandling af personoplysninger har hjemmel i forordningens artikel 6, 9 og 10.

2.2.5.1 Behandling af almindelige personoplysninger

Forordningens artikel 6 er negativt afgrænset og finder anvendelse på behandling af personoplysninger, som ikke er omfattet af forordningens artikel 9 vedrørende følsomme personoplysninger. Oplysninger omfattet af forordningens artikel 6 betegnes som almindelige personoplysninger.⁸⁵

Forordningens artikel 6 fastsætter de generelle regler for en lovlig behandling af personoplysninger. En behandling af almindelige personoplysninger kan kun anses for lovlig, i det omfang ét af forholdene i forordningens artikel 6, stk. 1, litra a-f gør sig gældende.

Gennemgående for forordningens artikel 6 er, at de behandlinger, som den dataansvarlige foretager skal være nødvendige. Hermed udtrykkes forordningens generelle behandlingsprincip om proportionalitet som fastsat i forordningens artikel 5, stk. 1, litra c.

I det følgende behandles alene de behandlingshjemler i artikel 6, stk. 1, som findes relevante for nærværende afhandling.

2.2.5.1.1 Forordningens artikel 6, stk. 1, litra a – samtykke

Hvis den registrerede giver sit samtykke til behandlingen af det pågældende formål, anses behandlingen for lovlig, jf. forordningens artikel 6, stk. 1, litra a. Definitionen af et samtykke er nærmere specificeret i forordningens art. 4, nr. 11, hvorefter et samtykke skal være frivilligt, specifikt, informeret og utvetydigt.

⁸⁵ Blume, Peter, 2018, s. 95 og Trzaskowski, Jan, 2017, s. 131.

For at afgøre om der foreligger et gyldigt samtykke, skal betingelserne i forordningens artikel 7 være opfyldt. Heraf fremgår blandt andet, at den dataansvarlige skal kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger, jf. forordningens artikel 7, stk. 1. Derudover skal den registrerede oplyses om muligheden for at trække sit samtykke tilbage inden et sådant afgives, jf. forordningens artikel 7, stk. 3.

2.2.5.1.2 Forordningens artikel 6, stk. 1, litra b - opfyldelse af en kontrakt

Efter forordningens artikel 6, stk. 1, litra b kan den dataansvarlige behandle personoplysninger om den registrerede, såfremt behandlingen sker til opfyldelsen af en kontrakt, som den registrerede er part i.

2.2.5.1.3 Forordningens artikel 6, stk. 1, litra c – retlig forpligtelse

I medfør af forordningens artikel 6, stk. 1, litra c kan den dataansvarlige behandle personoplysninger, hvis behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige. Ved en retlig forpligtelse forstås en forpligtelse som følger af blandt andet loven, internationale regler samt afgørelser.⁸⁶

Bestemmelsens anvendelsesområde er yderligere præciseret i forordningens artikel 6, stk. 3. Heraf følger, at den retlige forpligtelse kan udspringe på baggrund af henholdsvis EU-retten eller den nationale lovgivning, som den dataansvarlige er underlagt.

2.2.5.1.4 Forordningens artikel 6, stk. 1, litra f – interesseafvejningsreglen

I det omfang et retligt behandlingsgrundlag ikke kan findes i forordningens artikel 6, stk. 1, litra a-e kan forordningens artikel 6, stk. 1, litra f overvejes.⁸⁷ Herefter er det muligt at foretage en lovlig behandling, hvis behandlingen er nødvendig for, at den dataansvarlige eller tredjemand kan forfølge en legitim interesse. Den legitime interesse skal imidlertid afvejes overfor hensynet til den registreredes interesser, grundlæggende rettigheder samt frihedsrettigheder, jf. forordningens, artikel 6, stk. 1, litra f. Denne bestemmelse er udtryk for en interesseafvejningsregel.⁸⁸ Den dataansvarlige skal således vurdere, hvorvidt den registreredes interesser overstiger de interesser, som ønskes forfulgt med den pågældende behandling.⁸⁹

Hvad der skal forstås ved en legitim interesse, beror på en konkret vurdering, herunder om den registrerede kan forventes at være bekendt med det formål, hvorunder behandlingen finder sted.⁹⁰

⁸⁶ Trzaskowski, Jan, 2017, s. 132.

⁸⁷ Trzaskowski, Jan, 2017, s. 133.

⁸⁸ Trzaskowski, Jan, 2017, s. 133.

⁸⁹ Trzaskowski, Jan, 2017s. 134.

⁹⁰ Betænkning nr. 1565, s. 134.

2.2.5.2 Behandling af følsomme personoplysninger

Artikel 9 vedrører behandling af følsomme personoplysninger. Følsomme personoplysninger er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, jf. artikel 9, stk. 1. De oplyste personoplysninger i bestemmelsen er udtømmende.⁹¹ Behandlingen af disse oplysninger er som udgangspunkt forbudt. I artikel 9, stk. 2, litra a-j er oplyst en række undtagelser, hvorefter behandling af følsomme personoplysninger er lovlig. Nedenfor behandles alene behandlingshjemler, som findes relevante for nærværende afhandling.

2.2.5.2.1 Forordningens artikel 9, stk. 2, litra a - udtrykkeligt samtykke

Efter forordningens artikel 9, stk. 2, litra a, kan personoplysninger behandles af en dataansvarlig, hvis den registrerede har givet sit udtrykkelige samtykke til behandlingen.

Følsomme personoplysninger kan dermed, ligesom almindelige personoplysninger, behandles på baggrund af den registreredes samtykke. Dog er det ikke et krav ved behandling af almindelige personoplysninger, at samtykket skal være udtrykkeligt. Det udtrykkelige samtykke skal imidlertid ikke anses for et skærpet krav til et gyldigt samtykke. Dette kommer særligt til udtryk i forordningens artikel 7, vedrørende betingelserne til et gyldigt samtykke, da denne bestemmelse ikke sonder imellem, hvorvidt et samtykke er udtrykkeligt eller ej. Begrebet "udtrykkeligt" understreger blot vigtigheden af, at der ikke må være tvivl om, at der foreligger et samtykke.⁹²

Betingelserne for et samtykke i forordningens artikel 6, stk. 1, litra a og det udtrykkelige samtykke i forordningens artikel 9, stk. 2, litra a er således sammenfaldende. Der kan i den forbindelse henvises til afsnit 2.2.5.1.1 vedrørende samtykke ved behandling af almindelige personoplysninger.

2.2.5.2.2 Forordningens artikel 9, stk. 2, litra f - retskrav

I medfør af forordningens artikel 9, stk. 2, litra f kan personoplysninger behandles, hvis det er nødvendigt for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Dette retlige grundlag for behandling af følsomme personoplysninger finder anvendelse, uanset om behandlingen foretages i den registreredes eller i den dataansvarliges interesse.⁹³ Forordningens artikel 9, stk. 2, litra f omfatter tillige tilfælde, hvor behandling af personoplysninger er nødvendigt for at afgøre, om en tredjemand kan gøre et retskrav gældende.⁹⁴

⁹¹ Blume, Peter, 2018, s. 96.

⁹² Betænkning nr. 1565 s. 210.

⁹³ Trzaskowski, Jan, 2017, s. 136.

⁹⁴ Trzaskowski, Jan, 2017, s. 136.

Af forordningens præambelbetragtning nr. 52 fremgår, at behandling af følsomme oplysninger efter denne bestemmelse kan foretages, uanset om behandlingen sker i forbindelse med anlæg af en retssag.

2.2.5.2.3 Forordningens artikel 9, stk. 2, litra g - væsentlige samfundsinteresser

Følsomme personoplysninger kan behandles i det omfang, det er nødvendigt af hensyn til væsentlige samfundsinteresser på grundlag af national eller EU-lovgivningen. Efter bestemmelsen skal denne lovgivning stå i et rimeligt forhold til de mål, der forfølges. Bestemmelsen er dermed også et udtryk for et proportionalitetsprincip. Efter betænkningen skal dette proportionalitetsprincip forstås i overensstemmelse med forordningens artikel 5, stk. 1, litra c vedrørende dataminimering.⁹⁵

Ifølge forordningens præambelbetragtning nr. 52, sigter denne bestemmelse navnlig mod “... *behandling af personoplysninger inden for ansættelsesret, socialret, herunder pensioner og med henblik på sundhedssikkerhed, overvågning og varsling, forebyggelse eller kontrol af overførbare sygdomme og andre alvorlige trusler mod sundheden.*”

2.2.5.3 Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser

Artikel 10 angår behandling af personoplysninger vedrørende straffedomme og lovovertrædelser. Denne type af personoplysninger er ikke oplistet i forordningens artikel 9, hvorfor disse personoplysninger ikke betragtes som følsomme personoplysninger. Derimod er udgangspunktet, at personoplysninger vedrørende straffedomme og lovovertrædelser udgør almindelige personoplysninger. Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser er dog underlagt skærpede behandlingsregler i medfør af forordningens artikel 10. Behandlingen må herefter alene ske, under kontrol af en offentlig myndighed eller med hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for den registreredes frihedsrettigheder. I dansk ret er der hjemmel til en sådan behandling i databeskyttelseslovens §§ 8-10, hvor databeskyttelseslovens § 8 er interessant for nærværende afhandling.

I hvilket omfang private må behandle oplysninger om strafbare forhold, er behandlet i databeskyttelseslovens § 8, stk. 3. Heraf fremgår, at private må behandle oplysninger om strafbare forhold, hvis der er givet et udtrykkeligt samtykke hertil. Herudover kan behandlingen foretages, hvis den er nødvendig for varetægelse af en berettiget interesse og denne interesse overstiger hensynet til den person, som oplysningerne vedrører.

I det omfang oplysninger om strafbare forhold ønskes videregivet, følger det af databeskyttelseslovens § 8, stk. 4, 1. led, at dette kun må ske, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Dette er altså i overensstemmelse med, hvad der gælder for

⁹⁵ Betænkning nr. 1565 s. 218.

behandling af følsomme oplysninger i henhold til forordningens artikel 9, stk. 2, litra a. Videregivelse af denne type af oplysninger kan dog også ske uden samtykke fra den registrerede, hvis det er for varetægelse af offentlige eller private interesser, som klart overstiger hensynet til hemmeligholdelse af oplysningerne, jf. databeskyttelseslovens § 8, stk. 4, 2. led.

Desuden fremgår det af databeskyttelseslovens § 8, stk. 5, at behandling af oplysninger om strafbare forhold kan ske, hvis betingelserne i databeskyttelseslovens § 7 er opfyldt. Databeskyttelseslovens § 7 henviser til forordningens artikel 9, som tillader behandling af følsomme oplysninger, hvis behandlingen kan omfattes af en af behandlingshjemlerne i forordningens artikel 9, stk. 2, a-j. Databeskyttelsesloven § 8, stk. 5 leder således til samme behandlingsgrundlag, som forekommer ved behandling af følsomme personoplysninger.

2.3 Øvrig relevant lovgivning

Udover forordningen og databeskyttelsesloven er det tillige relevant at præsentere en række andre regelsæt, som vil blive inddraget ved behandling af problemstillingen i nærværende afhandling.

Med udgangspunkt i eksemplet vedrørende Rasmus, kan det tillige illustreres, at andre regelsæt er af betydning for afhandlingens fokusområde.

I eksemplet med Rasmus anvender Zentropa Productions tredjemandsedition under isoleret bevisoptagelse med henblik på at få udleveret personoplysningerne, som kan identificere den fysiske person bag IP-adressen. Hjemlen hertil findes i retsplejeloven. Endvidere opbevarer Telenor personoplysningerne, som kan knyttes til den pågældende IP-adresse. Der er blandt andet hjemmel til denne opbevaring i logningsbekendtgørelsen.

2.3.1 Retsplejeloven

Retsplejeloven indeholder i dennes tredje bog regler om civile retssager. Ved en civilretlig sag kan to eller flere parter få deres tvist afgjort ved domstolen. Der er som udgangspunkt ingen begrænsninger for, hvad en civil sag kan omhandle. Ofte vil en civil sag imidlertid omhandle krav om en økonomisk kompensation.⁹⁶ De ophavsretlige krænkelse udgør i nærværende afhandling civilretlige krav.

Til illustration af et civilretlig krav kan nævnes eksemplet vedrørende Rasmus. Rettighedshaveren, Zentropa Productions, gør den mulige krænkelse gældende over for Rasmus. Rettighedshaveren ønsker at opnå en økonomisk kompensation fra Rasmus som følge af krænkelsen. Der er dermed tale om et civilretligt krav.

⁹⁶ Danmarks Domstole, civil sag.

Retsplejeloven indeholder i dennes tredje bog regler om isoleret bevisoptagelse og tredjemandsedition, som er særligt relevante for nærværende afhandling.

I retsplejelovens § 343, stk. 1 findes en bestemmelse vedrørende isoleret bevisoptagelse i civilretlige sager. Herefter kan retten tillade ”... *at der optages bevis, selv om dette ikke sker til brug for en verserende retssag...*”. I forbindelse med en isoleret bevisoptagelse kan der anmodes om tredjemandsedition efter retsplejelovens § 299, stk. 1.

I henhold til retsplejelovens § 299, stk. 1 kan retten, i civilretlige sager, efter begæring pålægge en tredjemand at udlevere dokumenter, som har betydning for sagen. Dette gælder dog som udgangspunkt ikke, såfremt der vil fremkomme oplysninger, som pågældende ville være udelukket eller fritaget for at afgive forklaring om som vidne.

I relation til eksemplet med Rasmus er det i medfør af disse bestemmelser, at Zentropa Productions anmoder retten om at pålægge Telenor at videregive personoplysningerne. Retsplejelovens regler om isoleret bevisoptagelse § 343 og tredjemandsedition § 299 anvendes, da der endnu ikke er anlagt en retssag, og da Telenor er udenforstående i relation til retskravet.

2.3.2 Logningsbekendtgørelsen

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

Formålet med logningsbekendtgørelsen er, at “*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*”, jf. logningsbekendtgørelsens § 1, stk. 1. Logningsbekendtgørelsen pålægger således en registrerings- og opbevaringspligt af visse oplysninger. Udbydere af elektronisk kommunikationsnet eller tjenester skal blandt andet registrere navn og adresse på den abonnent eller registrerede bruger, hvortil en IP-adresse er tilknyttet på kommunikationstidspunktet, jf. logningsbekendtgørelsens § 5, stk. 1, nr. 3. Oplysningerne skal opbevares i 1 år, jf. logningsbekendtgørelsens § 9. Denne opbevaringsperiode er ligeledes fastslået i retsplejelovens § 786, stk. 4.

I relation til eksemplet med Rasmus er Telenor forpligtet til at registrere og opbevare personoplysninger på deres abonnenter i henhold til logningsbekendtgørelsen.

2.3.2.1 Logningsdirektivet (direktiv 2006/24/EF)

Logningsbekendtgørelsen gennemfører dele af logningsdirektivet. Formålet med dette direktiv er at harmonisere lovgivningen om lagring af visse data blandt udbydere af offentligt

tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet med henblik på at sikre tilgængeligheden af disse data i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet som defineret af de enkelte medlemsstater i deres nationale lovgivning, jf. logningsdirektivets artikel 1. Dette direktiv er imidlertid kendt ugyldigt som følge af Digital Rights Ireland Ltd (C-293/12). I denne afgørelse blev det fastslået, at logningsdirektivet udgjorde et indgreb i de grundlæggende rettigheder vedrørende retten til privatliv og beskyttelse af personoplysninger, da logning i henhold til direktivet ikke fandtes proportional, jf. præmis 65 og 69.

2.3.2.2 E-databeskyttelsesdirektivet (direktiv 2002/58/EF)

Logningsdirektivet udgør et supplement til e-databeskyttelsesdirektivet. Formålet med e-databeskyttelsesdirektivet er defineret i artikel 1, stk. 1, som *“tager sigte på en harmonisering af medlemsstaternes bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig privatlivets fred i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor...”* For at opnå et ensartet niveau i beskyttelsen supplerer og specificerer e-databeskyttelsesdirektivets bestemmelser persondatadirektivet, jf. e-databeskyttelsesdirektivets artikel 1, stk. 2. Persondatadirektivet ses i det væsentligste videreført i forordningen.⁹⁷

I e-databeskyttelsesdirektivet er de relevante bestemmelser for nærværende afhandling artikel 6 vedrørende trafikdata og artikel 15 vedrørende anvendelsesområdet for visse bestemmelser i persondatadirektivet.

I henhold til artikel 6, stk. 1 skal trafikdata vedrørende abonnenter og brugere lagres af udbyderne af et offentligt kommunikationsnet eller en offentlig tilgængelig elektronisk kommunikationstjeneste. Trafikdata skal herefter slettes eller anonymiseres, når disse data ikke længere er nødvendige for fremføringen af kommunikationen. Behandling af trafikdata med henblik på debitering og afregning er dog tilladt, jf. artikel 6, stk. 2. Artikel 6 er i dansk ret implementeret i udbudsbekendtgørelsens § 23.

Medlemsstaterne har mulighed for at indskrænke rækkevidden af rettighederne og forpligtelserne i artikel 6 i medfør af artikel 15. Indskrænkningerne som medlemsstaterne kan fastsætte skal være *“... passende og forholdsmæssig[e] i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem...”*, jf. e-databeskyttelsesdirektivets artikel 15, stk. 1.

⁹⁷ Betænkning nr. 1565, s. 15.

Kapitel 3

3.1. Den nuværende retstilstand

I relation til problemstillingen i nærværende afhandling er det essentielt at skabe et overblik over den nuværende retstilstand vedrørende rettighedshaveres mulighed for at få udleveret navne- og adresseoplysninger, som kan tilknyttes IP-adresserne, hvorfra der er sket en ophavsretlig krænkelse.

Retspraksis på området er ikke ensartet. Tendensen har dog været, at retten har pålagt teleudbydere at videregive navne- og adresseoplysninger på deres abonnenter, som kan tilknyttes de pågældende IP-adresser. Dette fremgår blandt andet af kendelsen afsagt af Retten på Frederiksberg den 3. november 2017 (sag nr. BS A-1417/2017), kendelsen afsagt af Retten på Frederiksberg den 16. august 2017 (sag nr. BS K-741/2017), kendelsen afsagt af Retten på Frederiksberg den 10. november 2015 (sag nr. BS E-1984/2015), med videre.⁹⁸

En forholdsvis ny og særlig interessant kendelse er afsagt af Østre Landsret i U.2019.2019 Ø (herefter Østre Landsrets kendelse af den 7. maj 2018). I byretten blev Telenor og Telia pålagt at videregive navne- og adresseoplysninger om deres abonnenter, som rettighedshaverne ønskede at få udleveret som led i forfølgelse af en række ophavsretlige krænkelse. Telenor og Telia valgte herefter at kære byrettens kendelsen. I Østre Landsrets begrundelse og resultat blev det anført, at *“[s]elv om det må antages, at rettighedshaverne ikke uden udlevering af oplysningerne kan forfølge et eventuelt krav direkte over for de abonnenter, hvis internetforbindelse har været anvendt til disse ophavsretskrænkelser, finder landsretten efter en samlet afvejning, at CMS’s interesse [repræsentant for rettighedshaverne] i at få udleveret oplysningerne over for hensynet til de enkelte abonnenters krav på hemmeligholdelse ikke kan begrunde en udlevering af de under sagen omhandlede oplysninger i medfør af retsplejelovens § 343, jf. § 299.”* Østre Landsret har således foretaget en interesseafvejning af henholdsvis hensynet til abonnenternes rettigheder over for rettighedshavernes interesse i at få personoplysningerne udleveret. Efter en samlet afvejning fandt landsretten, at abonnenternes beskyttelsesinteresse vægtede højest. Denne kendelse indikerer, at der i denne type af sager foreligger en skærpet adgang for rettighedshaverne til få udleveret oplysninger til civilretlig forfølgning af de ophavsretlige krænkelse.

Med udgangspunkt i ovennævnte eksempel vedrørende Rasmus er retstilstanden efter Østre Landsrets kendelse dermed, at Zentropa Productions alene kan få udleveret de pågældende personoplysninger, hvis en afvejning af parternes modstridende interesser resulterer i, at Zentropa Productions’ interesse vægter højest.

I nærværende analyse behandles de persondataretlige problemstillinger, som kan opstå, når teleudbydere pålægges at videregive navne- og adresseoplysninger tilknyttet IP-adresser til

⁹⁸ Se bilag 2-4 og bilag 10.

rettighedshaveres civilretlige forfølgelse af ophavsretlige krænkelse. I denne forbindelse inddrages relevant retspraksis fra henholdsvis Danmark og EU.

3.2 Retspraksis

I det følgende behandles retspraksis, som anvendes gennemgående i afhandlingen. Nærværende retspraksis er afsagt af såvel danske domstole som EU-domstolen.

3.2.1 Østre Landsrets kendelse af den 7. maj 2018 (U.2019.2019 Ø)

Som allerede berørt i ovennævnte er Østre Landsrets kendelse af den 7. maj 2018 særlig interessant for udviklingen i retspraksis på området. I det følgende vil denne kendelse blive behandlet, således der opnås en forståelse af sagens faktum samt landsrettens begrundelse og resultat.

Østre Landsrets kendelse er afsagt før den 25. maj 2018, hvorfra forordningen fandt anvendelse, jf. forordningens artikel 99, nr. 2. Da de persondataretlige principper er videreført i forordningen, forekommer kendelsen fortsat relevant.⁹⁹

Kendelsen vedrører teleudbyderne Telenor og Telia over for Copyright Management Services Ltd (herefter CMS), som repræsenterer en række rettighedshavere. I byretten blev Telenor og Telia pålagt at videregive navne- og adresseoplysninger tilknyttet bestemte IP-adresser, som led i CMS' forfølgelse af ophavsretlige krænkelse i form af deling af beskyttede filer på internettet. Telenor og Telia blev pålagt at videregive de pågældende oplysninger i medfør af retsplejelovens regler om tredjemandsedition i § 299 og isoleret bevisoptagelse i § 343.

Sagen omhandler mere konkret Telia og Telenors videregivelse af deres abonnenters navne- og adresseoplysninger, som var tilknyttet 4.011 IP-adresser. Der var ikke tvivl om, at Telia og Telenor var i besiddelse af oplysningerne, som CMS krævede udleveret. IP-adresserne havde ifølge CMS været anvendt til ophavsretlige krænkelse, i form af deling af beskyttet materiale på internettet. CMS var kommet i besiddelse af de pågældende IP-adresser fra virksomheden MaverickEye.

CMS var i sagen repræsenteret ved NJORD Law Firm. NJORD Law Firm havde tidligere repræsenteret andre klienter i lignende sager, hvor navne- og adresseoplysninger tilknyttet IP-adresser var blevet udleveret på baggrund af reglerne i retsplejeloven om henholdsvis isoleret bevisoptagelse og tredjemandsedition. Personoplysningerne var efterfølgende blevet anvendt til at fremsende forligsbreve til de identificerede abonnenter.

I denne kendelse modsatte Telia og Telenor sig at videregive de pågældende navne- og adresseoplysninger, som CMS krævede udleveret. Telia og Telenor gjorde blandt andet

⁹⁹ Betænkning nr. 1565, s. 15.

gældende, at disse oplysninger ikke lovligt kunne videregives til brug for forfølgelse af civilretlige krav i form af de ophavsretlige krænkelse. Til støtte herfor blev det anført, at Telia og Telenor alene var i besiddelse af personoplysningerne som følge af opbevaringsforpligtelsen i medfør af logningsbekendtgørelsen. I denne sammenhæng gjorde Telia og Telenor gældende, at videregivelse ville være i strid med persondatarettens finalité-princip, idet forfølgelse af civilretlige krav ikke angives som et formål i lognings-bekendtgørelsen. Det blev i tilknytning hertil anført, at en videregivelse alene kunne foretages, i det omfang det var med henblik på forebyggelse, efterforskning, afsløring og retsfølgning af straffelovsovertrædelser. Yderligere fastslog Telia og Telenor at en sådan videregivelse krævede, en proportionalitetsafvejning mellem CMS's interesser over for abonnenternes grundlæggende rettigheder, herunder retten til privatliv samt beskyttelse af personoplysninger. Desuden fremhævede Telia og Telenor, at de var underlagt en lovhjemlet pligt til at hemmeligholde de loggede personoplysninger. Endvidere gjorde Telia og Telenor gældende, at retsplejelovens regler om isoleret bevisoptagelse og edition ikke var opfyldt, da en videregivelse af de pågældende personoplysninger ikke skete til anlæg af en retssag.

Heroverfor anførte CMS blandt andet, at det hverken af logningsbekendtgørelsen eller dennes forarbejder fremgår, at der ikke kan ske videregivelse til civilretlige krav. Yderligere fremførte CMS, at det ikke på anden måde var muligt at forfølge de ophavsretlige krænkelse uden de pågældende oplysninger. Endvidere anførte CMS, at det hverken kunne udledes af retsplejelovens ordlyd i § 343 om isoleret bevisoptagelse og § 299 om tredjemandsedition, retsplejelovens forarbejder eller retspraksis, at CMS efterfølgende var forpligtet til at anlægge en retssag. Derudover gjorde CMS gældende, at danske domstole tidligere har behandlet editionsbegæring og pålagt teleudbydere at udlevere navne- og adresseoplysninger tilknyttet IP-adresser.

Først og fremmest fandt Østre Landsret, at ordlyden i retsplejelovens § 343, stk. 1 vedrørende isoleret bevisoptagelse forudsætter, at en isoleret bevisoptagelse ”... *sker med henblik på at tilvejebringe bevis til brug for en retssag eller til brug for overvejelser om, hvem en retssag skal anlægges mod.*” Østre Landsret fastslog i forlængelse heraf, at udlevering af oplysningerne bidrog til afklaring af, hvem en senere sag kunne anlægges mod, hvorfor optagelse af et sådant bevis ansås for hensigtsmæssigt.

Dernæst behandlede Østre Landsret spørgsmålet vedrørende tredjemandedition efter retsplejelovens § 299, stk. 1. I denne tilknytning lagde retten til grund, at Telenor og Telia havde rådighed over de pågældende oplysninger og at oplysningerne var nødvendige for at afklare, hvem en sag kunne anlægges mod. Oplysninger var således af betydning for sagen. Østre Landsret tog derefter stilling til teleudbydernes vidnepligt, herunder deres pligt til hemmeligholdelse af abonnenternes personoplysninger og væsentligheden af dette hensyn. Derefter foretog Østre Landsret en afvejning af henholdsvis abonnenternes og rettighedshavernes interesser. Østre Landsret fastslog i denne forbindelse, at selvom rettighedshaverne ikke kunne forfølge sit krav uden udlevering af navne- og adresseoplysningerne, vægtede hensynet til den enkelte abonnents krav på hemmeligholdelse højere, end CMS' interesse i at få udleveret oplysningerne med henblik på at forfølge

krænkelsen civilretligt. I denne forbindelse lagde Østre Landsret endvidere vægt på, at teleudbyderne opbevarede oplysningerne efter reglerne i logningsbekendtgørelsen, som er udstedt i medfør af strafferetsplejen.

Østre Landsrets kendelse fastslår således, at retsplejelovens regler om isoleret bevisoptagelse og tredjemandsedition kan anvendes ved videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser til forfølgelse af civilretlige krav. Afgørende for hvorvidt videregivelse kan ske, er således afvejningen af parternes interesser.

Østre Landsret ændrede herved byrettens kendelse, hvorfor CMS' begæring om tredjemandsedition under den isolerede bevisoptagelse ikke blev taget til følge.

Østre Landsrets kendelse af den 7. maj 2018 er særlig relevant for nærværende afhandling og retstilstanden på området, da kendelsens begrundelse og resultat leder retspraksis i en ny retning.

Det forekommer særligt interessant, at videregivelse nægtes i denne kendelse, når en række tidligere afgørelser har pålagt teleudbydere en sådan videregivelse. I denne sammenhæng kan der blandt andet henvises til kendelsen afsagt af Retten på Frederiksberg den 15. juni 2017 (sag nr. BS A-681/2017), kendelsen afsagt af Retten på Frederiksberg den 11. maj 2016 (sag nr. BS B-2443/2015), kendelsen afsagt af Retten på Frederiksberg den 22. september 2015 (sag nr. BS K-1271/2015), med videre.¹⁰⁰

Begrundelsen og resultatet i Østre Landsrets kendelse af den 7. maj 2018 er gengivet i en dom afsagt af Retten på Frederiksberg den 22. maj 2019 (sag BS-31445/2018-FRB). Østre Landsrets kendelse har således haft indvirkning på retspraksis afsagt efter den 7. maj 2018.

Uanset at videregivelse nægtes i Østre Landsrets kendelse af den 7. maj 2018, er kendelsen ikke udtryk for, at der aldrig kan ske videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser til forfølgelse af civilretlige krav. Østre Landsrets kendelse understreger imidlertid, at der skal foretages en nøje afvejning af parternes interesser og rettigheder.

3.2.2 Tele2/Watson-dommen (C-203/15 og C-698/15)

Denne afgørelse omhandler to sager, som blev behandlet i forening af EU-domstolen. Sagerne opstod som følge af, at logningsdirektivet blev erklæret ugyldigt. Denne afgørelse behandler omfanget af teleudbyderes pligt til logning af data samt myndigheders adgang til disse data.

Den første tvist (C-203/15) vedrører Tele2 Sverige AB (herefter Tele2) over for Post- og telestyrelsen. Tele2 var i medfør af national lovgivning blevet pålagt at lagre sine abonnenters og registrerede brugeres trafikdata. Som følge af logningsdirektivets ugyldighed nægtede Tele2 at lagre yderligere data og slettede allerede lagret data. I denne sammenhæng ophørte Tele2

¹⁰⁰ Se bilag 5-7 og bilag 10.

således med at videregive data. Det blev herefter forelagt EU-domstolen, hvorvidt “...en generel forpligtelse til at lagre trafikdata, som omfatter alle personer, alle elektroniske kommunikationsmidler og alle trafikdata uden forskel, begrænsninger eller undtagelser med henblik på at bekæmpe strafbare lovovertrædelser [...], [er] forenelig med artikel 15, stk. 1, i direktiv 2002/58 [e-databeskyttelsesdirektivet], henset til chartrets artikel 7, artikel 8 og artikel 52, stk. 1”

Den anden tvist (C-698/15) vedrører Tom Watson, Peter Brice og Geoffrey Lewis over for Secretary of State for the Home Department. Sagen blev anlagt med henblik på en prøvelse af national lovgivning vedrørende teleoperatørers lagring og adgang til data ved “... enhver posttjeneste eller enhver telekommunikationstjeneste...”, hvor lagring og adgang kunne ske uden forudgående tilladelse fra en domstol eller uafhængig administrativ myndighed, jf. præmis 53 og 55.

EU-domstolen udtalte sig samlet om de præjudicielle spørgsmål.

For så vidt angår teleudbydernes pligt til logning fandt EU-domstolen; “...at bestemmelsen [i artikel 15, stk. 1 i e-databeskyttelsesdirektivet sammenholdt med charterets artikel 7, artikel 8 og artikel 52, stk. 1] er til hinder for en national lovgivning, [...] der fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere...”.

Vedrørende myndighedernes adgang til sådanne data fastslog EU-domstolen, at adgangen til disse data alene kan tillades ved grov kriminalitet, og at adgang kun bør gives ved forudgående kontrol foretaget af en domstol eller en anden administrativ myndighed.

Det skal bemærkes, at EU-domstolen i denne afgørelse tager stilling til muligheden for at foretage indskrænkninger i medfør af e-databeskyttelsesdirektivets artikel 15. Imidlertid omhandler afgørelsen e-databeskyttelsesdirektivets artikel 5 vedrørende kommunikationshemmeligheden og ikke den for afhandlingen relevante artikel 6 vedrørende sletning og anonymisering af trafikdata. Artikel 15 giver dog mulighed for, at medlemsstaterne i samme omfang kan gøre indskrænkninger i rækkevidden af de rettigheder og forpligtelser, som følger af artikel 6, jf. ordlyden i artikel 15, stk. 1; ” [m]edlemsstaterne kan vedtage retsfor skrifter 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... ” Det er således de samme hensyn, som inddrages ved indskrænkninger af henholdsvis e-databeskyttelsesdirektivets artikel 5 og 6.

3.2.3 Promusicae (C-275/06)

Denne dom vedrører Productores de Música de España (herefter Promusicae) over for Telefónica de España SAU (herefter Teleselskabet). Promusicae fremsatte en begæring om, at

Teleselskabet skulle videregive navne- og adresseoplysninger tilknyttet en række IP-adresser. Teleselskabet nægtede at videregive disse oplysninger.

Anmodningen om den præjudicielle forelæggelse vedrørte fortolkning af henholdsvis tre direktiver; direktiv 2000/31¹⁰¹, 2001/29¹⁰² og 2004/48¹⁰³ samt charteret. I denne sammenhæng fandt EU-domstolen, at det var relevant at inddrage e-databeskyttelsesdirektivet. Særligt undersøges det hvorvidt, direktivets artikel 15 udelukker, at medlemsstaterne kan fastsætte en pligt til at videregive personoplysninger til det formål at sikre en effektiv beskyttelse af ophavsretten ved at anlægge en civil retssag, jf. præmis 46 og 49.

Om det præjudicielle spørgsmål udtalte EU-domstolen i tilknytning til e-databeskyttelsesdirektivet, at direktivet ikke pålægger medlemsstaterne at fastsætte en pligt *“...til at videregive personoplysninger med henblik på at sikre den effektive beskyttelse af ophavsretten under en civil retssag.”* I det omfang, at medlemsstaterne fastsætter en sådan pligt, skal denne fortolkes i overensstemmelse med direktivet og de grundlæggende rettigheder.

Tilsvarende skal det, som i Tele2/Watson-dommen, bemærkes, at denne afgørelse omhandler e-databeskyttelsesdirektivets artikel 5 vedrørende kommunikationshemmeligheden. Som anført ovenfor er det de samme hensyn, oplistet i artikel 15, som inddrages i tilknytning til artikel 6.

3.3 Forordningens genstand og formål

Forordningens genstand og formål er ovenfor fastsat i afsnit 2.2.1, hvorefter forordningen beskytter fysiske personer i forbindelse med behandling af personoplysninger, jf. forordningens artikel 1.

I henhold til afhandlingens problemstilling er det centralt at undersøge, hvorvidt de pågældende oplysninger, som rettighedshaverne ønsker videregivet kan betragtes som en personoplysning og dermed er omfattet af forordningen. Desuden er det relevant at undersøge, om en abonnent udgør en fysisk person.

3.3.1 Personoplysning

Ved en personoplysning forstås, som nævnt i afsnit 2.2.3.1, enhver form for information om en identificerbar fysisk person. I afhandlingen behandles oplysninger om henholdsvis navne,

¹⁰¹ Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»Direktivet om elektronisk handel«).

¹⁰² Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet.

¹⁰³ Europa-Parlamentets og Rådets direktiv 2004/48/EF af april 2004 om håndhævelsen af intellektuelle ejendomsrettigheder.

adresser og IP-adresser. Det fremgår direkte af forordningens artikel 4, stk. 1, at navne- og adresseoplysninger udgør en personoplysning. Interessant er imidlertid, hvorvidt en IP-adresse udgør en personoplysning.

3.3.1.1 IP-adresser som personoplysning

Af forordningens præambelbetragtning nr. 30 fremgår, at fysiske personer kan tilknyttes onlineidentifikationer såsom IP-adresser. Disse kan efterlade spor, som medfører, at de ved kombination med andre oplysninger kan anvendes til identifikation af fysiske personer.¹⁰⁴

Frem til oktober 2016 har det været uklart, hvorvidt en IP-adresse udgør en personoplysning i henhold til persondataretten. Denne usikkerhed blev afklaret ved EU-domstolen i sagen vedrørende Patrick Breyer mod Bundesrepublik Deutschland (C-582/14).

Denne sag behandler, hvorvidt dynamiske IP-adresser kan anses som værende en personoplysning, hvis en tredjemand (i denne sag teleudbyderne) har yderligere information, som kan forbinde IP-adressen med identiteten på den fysiske person bag denne.

Der findes to måder at tildele en IP-adresse på; enten som en dynamisk eller statisk IP-adresse. Er man tildelt en dynamisk IP-adresse, betyder dette, at IP-adressen kan ændre sig med jævne timebaserede intervaller, alt efter hvor ofte teleudbyderen vælger, at dette skal ske, hvorimod en statisk IP-adresse aldrig ændrer sig, jf. præmis 36.

Twisten i sagen omhandler Patrick Breyers søgninger på flere tyske forbundsinstitutioners internetsider. I forbindelse med disse søgninger registrerede den tyske forbundsrepublik alle søgningerne i logfiler. I disse logfiler opbevaredes blandt flere, datoen og tidspunktet for søgningen samt IP-adressen på den computer, hvorfra søgningen blev foretaget. Patrick Breyer anlagde sag, med påstand om, at det var ulovligt at opbevare IP-adressen, såfremt denne opbevaring ikke var nødvendig til at genetablere disse mediers formidling i tilfælde af funktionssvigt.

EU-domstolen nåede i sagen frem til, *"... at en dynamisk internetprotokoladresse, som en udbyder af online-medietjenester registrerer i forbindelse med en søgning foretaget af en person på en internetside, som denne udbyder gør tilgængelig for offentligheden, i forhold til den nævnte udbyder, udgør en personoplysning ... når udbyderen råder over lovlige hjælpemidler, der gør det muligt for denne at få identificeret den registrerede gennem den yderligere viden, som denne persons internetudbyder råder over."*

En dynamisk IP-adresse udgør således en personoplysning, da personen bag denne indirekte kan identificeres, jf. præmis 40. Der vil være tale om indirekte identifikation, da den yderligere viden, som kræves for at identificere brugeren, er i teleudbyderens besiddelse, jf. præmis 30. Det fremgår af sagens præmis 43, at det ikke er påkrævet, *"at alle de oplysninger, der gør det*

¹⁰⁴ Forordningen, præambelbetragtning nr. 30.

muligt at identificere den registrerede, skal befinde sig hos en enkelt person.” Der vil dog ikke være tale om personoplysninger, hvis ”identificeringen af den registrerede er forbudt ved lov eller praktisk ugennemførlig, f.eks. på grund af det forhold, at den vil indebære en større indsats i tid, omkostninger og arbejde, således at risikoen for en identificering i virkeligheden synes ubetydelig.”, jf. præmis 46. Da der findes lovlige veje for udbyderen af online-medietjenester at komme i besiddelse af disse identificerende oplysninger og da disse med rimelighed tænkes bragt i anvendelse, er der tale om personoplysninger, jf. præmis 47-48.

3.3.2 Fysisk person

Forordningen definerer en fysisk person, som en person der direkte eller indirekte kan identificeres, jf. forordningens artikel 4, nr. 1. I nærværende afhandling ønsker rettighedshaverne at komme i besiddelse af personoplysninger vedrørende teleudbydernes abonnenter. I denne sammenhæng forekommer det centralt at undersøge, hvorvidt erhvervsabonnenter er omfattet af forordningen.

Et erhvervsabonnement tilknyttet en juridisk person vil som udgangspunkt ikke være omfattet af forordningen. Dette følger dels af ordlyden af forordningens artikel 1 og dels af forordningens præambelbetragtning nr. 14, hvoraf fremgår: *”[d]enne forordning finder ikke anvendelse på behandling af personoplysninger, der vedrører juridiske personer, navnlig virksomheder, der er etableret som juridiske personer, herunder den juridiske persons navn, form og kontaktoplysninger”*. Det er således afgørende, hvorvidt en fysisk person kan identificeres. Det fremgår af præambelbetragtning nr. 26 til forordningen at, *”[f]or at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende.”* I det tilfælde hvor abonnenten bag IP-adressen er en juridisk person, vil denne således være omfattet af forordningen i det omfang, at en fysisk person med rimelighed kan identificeres i tilknytning hertil. Dette vil eksempelvis være tilfældet, hvis der er tale om en juridisk person, hvor der alene er en enkelt person ansat eller andre rimelige muligheder for identifikation. Hvis der derimod er tale om en større virksomhed, vil en sådan identifikation være vanskeligere at foretage alene ud fra oplysninger om virksomhedens navn og adresse. Kan identifikation af en fysisk person ikke ske, vil forordningen ikke finde anvendelse.

Afgørende, for om forordningen finder anvendelse, er således, om en fysisk person direkte eller indirekte kan identificeres i tilknytning til abonnementet.

3.4 Forordningens anvendelsesområde

Det er relevant at undersøge, hvorvidt teleudbyderes behandling af navne- og adresseoplysninger tilknyttet IP-adresser er omfattet af forordningens anvendelsesområde.

Teleudbyderne er udbydere af elektroniske kommunikationsnet og -tjenester. I denne forbindelse opbevarer teleudbyderne oplysninger om teletrafik. Det må herved forudsættes, at der foretages en elektronisk databehandling, hvorfor behandlingen af personoplysningerne er omfattet af forordningens materielle anvendelsesområde, jf. forordningens artikel 2, stk. 1.

De i afhandlingen omhandlende teleudbydere er endvidere etableret i EU, hvorfor behandlingen af personoplysninger er omfattet af forordningens territoriale anvendelsesområde, jf. forordningens artikel 3, stk. 1.

3.5 Kategorier af personoplysninger

Navne- og adresseoplysninger tilknyttet IP-adresser udgør, som anført i afsnit 3.3.1, personoplysninger. Det er herefter relevant at undersøge, hvilken type af personoplysninger disse udgør.

Forordningen sonder mellem følsomme og almindelige personoplysninger. Følsomme personoplysninger er, som nævnt i afsnit 2.2.5.2, udtømmende oplistet i forordningens artikel 9. I henhold til artikel 9, stk. 1 er der tale om en følsom personoplysning, hvis oplysninger vedrører *”race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering”*. Det kan således udledes af forordningens artikel 9, stk. 2 modsætningsvist, at navne- og adresseoplysninger tilknyttet IP-adresser må betragtes som almindelige personoplysninger. I denne sammenhæng kan der endvidere henvises til kendelsen afsagt af Retten på Frederiksberg den 24. oktober 2017, hvor retten i sin begrundelse og resultat angiver, at abonnentens navn og adresse isoleret set anses for *”... ikke personfølsomme oplysninger.”* og dermed udgør almindelige personoplysninger. Tillige har Datatilsynet i deres afgørelse publiceret den 12. juli 2017 (journalnr. 2016-217-1119) anført, at navne, adresser og IP-adresser som udgangspunkt udgør almindelige ikke-følsomme oplysninger. Det klare udgangspunkt må herefter være, at navne- og adresseoplysninger tilknyttet IP-adresser udgør almindelige personoplysninger.

Der kan dog argumenteres for, at navne- og adresseoplysninger tilknyttet IP-adresser kan være omfattet af forordningens artikel 9 om følsomme personoplysninger eller forordningens artikel 10, som omhandler personoplysninger vedrørende straffedomme og lovovertrædelser.

Navne- og adresseoplysningerne tilknyttet IP-adresser kan betragtes som værende følsomme, når kombinationen af abonnentens identitet og materialets indhold angiver oplysninger af følsom karakter om abonnenten i medfør af forordningens artikel 9, stk. 1. Dette kan eksempelvis være tilfældet, hvis materialet vedrører porno eller indeholder religiøse eller politiske budskaber. Materialets indhold skal således påvise abonnentens seksuelle orientering, religiøse eller politisk overbevisning. Førend oplysningerne kan ændre karakter til følsomme personoplysninger, som følge af materialets indhold, må det antages, at mængden af det

tilgåede materiale skal være betydelig, at karakteren heraf skal være ensartet, samt at materialet skal være tilgået over en længere periode. Dette er begrundet i, at abonnentens personlige standpunkt utvivlsomt skal kunne udledes af materialets indhold, før oplysninger udgør en følsom personoplysning i medfør af forordningens artikel 9, stk. 1.

Endvidere kan det anføres, at kombinationen af abonnentens identitet og en ophavsretlig krænkelse kan udgøre en oplysning om en strafbar handling. Dette kan være tilfældet, når personoplysninger videregives med henblik på at forfølge en ophavsretlig krænkelse. Det ligger dermed indirekte ved videregivelsen af navne- og adresseoplysningerne tilknyttet IP-adresser, at vedkommende formentlig har begået noget strafbart. Dette synspunkt anføres tillige i en afgørelse fra Datatilsynet publiceret den 12. juli 2017 (journalnr. 2016-217-1119), hvor det udtaltes, at en IP-adresse tilknyttet en fysisk person kan udgøre en oplysning om vedkommendes strafbare forhold, når denne kædes sammen med ulovlig download og fildeling.

Det kan således fastslås, at navne- og adresseoplysninger tilknyttet IP-adresser kan ændre karakter fra almindelige personoplysninger til henholdsvis følsomme personoplysninger og oplysninger om strafbare forhold. I henhold til nærværende afhandling kan dette alene ske som følge af en rettighedshavers anmodning om udlevering af navne- og adresseoplysninger, da oplysningerne i forbindelse hermed tilknyttes materialets indhold samt rettigheds-krænkelsen. I denne tilknytning kan der henvises til kendelsen afsagt af Retten på Frederiksberg fra den 14. maj 2012 (sagerne nr. BS Z-439/2012, BS Z-440/2012 og BS Z-441/2012)¹⁰⁵, hvoraf fremgår ”... at indehaverne af IP-adresserne i bilag 1 - 9 på de nævnte tidspunkter har medvirket til tilgængeliggørelse, distribution og kopiering af filmværkerne ”Across the line”, ”Café” og ”Without men”, hvortil rekvirenten har rettighederne.” Det tydeliggøres herved, at teleudbyderen i forbindelse med editionskendelsen bliver gjort bekendt med den påståede ophavsretlige krænkelse samt materialets indhold.

3.6 Behandling af personoplysninger

Førend en behandling af personoplysninger kan finde sted, skal den dataansvarlige have et retligt grundlag for behandlingen af de pågældende oplysninger. Med henvisning til afsnit 3.5 afhænger behandlingshjemlen af den kategori af personoplysning, som behandlingen vedrører.

Med udgangspunkt i eksemplet vedrørende Rasmus foretager teleudbyderen særligt to behandlinger af personoplysninger, som er relevante for nærværende afhandling. Såvel Telenors opbevaring af navne- og adresseoplysninger tilknyttet IP-adresser som videregivelsen til Zentropa Productions udgør en behandling, idet behandlingen af personoplysninger er defineret som enhver aktivitet, herunder opbevaring og videregivelse, jf. forordningens artikel 4, nr. 2. Desuden skal Telenor iagttage, at Zentropa Productions har et lovligt behandlingsgrundlag, som nævnt i afsnit 2.2.5.

¹⁰⁵ Se bilag 9.

Tilsvarende kan der henvises til en række afgørelser fra dansk retspraksis, hvor de samme omstændigheder, som i eksemplet, gør sig gældende. Her kan blandt andet nævnes Østre Landsrets kendelse af den 7. maj 2018, hvor Telenor og Telia opbevarer navne- og adresseoplysninger tilknyttet IP-adresser, som CMS ønsker udleveret. Endvidere kan nævnes afgørelsen afsagt af Retten på Frederiksberg d. 22. maj 2019, hvor YouSee opbevarer navne- og adresseoplysninger tilknyttet IP-adresser, som CMS ønsker udleveret.

Det er derfor relevant at belyse på hvilke persondataretlige grundlag, teleudbydere kan opbevare og videregive personoplysninger.

3.6.1 Behandling af almindelige personoplysninger

Udgangspunktet er, som nævnt i afsnit 3.3.1, at navne- og adresseoplysninger tilknyttet IP-adresser udgør en almindelig personoplysning, hvorfor den specifikke behandlingshjemmel findes i forordningens artikel 6, stk. 1.

Forordningens artikel 6, stk. 1, litra a-f oplister de mulige behandlingshjemler for almindelige personoplysninger, som behandlet i afsnit 2.2.5.1. I det følgende belyses, hvilke behandlingshjemler teleudbyderne benytter i forbindelse med henholdsvis opbevaring og videregivelse af personoplysninger.

3.6.1.1 Teleudbyderes opbevaring af personoplysninger

Teleudbyderes opbevaring af navne- og adresseoplysninger tilknyttet IP-adresser vil altid udgøre en behandling af almindelige personoplysninger.

Teleudbyderne opbevarer navne- og adresseoplysninger tilknyttet IP-adresser dels på grundlag af aftaleforholdet med abonnenten og dels som følge af en retlig forpligtelse. Der er således flere behandlingshjemler, som muliggør teleudbydernes opbevaring af navne- og adresseoplysninger.

Baggrunden for at teleudbyderen er i besiddelse af de pågældende personoplysninger, hviler på et aftaleforhold mellem teleudbyderen og abonnenten. Dette aftaleforhold består i, at teleudbyderen har forpligtet sig til at levere en internetforbindelse til abonnenten. Teleudbyderne opbevarer i denne forbindelse personoplysningerne på baggrund af forordningens artikel 6, stk. 1, litra b. Herefter kan teleudbyderne behandle person-oplysninger om abonnenten, såfremt behandlingen sker til opfyldelse af en kontrakt, som denne er part i. Det er en forudsætning, at behandlingen af personoplysningerne er nødvendig for opfyldelse af kontrakten. I Østre Landsrets kendelse af den 7. maj 2018 udtaler en række teleudbydere, i hvilket omfang opbevaring er nødvendig for at opfylde kontrakten. Telenor oplyser blandt andet, at IP-adresserne gemmes i deres almindelige system i op til 30 dage af hensyn til driften, således Telenor kan foretage fejlretninger. Tilsvarende opbevarer Telia oplysninger i tre uger

med henblik på fejlretning. Endvidere udtaler TDC, at de, til eget brug, gemmer IP-adresserne i mindre end en måned. På baggrund af disse forklaringer lægger landsretten til grund, at teleudbyderne har brug for de loggede data i henholdsvis 30 dage og 3 uger til opfyldelse af egne formål. Opbevaring af navne- og adresseoplysninger tilknyttet IP-adresser kan således opbevares i henholdsvis 30 dage eller tre uger i medfør af forordningens artikel 6, stk. 1, litra b.

Alternativt kan behandlingen støttes på et samtykke fra abonnenten, jf. forordningens artikel 6, stk. 1, litra a. Hvis behandlingen er baseret på et samtykke, vil omfanget af opbevaringen kunne gå videre end, hvad der er nødvendigt i forhold til opfyldelse af kontrakten. Et samtykke kan imidlertid tilbagetrækkes til enhver tid af abonnenten, jf. forordningens artikel 7, stk. 3. Behandlingsgrundlaget er således udtryk for abonnentens vilje, hvorfor et andet behandlingsgrundlag vil være mere stabilt.¹⁰⁶

Opbevaring udover den periode, som er nødvendig for opfyldelse af kontrakten mellem abonnenten og teleudbyderen, kan begrundes i forordningens artikel 6, stk. 1, litra c. Behandlingen kan herefter ske, hvis det er nødvendigt for at overholde en retlig forpligtelse, som påhviler teleudbyderen. En sådan pligt påhviler teleudbydere efter lognings-bekendtgørelsens § 1, stk. 1, som behandles nærmere nedenfor.

3.6.1.2 Teleudbyderes videregivelse af personoplysninger

Teleudbyderne anmodes om at videregive navne- og adresseoplysningerne tilknyttet IP-adresserne til rettighedshaverne. Det er således relevant at belyse, hvorvidt teleudbyderne kan videregive de pågældende oplysninger, særligt om en sådan videregivelse skal ske på baggrund af en editionskendelse.

3.6.1.2.1 Videregivelse ved editionskendelse

I det omfang teleudbydere pålægges at videregive navne- og adresseoplysninger tilknyttet IP-adresser, som følge af en editionskendelse, er teleudbyderene retligt forpligtet hertil. Det retlige grundlag for behandling følger således af artikel 6, stk. 1, litra c, hvorefter behandlingen hviler på en retlig forpligtelse. I nærværende findes den retlige forpligtelse i retsplejelovens § 299, stk. 1 vedrørende tredjemandsedition. I henhold til denne bestemmelse kan retten pålægge en tredjemand, herunder en teleudbyder, at udlevere eller forevise dokumenter af betydning for en civilretlig sag. Umiddelbart findes der således en hjemmel til videregivelse i retsplejeloven. Det er i denne sammenhæng relevant at belyse, hvorvidt de i retspraksis foretagne afvejninger er i overensstemmelse med persondataretten. En særlig relevant problemstilling i tilknytning hertil er, at teleudbyderne opbevarer de pågældende oplysninger som følge af en forpligtelse i henhold til logningsbekendtgørelsen. Denne forpligtelse til at opbevare oplysningerne vil blive behandlet nærmere nedenfor.

¹⁰⁶ Datatilsynets vejledning: samtykke, 2019, s. 15.

3.6.1.2.2 Videregivelse uden editionskendelse

I tilfælde hvor der ikke foreligger en editionskendelse, er det relevant at belyse, på hvilket retligt grundlag en videregivelse kan foretages.

Datatilsynet har i deres afgørelse publiceret den 20. november 2003 (journalnr. 2002-219-0135) udtalt sig om, hvilke persondataretlige behandlingshjemler, som kan være relevante i forbindelse med videregivelse af personoplysninger i sager, hvor der ikke foreligger en editionskendelse.

I denne afgørelse blev Antipiratgruppen af Datatilsynet pålagt at udarbejde en redegørelse om deres indhentelse af personoplysninger fra teleudbydere uden forudgående retskendelse. Antipiratgruppen ønskede i den forbindelse, at Datatilsynet tog stilling til, hvorvidt videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser var i strid med persondataretten, når der ikke forelå en retskendelse.

Datatilsynet udtaler i denne afgørelse, at videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser i første omgang skal ske på baggrund af en vurdering foretaget af den dataansvarlige i medfør af persondatalovens § 6, stk. 1, nr. 1-7. Den dagældende persondatalovs regel i § 6, stk. 1 svarer i det væsentligste til forordningens artikel 6, stk. 1, som omhandler det retlige grundlag for behandling af almindelige personoplysninger.¹⁰⁷

Indledningsvist ligger Datatilsynet til grund, at der ikke synes at foreligge et samtykke til videregivelse af personoplysningerne fra abonnenten, jf. persondatalovens § 6, stk. 1, nr. 1, som i det væsentligste svarer til forordningens artikel 6, stk. 1, litra a.¹⁰⁸ Det må på baggrund heraf udledes, at en abonnent kan give samtykke til videregivelse af sine navne- og adresseoplysninger tilknyttet IP-adresser i medfør af forordningens artikel 6, stk. 1, litra a.

Dernæst tager Datatilsynet stilling til, hvorvidt videregivelse kan ske som følge af en retlig forpligtelse. Hertil udtaler Datatilsynet, at der ikke synes at foreligge en retlig pligt for teleudbyderne til at videregive personoplysningerne, jf. persondatalovens § 6, stk. 1, nr. 3, som i det væsentligste svarer til forordningens artikel 6, stk. 1, litra c.¹⁰⁹ Dette bemærker Datatilsynet også indledningsvist i deres udtalelse, hvor det anføres, at persondatalovens regler er ”... *må og kan-regler*.” forstået på den måde, at reglerne ikke pålægger teleudbyderne at videregive personoplysningerne til Antipiratgruppen. Dette er også i overensstemmelse med retspraksis fra EU. EU-domstolen konkluderede i *Promusicae* (C-275/06), at e-databeskyttelsesdirektivet ikke udelukker, at medlemsstaterne kan fastsætte en pligt til at videregive personoplysninger under en civilretlig sag. Medlemsstaterne er imidlertid ikke tvunget til at fastsætte en sådan pligt, jf. præmis 54-55. Der foreligger hermed ikke en almindelig pligt for teleudbyderne til at videregive personoplysningerne til forfølgelse af civilretlige krav i henhold til EU-retten. Dette synspunkt er også tiltrådt i *Bonnier Audio AB*

¹⁰⁷ Betænkning nr. 1565, s. 15.

¹⁰⁸ Betænkning nr. 1565, s. 126.

¹⁰⁹ Betænkning nr. 1565, s. 129.

(C-461/10) i præmis 55. Endvidere er synspunktet fremhævet i dansk ret. I Østre Landsrets kendelse af den 7. maj 2018 udtalte landsretten, at e-databeskyttelsesdirektivet ikke forhindrer nationale regler om videregivelse.

Datatilsynet finder afslutningsvis, at videregivelse formentlig kan ske, såfremt dette er i overensstemmelse med persondatalovens § 6, stk. 1, nr. 7, som i det væsentligste svarer til forordningens artikel 6, stk. 1, litra f.¹¹⁰ Som ovenfor omtalt i afsnit 2.2.5.1.4 er forordningens artikel 6, stk. 1, litra f udtryk for en interesseafvejningsregel. Herved forstås, at en behandling kan foretages, hvis det er nødvendigt for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse og at denne interesse ikke overstiger hensynet til den registreredes rettigheder eller grundlæggende frihedsrettigheder. Datatilsynet vurderer i den forbindelse, at Antipiratgruppen har en legitim interesse i at få udleveret oplysningerne, således at Antipiratgruppen har mulighed for at gøre den ophavsretlige krænkelse gældende. Dog vurderer Datatilsynet, at videregivelse af personoplysningerne fra teleudbyderne kan have vidtrækkende konsekvenser for abonnenterne, hvorfor der er væsentlige hensyn at tage til disse.

Samlet finder Datatilsynet, at der ikke er grundlag for at videregive personoplysningerne på baggrund af interesseafvejningsreglen, idet hensynene i afvejningen er af så væsentlige og modsatrettede karakter, at de bør forelægges en domstol. Det er således Datatilsynets vurdering, at der ikke bør ske videregivelse af personoplysninger uden en retskendelse. Datatilsynets afgørelse er navnlig begrundet i, at sammenhængen mellem IP-adresserne og det ulovligt downloadede materiale, kan udgøre personoplysninger vedrørende strafbare forhold. Derudover anfører Datatilsynet i sin begrundelse, at politiet ikke har adgang til at få udleveret disse oplysninger uden en retskendelse. Datatilsynet lægger også hensynet til abonnenterne til grund, særligt den berettigede interesse som disse kan have om, at der ikke sker videregivelse af deres oplysninger, medmindre der foreligger en retskendelse.

Datatilsynets vurdering har tillige støtte i EU-retspraksis herunder i Tele2/Watson-dommen (C-203/15 og C-698/15). Denne afgørelse omhandler blandt andet fortolkning af e-databeskyttelsesdirektivets artikel 15, stk. 1. I sammenhæng med behandlingen af dette fortolkningsspørgsmål anførte EU-domstolen i præmis 120, at adgangen til data kun bør ske ved forudgående kontrol foretaget af en domstol eller en anden administrativ myndighed. Idet Datatilsynet i sin afgørelse lægger vægt på, at der ikke bør ske videregivelse af oplysningerne uden forudgående retskendelse, synes dette at være i overensstemmelse med EU-retspraksis på området.

Datatilsynets afgørelse indikerer, at teleudbyderne ikke bør videregive navne- og adresseoplysninger tilknyttet IP-adresser som følge af en interesseafvejning efter forordningens artikel 6, stk. 1, litra f. Såvel Datatilsynets afgørelse som Tele2/Watson-dommen (C-203/15 og C-698/15) angiver, at en retskendelse bør foreligge, før en videregivelse af personoplysninger kan ske. Dog synes en videregivelse på baggrund af abonnentens samtykke, efter forordningens

¹¹⁰ Betænkning nr. 1565, s. 134.

artikel 6, stk. 1, litra a, at være muligt. I denne forbindelse kræves dog, at betingelserne i forordningens artikel 7 vedrørende samtykke er opfyldt.

3.6.2 Behandling af følsomme personoplysninger

Navne- og adresseoplysninger tilknyttet IP-adresser kan, som nævnt i afsnit 3.5, i kombination med materialets indhold udgøre en følsom personoplysning. Betragtes oplysningerne som følsomme personoplysninger, skal et retligt behandlingsgrundlag findes i forordningens artikel 9, stk. 2, litra a-h. Navne- og adresseoplysninger tilknyttet IP-adresser kan ændre karakter til følsomme personoplysninger, når en rettighedshaver anmoder en teleudbyder om at videregive personoplysningerne. Det er dermed alene relevant at undersøge, på hvilket persondataretligt grundlag videregivelse af følsomme person-oplysninger kan ske.

3.6.2.1 Videregivelse ved editionskendelse

I det omfang teleudbydere pålægges at videregive navne- og adresseoplysninger tilknyttet IP-adresser, som i kombination med materialets indhold udgør oplysninger af følsom karakter, vil videregivelse af personoplysningerne have hjemmel i forordningens artikel 9, stk. 2, litra f. Efter denne bestemmelse må behandling af følsomme personoplysninger ske, hvis det er nødvendigt for, at et retskrav kan fastlægges eller gøres gældende.

I denne sammenhæng kan der henvises til Østre Landsrets kendelse af den 7. maj 2018, hvor Østre Landsret anfører, at rettighedshaverne ikke kan forfølge den eventuelle ophavsretlige krænkelse over for abonnenterne uden udlevering af navne- og adresseoplysningerne tilknyttet IP-adresserne. Endvidere lægger Datatilsynet til grund, i deres afgørelse publiceret den 12. juli 2017 (journalnr. 2016-217-1119), at hvis en behandling af personoplysninger ikke kan finde sted, vil rettighedshaverne være udelukket fra at forfølge de ophavsretlige krænkelse.

Dette underbygger således, at rettighedshavere ikke vil kunne gøre et retskrav gældende, medmindre teleudbydere videregiver navne- og adresseoplysningerne tilknyttet IP-adresser. Det må således fastslås, at teleudbydere kan videregive oplysninger til rettighedshavere efter behandlingshjemlen i forordningens artikel 9, stk. 2, litra f, såfremt der foreligger en editionskendelse.

Alternativt kan forordningens artikel 9, stk. 2, litra g overvejes som en mulig behandlingshjemmel. Efter denne artikel kan behandling af følsomme personoplysninger foretages, hvis det er nødvendigt af hensyn til samfundsinteresser på grundlag af henholdsvis national lovgivning eller EU-lovgivning. Ifølge forordningens præambelbetragtning nr. 52 sigter denne bestemmelse navnlig mod behandling af personoplysninger inden for blandt andet ansættelsesret og socialret. Hensynet med denne bestemmelse omfatter således ikke videregivelse af personoplysninger i forbindelse med ophavsretlige krænkelse, da dette ikke betragtes som en væsentlig samfundsinteresse i henhold til forordningen.

3.6.2.2 Videregivelse uden editionskendelse

Videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser er, som nævnt ovenfor, nødvendig for at rettighedshaverne kan fastlægge eller gøre deres retskrav gældende, jf. forordningens artikel 9, stk. 2, litra f. Spørgsmålet er imidlertid, om en sådan videregivelse er proportional uden en editionskendelse.

I Datatilsynets afgørelse publiceret den 20. november 2003 (journalnr. 2002-219-0135), som omtalt i afsnit 3.6.1.2.2, fandt Datatilsynet, at en videregivelse af almindelige personoplysninger på baggrund af en interesseafvejning ikke bør finde sted uden forelæggelse for en domstol. Det skal imidlertid bemærkes, at forordningens artikel 9, stk. 2 ikke indeholder en mulighed for at behandle følsomme personoplysninger på baggrund af en interesseafvejning, som det ellers er tilfældet ved behandling af almindelige personoplysninger, jf. forordningens artikel 6, stk. 1, litra f. På trods heraf, må en videregivelse af følsomme personoplysninger uden en editionskendelse virke betænkelig henset til Datatilsynets afgørelse. Det vil forekomme uhensigtsmæssigt, hvis videregivelse af følsomme personoplysninger kan finde sted uden forelæggelse for en domstol særligt af hensyn til personoplysningernes fortrolige karakter.

Endvidere er det et generelt persondataretligt princip, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til abonnenten, jf. forordningens artikel 5, stk. 1, litra a. Det forekommer tvivlsomt, om en videregivelse af følsomme personoplysninger uden en editionskendelse er rimelig for abonnenten. Dette særligt henset til at almindelige personoplysninger dermed vil opnå en større beskyttelse end følsomme personoplysninger i medfør af Datatilsynets afgørelse publiceret den 20. november 2003 (journalnr. 2002-219-0135).

Alternativt vil en behandling kunne støttes på et udtrykkeligt samtykke fra abonnenten, jf. forordningens artikel 9, stk. 2, litra a. Som anført ovenfor i afsnit 3.6.1.1 er et behandlingsgrundlag baseret på et samtykke ustabilt, da samtykket til enhver tid kan tilbagetrækkes.

3.6.3 Behandling af oplysninger om strafbare forhold

En videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser kan, i kombination med oplysninger om en ophavsretlig krænkelse, udgøre en oplysning om et strafbart forhold. Dette er behandlet nærmere i afsnit 3.5. Hjemlen til behandling af denne type af personoplysninger findes i forordningens artikel 10. I dansk ret er denne bestemmelse suppleret af databeskyttelsesloven, hvor særligt § 8, stk. 4-5 vedrørende videregivelse er relevante i det følgende.

I medfør af databeskyttelseslovens § 8, stk. 4, 1. led kan der ske videregivelse af personoplysninger, hvis der foreligger et udtrykkeligt samtykke. Som anført ovenfor i afsnit 3.6.1.1 er et behandlingsgrundlag baseret på et samtykke ustabilt, da samtykket til enhver tid kan tilbagetrækkes.

Videregivelse kan endvidere foretages uden samtykke, når det sker til varetagelse af offentlige eller private interesser, som klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, jf. databeskyttelseslovens § 8, stk. 4, 2. led. Der skal således foretages en afvejning af, hvorvidt rettighedshaverens interesse i at forfølge de ophavsretlige krænkelse overstiger abonnentens interesser i at dennes personoplysninger hemmeligholdes.

I denne forbindelse kan der henvises til Datatilsynets afgørelse publiceret den 20. november 2003 (journalnr. 2002-219-0135) som omtalt i afsnit 3.6.1.2.2. I denne afgørelse fandt Datatilsynet, at videregivelse af almindelige personoplysninger på baggrund af en interesseafvejning ikke bør finde sted uden forelæggelse for en domstol. Med denne afgørelse taget i betragtning vil det tilsvarende forekomme uhensigtsmæssigt, hvis udlevering af strafbare oplysninger kan finde sted uden forelæggelse for en domstol særligt af hensyn til personoplysningernes fortrolige karakter. I denne tilknytning vil det forekomme betænkeligt, hvis behandling af almindelige personoplysninger nyder en større beskyttelse end oplysninger om strafbare forhold. Modsat må det antages, at en interesseafvejning der medfører, at rettighedshaverens interesser klart overstiger abonnentens interesser, vil medføre at en videregivelse kan finde sted. Dette er dog under forudsætning af, at der foreligger en editionskendelse.

Endvidere kan oplysninger om strafbare forhold videregives efter samme betingelser som følsomme personoplysninger, jf. databeskyttelseslovens § 8, stk. 5. Det retlige grundlag for videregivelse af følsomme personoplysninger er behandlet ovenfor i afsnit 3.6.2.

3.6.4 Rettighedshaveres behandling af personoplysninger

Når teleudbydere videregiver oplysninger til rettighedshavere, er det ikke alene teleudbyderne, men også rettighedshaverne, der skal have et retligt grundlag for behandling af personoplysningerne. Teleudbyderne skal, basere sin behandling af navne- og adresseoplysninger tilknyttet IP-adresser på et lovligt grundlag, hvorfor teleudbyderne skal iagttage om rettighedshaverne har et lovligt behandlingsgrundlag, jf. forordningens artikel 5, stk. 1, litra a. I det følgende vil det undersøges, om rettighedshaverne har et sådant behandlingsgrundlag.

I denne tilknytning kan der henvises til Datatilsynets afgørelse publiceret den 12. juli 2017 (journalnr. 2016-217-1119). Afgørelsen omhandler, hvorvidt et advokatfirmas behandling af personoplysninger i forbindelse med civilretlig forfølgning af ophavsretlige krænkelse er i overensstemmelse med den dagældende persondatalov. Advokatfirmaet repræsenterer en rettighedshaver.

I afgørelsen er advokatfirmaet bekendt med en række IP-adresser, hvorfra der er foretaget ulovlig download og deling af ophavsretlig beskyttede værker. For at identificere de pågældende personer bag IP-adresserne anmodes retten om at pålægge teleudbyderne at videregive navne- og adresseoplysningerne tilknyttet IP-adresserne i medfør af retsplejelovens

regler om tredjemandsedition § 299, stk. 1 og isoleret bevisoptagelse § 343, stk. 1. Teleudbyderne videregiver, som følge af editionspålægget, abonnenternes personoplysninger. Datatilsynet anfører, at navne, adresser og IP-adresser som udgangspunkt udgør almindelige oplysninger. I denne sammenhæng finder Datatilsynet, at en rettighedshaver kan anvende persondatalovens § 6, stk. 1, nr. 7, som retligt grundlag til behandling af disse personoplysninger.

Denne afgørelse understøtter, som fastslået ovenfor i afsnit 3.5, at navne- og adresseoplysninger tilknyttet IP-adresser som udgangspunkt udgør almindelige personoplysninger. Det retlige behandlingsgrundlag for disse oplysninger skal derfor som udgangspunkt findes i forordningens artikel 6. Selvom om Datatilsynets afgørelse omhandler den dagældende persondatalovs § 6, stk. 1, svarer denne i det væsentlige til forordningens artikel 6, stk. 1. Interesseafvejningen i persondatalovens § 6, stk. 1, nr. 7, ses videreført i artikel 6, stk. 1, litra f.¹¹¹ Med henvisning til afsnit 2.2.5.1 samt denne afgørelse forekommer alene behandlingshjemlen i forordningens artikel 6, stk. 1, litra f relevant for rettighedshavernes behandling.

Af forordningens artikel 6, stk. 1, litra f følger, at behandling kan ske efter en interesseafvejning, hvis behandlingen er nødvendig for, at rettighedshaverne kan forfølge en legitim interesse. Da Datatilsynet anfører, at interesseafvejningsreglen er rette behandlingshjemmel, må det tilsvarende lægges til grund, at en rettighedshavers forfølgelse af en ophavsretlig krænkelse udgør en legitim interesse. Den legitime interesse skal imidlertid afvejes overfor hensynet til abonnentens interesser, grundlæggende rettigheder samt frihedsrettigheder. Den nærmere afvejning samt dennes resultat vil blandt andet afhænge af omfanget af den ophavsretlige krænkelse.

Datatilsynet anfører endvidere, at en sammenkobling af abonnentens identitet og en ophavsretlig krænkelse kan udgøre en behandling af vedkommendes strafbare forhold. I denne forbindelse fastslår Datatilsynet, at advokatfirmaets behandling af de pågældende personoplysninger kan foretages, hvis det er nødvendigt for at varetage en berettiget interesse og denne interesse klart overstiger hensynet til abonnenten, jf. persondatalovens § 8, stk. 4.

Persondatalovens § 8, stk. 4 antages i udgangspunktet at være videreført i sin helhed inden for rammerne af artikel 10, 1. pkt.¹¹² Det kan dermed fastslås, at en interesseafvejning efter databeskyttelseslovens § 8, stk. 4 kan anvendes som retligt behandlingsgrundlag.

Endvidere anfører Datatilsynet i afgørelsen, at et alternativt behandlingsgrundlag kan findes i persondatalovens § 7, stk. 2, nr. 4, jf. § 8, stk. 6, hvis behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares i forbindelse med en civilretlig forfølgning.

¹¹¹ Betænkning nr. 1565, s. 134.

¹¹² Betænkning nr. 1565, s. 246.

Persondatalovens § 7, stk. 2, nr. 4 svarer til ordlyden i forordningens artikel 9, stk. 2, litra f.¹¹³ Oplysninger om strafbare forhold kan behandles efter reglerne om behandling af følsomme oplysninger, jf. databeskyttelseslovens § 8, stk. 5. Det kan således fastslås, at rettighedshaverne kan anvende artikel 9, stk. 2, litra f som behandlingshjemmel, jf. databeskyttelseslovens § 8, stk. 5.

Desuden kan kombinationen af abonnentens identitet og materialets indhold udgøre behandling af følsomme personoplysninger i henhold til forordningens artikel 9. I denne tilknytning må forordningens artikel 9, stk. 2, litra f tilsvarende finde anvendelse som behandlingshjemmel.

Med nærværende afsnit fastslås, at rettighedshaverne har et retligt grundlag for behandlingen af navne- og adresseoplysninger tilknyttet IP-adresser.

3.7 Teleudbyderes forpligtelser efter logningsbekendtgørelsen

Logningsbekendtgørelsen er central for nærværende problemstilling, da teleudbydere, i medfør af logningsbekendtgørelsens § 1, skal foretage registrering og opbevaring af oplysninger om teletrafik, som behandles i teleudbyderens net. Navne- og adresseoplysninger tilknyttet IP-adresser, som rettighedshaverne ønsker udleveret, udgør logget data i medfør af logningsbekendtgørelsens § 5, stk. 1, nr. 3, hvorfor de pågældende oplysninger er omfattet af logningsbekendtgørelsens anvendelsesområde, jf. logningsbekendtgørelsens § 1.

Særligt relevant for nærværende afhandling er selve formålet med logningsbekendtgørelsen. Formålet er, at *“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”*, jf. logningsbekendtgørelsens § 1. Logningsbekendtgørelsen fastsætter dermed en opbevaringspligt således, at oplysninger om teletrafik kan anvendes til brug for efterforskning og retsforfølgning af strafbare forhold. I denne forbindelse er det interessant at undersøge om oplysningerne, der udleveres til civilretlig forfølgelse, alene er i teleudbydernes besiddelse, på baggrund af opbevarings-pligten, som følger af logningsbekendtgørelsen. Er dette tilfældet, er det ligeledes relevant at undersøge, hvorvidt navne- og adresseoplysninger tilknyttet IP-adresser alene kan videregives til brug for efterforskning og retsforfølgning af strafbare forhold. I denne forbindelse skal de persondataretlige regler og principper tillige tages i betragtning.

3.7.1 Opbevaring efter logningsbekendtgørelsen

Det er, som nævnt ovenfor, relevant at undersøge, hvorvidt navne- og adresseoplysninger tilknyttet IP-adresser alene er i teleudbydernes besiddelse som følge af opbevaringspligten, som følger af logningsbekendtgørelsen.

¹¹³ Betænkning nr. 1565, s. 215.

Det følger af logningsbekendtgørelsens § 5, stk. 1, nr. 3, at teleudbydere er forpligtet til at registrere navn og adresse på den abonnent eller registrerede bruger, hvortil der er tilknyttet en IP-adresse. I henhold til logningsbekendtgørelsen er teleudbyderne pålagt at opbevare disse oplysninger i 1 år, jf. logningsbekendtgørelsens § 9. Det er således interessant at undersøge, hvorvidt teleudbydere ville opbevare de pågældende oplysninger, hvis ikke logningsbekendtgørelsen pålagde teleudbyderne en sådan opbevaringspligt.

I Østre Landsrets kendelse af den 7. maj 2018 udtaler en række teleudbydere, i hvilket omfang opbevaring af navne- og adresseoplysninger tilknyttet IP-adresser er nødvendig til opfyldelse af egne formål. Telenor oplyser i denne forbindelse, at IP-adresserne gemmes i deres almindelige system i op til 30 dage af hensyn til driften, således Telenor kan foretage fejlretninger. Herefter overføres disse data til Telenors "politirapporteringssystem". Når oplysningerne overføres til dette system, anvendes disse data ikke til andet end politirapportering. Telenor gemmer dataene, fordi de er pålagt en forpligtelse i henhold til logningsbekendtgørelsen. Tilsvarende har Telia et system, hvor de gemmer data til brug for politiet. Telia ville alene opbevare oplysningerne i tre uger med henblik på fejlretning, hvis ikke de var pålagt en pligt til at opbevare de pågældende oplysninger. Endvidere udtaler TDC, at de, til eget brug, gemmer IP-adresserne i mindre end en måned. Herefter overføres oplysningerne til deres "loggingssystem", som anvendes til at varetage de pågældende forpligtelser, som TDC er pålagt i henhold til logningsbekendtgørelsen. I tilknytning hertil lægger Østre Landsret til grund, 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."* og at *"tilsvarende gør sig gældende for TDC..."* På baggrund af Østre Landsrets begrundelse og resultat, kan det udledes, at logningsbekendtgørelsen medfører en længerevarende opbevaring for teleudbyderne, end hvad teleudbydernes egne formål kræver.

I afsnit 3.3.1 er det fastslået, at navne- og adresseoplysninger tilknyttet IP-adresser udgør en personoplysning. Da der er tale om behandling af personoplysninger, er det relevant at undersøge, hvorvidt en behandling af disse personoplysninger er i overensstemmelse med de persondataretlige behandlingsprincipper. Dette uanset at logningsbekendtgørelsen hjemler en pligt til registrering og opbevaring af personoplysningerne.

Opbevaringen af de loggede data, herunder navne- og adresseoplysninger tilknyttet IP-adresser, skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålet med behandlingen, jf. princippet om dataminimering i forordningens artikel 5, stk. 1, litra c. Teleudbyderne opbevarer navne- og adresseoplysningerne tilknyttet IP-adresser til brug for egne formål, herunder fejlretning. Denne opbevaring er nødvendig for teleudbyderne i henholdsvis 30 dage og 3 uger, hvorfor en længerevarende opbevaring ikke vil være i overensstemmelse med princippet om dataminimering. Logningsbekendtgørelsen pålægger dog teleudbyderne en mere vidtgående opbevaringspligt, hvorefter opbevaring skal foretages i et 1 år, jf. logningsbekendtgørelsens § 9. Efter henholdsvis 30 dage og 3 uger er teleudbydernes

formål med opbevaringen således udelukkende at opfylde opbevarings-forpligtelsen, som følger af logningsbekendtgørelsen. Opbevaringsforpligtelsen er ikke ubegrænset, hvorfor teleudbyderne ikke må opbevare en større mængde data, end hvad logningsbekendtgørelsen fastsætter. Dette kan tilsvarende udledes af Datatilsynets afgørelse publiceret den 11. februar 2019 (journalnr. 2018-31-0070), som gennemgået ovenfor i afsnit 2.2.4.3. I denne sag opbevarede TDC en større mængde data end påkrævet til opfyldelse af forpligtelsen i logningsbekendtgørelsen, hvorfor princippet om dataminimering ikke var overholdt.

Endvidere skal de pågældende navne- og adresseoplysninger tilknyttet IP-adresser opbevares på en sådan måde, at det ikke er muligt at identificere abonnenterne i et længere tidsrum end nødvendigt til forfølgelse af formålet med behandlingen, jf. forordningens artikel 5, stk. 1, litra e. Til at forfølge formålet i logningsbekendtgørelsen er det fastsat, at navne- og adresseoplysninger tilknyttet IP-adresser skal opbevares i 1 år, jf. logningsbekendtgørelsens § 5, stk. 1, nr. 3, jf. § 9. Det er det således et krav, at teleudbyderne sletter eller på anden måde anonymiserer de pågældende oplysninger efter 1 år, således abonnenterne ikke længere kan identificeres i teleudbyderens system.¹¹⁴

Sammenfattende kan udledes, at teleudbyderne ikke fortsat ville være i besiddelse af navne- og adresseoplysninger tilknyttet IP-adresser, hvis ikke logningsbekendtgørelsen pålagde teleudbyderne en opbevaringspligt. Dette understreges tillige i Østre Landsrets kendelse af den 7. maj 2018, hvor landsretten fastslår, at navne- og adresseoplysninger tilknyttet IP-adresser ”... alene fortsat er i teleudbydernes besiddelse, fordi teleudbyderne ifølge logningsbekendtgørelsen ... er forpligtet til at opbevare dem med det formål, at de efter retskendelse skal kunne udleveres til politiet som led i efterforskning og retsforfølgning af strafbare forhold...”

I henhold til eksemplet med Rasmus betyder dette, at Telenor alene har behov for at opbevare navne- og adresseoplysningerne tilknyttet IP-adresser i op til 30 dage til egne formål. Telenor er dog forpligtet til at opbevare de pågældende personoplysninger vedrørende deres abonnenter i 1 år i henhold til logningsbekendtgørelsens § 9. Denne opbevaringsforpligtigelse medfører samtidig, at Telenor ikke er berettiget til at opbevare en større mængde data, end det de er forpligtet til at opbevare i medfør af logningsbekendtgørelsen §§ 4-6, jf. princippet om dataminimering i forordningens artikel 5, stk. 1, litra c. Endvidere må Telenor ikke opbevare navne- og adresseoplysninger tilknyttet IP-adresser i en længere periode end 1 år, da formålet med behandlingen alene kræver en opbevaring af denne varighed, jf. logningsbekendtgørelsens § 9.

3.7.2 Videregivelse efter logningsbekendtgørelsen

Det er relevant at undersøge, hvorvidt navne- og adresseoplysninger tilknyttet IP-adresser alene kan videregives til brug for efterforskning og retsforfølgning af strafbare forhold, når teleudbyderne alene, som ovenfor fastslået, opbevarer oplysningerne som følge af

¹¹⁴ Datatilsynets vejledning: databeskyttelsesforordningen, 2017, s. 11.

forpligtigelsen i medfør af logningsbekendtgørelsens § 1. Det skal således undersøges, hvilke forhold der kan forfølges i henhold til logningsbekendtgørelsen.

I nærværende afhandling vedrører problemstillingen videregivelse til civilretlig forfølgelse af ophavsretlige krænkelse. I det nedenstående behandles først de momenter, som understøtter, at videregivelse til civilretlig forfølgelse af ophavsretlige krænkelse er omfattet af logningsbekendtgørelsen. Dernæst gennemgås momenterne som understøtter, at videregivelse alene kan ske til strafferetlig forfølgelse i medfør af logningsbekendtgørelsen. Derudover inddrages en række af de persondataretlige principper med det formål at undersøge, om en videregivelse vil være i overensstemmelse hermed.

3.7.2.1 Videregivelse til forfølgelse af civilretlige krav

Formålet med logningsbekendtgørelsen er at *“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”*, jf. logningsbekendtgørelsens § 1. Umiddelbart angiver ordlyden i logningsbekendtgørelsens § 1 således intet om, at logningsdata kan anvendes til forfølgelse af civilretlige krav.

For at afgøre om logningsbekendtgørelsen omfatter videregivelse til civilretlige krav, bør der tages udgangspunkt i e-databeskyttelsesdirektivet, som logningsbekendtgørelsen bygger på samt relevant retspraksis.

Det følger af e-databeskyttelsesdirektivets artikel 6 og udbudsbekendtgørelsens § 23, at oplysningerne skal gøres anonyme eller slettes, når de ikke længere er nødvendige for fremføringen af kommunikationen. I medfør af artikel 15 i e-databeskyttelsesdirektivet har medlemsstaterne mulighed for at indskrænke rækkevidden af de forpligtelser, som fremgår af artikel 6. De indskrænkninger, som medlemsstaterne kan vedtage, skal være *“... passende og forholdsmæssig[e] i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1 i direktiv 95/46/EF [persondatadirektivet].”* Videre anføres det direkte, at *“... medlemsstaterne bl.a. kan vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke.”* Logningsbekendtgørelsen tillader en længere opbevaringsperiode end nødvendigt for fremføringen af kommunikationen, hvorfor bekendtgørelsen udgør en undtagelse til e-databeskyttelsesdirektivets artikel 6 og dermed tillige udbudsbekendtgørelsens § 23, stk. 1, jf. e-databeskyttelsesdirektivets artikel 15. Logningsbekendtgørelsens opbevaringsforpligtelse er begrundet i hensynet til forebyggelse, efterforskning, afsløring og retsforfølgning af straffesager.

Muligheden for at foretage indskrænkninger i anvendelsesområdet af e-databeskyttelsesdirektivets artikel 6 skal tillige ses i sammenhæng med forordningens hensyn og formål, hvor det i præambelbetragtning nr. 4 anføres, at beskyttelse af personoplysninger ikke udgør en absolut ret. Det er således i overensstemmelse med forordningen, at e-databeskyttelsesdirektivets artikel 15 muliggør indskrænkninger i retten til beskyttelse af personoplysninger.

Vedrørende de oplistede hensyn i e-databeskyttelsesdirektivets artikel 15 kan der henvises til Tele2/Watson-dommen (C-203/15 og C-698/15). I denne afgørelse understreger EU-domstolen, at opregningen i e-databeskyttelsesdirektivets artikel 15, stk. 1 er udtømmende, jf. præmis 90. Det er således et krav, at *"... adgangen til de lagrede data faktisk og præcist opfylde[r] et af disse mål."*, jf. præmis 115.

Det fremgår ikke umiddelbart af de oplistede hensyn i artikel 15, stk. 1, at forfølgelse af et civilretligt krav kan udgøre en indskrænkning i rækkevidden af forpligtelserne efter e-databeskyttelsesdirektivets artikel 6. Hvorvidt der kan ske videregivelse af personoplysninger til civilretlig forfølgelse af ophavsretlige krænkelse i medfør af e-databeskyttelsesdirektivet, har været forelagt EU-domstolen i Promusicae (C-275/06) som berørt ovenfor i afsnit 3.6.1.2.2. I Promusicae (C-275/06) fremgår det af præmis 51, at ingen af de i artikel 15, stk. 1 oplistede undtagelser; *"... vedrøre[r] situationer, der medfører anlæggelsen af civile retssager."* I samme præmis udtaler EU-domstolen, at undtagelserne vedrører statens aktiviteter og ikke den enkelte borgers aktiviteter. Det må herved forstås, at undtagelsen i e-databeskyttelsesdirektivets artikel 15, stk. 1 som udgangspunkt ikke er tiltænkt private anliggender, herunder forfølgelse af civilretlige krav. I forlængelse heraf understreger EU-domstolen dog i præmis 53, at opregningen i artikel 15, stk. 1 slutter med en udtrykkelig henvisning til persondatadirektivets artikel 13, stk. 1 og at denne bestemmelse tillader, at medlemsstaterne træffer foranstaltninger, der indskrænker beskyttelsen af personoplysninger, *"... når denne begrænsning er nødvendig, bl.a. til beskyttelsen af andres rettigheder og frihedsrettigheder."* Da det ikke er præciseret i e-databeskyttelsesdirektivets artikel 15, stk. 1 hvilke rettigheder og frihedsrettigheder, der er omfattet heraf, udtaler EU-domstolen, at det skal fortolkes *"... som udtryk for, at fællesskabslovgiver hverken ville udelukke ejendomsretten eller situationer, hvor ophavsmænd søger at opnå denne beskyttelse under en civil retssag, fra bestemmelseernes anvendelsesområde."* På baggrund heraf fastsættes det i præmis 54-55, at e-databeskyttelsesdirektivets artikel 15, stk. 1 ikke udelukker, at medlemsstaterne kan fastsætte en pligt for teleudbydere med henblik på at videregive personoplysninger til civilretlig forfølgelse af ophavsretlige krænkelse. Medlemsstaterne er dog ikke tvunget til at fastsætte en sådan pligt. Henset til dansk ret er der ikke fastsat en pligt for teleudbydere til at videregive personoplysninger til civilretlige krav.

Det kan dermed udledes af Promusicae (C-275/06), at e-databeskyttelsesdirektivet ikke udelukker videregivelse af personoplysninger til brug for civilretlig forfølgelse. Det er således relevant at undersøge, hvorvidt den danske regulering i henhold til logningsbekendtgørelsen udelukker en sådan videregivelse til forfølgelse af civilretlige krav.

Videregivelse af personoplysninger logget i medfør af forpligtelsen i lognings-bekendtgørelsen er behandlet af Østre Landsret i kendelsen af den 7. maj 2018. Østre Landsret foretog, som ovenfor nævnt i afsnit 3.2.1, en afvejning af hensynet til den enkelte abonnents rettigheder overfor rettighedshaverens interesse i at få udleveret de pågældende oplysninger. I forbindelse med denne afvejning udtalte Østre Landsret, at "... *teleudbyderne ifølge logningsbekendtgørelsen udstedt efter reglerne i strafferetsplejen er forpligtet til at opbevare [teledata] med det formål, at de efter retskendelse skal kunne udleveres til politiet som led i efterforskning og retsforfølgning af strafbare forhold...*" (egne understregninger). Henset til denne udtalelse bør særligt fremhæves, at Østre Landsret understreger, at logningsbekendtgørelsen er udstedt efter reglerne i strafferetsplejen og at formålet med opbevaringsforpligtelsen er til efterforskning og retsforfølgelse af strafferetlige krav. Østre Landsret tydeliggør hermed, at logningsbekendtgørelsen som udgangspunkt har sit hovedsigte på forfølgelse af strafferetlige krav og ikke civilretlige krav. Dog udelukker Østre Landsret ikke at videregivelse af de pågældende personoplysninger er en mulighed, hvis tungtvejende grunde gør sig gældende for rettighedshaveren. Det må i denne sammenhæng bemærkes, at Østre Landsret, ved at foretage den pågældende interesseafvejning, indikerer, at en videregivelse til civilretlig forfølgelse kan finde sted i henhold til lognings-bekendtgørelsen.

Østre Landsrets manglende konklusion på området, samt den generelle tendens til videregivelse i retspraksis forud for Østre Landsrets kendelse af den 7. maj 2018, synes således at indikere, at logningsbekendtgørelsen omfatter videregivelse til civilretlig forfølgelse. Denne tendens til videregivelse fremgår blandt andet af kendelsen afsagt af Retten på Frederiksberg den 3. november 2017 (sag nr. BS A-1417/2017), kendelsen afsagt af Retten på Frederiksberg den 16. august 2017 (sag nr. BS K-741/2017), kendelsen afsagt af Retten på Frederiksberg den 10. november 2015 (sag nr. BS E-1984/2015) med videre.¹¹⁵

3.7.2.2 Videregivelse til forfølgelse af strafferetlige krav

Formålet med logningsbekendtgørelsen er, som beskrevet ovenfor, at de opbevarede oplysninger kan "... *anvendes som led i efterforskning og retsforfølgning af strafbare forhold.*", jf. logningsbekendtgørelsens § 1. Det kan således udledes direkte af bestemmelsens ordlyd, at videregivelse som udgangspunkt kan ske til forfølgelse af strafbare forhold. Det er således relevant at belyse, hvad der forstås ved et strafbart forhold og om videregivelse alene bør ske til forfølgelse af et sådant forhold.

Ved et strafbart forhold forstås tilfælde, hvor der kan idømmes de almindelige straffe i dansk ret. I medfør af straffelovens § 31 udgør de almindelige straffe bøde og fængsel. Straf kan alene idømmes, hvis strafbarhed er hjemlet ved lov eller tilfælde der kan ligestilles hermed, jf. straffelovens § 1, 1. pkt.

Logningsbekendtgørelsen anfører, at de opbevarede oplysninger kan anvendes som led i efterforskning, jf. logningsbekendtgørelsens § 1. Det er som udgangspunkt politiet, som

¹¹⁵ Se bilag 2-3 og bilag 10.

iværksætter efterforskning, jf. retsplejelovens § 742, stk. 2. Det er imidlertid ikke udelukket, at andre aktører end politiet kan iværksætte efterforskning. Politiet har dog en lovhjemlet enekompetence til at foretage visse efterforskningsskridt i medfør af retsplejelovens andet afsnit. Endvidere må det bemærkes, at der ved en almindelig forståelse af begrebet ”efterforskning” associeres til politiets kompetence.¹¹⁶

I forlængelse heraf er det centralt at behandle, til hvilken personkreds videregivelse af personoplysninger kan ske efter logningsbekendtgørelsens § 1. Her er det særligt interessant at undersøge, om videregivelse alene kan ske til politi og anklagemyndighed, når logningsbekendtgørelsen fastsætter, at der skal være tale om efterforskning og retsforfølgning af strafbare forhold.

I denne forbindelse kan der henvises til Østre Landsrets udtalelse i kendelsen af den 7. maj 2018, som behandlet i afsnit 3.2.1. Østre Landsret anførte, som et moment i deres afvejning, at formålet med teleudbydernes opbevaring af teledata i medfør af logningsbekendtgørelsen er, *”...at de efter retskendelse skal kunne udleveres til politiet som led i efterforskning og retsforfølgning af strafbare forhold.”* (egen understregning). Landsretten indikerer således, at personkredsen, hvortil der kan ske udlevering, er politiet.

Endvidere kan der henvises til EU-retspraksis. EU-domstolen anfører i Tele2/Watson-dommen (C-203/15 og C-698/15), at e-databeskyttelsesdirektivets artikel 15, stk. 1 kræver, at der *”... fastsætte[s] 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.”* (egen understregning), jf. præmis 117. Det følger af denne udtalelse, at logget data alene kan videregives til en kompetent myndighed. Ved en kompetent national myndighed forstås næppe en privat virksomhed, men derimod en kompetent myndighed såsom politiet eller anklage-myndigheden. Tele2/Watson-dommen (C-203/15 og C-698/15) indikerer således, at der kun bør ske videregivelse til politiet og anklagemyndigheden.

Tele2/Watson-dommen (C-203/15 og C-698/15) og Østre Landsrets kendelse af den 7. maj 2018 synes således at stemme overens henset til den pågældende personkreds, hvortil logget data kan udleveres.

Af logningsbekendtgørelsens formål fremgår, at der skal være tale om et strafbart forhold. Det er således interessant at undersøge, om karakteren af det strafbare forhold kan have betydning for, hvorvidt de opbevarede oplysninger kan anvendes som led i efterforskning og retsforfølgning i medfør af logningsbekendtgørelsens § 1.

I denne tilknytning kan der tilsvarende henvises til Tele2/Watson-dommen (C-203/15 og C-698/15). I dommen blev det anført, at adgang til de lagrede data, på baggrund af hensynet i e-databeskyttelsesdirektivets artikel 15, stk. 1 vedrørende forebyggelse, efterforskning, afsløring

¹¹⁶ Koch, Henning, 2009.

og retsforfølgning af straffelovsovertrædelser, alene kan ske, såfremt der er tale om bekæmpelse af grov kriminalitet i, jf. præmis 115. Endvidere blev det anført, at indgrebet i de grundlæggende rettigheder, i form af lagring af trafikdata, alene kan ske med henblik på bekæmpelse af grov kriminalitet, jf. præmis 102. EU-domstolen fremhæver dermed, at der skal være tale om bekæmpelse af grov kriminalitet, førend det vil være i overensstemmelse med e-databeskyttelsesdirektivet at opbevare og videregive oplysningerne.

I Tele2/Watson-dommen er det ikke anført, hvad der skal forstås ved begrebet grov kriminalitet. Det kan imidlertid udledes, at EU-domstolen anser organiseret kriminalitet og terrorisme for at være omfattet af begrebet grov kriminalitet, jf. præmis 103. EU-domstolen omtaler ikke andre former for kriminalitet i dommen, men det må forudsættes, at kriminalitet af samme beskaffenhed tilsvarende må betragtes som grov. Til at afdække begrebet grov kriminalitet kan der henvises til artiklen ”Logning af teledata i lyset af Tele2-dommen” forfattet af Lene Wachter Lentz. I denne artikel anvendes fortolkningsbidrag fra en række EU-retsakter samt retspraksis fra Den Europæiske Menneskerettighedsdomstol (herefter EMD). På grundlag heraf kan det udledes, at ”... *terrorisme, menneskehandel og seksuel udnyttelse af kvinder og børn, ulovlig narkotikahandel, ulovlig våbenhandel, hvidvaskning af penge, korruption, forfalskning af betalingsmidler, edb-kriminalitet og organiseret kriminalitet.*” i henhold til TEUF artikel 83, stk. 1 anses for kriminalitet af særlig grov karakter. Endvidere følger det af retspraksis fra EMD, at drab og grovere personfarlige forbrydelser betragtes som ”serious crime”. Henset til “... *loyalitetsprincippet har danske domstole pligt til at iagttage praksis fra [EU-]Domstolen.*”¹¹⁷ I dansk ret må begrebet grov kriminalitet således harmonere med den EU-retlige opfattelse af dette begreb. Ovennævnte kriminalitetstyper må dermed tilsvarende udgøre grov kriminalitet efter dansk ret.

Det kan dermed udledes, at det ikke er enhver efterforskning og retsforfølgning af strafbare forhold, der giver adgang til videregivning af de loggede data, da det er en forudsætning at disse anvendes til bekæmpelse af grov kriminalitet.

Endvidere er det relevant at bemærke, at logningsbekendtgørelsen som nævnt er udstedt med hjemmel i retsplejelovens § 786, stk. 4. Denne bestemmelse er placeret under retsplejelovens kapitel 71 vedrørende indgreb i meddelelseshemmeligheden, observation, dataaflysning, forstyrrelse eller afbrydelse af radio- og telekommunikation og blokering af hjemmesider. Placeringen af bestemmelsen er således med til at indikere, at logningsbekendtgørelsen har sit hovedsigte på retsforfølgning af strafferetlige krav. Dette indgår tillige som et moment i Østre Landsrets afvejning i kendelsen fra den 7. maj 2018, hvor det blev anført, at ”...*logningsbekendtgørelsen er udstedt efter reglerne i strafferetsplejen...*”.

Henset til de persondataretlige principper i forordningens artikel 5 synes det særligt relevant at inddrage forordningens artikel 5, stk. 1, litra a vedrørende lovlighed, rimelighed og gennemsigtighed. Efter dette princip skal teleudbydere behandle personoplysninger på en lovlig, rimelig og gennemsigtig måde i forhold til sine abonnenter. Kravet om rimelighed

¹¹⁷ Vestergaard, Jørn, TfK2016.429.

indebærer, at behandlingen af personoplysninger skal foretages i overensstemmelse med forordningens hensyn og formål, således der opnås retssikkerhed og gennemsigtighed for abonnenterne, jf. præambelbetragtning nr. 13. Dette skal ses i sammenhæng med, at en abonnent skal være bekendt med behandlingens formål samt i hvilket omfang dennes personoplysninger behandles og fremadrettet vil blive behandlet af teleudbyderne, jf. præambelbetragtning nr. 39. Logningsbekendtgørelsens § 5 fastsætter klare rammer for omfanget af registrerings- og opbevaringspligten af de loggede oplysninger i forbindelse med abonnenternes adgang til internettet. Desuden fremgår, som nævnt, formålet med denne opbevarings- og registreringspligt i logningsbekendtgørelsens § 1 samt i hvilket omfang disse loggede oplysninger kan videregives. Umiddelbart forekommer teleudbydernes behandling således lovlig, rimelig og gennemsigtig for abonnenterne, såfremt videregivelsen sker til forfølgelse af et strafbart forhold i medfør af logningsbekendtgørelsens § 1.

3.7.2.3 Rækkevidden af logningsbekendtgørelsens formål

På baggrund af afsnit 3.7.2.1 og afsnit 3.7.2.2 kan det sammenfattende udledes, at der i retspraksis har eksisteret en generel tendens til at videregive navne- og adresseoplysninger tilknyttet IP-adresser til forfølgelse af civilretlige krav forud for Østre Landsrets kendelse af den 7. maj 2018. Endvidere kan det konstateres, at Promusicae (C-275/06) ikke udelukker, at videregivelse kan ske til forfølgelse af civilretlige krav.

Imidlertid indikerer afsnit 3.7.2.2, at videregivelse alene bør ske til efterforskning og retsforfølgelse af strafbare forhold som følge af logningsbekendtgørelsens formål. Dette begrundes med, at politiet har den mest vidtgående kompetence til at foretage efterforskning, at retspraksis indikerer, at videregivelse alene kan ske til myndigheder og at videregivelse alene kan ske til bekæmpelse af grov kriminalitet. Henset til begrebet om grov kriminalitet, som beskrevet i EU-retspraksis og TEUF, må det udledes, at civilretlige forfølgelser af ophavsretlige krænkelse ikke udgør grov kriminalitet.

Yderligere understøtter forordningens artikel 5, stk. 1, litra a, at en videregivelse til civilretlig forfølgelse ikke forekommer i overensstemmelse med princippet om lovlighed, rimelighed og gennemsigtighed. Særligt forekommer det ikke gennemsigtigt for en abonnent, hvis videregivelse tillige kan ske til forfølgelse af civilretlige krav, når ordlyden i logningsbekendtgørelsens § 1 direkte anfører, at videregivelse sker til brug for efterforskning og retsforfølgning af strafbare forhold.

Endvidere har Østre Landsret i kendelsen af den 7. maj 2018 tydeliggjort, at logningsbekendtgørelsen er udstedt efter reglerne i strafferetsplejen og at formålet med logningsbekendtgørelsen relaterer sig til anvendelse ved efterforskning og retsforfølgning af strafbare forhold. Landsretten synes herved at indikere, at logningsbekendtgørelsens hovedsigte er forfølgelse af strafferetlige krav og ikke civilretlig forfølgelse af ophavsretlige krav. Imidlertid foretager Østre Landsret en interesseafvejning, hvorfor landsretten tillige

indikerer, at videregivelse til civilretlig forfølgelse kan finde sted i henhold til logningsbekendtgørelsen.

Det må, på baggrund af logningsbekendtgørelsens formål og EU-retspraksis, udledes, at data logget efter logningsbekendtgørelsen alene bør videregives til strafferetlig forfølgning, da dette direkte fremgår af logningsbekendtgørelsens formål i § 1. Derimod kan det ikke udelukkes, hverken efter dansk retspraksis eller EU-retspraksis, at de loggede oplysninger lovligt kan videregives til forfølgelse af civilretlige krav.

Helt centralt for den persondataretlige regulering er formålet med behandlingen af personoplysninger. Personoplysninger må alene indsamles til de udtrykkeligt angivne og legitime formål, jf. finalité-princippet i forordningens artikel 5, stk. 1, litra b. Det er således væsentligt, at formålet med den pågældende behandling er baseret på et udtrykkeligt og legitimt formål allerede ved indsamlingen, jf. præambelbetragtning nr. 39. Kravet om udtrykkelighed har tæt sammenhæng med behandlingsprincippet i forordningens artikel 5, stk. 1, litra a, således der skabes gennemsigtighed for abonnenten ved at angive et veldefineret og præcist formål med behandlingen.¹¹⁸ Teleudbydernes formål med behandlingen af de loggede personoplysninger fremgår direkte af logningsbekendtgørelsens § 1, hvorefter oplysningerne skal anvendes til efterforskning og retsforfølgning af strafbare forhold. Der kan ikke ske en viderebehandling af disse personoplysninger, hvis det er uforeneligt med dette oprindelige formål, jf. forordningens artikel 5, stk. 1, litra b. Dette indebærer, at teleudbyderne ikke kan videregive de loggede personoplysninger til forfølgelse af civilretlige krav, såfremt dette er uforeneligt med formålsbestemmelsen i logningsbekendtgørelsen. Logningsbekendtgørelsen angiver ikke klart, som ovenfor omtalt, hvorvidt der kan ske videregivelse af de loggede oplysninger til forfølgelse af civile krav.

Trafikdata skal som udgangspunkt slettes eller anonymiseres, når disse ikke længere er nødvendige for fremføringen af kommunikationen i medfør af henholdsvis e-databeskyttelsesdirektivets artikel 6 som implementeret i udbudsbekendtgørelsen § 23. Logningsbekendtgørelsen udgør dermed et indgreb i beskyttelsen af privatlivets fred. Idet der er tale om et indgreb i en grundlæggende rettighed, skal logningsbekendtgørelsen fortolkes indskrænkende. Ved en indskrænkende fortolkning skal den snævraste forståelse af formålsbestemmelsen i logningsbekendtgørelsens § 1 lægges til grund.¹¹⁹ Efter logningsbekendtgørelsens § 1 fremgår det umiddelbart kun, at der kan ske videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser til efterforskning og retsforfølgning af strafbare forhold. Da formålet med behandlingen skal angives udtrykkeligt over for abonnenten og, med henvisning til forordningens artikel 5, stk. 1, litra a, behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til abonnenten, bør en viderebehandling til civilretlig forfølgelse ikke kunne rummes i formålsbestemmelsen i logningsbekendtgørelsen.

Da logningsbekendtgørelsens formålsbestemmelse ikke umiddelbart omfatter viderebehandling til civilretlig forfølgelse, er det relevant at undersøge, hvorvidt videregivelse er

¹¹⁸ Trzaskowski, Jan, 2017, s. 121.

¹¹⁹ Munk-Hansen, Carsten, 2014, s. 292.

forenelig med logningsbekendtgørelsens formål. Forordningens artikel 6, stk. 4 oplister en række hensyn, som bør indgå i teleudbydernes vurdering af, om en videregivelse af de loggede oplysninger til civilretlig forfølgelse er forenelig med det oprindelige formål, som oplysningerne blev indsamlet til. Som nævnt i afsnit 2.2.4.2.2 benævnes denne vurdering forenelighedstesten.

3.7.2.3.1 Forenelighedstesten

De hensyn der kan indgå i forenelighedstesten, følger af forordningens artikel 6, stk. 4, litra a-e. Denne opstilling fremgår ligeledes af præambelbetragtning nr. 50, 1. led, sidste pkt. Herefter bør den dataansvarlige blandt andet tage hensyn til; ”...*enhver forbindelse mellem disse formål og formålet med den påtænkte viderebehandling, den sammenhæng, som personoplysningerne er blevet indsamlet i, navnlig de registreredes rimelige forventninger til den videre anvendelse heraf på grundlag af deres forhold til den dataansvarlige, personoplysningernes art, konsekvenserne af den påtænkte viderebehandling for de registrerede og tilstedeværelse af fornødne garantier i forbindelse med bade de oprindelige og de påtænkte yderligere behandlingsaktiviteter.*” Det skal bemærkes, at opstillingen, af de hensyn teleudbyderne bør iagttage i deres vurdering, ikke er udtømmende, jf. forordningens artikel 6, stk. 4. I nedenstående vil de relevante hensyn, som teleudbyderne bør iagttage i forbindelse med videregivelse til civilretlig forfølgelse blive belyst.

Teleudbyderne bør tage hensyn til enhver forbindelse mellem det oprindelige formål samt deres formål med viderebehandlingen, jf. forordningens artikel 6, stk. 4, litra a. Videregivelsen af navne- og adresseoplysninger tilknyttet IP-adresser, til henholdsvis strafferetlig og civilretlig forfølgelse, foretages i begge tilfælde for at holde den pågældende abonnent ansvarlig for en udført handling. Videregivelse til civilretlig forfølgelse af ophavsretlige krænkelse synes således at have en vis lighed med det oprindelige formål om anvendelse til efterforskning og retsforfølgning af strafbare forhold. I denne forbindelse bør teleudbyderne tillige overveje, hvilke konsekvenser en viderebehandling, til det påtænkte formål vedrørende civilretlig forfølgelse, kan have for abonnenten, jf. forordningens artikel 6, stk. 4, litra d. Rettighedshavernes krav udgør i nærværende afhandling en påstand om økonomisk kompensation. I denne forbindelse bør det tages i betragtning, at strafferetlig forfølgning som udgangspunkt er af grovere karakter, end krav der kan følges civilretligt. Det skal tillige bemærkes, at det vil udgøre en forskel for abonnenten, om oplysningerne videregives til en myndighed eller til en privat aktør i form af en rettighedshaver. Dette kan blandt andet understøttes af, at offentlige myndigheder er underlagt en lovbestemt tavshedspligt efter forvaltningslovens § 27, hvorimod private aktører alene er underlagt en tavshedspligt, hvis dette fremgår af særlovgivning eller aftale. Generelt er lovgrundlaget på det offentligretlige område udformet præceptivt, hvilket indebærer, at disse regelsæt ikke må fraviges til skade for en borger.¹²⁰ Desuden vil en konsekvens være, at videregivelsen udgør et indgreb i abonnenternes grundlæggende rettigheder, herunder retten til privatlivets fred. Teleudbyderne bør således være varsomme med at foretage en viderebehandling af hensyn til beskyttelse af abonnenternes grundlæggende rettigheder.

¹²⁰ Bønsing, Steen, 2013, s. 102.

Teleudbyderne indsamler de pågældende oplysninger som led i kontraktforholdet med abonnenterne. I denne forbindelse bør teleudbyderne vurdere sammenhængen, som oplysningerne er blevet indsamlet i, jf. forordningens artikel 6, stk. 4, litra b. Henset til forholdet mellem en teleudbyder og en abonnent bør det tages i betragtning, at abonnenten er forbruger, og dermed fremstår som en svagere part i forhold til teleudbyderen. I tilknytning til dette kontraktforhold er teleudbyderen pålagt en retlig forpligtelse i medfør af logningsbekendtgørelsens § 1, hvorefter en række oplysninger desuden skal indsamles, således disse oplysninger kan anvendes til efterforskning og retsforfølgning af strafbare forhold. Abonnenterne bør, ved indgåelsen af kontraktforholdet, være blevet oplyst om de udtrykkelige og legitime formål med behandlingen, jf. forordningens artikel 5, stk. 1, litra b. I denne sammenhæng kan der blandt andet henvises til Telenors databeskyttelsespolitik, hvor Telenor anfører, at de *“...i henhold til Logningsbekendtgørelsen [er] forpligtet til at opbevare visse typer oplysninger om teletrafik, der genereres og behandles i Telenors net, således at disse oplysninger vil kunne anvendes som led i politiets efterforskning og retsforfølgning af strafbare forhold.”*¹²¹ Endvidere kan henvises til Telias vilkår, hvor det anføres, at *“[v]i registrerer og opbevarer også de oplysninger, der er nødvendige til opfyldelse af reglerne i logningsbekendtgørelsen. Oplysninger omfattet af logningsbekendtgørelsen udleveres alene til myndighederne på grundlag af en kendelse fra en domstol.”*¹²² Videregivelse til civilretlig forfølgelse synes således ikke at være i overensstemmelse med det oplyste formål ved kontrakternes indgåelse.

Henset til kategorien af personoplysninger er udgangspunktet, som behandlet i afsnit 3.3.1, at navne- og adresseoplysningerne tilknyttet IP-adresser udgør almindelige personoplysninger. Dog kan der være tilfælde, hvor disse personoplysninger – i kombination med det tilgæede materiales indhold – udgør følsomme personoplysninger eller oplysninger om strafbare forhold. I henhold til forordningens artikel 6, stk. 4, litra c bør teleudbyderne tage hensyn til, hvilken kategori af personoplysninger der indsamles. Teleudbyderne bør være særligt forsigtige med at tillade viderebehandling, når viderebehandlingen vedrører følsomme personoplysninger eller oplysninger om strafbare forhold, da disse oplysninger er underlagt en større beskyttelse. Det anføres direkte i præambelbetragtning nr. 51, at følsomme personoplysninger skal nyde en specifik beskyttelse, da behandlingen af sådanne personoplysninger kan medføre betydelige risici for abonnentens grundlæggende rettigheder. Endvidere er der en særligt skærpet adgang til at behandle følsomme personoplysninger samt oplysninger om strafbare forhold, jf. forordningens artikel 9 og artikel 10, jf. databeskyttelseslovens § 8-10.

I forlængelse af forenelighedstesten er det relevant at inddrage kendelsen behandlet af Østre Landsret den 12. december 2016 (U.2017.1092Ø). Denne kendelse omhandler, hvorvidt politiet kunne få udleveret en blodprøve fra Statens Serum Institut til efterforskning af et drabsforsøg. Politiet ønskede at udarbejde en DNA-personprofil på den mistænkte. Blodprøven

¹²¹ Telenor.

¹²² Telia, 2020.

var udtaget med forældrenes samtykke, umiddelbart efter den mistænkte blev født. Formålet med blodprøven var at screene den mistænkte for medfødte sygdomme. Østre Landsret lagde i deres begrundelse vægt på, til hvilket formål blodprøven var udtaget. Endvidere lagde landsretten vægt på, at adgangen til blodprøven, efter reglerne om edition, ville medføre en tilsidesættelse af hensynene i DNA-profilregisterloven, herunder privatlivets fred i medfør af EMRK artikel 8. På denne baggrund fandt Østre Landsret, at politiet måtte være henvist til selv at indhente blodprøven efter de almindelige regler i retsplejelovens § 792b, stk. 1. Dette til trods for at sagen vedrørte en alvorlig forbrydelse og at den mistænkte var udrejst af landet. Østre Landsret tog således ikke editionsbegæringen om udlevering af blodprøven til følge.

Østre Landsret tog i U.2017.1092Ø hensyn til det formål, som blodprøven oprindeligt blev indsamlet til. Det må antages, at Østre Landsret i sin begrundelse indirekte lægger vægt på, at en videregivelse af blodprøven til efterforskning af politiet vil være uforeneligt med det oprindelige formål, som blodprøven blev indsamlet til, nemlig screening for medfødte sygdomme samt forskning. Kendelsen illustrerer således, at selvom alvorlige samfundsmæssige hensyn gør sig gældende, kræves særligt tungtvejende grunde, førend formålet kan anses for at være foreneligt med det oprindelige formål.

På baggrund af ovenstående kan det udledes at samme interesse ønskes forfulgt, uanset om viderebehandlingen sker til strafferetlig eller civilretlig forfølgelse, da abonnenterne i begge tilfælde ønskes retsforfulgt som følge af en udført handling. Henset til dette forekommer en viderebehandling til civilretlig forfølgelse ikke uforenelig med det oprindelige formål vedrørende efterforskning og retsforfølgning af strafbare forhold.

Modsat kan det udledes, at det udgør en væsentlig forskel for abonnenterne, hvorvidt viderebehandling foretages af en offentlig myndighed eller en rettighedshaver. Endvidere vil det for abonnenterne forekomme mere indgribende i disses grundlæggende rettigheder, at der sker viderebehandling til brug for civilretlig forfølgelse, da karakteren heraf ikke må forventes at have samme grovhed som strafbare forhold. En civilretlig forfølgelse vil således medføre, at abonnenterne kan retsforfølges for forhold af mindre grov karakter. Til sammenligning fremgår det af U.2017.1092.Ø, at en videregivelse ikke kan rummes i det oprindelige formål, uanset at videregivelse skulle ske til forfølgelse af grov kriminalitet. Det forekommer således uhensigtsmæssigt, hvis viderebehandling kan ske til forfølgelse af mindre grove forhold end fastsat i det oprindelige formål.

Sammenfattende kan det, som følge af forenelighedstesten i forordningens artikel 6, stk. 4 samt U.2017.1092Ø, udledes, at viderebehandling, med henblik på videregivelse til civilretlig forfølgelse, ikke vil være foreneligt med det oprindelige formål vedrørende efterforskning og retsforfølgning af strafbare forhold.

3.8 Teleudbyderes videregivelse uden for logningsbekendtgørelsens anvendelsesområde

Logningsbekendtgørelsen angiver, som nævnt i afsnit 3.7.2.3, ikke tydeligt i hvilket omfang, det er tilladt at videregive navne- og adresseoplysninger tilknyttet IP-adresser til forfølgelse af civilretlige krav. Imidlertid forekommer det mest hensigtsmæssigt, hvis en sådan videregivelse ikke kan ske henset til logningsbekendtgørelsens formål samt uoverensstemmelsen med de persondataretlige regler og principper. Dette vil for rettighedshaverne betyde, at en civilretlig forfølgelse af de ophavsretlige krænkelse er udelukket, da rettighedshaverne, først bliver bekendt med de potentielle krænkeres identitet ved udlevering af navne- og adresseoplysninger tilknyttet IP-adresser fra teleudbyderne.

Det må dog tilsvarende findes uhensigtsmæssigt, at rettighedshavere fratages deres eneste mulighed for at forfølge de ophavsretlige krænkelse. Det er derfor relevant at undersøge, i hvilket omfang der kan ske videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser uden for logningsbekendtgørelsens formål og anvendelsesområde.

En særlig problemstilling i denne tilknytning er, at teleudbydere opbevarer oplysningerne i en længerevarende periode, end hvad teleudbydernes egne formål kræver. Dette sker alene på baggrund af opbevaringsforpligtelsen på 1 år i logningsbekendtgørelsens § 9. I denne sammenhæng kan der henvises til afsnit 3.7.1, hvor det uddybes, at Telenor, Telia og TDC opbevarer oplysningerne i henholdsvis 30 dage og 3 uger til egne formål med henblik på fejlretning. Når perioden på henholdsvis 30 dage og 3 uger er forløbet, sker den længerevarende opbevaring som følge af opbevaringsforpligtelsen i logningsbekendtgørelsen. Teleudbyderne vil således ikke være i stand til at videregive navne- og adresseoplysningerne efter perioden på henholdsvis de 30 dage og 3 uger er forløbet, hvis ikke det var for opbevaringsforpligtelsen i logningsbekendtgørelsen. Det er således interessant at belyse, hvorvidt der kan ske videregivelse af de pågældende oplysninger inden for den periode, hvor teleudbyderne behandler oplysningerne til egne formål. I det følgende behandles teleudbydernes behandlingsgrundlag i henhold til forordningens regler og principper.

I henhold til eksemplet med Rasmus betyder dette, at Telenor alene vil være i besiddelse af abonnenternes personoplysninger i op til 30 dage som følge af deres egne formål med behandlingen.

3.8.1 Behandling af personoplysninger

Teleudbyderne skal have et retligt grundlag for behandlingen af de pågældende navne- og adresseoplysninger tilknyttet IP-adresser. Det retlige grundlag for behandlingen er gennemgået i afsnit 2.2.5, hvilket i det væsentligste er sammenfaldende med teleudbydernes behandlingsgrundlag i det følgende, både for så vidt angår teleudbyderens opbevaring og videregivelse.

Imidlertid vil teleudbydernes retlige grundlag for opbevaringen ikke kunne støttes på en retlig forpligtelse, når der i nærværende afsnit ses bort fra opbevaringspligten i medfør af logningsbekendtgørelsen, jf. forordningens artikel 6, stk. 1, litra e. Teleudbydernes retlige grundlag for behandlingen vil i det følgende hvile på aftaleforholdet mellem teleudbyderen og abonnenten, jf. forordningens artikel 6, stk. 1, litra b eller alternativt støttes på et samtykke fra abonnenten, jf. forordningens artikel 6, stk. 1, litra a.

Det retlige grundlag for videregivelsen af de pågældende oplysninger vil derimod være identisk med de gennemgåede behandlingsgrundlag i afsnit 3.6.

Uanset at der foreligger et retligt behandlingsgrundlag til videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser, er det tillige relevant at undersøge, hvorvidt videregivelsen er i overensstemmelse med de grundlæggende persondataretlige behandlingsprincipper.

Henset til de persondataretlige principper i forordningens artikel 5 forekommer det særligt relevant at inddrage forordningens artikel 5, stk. 1, litra a vedrørende lovlighed, rimelighed og gennemsigtighed. Herefter skal teleudbyderne behandle personoplysninger på en lovlig, rimelig og gennemsigtig måde i forhold til sine abonnenter, jf. forordningens artikel 5, stk. 1, litra a. Dette indebærer, at en abonnent skal være bekendt med behandlingens formål samt i hvilket omfang dennes personoplysninger behandles og fremadrettet vil blive behandlet af teleudbyderen. Formålet skal være veldefineret og præcist angivet således, at der skabes gennemsigtighed for abonnenten i forhold til behandlingen af dennes personoplysninger, jf. præambelbetragtning nr. 39. Formålet med teleudbydernes behandling af navne- og adresseoplysninger tilknyttet IP-adresser er, som angivet i Østre Landsrets kendelse af den 7. maj 2018, fejlretning. En abonnent forventes således ikke at kunne påregne, at de pågældende oplysninger tillige anvendes til civilretlig forfølgning. I relation til formålet forekommer en videregivelse til forfølgelse af et civilretligt krav således hverken rimelig eller gennemsigtig for abonnenten.

Formålet med behandlingen har tillige betydning i relation til forordningens artikel 5, stk. 1, litra b vedrørende finalité-princippet. Som følge af finalité-princippet må navne- og adresseoplysninger tilknyttet IP-adresser alene behandles til de udtrykkeligt angivne og legitime formål, og må ikke viderebehandles på en måde, der er uforeneligt med dette oprindelige formål. Teleudbydernes udtrykkeligt angivne og legitime formål med behandlingen af oplysningerne er som nævnt at kunne foretage fejlretning. En videregivelse til forfølgelse af civilretlige krav synes ikke at være omfattet af det oprindelige formål vedrørende fejlretning. Spørgsmålet er således, hvorvidt en viderebehandling til civilretlig forfølgelse er forenelig med dette formål.

I teleudbyderens vurdering af hvorvidt en viderebehandling er forenelig med det oprindelige formål, kan der henvises til en række hensyn i forordningens artikel 6, stk. 4 samt præambelbetragtning nr. 51. Denne vurdering kaldes forenelighedstesten og er behandlet i afsnit 2.2.4.2.2.

Henset til ovenstående er det oprindelige formål med teleudbydernes behandling fejlretning og formålet med den påtænkte viderebehandling til civilretlig forfølgelse. Der er som udgangspunkt ikke nogen forbindelse mellem det oprindelige formål og formålet med den påtænkte viderebehandling. Desuden vil en viderebehandling til civilretlig forfølgelse medføre uforudsigelige konsekvenser for abonnenterne, som ikke kan påregnes at være omfattet af teleudbydernes formål vedrørende fejlretning. En videregivelse til civilretlig forfølgelse synes således umiddelbart at stå i kontrast til dette formål.

Endvidere er forenelighedstesten behandlet i afsnit 3.7.2.3.1 i relation til logningsbekendtgørelsen. I denne forenelighedstest er det oprindelige formål med behandlingen videregivelse til efterforskning og retsforfølgning af straffbare forhold, mens formålet med den påtænkte viderebehandling er civilretlig forfølgning. Det blev i denne forbindelse udledt, at viderebehandling til civilretlig forfølgelse ikke vil være i overensstemmelse med det oprindelige formål. Henset til formålet vedrørende fejlretning må det tages i betragtning, at strafferetlig forfølgning har flere ligheder med civilretlig forfølgning end fejlretning. Uanset at strafferetlig forfølgning har flere ligheder med civilretlig forfølgning fandtes en sådan viderebehandling stadig ikke forenelig.

Det kan på denne baggrund udledes, at viderebehandling til civilretlig forfølgelse næppe vil være forenelig med det oprindelige formål vedrørende fejlretning.

På baggrund af ovenstående kan det sammenfattende fastslås, at teleudbyderne har et retligt behandlingsgrundlag til henholdsvis opbevaring og videregivelse uden for logningsbekendtgørelsens formål og anvendelsesområde. Uanset at teleudbyderne har et retligt grundlag for behandlingen, findes denne behandling ikke at være i overensstemmelse med de persondataretlige behandlingsprincipper i forordningens artikel 5.

Rettighedshavernes mulighed for at få udleveret navne- og adresseoplysningerne tilknyttet IP-adresser forekommer således sammenfaldende, uanset om teleudbyderne opbevarer disse oplysninger til egne formål eller i medfør af logningsbekendtgørelsens formål.

Kapitel 4

4.1 Konklusion

Hensigten med nærværende afhandling har været at belyse, hvorvidt teleudbyderes videregivelse af en abonnents navne- og adresseoplysninger tilknyttet IP-adresser er i overensstemmelse med persondataretten, når oplysningerne videregives til rettighedshavere, der ønsker at forfølge ophavsretlige krænkelse civilretligt.

Henset til ovenstående kan det konkluderes, at en abonnent er omfattet af forordningens anvendelsesområde, hvis denne er en fysisk person, som direkte eller indirekte kan

identificeres. Navne- og adresseoplysninger vedrørende abonnenter udgør personoplysninger i medfør af forordningens artikel 4, nr. 1. Endvidere kan det på baggrund af Patrick Breyer mod Bundesrepublik Deutschland (C-582/14) konkluderes, at dynamiske IP-adresser udgør personoplysninger.

Udgangspunktet er, at navne, adresser og IP-adresser isoleret set udgør almindelige personoplysninger. Dette følger af forordningens artikel 9, stk. 1 modsætningsvis. Tilsvarende er dette fastslået af retten på Frederiksberg i deres kendelse af den 24. oktober 2017 samt Datatilsynets afgørelse publiceret den 12. juli 2017 (journalnr. 2016-217-1119).

Navne- og adresseoplysninger tilknyttet IP-adresser kan ændre karakter fra almindelige personoplysninger til følsomme personoplysninger, når disse kombineres med det tilgæede materiales indhold. Dette forudsætter dog, at materialets indhold tydeliggør, at dette vedrører følsomme personoplysninger som omfattet af forordningens artikel 9, stk. 1. Ligeledes kan navne- og adresseoplysninger tilknyttet IP-adresser udgøre oplysninger om strafbare forhold, når disse kombineres med oplysninger om den ophavsretlige krænkelse. Dette fastsætter Datatilsynet tillige i deres afgørelse publiceret den 12. juli 2017 (journalnr. 2016-217-1119).

Teleudbydernes behandling af de pågældende navne- og adresseoplysninger tilknyttet IP-adresser består i henholdsvis opbevaring og videregivelse.

På baggrund af ovenstående kan det fastslås, at opbevaring af navne- og adresseoplysninger tilknyttet IP-adresser udelukkende vil udgøre behandling af almindelige personoplysninger, hvorfor det retlige behandlingsgrundlag skal findes i forordningens artikel 6. Det kan i denne forbindelse konkluderes, at teleudbyderne dels opbevarer de pågældende personoplysninger på grundlag af aftaleforholdet med abonnenten og dels som følge af en retlig forpligtelse. Desuden kan teleudbyderne opbevare personoplysningerne på grundlag af et samtykke fra abonnenten.

Det kan fastslås, at en retlig forpligtelse til opbevaring følger af logningsbekendtgørelsen, da navne- og adresseoplysninger tilknyttet IP-adresser udgør logget data. Forpligtelsen i logningsbekendtgørelsen indebærer, at teleudbydere skal opbevare oplysningerne i 1 år, hvilket medfører en længere opbevaringsperiode end nødvendigt for opfyldelse af aftaleforholdet. Det kan således konkluderes, at teleudbydere ikke fortsat ville være i besiddelse af navne- og adresseoplysningerne tilknyttet IP-adresser, hvis ikke logningsbekendtgørelsen pålagde en opbevaringspligt. Dette anføres tillige af Østre Landsret i deres kendelse af den 7. maj 2018. I forlængelse heraf kan det fastslås, at teleudbyderne ikke må opbevare en større mængde data eller opbevare disse data i et længere tidsrum end hvad logningsbekendtgørelsen fastsætter, jf. forordningens principper om dataminimering og opbevaringsbegrænsning.

Navne- og adresseoplysninger tilknyttet IP-adresser kan ændre karakter til henholdsvis følsomme personoplysninger og oplysninger om strafbare forhold. Dette sker, når oplysningerne sættes i forbindelse med det tilgæede materiales indhold og/eller rettighedskrænkelsen, hvorfor rette behandlingshjemmel til videregivelse skal findes i henholdsvis forordningens artikel 6, 9 og 10. I forbindelse hermed kan det konkluderes, at

teleudbydere lovligt kan videregive navne- og adresseoplysninger tilknyttet IP-adresser, såfremt der foreligger en editionskendelse.

Såfremt der ikke foreligger en editionskendelse, kan det konkluderes, med henvisning til Datatilsynets afgørelse publiceret den 20. november 2003 (journalnr. 2002-219-0135), at en videregivelse er lovlig, såfremt interesseafvejningsreglen i forordningens artikel 6, stk. 1, litra f tillader dette. Hensynene i denne afvejning er dog af så væsentlig og modsatrettede karakter, at der bør foreligge en editionskendelse. Herudover kan det på grundlag af Tele2/Watson-dommen (C-203/15 og C-698/15) konkluderes, at adgangen til loggede data alene bør gives efter forudgående kontrol af en domstol eller administrativ myndighed. På baggrund af disse afgørelser må det fastslås, at videregivelse af henholdsvis følsomme personoplysninger og oplysninger om strafbare forhold ligeledes ikke bør ske uden en editionskendelse, særligt henset til oplysningernes fortrolige karakter og disse oplysningers beskyttelsesinteresse. Dette uanset at der ikke fremgår en interesseafvejningsregel af forordningens artikel 9, stk. 2.

I retspraksis har der eksisteret en generel tendens til at videregive navne- og adresseoplysninger tilknyttet IP-adresser til rettighedshavere, som ønsker at forfølge en krænkelse civilretligt. Oplysningerne, der videregives, er imidlertid omfattet af logningsbekendtgørelsen. På baggrund af logningsbekendtgørelsens klare formål kan det konkluderes, at videregivelse alene bør ske til efterforskning og retsforfølgelse af strafbare forhold. Dette henset til at politiet har den mest vidtgående kompetence til at foretage efterforskning, at retspraksis indikerer, at videregivelse alene kan ske til myndigheder og at videregivelse alene kan ske til bekæmpelse af grov kriminalitet. Desuden kan det konkluderes, at en videregivelse til civilretlig forfølgelse ikke vil være i overensstemmelse med princippet om lovlighed, rimelighed og gennemsigtig i forhold til abonnenten. Dog indikerer Østre Landsrets kendelse af den 7. maj 2018, at en videregivelse til civilretlig forfølgning ikke kan udelukkes i medfør af logningsbekendtgørelsen.

Uanset at videregivelse til civilretlig forfølgelse må konkluderes ikke at være omfattet af logningsbekendtgørelsens formål, kan det som følge af Promusicae (C-275/06) fastlægges, at det ikke forhindrer Danmark i at vedtage national lovgivning, der fastsætter en sådan pligt.

I forlængelse heraf kan det konkluderes, at princippet om formålsbegrænsning, hensynene i forenelighedstesten samt U.2017.1092Ø medfører, at viderebehandling, med henblik på videregivelse til civilretlig forfølgelse, ikke vil være forenelig med det oprindelige formål i logningsbekendtgørelsen vedrørende efterforskning og retsforfølgning af strafbare forhold.

Uden for logningsbekendtgørelsens formål og anvendelsesområde kan det fastslås, at teleudbyderne har et retligt grundlag til henholdsvis opbevaring og videregivelse af navne- og adresseoplysninger tilknyttet IP-adresser, når disse opbevares til teleudbydernes egne formål. Det må imidlertid konkluderes, at en videregivelse af disse oplysninger ikke vil være i overensstemmelse med de persondataretlige principper, uanset at der foreligger et retligt behandlingsgrundlag.

Uanset at teleudbyderne har et retligt behandlingsgrundlag, må det konkluderes, at det i medfør af princippet om lovlighed følger, at rettighedshaverne tillige skal have et behandlingsgrundlag for at modtage de pågældende personoplysninger, førend teleudbydernes videregivelse er lovlig. I forlængelse heraf kan det konkluderes, at rettigheds-haverne har et retligt grundlag for behandling af navne- og adresseoplysninger tilknyttet IP-adresser

Sammenfattende kan det konkluderes, at teleudbyderes videregivelse af de pågældende personoplysninger ikke er i overensstemmelse med persondataretten, når dette sker til rettighedshaveres civilretlige forfølgelse af ophavsretlige krænkelse. Dette uanset om oplysningerne er opbevaret i medfør af logningsbekendtgørelsens formål eller til teleudbydernes egne formål.

Kapitel 5

5.1 Perspektivering til nordiske lande

Henledes opmærksomheden på andre nordiske lande findes henholdsvis en afgørelse fra den finske højesteret (KKO:2017:85) og en afgørelse fra den norske højesteret (HR-2017-883-A) med lignende problemstillinger. Disse problemstillinger vedrører tilsvarende, hvorvidt der kan ske videregivelse af abonnenters oplysninger til civilretlig forfølgelse af ophavsretlige krænkelse.

I denne sammenhæng er det væsentlig at bemærke, at nordisk retspraksis ikke har nogen direkte betydning for dansk ret. Derimod er det åbenbart, at der indhentes inspiration fra andre landes praksis, hvorfor det forekommer interessant at sammenholde dansk ret med disse sammenlignelige afgørelser fra disse nordiske lande.¹²³

Imidlertid er behandlingen af personoplysninger i det væsentligste reguleret i forordningen. Denne forordning er direkte anvendelig i EU-medlemsstaterne og dermed Finland og Danmark.¹²⁴ Uanset at Norge ikke er medlem af EU, skal de, som følge af deres medlemskab af Det Europæiske Økonomiske Samarbejdsområde (EØS), overholde forordningen.¹²⁵ Den persondataretlige regulering er derfor i det væsentligste identisk i de nordiske lande.

I det følgende vil der blive perspektiveret til, hvorledes videregivelse af abonnenters personoplysninger til civilretlig forfølgelse bedømmes i udvalgt nordisk retspraksis. Nedenstående afgørelser er valgt, da de er afsagt i de pågældende landes højesteret og samtidig er forholdsvis nye, hvorfor de har høj præjudikatværdi.

¹²³ Munk-Hansen, Carsten, 2014, s. 256.

¹²⁴ Munk-Hansen, Carsten, 2014, s. 260.

¹²⁵ Den generelle forordning om databeskyttelse: nye muligheder, nye forpligtelser, s. 15.

5.1.1 Finsk Højesteretsafgørelse af den 8. december 2017 (KKO:2017:85)

Sagen omhandler i hovedtræk, hvorvidt en teleudbyder kan tilpligtes at videregive kontaktoplysninger på sine abonnenter til en rettighedshaver med henblik på, at rettighedshaveren kan identificere en mulig krænker og omfanget af ophavsretskrænkelsen.

Indledningsvist skal det bemærkes, at der i den finske lovgivning findes to bestemmelser, som giver adgang til videregivelse af kontaktoplysninger på teleudbyderes abonnenter. I medfør af kodeks for informationssamfundets § 137 kan teleudbyderne lagre oplysninger til egne behov i 6 måneder. Bestemmelsen fastslår, at behandling af oplysningerne kun må ske til de krævede formål og ikke må begrænse beskyttelsen af privatlivets fred mere end nødvendigt. I kodeks for informationssamfundets § 157 pålægges teleudbyderne at lagre oplysninger i 9 måneder til myndighedsbehov, hvorefter oplysningerne alene må anvendes med henblik på afklaring af lovovertrædelser og strafferetlig forfølgning, jf. præmis 8-9.

I sagen modsatte teleudbyderen sig at videregive oplysningerne, som var lagret til myndighedernes behov i medfør af kodeks for informationssamfundets § 157, da teleudbyderen hverken anså sig for berettiget eller forpligtet til at videregive disse oplysninger til rettighedshaveren.

Den finske højesteret fastslår i afgørelsen, at de loggede oplysninger er omfattet af forfatningens § 10 vedrørende privatlivets fred og fortrolig kommunikation, jf. præmis 11. Endvidere fastslår den finske højesteret, hvad der forstås ved ordlyden i § 157. Herefter fastsætter den finske højesteret, at oplysningerne lagret i henhold til § 157 udelukkende kan videregives til myndigheder og til de i bestemmelsen udtrykkeligt fastsatte formål, jf. præmis 17. I denne sammenhæng finder den finske højesteret, at rettighedshaveren ikke udgør en sådan myndighed. Desuden lægger den finske højesteret til grund, at rettighedshaveren ikke skal anvende oplysninger til et af de i bestemmelsen fastsatte formål. Den finske højesteret fastslår derfor, at der ikke kan ske videregivelse til rettighedshaveren af de kontaktoplysninger, som teleudbyderen behandler til myndighedernes behov efter kodeks om informationssamfundets § 157.

Den finske højesteret anfører endvidere, at oplysninger lagret til teleudbydernes egne behov efter kodeks om informationssamfundets § 137 kan videregives til rettighedshaveren. Den finske højesteret konstaterer i forbindelse hermed, at der ved anvendelse af § 137 skal iagttages et centralt princip, hvorefter teleudbyderenes behandling af elektroniske meddelelser og formidlingsoplysninger alene må ske til de krævede formål og ikke må begrænse beskyttelsen af privatlivets fred mere end nødvendigt. I denne forbindelse henviser den finske højesteret til retspraksis fra EU-domstolen for at understrege, at begrænsninger i de grundlæggende rettigheder, herunder beskyttelsen af personoplysninger, alene kan gennemføres efter en proportionalitetsafvejning og alene når det findes strengt nødvendigt, jf. præmis 16.

5.1.2 Norsk Højesteretsafgørelse af 26. april 2017 (HR-2017-833-A)

Sagen omhandler, hvorvidt en rettighedshaver kan få udleveret identiteten på abonnenter bag en række angivne IP-adresser på baggrund af § 56b tredje led i åndsverkloven. I denne forbindelse opstår der spørgsmål om forståelsen af tredje led i åndsverkslovens § 56b. Den norske Højesteret havde i sagen alene kompetence til at tage stilling til landsrettens generelle lovforklaring.

Åndsverkslovens § 56b, tredje led angiver, at der, i forbindelse med videregivelse af identiteten på abonnenter, skal foretages en afvejning af rettighedshaverens interesser over for abonnentens interesser. I denne afvejning skal der tages hensyn til krænkelsens grovhed, omfang og skadevirkninger. Den norske Højesteret uddyber det centrale i afvejningen ved at inddrage lovens forarbejder, hvorefter *"[r]ettighetshaverens interesser må altså veies mot hensynet til abonnentens personvern. Krenkelsens alvorlighetsgrad vil være et sentralt moment i vurderingen. Hvis krenkelsen er av et visst omfang, bør utgangspunktet være at det gis tilgang til opplysningene"*, jf. præmis 36. Den Norske Højesteret, når dermed frem til, at videregivelsen af navne- og adresseoplysninger tilknyttet en IP-adresse beror på en vurdering af hensynet til abonnentens krav på beskyttelse af privatlivets fred over for hensynet til krænkelsens grovhed.

5.1.3 Sammenfattende om nordisk retspraksis

Afgørelserne fra henholdsvis den norske og den finske højesteret illustrerer, at lignende problemstillinger vedrørende videregivelse af personoplysninger til forfølgelse af ophavsretlige krænkelse utvivlsomt forekommer i andre nordiske lande. Henset til ovenstående afgørelser forudsætter videregivelse en interesseafvejning af henholdsvis abonnentens og rettighedshaverens interesser. I denne afvejning skal der særligt tages hensyn til abonnentens ret til privatlivets fred og dermed retten til beskyttelse af personoplysninger.

Der ses herved en lighed mellem afgørelserne fra henholdsvis den norske og finske højesteret samt dansk retspraksis, herunder Østre Landsrets kendelse af den 7. maj 2018. Disse afgørelser fastslår, at en interesseafvejning er påkrævet, førend der kan ske videregivelse af abonnenters personoplysninger. I den påkrævede interesseafvejning er det i alle tilfælde et væsentligt hensyn at inddrage abonnenternes ret til privatlivets fred og dermed retten til beskyttelse af personoplysninger.

Perspektiveringen indikerer, at der tilsvarende i Norge og Finland, foreligger en skærpet adgang for rettighedshavere til få udleveret oplysninger til retsforfølgning af ophavsretlige krænkelse. Privatlivets fred er et tungtvejende hensyn i interesseafvejningen, uanset at alternativet for rettighedshaverne er, at de ophavsretlige krænkelse ikke kan forfølges.

Litteraturliste

Litteratur

Blume, Peter, "Den nye persondataret", 2. udgave, Jurist- og Økonomforbundets Forlag, 2018.

(Forkortes: Blume, Peter, 2018)

Bønsing, Steen, "Almindelig Forvaltningsret", 3. udgave, Jurist- og Økonomforbundets Forlag, 2013.

(Forkortes: Bønsing, Steen, 2013)

Christensen, Jens Peter, m.fl., "Dansk Statsret", 1. udgave, Jurist- og Økonomforbundets Forlag, 2012.

(Forkortes: Christensen, Jens Peter, m.fl., 2012)

Evald, Jens, "Retskilderne og den juridiske metode", 2. udgave, Jurist- og Økonomforbundets Forlag, 2000.

(Forkortes: Evald, Jens, 2000)

Langsted, Lars Bo, "Waaben Strafferettens almindelige del Ansvarslæren", 6. udgave, Karnov Group Denmark A/S, 2015.

(Forkortes: Langsted, Lars Bo, 2015)

Munk-Hansen, Carsten, "Retsvidenskabsteori", 1. udgave, Jurist- og Økonomforbundets Forlag, 2014.

(Forkortes: Munk-Hansen, Carsten, 2014)

Trzaskowski, Jan, m.fl., "Internetretten", 3. udgave, Ex Tutu Publishing A/S, 2017.

(Forkortes: Trzaskowski, Jan, 2017)

Lovreferencer

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

(Forkortes: Logningsbekendtgørelsen)

Bekendtgørelse 2011-06-23 nr. 715 vedrørende udbud af elektroniske kommunikationsnet og -tjenester

(Forkortes: Udbudsbekendtgørelsen)

Den Europæiske Menneskerettighedskonvention, Konvention til beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder, ændret ved 3., 5., 8., 11. og 14. tillægsprotokol.

(Forkortes: EMRK)

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

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

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

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

Europæiske Unions Charter om Grundlæggende Rettigheder, (2010/C 83/02).
(Forkortes: Chateret)

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

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

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

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

Lovbekendtgørelse 2014-04-22 nr. 433, Forvaltningsloven
(Forkortes: Forvaltningsloven)

Lovbekendtgørelse 2019-09-10 nr. 938 om rettens pleje
(Forkortes: Retsplejeloven)

Lovbekendtgørelse 2019-09-17 nr. 976, Straffeloven
(Forkortes: Straffeloven)

Verdenserklæringen om Menneskerettigheder, udstedt af de Forenede Nationers
Generalforsamling den 10. december 1948.
(Forkortes: Verdenserklæringen om menneskerettigheder, 1948)

Forarbejder

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

Forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i
forbindelse med behandling af personoplysninger og om fri udveksling af sådanne
oplysninger (generel forordning om databeskyttelse), den 25. januar 2012.
(Forkortes: Forslag til databeskyttelsesforordningen, 2012)

Lovforslag nr. 68 om supplerende bestemmelser til forordning om beskyttelse af fysiske
personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne
oplysninger (databeskyttelsesloven) fremsat den 25. oktober 2017
(Forkortes: Lovforslag nr. 68)

Tidsskriftsartikler

Lentz, Lene Wachter, "Logning af teledata i lyset af Tele2-dommen", Juristen nr. 5, Jurist- og
Økonomforbundets Forlag, 2017.
(Forkortes: Lentz, Lene Wachter, 2017)

Vestergaard, Jørn, "EU-strafferetten og individets grundlæggende rettigheder", Tidsskrift for
Kriminalret, TfK2016.429, Karnov Group Denmark A/S, 2016.
(Forkortes: Vestergaard, Jørn, TfK2016.429)

Dansk retspraksis

U.2017.1092 Ø
U.2019.2019 Ø

Utrykt retspraksis

Kendelse afsagt af Retten på Frederiksberg fra den 14. maj 2012: BS Z-439/2012, BS Z-
440/2012 og BS Z-441/2012, bilag 9

Kendelse afsagt af Retten på Frederiksberg den 11. maj 2016: sag nr. BS B-2443/2015, bilag
6.

Kendelse afsagt af Retten på Frederiksberg den 10. november 2015: sag nr. BS E-1984/2015, bilag 4.

Kendelse afsagt af Retten på Frederiksberg den 22. september 2015: BS K-1271/2015, bilag 7.

Kendelse afsagt af Retten på Frederiksberg den 15. juni 2017: sag nr. BS A-681/2017, bilag 5.

Kendelse afsagt af Retten på Frederiksberg den 16. august 2017: sag nr. BS K-741/2017, bilag 3.

Kendelse afsagt af Retten på Frederiksberg den 3. november 2017: sag nr. BS A-1417/2017, bilag 2.

Øvrige kendelser, hvor teleudbydere er blevet pålagt at videregive oplysninger, bilag 10.

Dom afsagt af Retten på Frederiksberg den 22. maj 2019: sag BS-31445/2018-FRB, bilag 8.

EU-retspraksis

C-275/06, den 29. januar 2008

C-461/10, den 19. april 2012

C-293/12, den 8. april 2014

C-582/14, den 19. oktober 2016

C-203/15 og C-698/15, den 21. december 2016

Nordisk retspraksis

Afgørelse afsagt af Norges Højesteret den 26. april 2017: HR-2017-833-A (sag nr. 2016(2216), bilag 12.

Afgørelse afsagt af Finlands Højesteret den 8. december 2017: KKO:2017:85, bilag 11.

Administrativ praksis

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

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

Journalnr. 2018-31-0070, ”Klage over TDC’s registrering af trafik- og lokaliseringsdata”, Datatilsynet, den 11. februar 2019

Vejledninger

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

Datatilsynet, ”Samtykke”, Justitsministeriet, september 2019.
(Forkortes: Datatilsynets vejledning: samtykke, 2019)

Datatilsynet, ”Vejledning om dataansvarlige og databehandlere”, Justitsministeriet, november 2017.
(Forkortes: Datatilsynets vejledning om dataansvarlige og databehandlere, 2017)

Retten på Frederiksberg, ”Vejledning til parterne i sager om ulovlig download og deling af film”, Danmarks Domstole, den 5. februar 2020.
(Forkortes: Retten på Frederiksbergs vejledning af den 5. februar 2020)

Internetkilder

Andersen, Mads Bryde, ”tredjemand”, Gyldendal - Den Store Danske, den 2. juni 2014, http://denstoredanske.dk/Samfund,_jura_og_politik/Jura/Obligationsret/tredjemand (besøgt d. 03-03-20).
(Forkortes: Andersen, Mads Bryde, 2014).

Breinstrup, Thomas, ”Teleselskaber vil bremse advokaters jagt på tusindvis af danske piratkopister”, Berlingske, den 3. marts 2020, bilag 1.
(Forkortes: Breinstrup, Thomas, 2020)

Danmarks Domstole, ”Anlæg civil sag”, <https://www.domstol.dk/saadangoerdu/civilesager/Pages/default.aspx> (besøgt d. 08-04-20)
(Forkortes: Danmarks Domstole, civil sag)

Danmarks Domstole, ”Orientering til parterne i sager omkring fildeling”, den 24. Februar 2020, https://www.domstol.dk/koebenhavn/aktuelt/2020/2/orientering-til-parterne-i-sager-omkring-fildeling/?fbclid=IwAR3eW_6PXff7zFFTjJANB3CefOt-Bf2UD7Szz-UmYFihfe6m5QEWcyiYj4s (besøgt d. 06-03-20)
(Forkortes: Danmarks Domstole, fildeling)

Europa-Kommissionen, ”Den generelle forordning om databeskyttelse: nye muligheder, nye forpligtelser”, Den Europæiske Unions Publikationskontor, 2018, https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_da.pdf (besøgt d. 01-05-20)
(Forkortes: Den generelle forordning om databeskyttelse: nye muligheder, nye forpligtelser)

Koch, Henning, ”efterforskning”, Gyldendal - Den Store Danske, den 30. januar 2009, http://denstoredanske.dk/Samfund,_jura_og_politik/Politi/Politivirksomhed/efterforskning (besøgt d. 29-04-20).

(Forkortes: Koch, Henning, 2009)

Poulsen, Dan, ” Anklagerne rammer som spredhagl”, Artikelserien Piratbrevenes Årti - del 2, K-News, den 10. januar 2020, <https://www.k-news.dk/nyheder/piratbrevenes-aarti.-anklagerne-rammer-som-spredhagl> (besøgt d. 02-03-20).

(Forkortes: Poulsen, Dan, del 2, 2020)

Poulsen, Dan, ” Forretning eller retfærdighed”, Artikelserien Piratbrevenes Årti - del 1, K-News, den 9. januar 2020, <https://www.k-news.dk/nyheder/piratbrevenes-aarti-forretning-eller-retfaerdighed.-del-1> (besøgt d. 05-03-20).

(Forkortes: Poulsen, Dan, del 1, 2020)

Poulsen, Dan, ”Retspræsident om Piratsagerne: ”Man bør nok ikke prøve at få folk til at betale noget”, Artikelserien Piratbrevenes Årti - nyhed, K-News, den 10. februar 2020, <https://www.k-news.dk/nyheder/retspraesident-om-piratbrevskravene-man-boer-nok-ikke-proeve-at-faa-folk-til-at-betale-noget> (besøgt d. 21-04-20).

(Forkortes: Poulsen, Dan, nyhed, 10-02-2020)

Poulsen, Dan, ” Ukendt beløb hentes hjem”, Artikelserien Piratbrevenes Årti - del 3, K-News, den 13. januar 2020, <https://www.k-news.dk/nyheder/ukendt-beloeb-hentes-hjem-i-piratbrevenes-aarti> (besøgt d. 05-03-20).

(Forkortes: Poulsen, Dan, del 3, 2020)

Poulsen, Dan, ” Usædvanlig vejledning om piratbreve til alle byretter”, Artikelserien Piratbrevenes Årti - nyhed, K-News, den 7. februar 2020, <https://www.k-news.dk/nyheder/usaedvanlig-vejledning-om-piratbreve-sendt-til-alle-byretter> (besøgt d. 22-04-20).

(Forkortes: Poulsen, Dan, nyhed, 07-02-2020)

Peteresen, Steen, ”Uskyldige internetbrugere stævnes for ulovlig download”, Ret&Råd, den 19. juli 2019, <https://www.ret-raad.dk/blog/internetbrugere-staevnes-for-ulovlig-download> (besøgt d. 02-03-20).

(Forkortes: Peteresen, Steen, 2019)

Stenz, Emil, ” It-jurist: Advokater skræmmer folk med tynde bøder for ulovlig download af film”, Politikken, den 16. februar 2016, <https://politiken.dk/forbrugogliv/digitalt/art5611444/It-jurist-Advokater-skræmmer-folk-med-tynde-bøder-for-ulovlig-download-af-film> (besøgt d. 02-03-20).

(Forkortes: Stenz, Emil, 2016)

Telenor A/S, ”Databeskyttelsespolitik”, <https://www.telenor.dk/andet/privacyregler/> (besøgt d. 30-04-20).

(Forkortes: Telenor)

Telia Danmark A/S, ”Vilkår for privatkunder i Telia”, februar 2020,
https://www.telia.dk/globalassets/om-telia/pdf/b22_310120_betingelser_feb_2020.pdf
(besøgt d. 30-04-20).
(Forkortes: Telia, 2020)

Bilagsoversigt

- Bilag 1: Business Danmark, ”Teleselskaber vil bremse advokaters jagt på tusindvis af danske piratkopister”, 29. maj 2017
- Bilag 2: Kendelse afsagt af Retten på Frederiksberg den 3. november 2017: sag nr. BS A-1417/2017
- Bilag 3: Kendelse afsagt af Retten på Frederiksberg den 16. august 2017: sag nr. BS K-741/2017
- Bilag 4: Kendelse afsagt af Retten på Frederiksberg den 10. november 2015: sag nr. BS E-1984/2015
- Bilag 5: Kendelse afsagt af Retten på Frederiksberg den 15. juni 2017: sag nr. BS A-681/2017
- Bilag 6: Kendelse afsagt af Retten på Frederiksberg den 11. maj 2016: sag nr. BS B-2443/2015
- Bilag 7: Kendelse afsagt af Retten på Frederiksberg den 22. september 2015: BS K 1271/2015
- Bilag 8: Dom afsagt af Retten på Frederiksberg den 22. maj 2019: sag BS-31445/2018-FRB
- Bilag 9: Kendelse afsagt af Retten på Frederiksberg fra den 14. maj 2012: BS Z-439/2012, BS Z-440/2012 og BS Z-441/2012
- Bilag 10: Øvrige kendelser, hvor teleudbydere er blevet pålagt at videregive oplysninger
- Bilag 11: Afgørelse afsagt af Finlands Højesteret den 8. december 2017: S2016/899
- Bilag 12: Afgørelse afsagt af Norges Højesteret den 26. april 2017: HR-2017-833-A (sag nr. 2016(2216))
- Bilag 13: Samarbejdsaftale

Bilag 14: Procesafsnit

Antal anslag omfatter al brødtekst inkl. mellemrumslanslag undtagen forside, fodnoter, abstract, indholdsfortegnelse, litteraturliste og bilag:

Ordoptælling

Statistik:

Sider	65
Ord	23.897
Tegn (uden mellemrum)	156.943
Tegn (med mellemrum)	180.748
Afsnit	441
Linjer	2.556

☐ Medtag fodnoter og slutnoter

Luk