# ULOVLIG NEDLASTNING -
# IDENTIFISERINGSPROSESSER OG PERSONVERN.

Kandidatnummer: 578

Leveringsfrist: 25.11.2009

( * regelverk for spesialoppgave på:

http://www.jus.uio.no/studier/regelverk/utf-forskr-vedlegg-i.html

regelverk for masteroppgave på:

http://www.jus.uio.no/studier/regelverk/master/eksamensforskrift/kap6.html )

Til sammen 17 613 ord

23.11.2009

# Innholdsfortegnelse

# 1 INNLEDNING

## 1.1 Problemstilling, mål, tema og aktualitet

I dag identifiseres personer som driver med ulovlig fildeling via ip-adresser.[1] Det er internettilbydere som identifiserer den ulovlige bruken, og overleverer data til politiet. Det har også forekommet at private aktører har overvåket ip-adresser, men disse aktørene har ikke hatt tilgang til å knytte ip-adressen opp mot et navn. Private aktører har ikke hatt denne tilgangen fordi internettilbydere helst ikke utleverer personopplysninger.

Hovedproblemstillingen for denne oppgaven er hvilke identifiseringsprosesser som er tillatt de lege lata for politiet, sivile parter, herunder internettilbydere, og en drøftelse om hvorvidt ip-adresser er å anse som personopplysninger. Et annet spørsmål er hvordan håndhevelsen av opphavsrett som munner ut i krav om identifisering kan få gjennomslag i forhold til personvernet. Deretter hva som bør skje de lege ferenda?

Målet med oppgaven er å vise hvordan teknikken i dagens samfunn påvirker jussen, og visa verca.

Jeg vil kort konstantere at det er et stort omfang av brudd på åndsverksloven i Norge i form av ulovlig fildeling. Et eksempel som viser dette er en undersøkelse foretatt av MMI for Norwaco i 2005, som viser at 922.000 nordmenn i løpet av de siste syv dager før undersøkelsen ble foretatt hadde kopiert musikk. Totalt denne uken ble det kopiert 35,4 millioner låter/musikkstykker, hvorav 21,6 millioner var ulovlig kopiert eller lastet ned.[2]

---

[1] Ip-adresser er et unikt nummer som identifiserer en datamaskin over et gitt tidspunkt. Ip-adresser er sendt ut fra internettilbyderen for blant annet å få tilgang til internett. For en mer utførlig redegjørelse se kapittel 2.1.

[2] Jfr. NOU 2007:2 s. 36

I Ot.prp. nr. 46 (2004-2005) s. 9, punkt 2.2.1: ”Utfordringer som følge av ny teknologi” legges det vekt på de utfordringer som følger av ulovlig kopiering. Sårbarheten som ligger i digitale utgivelser, de økonomiske tapene, og den balansen som ønskes å ivaretas i forhold til vernet for den skapende innsats, og avgrensninger i forhold til personvern og andre samfunnshensyn. Vernet etter åndsverksloven forsøker således å imøtekomme den nye teknologien og tilpasse lovgivningen etter denne.

Derimot er det sjelden at politiet og påtalemyndigheten har ressurser til å prioritere etterforskning av ulovlig nedlastning. Et annet problem ligger i den tekniske begrensningen som ligger i innhentning av ip-adresse og tidsfrister for identifikasjon av brukeren. Et eksempel på disse forhold er fra 2008 hvor bransjeorganisasjonene Ifpi, Norske Videogramforening og amerikanske Motion Picture Association anmeldte 182 saker som omhandlet brudd på opphavsretten. Av disse kom 4 under etterforskning.[3] Det kan være flere forklaringer på hvorfor ikke flere saker er etterforsket: Typisk vil alvorlighetsgraden og omfanget av saken ha betydning for prioriteringsspørsmålet. Hvilke saker politiet skal prioritere gis i et skriv fra Riksadvokaten hvert år jfr. Rundskriv nr 1/2009. Det som skal prioriteres etter rundskrivet er organisert kriminalitet, hallikvirksomhet, voldskriminalitet og lignende. Listen inneholder 11 punkter og ingen av disse punktene omhandler ulovlig fildeling. En antakelse er at slike saker i motsatt fall nedprioriteres.

Forholdsmessighetsprisnippet er også en viktig begrensing når det gjelder ressursbruk hos politiet og påtalemyndigheten. Dette er prinsippet om at en etterforskning må stå i forhold til den straffbare handlingens art og alvorlighet. Eksempelvis vil en sak om ulovlig nedlastning av MP3 filer klart vike fremfor en sak om grov vold ved spørsmål om prioritering.
At den ulovlige nedlastningen ikke prioriteres hos politiet fører derimot til at de private interesseorganisasjonene, som Tono, Ifpi, osv, ønsker å bekjempe den ulovlige nedlastningen og fildelingen på annet vis. I Norge er det flere advokat firmaer, blant annet Simonsen advokatfirma DA, som bistår dem med å tilrettelegge bekjempelsen av ulovlig fildeling.

[3] Hagen, A. (2008)

Simonsen advokatfirma DA hadde tidligere konsesjon fra Datatilsynet for å overvåke ip-adresser til brukere som laster ned ulovlig materiale. Ip-adresser knytter seg til identifikasjon av brukere på internett, noe som jeg vil komme tilbake til under kapittel 2.

Det kan hevdes at internettilbyderes vegring for å hindre den ulovlige nedlastningen er begrunnet i salg av tjenester hos internettilbydere. Det er omsetningstall for de to bransjene som bygger opp under denne teorien. Tall fra IFPI som er publisert i St. meld. Nr. 21 (2007-2008) "Samspill" s. 50 viser at salg av fysiske produkter i 1998 utgjorde NOK 991 millioner for platebransjen. Salget på tilsvarende fysiske produkter utgjorde i 2007 NOK 658 millioner, og i tillegg kom salg av nedlastede produkter på NOK 42 millioner. Samlet gir dette en omsetning på NOK 700 millioner. Det er en reduksjon på 29,9 % i omsetningen til platebransjen. Til sammenligning var omsetningen for Telenor Internett i 1998 på NOK 469 millioner, jfr. Telenor annual report 1999, s 36. Omsetningen for 2007 var på NOK 2566 millioner, jfr. Telenor Q4 2008 report, side 4.[4] I tillegg er det viktig å merke seg at Telenor er den største internettleverandøren i Norge i dag, men utgjør ikke på nær den totale omsetningen for bredbånd i Norge som i 2007 var på ca NOK 5500 millioner, jfr. Post og teletilsynets "Det norske ekommarkedet per 3. kvartal 2008", side 16. Det er innholdet i tjenestene internettilbyderne selger som gjør at brukere betaler betydelige summer for god båndbredde på internett. Telenor oppgir at fildeling står for 70-75 % av kapasiteten på deres nettverk. Det utgjør altså en stor del av kapasiteten, men det beskriver ikke gjennomsnitt pr. bruker, for fildeling er en tjeneste som krever mye volum. Telenor uttaler i samme artikkel at det er kun 15 prosent av bredbåndskundene som bruker 70-75 prosent av kapasiteten.[5]
I St.meld. nr 21 (2007-2008) – samspill, side 49 står det: "Det er grunn til å tro at nedgangen i platesalg først og fremst skyldes ulovlig nedlasting. Samtidig har nye produkter som f.eks. ringetoner vokst frem. Konkurranse fra slike nye produkter (DVD, mobilt innhold m.m.) kan nok også være med å forklare noe av nedgangen." Det er altså først og fremst ulovlig nedlastning som gir nedgang i platesalget, men det er nok som det

[4] Tilgjengelig på: http://www.telenor.com/en/resources/images/2008-q4-telenor-report_tcm28-37362.pdf

[5] Blaker, Magnus (2008)

også gis utrykk for et mer komplekst bilde av markedet i dag enn det har vært før. Den stadig voksende spill bransjen antas også å ha hatt innvirkning på musikk og film bransjen. Endringene kan ikke sees svart hvitt, men det er ikke til å komme utenom at ulovlig nedlastning tar opp en god del av profitten til musikk og platebransjen. Det er derimot viktig å merke seg at det ikke er et 1:1 forhold mellom nedlastning og tap. Et eksempel her er antall filer lastet ned opp mot et potensielt salg. Som vist fra det forrige eksempelet om undersøkelsen foretatt av MMI[6], hvorav 21,6 millioner filer var ulovlig kopiert eller lastet ned, er det dermed ikke sagt at disse 21,6 millionene som var lastet ned ulovlig ville blitt kjøpt. Men det understreker også at den ulovlige nedlastningen har påvirkning på salget av musikk ut fra omfanget av ulovlig nedlastning.

Oppgavens aktualitet er stort i dagens samfunn. Et eksempel med stor internasjonal oppmerksomhet er The Piratebay saken i Sverige jfr. Stockholms tingsrätt [2009-04-17] mål nr: B 13301-06. Saken gjelder medvirkning og forberedelse til brudd på opphavsrett, gjennom internett siden thepiratebay.org. Gjennom denne siden kan man dele filer via bit-torrent teknologi.[7] De fire som sto tiltalte var Peter Sunde, Gottfrid Svartholm Warg, Fredrik Neij og Carl Lundström. De ble dømt i første rettsinstans til ett års fengsel og til å betale 30 millioner svenske kroner i erstatning. De tiltalte har varslet at saken ankes. Saken er ventet å gå helt til Högsta domstolen i Sverige.

Oppgaven vil omfatte det mulige vedtaket av datalagringsdirektivet i Norge. Det er enda ikke kommet et vedtak, men jeg vil inkludere en drøftelse av datalagringsdirektivet. Jeg inkluderer drøftelsen på grunn av at vedtaket kan forelenge tiden internettilbydere må lagre ip-adresser, og dermed hvordan tilgangen til ip-adresser blir for politiet.

[6] Jfr. NOU 2007:2 s. 35

[7] Jfr. bit-torrent teknologi i kapittel 2

## 1.2 AVGRENSING

Oppgaven omhandler fildeling i dagens samfunn knyttet til dagens rettstilstand og hvordan denne rettstilstanden eventuelt bør være, altså de lege lata og de lege ferenda drøftelser. Derimot ville en slik klassisk gjennomgang av "gjeldende rett" være for rettsdogmatisk. Det er vel knapt noen som tror på at det finnes kun en gjeldende rett, hvor man kan få svar på alle sine spørsmål. Da ville spørsmålet være om hvor god man er til å lete opp svar i en juridisk sammenheng. En dissensdom i Høyesterett ville således ha innebåret at flertallet var bedre til å lete etter svar, enn mindretallet, og mindretallet dermed tok feil. Så en gjennomgang av alle spørsmål innefor området ulovlig fildeling og identifisering vil ikke være mulig.

De spørsmål som skal besvares i oppgaven krever innsikt i to store og nokså ulike fagfelt; teknologien og jussen. Kompleksiteten dette fordrer gjør det nødvendig å hente kunnskap fra flere ulike områder.
Oppgavens tema legger opp til en fremstilling av både tekniske og juridiske problemstillinger. Det er derimot viktig å merke seg at dette er en juridisk oppgave og ikke en teknisk oppgave, selv om den inneholder en teknisk del. Den tekniske fremstillingen er begrenset til det som er nødvendig for å få et helhetsinntrykk av oppgaven og hva temaet dreier seg om, særlig i forhold til hvordan ip-adresser og torrent-teknologien fungerer. Videre hvilke problemer temaet fører til når det gjelder identifikasjon og samfunnsholdning. Det tekniske er en viktig del av forståelsen for hva oppgaven egentlig dreier seg om.

I oppgaven skiller jeg ikke mellom musikk, filmer, spill og lignende, dette fordi jeg bruker begrepet ulovlig fildeling og nedlastning i vid forstand. Identifikasjonen og internettilbyder sitt ansvar vil være det samme for alle disse. Det kan stille seg annerledes i forhold til barnepornografi og lignende, da vil andre straffebud gjøre seg gjeldende. Jeg vil ikke komme

inn på fildeling av pornografisk innhold, kun holde meg til den mer ”allmenne” sorten av ulovlig fildeling: Musikk, filmer, og dataspill og programvare.

Oppgaven avgrenses ytterligere mot patentrettslige problemstillinger.

Jeg vil i oppgaven ta det standpunkt at det har forekommet ulovlig nedlastning og det er rammene rundt diskusjoner og argumentasjoner.

## 1.3 DEFINISJONER OG BEGREPS AVKLARINGER

I dette avsnittet defineres de vanligste begrepene som brukes i oppgaven:[8]

Bevis er et middel som skal dokumentere et påstått faktum. Beviset kan være personlig (vitnebevis) eller såkalt tinglig, dvs. reelle bevis f eks et åsted, gjenstander og dokumenter.[9]

Bruker: enhver fysisk eller juridisk person som bruker elektronisk kommunikasjonsnett eller -tjeneste til egen bruk eller som innsatsfaktor for produksjon av andre tjenester.[10]

Data: Den fysiske representasjonen av kjensgjerninger og lignende. For eksempel: Skrift på papir, eller lyd/lys/elektriske signaler.[11]

Informasjon: I dagligtale kan data og informasjon ofte overlappe, i forbindelse med elektronisk databehandling skiller man derimot mellom begrepene. Informasjon er det

[8] Jeg vil legge meg på linje med begrepsbruken til personvernkommisjonen, da jeg finner denne godt redegjort for i NOU 2009:1 Individ og integritet og jeg kan slutte meg til begrepsbruken her. Definisjonene er i hovedsak hentet herfra.

[9] Moe, Erling (Juridisk ordliste) (2009)

[10] Jfr. Ekomloven §1-5 nr. 12

[11] Jfr. NOU 2009:1, side 45

meningsbærende innholdet som kan trekkes ut fra data, som kan tolkes og forstås. For å forstå informasjon er et tenkende menneske en forutsetning.

Integritet: Individets rett til å uttrykke seg som en fullstendig person med egne meninger og tanker. Integritet kan deles inn i flere underkategorier basert på; kroppslig integritet, psykisk integritet, kommunikasjonsintegritet, informasjonsintegritet.[12]

Internett portal: En søkemotor som tilbyr en del ekstra tjenester som valutakurs, e-post, nyheter og lignende.

ISP/internettleverandører/internetttilbyder: (Internett Service Provider.) Jeg vil bruke disse begrepene for variasjon. Definisjonen av ordenes betydning forblir den samme. Eksempler på internettilbydere er Telenor, Nextgentel, Tele 2 og lignende. Internettilbydere, eller mellommenn som det kalles, kan etter ehandelsloven[13], § 1 andre avsnitt, litra b, kategoriseres i tre grupper: Rene videreformidlere, mellomlagrere og nettverter.[14] Se den tekniske beskrivelsen av internetts oppbygning som nettverk under kapittel 2.

Nettsted/internettside: En samling av informasjon, samlet som en enhet under en ledelse, som er tilgjenglig via internett.[15]

P2P (Peer-to-peer.): P2P er en beskrivelse av et fildelingsnettverk, hvor brukere har mulighet til å dele materialet sitt med andre på et bestemt nettverk. Peers, altså brukerne, både sender og mottar data uten en spesiell infrastruktur. Man trenger ikke et senter for fildelingen, slik som en server. Hovedmålet til P2P kan forklares slik: å effektivt distribuere data til en stor gruppe brukere ved å tvinge dem til å bidra i prosessen. Ved å laste ned noe, tvinges man på samme tid å laste opp noe i gjengjeld. Takket være denne teknikken kan

---

[12] Jfr. NOU 2009:1 s. 36

[13] Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester

[14] Jfr. Ot.prp. nr. 31 (2002-2003)

[15] Jfr. NOU 2009:1, s. 225

slik deling skje i svært stor skala. Den vanligste bruken av denne teknikken er spredning av opphavsrettsbeskyttet film og musikk.[16]

Person: En person er et levende individ.

Personvern: Personvern begrepet er et til dels særnorsk fenomen.[17] Det tradisjonelle juridiske personvern begrepet omfatter respekt for og beskyttelse av integritet og individets ukrenkelighet. Personvern kan knyttes opp mot rettssikkerhet, og disse to begrepene kan til dels overlappe hverandre.

Personopplysninger: Defineres etter personopplysningsloven ”som opplysninger og vurderinger som kan knyttes til en enkeltperson”. Dette utelukker selskaper og stiftelser og lignende. Opplysninger om døde personer vil heller ikke være å oppfatte som ”personopplysninger.
Personvern og retten til privatliv handler ikke bare om å beskytte sensitiv informasjon i forhold til myndighetene, men også om retten til å beskytte informasjon om seg selv, og retten til å være anonym.

Personopplysningsvern: Vern av retten til å ha innflytelse på bruk og spredning av informasjon om seg selv.[18]

Privatperson: Kan forstås som en som ikke er del av politikken eller det offentlige.[19]

Piratkopiering: Kan brukes om kopier, altså ulovlig kopiert originalprodukter, som filmer, musikk og programvare. Ordet piratkopiering, og ulovlig nedlastning brukes i oppgaven kun om P2P forhold. Det vil si deling av filer over et nettverk jfr. kapittel 2.3.

---

[16] ibid. s. 114

[17] Jfr. NOU 2009:1, side 30

[18] ibid., side 34

[19] ibid., s. 37

Rettssikkerhet: Defineres som ”den alminnelige sikkerheten for liv, eiendom mv. som rettsordenen gir”.[20]

Ulovlig nedlastning/fildeling: distribusjon eller nedlastning av opphavsrettslig vernet materiale, eller spredning av rettighetsbeskyttet materiale på internett uten rettighetshavers samtykke.

Streaming: Overføring av bilde eller lyd over internett i sanntid, som ikke lagres på datamaskinen.

## 1.4 METODE

Oppgaven er skrevet etter juridisk metode. Spørsmålene i problemstillingen ble besvart ved hjelp av litteratur søk og informasjon innhentet fra internett. Det ble blant annet foretatt søk i databaser som Bibsys, X-port, Idunn, Google Scolar, Google, hos det juridiske fakultets bibliotek og biblioteket ved senter for rettsinformatikk. For å innhente informasjon fra det praktiske feltet ble det gjort ustrukturerte intervju i form av e-post- korrespondanse med advokat Rune Ljostad, etterfulgt av et møte hos Simonsen advokatfirma. Videre var jeg i møte med professor ved senteret for rettsinformatikk, Jon Bing. Jeg har vært i samtale med Svein Willassen, som av mange regnes som Norges fremste ekspert på databevis og dataetterforskning. Naturligvis har jeg også vært i samtale med og hatt god hjelp av min veileder dr.jur. Lee Bygrave.
Jeg valgte ustrukturert form ved de møtene/samtalene jeg hadde, da jeg ikke hadde inngående kunnskap på dette feltet og ønsket ikke å gi noen føringer på de svar jeg fikk.
Jeg har i all hovedsak basert meg på to metodiske tilnærminger; litteraturstudier og ustrukturert intervju. Jeg har anvendt juridisk og forvaltningsinformatisk teori i forbindelse med behandling av rettskilder og rettslige spørsmål.

[20] Jfr. NOU 2009:1, side 33

# 2 TEKNISK

## 2.1 Ip-adresser og nettverk[21]

Ip-adresser er sentralt i forståelsen av hvordan et nettverk fungerer og således hvordan internett fungerer. Jeg vil kun gjennomgå den mest brukte standarden i dag, internett protokoll versjon 4, [22] da IPv6 kun er i en implantasjonsfase.[23]

Ip-adresser brukes for å identifisere datamaskinen på nettverket. Internett består av nettverk, og nettverk er enkelt sagt kabler som knytter de forskjellige PC-ene sammen. For at dette skal være mulig er det satt opp servere som hjelper PC-ene å finne internett siden de leter etter. Dette gjøres ved at det er utformet "språk" eller "protokoller" som definerer hva, hvordan og på hvilken måte maskinene skal kommunisere. Den vanligste av disse protokollene, den som man møter når man skal surfe på nettet er "HyperText Transfer Protocol", forkortet http. [24] Man trenger ikke til vanlig å fylle inn denne forkortelsen, da http er den mest brukt protokollen og netteleseren fyller inn dette automatisk.

Den adressen som står i adressefeltet kan også uttrykkes i tall, en ip-adresse. En ip-adresse er fire tall som rangerer fra 0 til 250. Eksempel 0.0.0.0 til 255.255.255.255. Dette er rekkevidden til IPv4. Disse tallene er unike for en maskin, og brukes til å identifisere akkurat den på internett. Tilbyr adressen en internettside vises denne. Et eksempel er tallene 193.69.165.21. Hvis man skriver inn disse tallene i nettleseren kommer man til www.vg.no. Denne teknologien kalles for navnetjenere eller DNS-servere, og er en

---

[21] Dette kapittelet er hentet fra egen arbeidskunnskap, og fra
Conradi, Christopher (2008)

[22] Forkortet til IPv4

[23] Det er på det rene at IPv6 vil komme til å måtte ta over pga begrensningen på 4 294 967 296 (232) mulige unike adresser som snart er brukt opp, og man trenger dermed en utvidelse.

[24] Se illustrasjonen under.

teknologi hvor DNS-servere oversetter en ip-adresse til en nettadresse. Dette er fordi en ip-adresse er betydelig mer vanskelig å huske enn en nettadresse.


**Figur 1: Figuren viser den tekniske informasjonen i en nettleser gir; Protokoll, underdomene,domenet, overdomenet, og eventuell mappe og fil lokasjon.**

Videre når man f.eks streamer en video eller hører på musikk på youtube.com er det store mengder med data som skal komme raskt og presist fram. Data består av 1-er og 0-er, binær kode, også kalt bits.[25] Dataene blir så delt opp i pakker kalt TCP[26] for å nå riktig destinasjon i riktig dataform. TCP er en forbindelsesorientert protokoll som gir pålitelig overføring av informasjon. (I motsetning til internett protokoll).
TCP arbeider opp mot ip-adresser og man slår som regel disse teknologiene sammen med forkortelsen TCP/IP. Sammen utfyller disse teknologiene hverandre og fører data raskt og pålitelig rundt i nettverket.
Det faktum at det er et nettverk av rutere, gjør internett så sterkt, i motsetning til om det hadde vært en linje eller en sirkel. Det er en rekke knutepunkter, så hvis et knutepunkt blir borte er det fremdeles ekstremt mange veier til den samme internettsiden. På samme måte er ikke nødvendigvis den raske veien den korteste geografisk, men det er den som er minst trafikkert. Det er rutere som holder orden på alle veiene å gå.

[25] Av eng. **bin**ary digi**t.**

[26] Transfer Control Protocol

En datamaskin kan kun ha en ip-adresse. Hvordan blir dette løst om det er flere datamaskiner koblet sammen i et lokalt nettverk? Løsningen er å bruke en slags utvidelse av ip-adresse, kalt porter. Porter brukes når det er programmer eller maskiner ip-adresser ikke klarer å identifisere. Ved tilfeller hvor man laster ned et program samtidig som man surfer på internett, vil man da skille de forskjellige innkommende TCP-pakkene ved hjelp av porter. Hvert program, eller hver tilkobling, angis av et portnummer som identifiserer akkurat denne tilkoblingen og gjør at man skiller de innkommende pakkene. Det samme gjelder internt i et nettverk. Har brukeren flere datamaskiner på nettverket hjemme, vil denne brukeren fortsatt kun ha én ip-adresse utad. Dette er viktig å merke seg i forhold til identifiseringen av brukeren. Så selv om man kun har en ip-adresse inn til en husstand, vil det kunne være flere brukere. Noe som igjen kan føre til problemer rundt identifiseringsprosessen av brukeren som har foretatt den ulovlige nedlastningen. Utad er det den som står som juridisk ansvarlig for abonnementet som har ansvaret for hva som skjer på linjen. Det kan derimot tenkes situasjoner hvor den som har abonnementet ikke kan stilles ansvarlig. Det kan være andre brukere som ikke skal ha tilgang til nettverket, f.eks en nabo som kobler seg på et usikret trådløst nettverk eller lignende.

I den overstående forklaringen av ip-adresser kommer det klart frem at ip-adresser er noe teknisk som kan identifisere et nettverk, eller en datamaskin. Videre må man da kunne trekke den slutning at selv om ip-adresser kan identifisere bruken av en datamaskin på internett, så er ikke dette ensbetydende med å identifisere individet som er brukeren. Noe som fører til tvil i saker hvor man ønsker å identifiserer brukeren som har foretatt en ulovlig nedlastning.

## 2.2 Dynamiske og statiske ip-adresser

Ip-adresser er ikke nødvendigvis faste tall angitt til et nettverk eller en datamaskin. Ip-adresser lagres i oppkoblingslogger. Oppkoblingslogger er internettilbyderen sin logg over når brukeren har koblet seg opp på internett, og hvilken ip-adresse de har for hver gang de har koblet seg opp. Denne lagres for faktureringsformål, og for å kunne yte bistand til

politiet i en eventuell etterforskning. Denne type logger baserer seg på ip-adresser. Det er internettilbyderen som gir ut ip-adresser fra sitt ”lager” av adresser. En statisk ip-adresse er et fast nummer til en datamaskin sin permanente adresse på internett. En dynamisk ip-adresse vil en datamaskin få for å kommunisere med andre maskiner, hvis den ikke er permanent oppkoblet til internett. Denne ip-adressen hentes fra internettilbyderen sitt forbeholdte ”lager” av ip-adresser. Når en ny oppkobling oppstår vil datamaskinen bli gitt en ny ip-adresse fra internettilbyderen sitt ”lager”. Forskjellen mellom disse kan ha betydning i rettslig sammenheng, ut fra hvorvidt en ip-adresse er å anse som personopplysning, og dermed om personopplysningsloven får anvendelse, jfr. kravene som oppstilles for begrepet i kapittel 3.3.

Bedrifter har som regel en fast ip-adresse knyttet til seg, mens private ofte har en dynamisk ip-adresse. Noe som betyr at de får tildelt ulik ip-adresse for hver gang de er oppkoblet til internett, avhenging av hva som er tilgjenglig. Dette fordi det er et begrenset antall ip-adresser tilgjengelig på verdensbasis, og et land har en bestemt kvote, jfr. kapittel 2.1. En del private brukere med xDSL linje har en fast ip-adresse. [27] Det er vanlig at internettilbydere loggfører ip-adressen ca hver tredje time hos private brukere som har linjer som xDSL med lang oppkoblingstid. Bedrifter med kun en Ip-adresse tilknyttet seg har ofte teknologi som deler denne innad i nettverket, og maskinene på det lokale nettverket vil fremstå som en maskin utad. Noe som igjen kan føre til problemer med skiftende ip-adresser innad i nettverket, og utad er det ikke mulig å identifisere hvilken maskin på nettverket som har gjort hvilken handling. Det er dermed, sett fra internettilbydere sitt ståsted, vanskelig å identifisere brukeren som har foretatt en ulovlig nedlastning på et bedriftsnettverk. Man må i så fall inn i bedriften og se hvorvidt de har en oppkoblingslogg innad i nettverket som kan identifisere brukeren som har foretatt den ulovlige nedlastningen. Har ikke nettverket en slik intern logg, eller et brukernavn for å registrere individet, vil det ikke være mulig å identifisere hvem som har foretatt den

[27] Eksempel: SDSL /ADSL

ulovlige nedlastningen. Dette er et hovedproblem i en etterforskning og viser den kritiske forskjellen mellom statisk og dynamisk ip-adresse.
Man kan også sammenligne ip-adresser med en telefonlinje, hvor en statisk ip-adresse vil tilsvare fasttelefoni der et permanent telefonnummer er knyttet til et individ, mens det ikke vil finnes en motsetning til den dynamiske ip-adressen, som ville tilsvare at man fikk et nytt nummer hver gang man ønsket å ringe.

## 2.3 Peer-to-peer problematikk.

Jeg har kort skissert hvordan peer-to-peer fungerer under kapittel 1.3. Det jeg derimot ikke har skissert er de juridiske utfordringene denne teknologien gir. Denne teknikken er kontroversiell fordi den tvinger hver bruker til å laste opp, for så å kunne laste ned materiale. Noe som kan føre til problemer i forhold til at flere personer bidrar til at en annen person laster ned ulovlig, grensedragningen mellom hvem som har lastet opp og ned hva kan slik sett bli vanskelig. At noen har lastet ned en fil er ikke vanskelig å identifisere i seg selv, hvem som har bidratt til den ulovlige fildelingen vil kunne være vanskelig på grunn av at brukerne er fra flere land, og at det ikke er en struktur i peer-to-peer nettverket. Slik sett lastes det ikke ned fra en datamaskin, eller en server, men fra et større nettverk av datamaskiner. Det er dermed vanskelig å si hvilken del av det ulovlig nedlastede materiale som stammer fra hvilken maskin og visa verca, ettersom at en fil sjelden lastes ned kun fra en bruker.

# 3 JURIDISK

## 3.1 Generelt[28]

Opphavsretten og personvernet er ikke så ulike rettigheter. Det kan argumenteres for at de springer ut fra den samme form for rett. Retten til å ivareta og beskytte det som er sitt, i sin egen sfære. I USA kan man si at personvernet springer ut fra opphavsretten. Warren og Brandeis, som noen regner som grunnleggerne av personvernet der, kan sies å ha tegnet opp et utkast til opphavsretten i USA for å støtte opp om sin personvern tese. Det er derimot klart at disse to rettighetene vil kunne komme i konflikt hvis de skal beskytte motstående parter. Det er ikke før ganske nylig at personer som ønsker å beskytte sin opphavsrett har måtte trenge inn i den personrettslige sfære til brukerne deres.

Etter loven er det politiet som skal etterforske og påtalemyndigheten som skal straffeforfølge forbrytelser i Norge. Spørsmålet er så hvordan denne identifiseringsprosessen skjer og hvordan personvernet ivaretas.

### 3.1.1 Opphavsrett.

Opphavsretten er en del av immaterialretten. I dag er dette den mest vidtfavnende delen av immaterialretten. Opphavsretten legitimerer identifiseringen av brukere som laster ned ulovlig, for å verne opphavsmenns rettigheter.

Lov 12. mai 1961 nr. 2 om opphavsrett til åndsverker (åvl.) § 1 uttrykker lovens sentrale element i en enkel setning: ”Den som skaper et åndsverk, har opphavsrett til verket.” Prinsipielt gjelder loven litterære, vitenskapelige eller kunstneriske verk av enhver art. Det er forfatternes og kunstnernes rettsbeskyttelse av deres verker. Slik var utgangspunktet da

[28] Avsnittet er hentet fra: Hugenholtz, P. Bernt (2000) s. 97

loven ble vedtatt. I dag er det annerledes. Nå er det kommunikasjon og underholdningsindustrien som dominerer. Opphavsretten har med det fått en økonomisk dimensjon av betraktelig størrelse. Som igjen har ført til økt interesse fra forskjellige private aktører.[29] Av den grunn kan man ikke avskrive personvernet til fordel for opphavsretten. Det er vanskelig å skulle si at en rett skal være sterkere enn en annen rett. Opphavsretten kan ikke anses som tyngre enn personvernet. Opphavsretten kan ikke sies å ha en normativ forrang for personvernet grunnet private organisasjoner og opphavsmenns økonomiske interesse eller rett til vern for sitt verk.

Opphavsretten er en lov som er et eksempel på at en tradisjonell lov blir gitt en ny anvendelse for dagens teknologi. Dette er derimot ikke første gang loven er blitt anvendt på ny teknologi. Loven har "tålt" overgangen til ny teknologi tidligere. Da loven trådte i kraft i 1961 var TV ennå ikke vanlig, bare radio. Tv-en var ikke etablert som et medium. Likevel ble den gitt anvendelse på denne nye teknologien. Lovgiver har en tendens til å tilpasse loven til nye teknologier. Noe som er gjort gjennom teknologinøytrale paragrafer for at loven ikke skal bli utdatert av nye medier.[30] Det er tilkommet en del endringer blant annet den såkalte MP3 loven, som i virkeligheten er innføring av nye regler om bla. lovlig kopieringsgrunnlag (ål § 12, 5. ledd), beskyttelse av kopisperrer (ål § 53d) med mer.

## 3.2 Personvern

### 3.2.1 Personvern og identifisering av brukere ved ulovlig nedlastning

Utviklingen av personvernet viser at man står overfor mange potensielle konfliktområder når ”private” elektroniske opplysninger etterspørres som bevismateriale. Problemer kan på

[29] Koktvedgaard , Mogens (2005)

[30] Bing, Jon (1991) s. 15

grunn av hensyn til personvernet og individets rettigheter oppstå lenge før identifikasjon foreligger som bevis i retten.

Ved personopplysningsloven er EU's personverndirektiv implementert i norsk rett.[31] Formålet med loven uttrykkes i § 1: "å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger". Det er i denne loven lagt vekt på de grunnleggende personvernhensynene som behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene.[32]

I forhold til identifisering av brukere som foretar ulovlige nedlastninger kan man spørre seg om hvor grensen går for alvorligheten av forbrytelsen og hvor mye sensitiv informasjon som lekker ut gjennom identifiseringsprosessen. Noe som medfører at det burde være streng intern kontroll uansett om det er privat eller offentlig instans som foretar identifiseringsprosessen. Private aktører kan per i dag ikke identifisere navn og adresse, altså brukerinformasjon, men det kan politiet. Politiets mulighet begrenses derimot i dag til et par dager, som vist under drøftelsen i kapittel 3.3.2.

Spørsmålet videre er hvilke tiltak som er nødvendige for å sikre personvernet i forhold til identifiseringen ved ulovlig nedlastning.
Det er mange hensyn, inklusive personvernhensyn, som tilsier at det bør være mulig å ytre seg anonymt eller med skjult identitet, både på trykk og på nett. At man kan uttrykke seg anonymt fører derimot til at skjult identitet gjør at den enkelte, uten å frykte for å måtte stå til ansvar, sprer ærekrenkelser og lignende på en måte som krenker andres personvern. Også andre rettsstridige ytringer, og da særlig opphavsrettsbrudd gjøres under skjult identitet i dag. Det er viktig at hvor media som tillater eller muliggjør ytringer med skjult identitet, bør det finnes et klart definert ansvarssubjekt. I den utstrekning tilbydere av fildelingstjenester, og andre, legger til rette for anonymitet, bør disse også ha ansvaret for å

[31] EØS-komiteens beslutning nr. 83/1999 og deler av direktivet vedrørende forholdet mellom nasjonale myndigheter og fellesskapet, kommer imidlertid ikke til uttrykk i personopplysningsloven.

[32] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 105

forhindre at slike ytringer gjør skade. Et slikt krav til et ansvarssubjekt er ikke nedfelt i lov i dag, men etter min mening er det en nødvendighet. Nettverter bør minimum ha et beredskaps apparat som er tilgjengelig for å motta klager på skadelige ytringer og uten ugrunnet opphold fjerne ytringer som krenker personvernet eller andre lover.[33]
Det kan være flere muligheter for hvordan man får til en løsning, men den mest nærliggende er at nettverten eller det organ som muliggjør ytringen, også skal ha et ansvar. Man skal ha en mulighet til å klage et sted, og da er nettverten nærliggende.

I følge Personvernkommisjonen bør det opprettes et eget organ (jf. den nå nedlagte Nettnemnda), som til dels kan bidra til å utvikle gode etiske retningslinjer for nettytringer og dels kan respondere på og løse ulike konflikter i samband med nettytringer.[34]
Datatilsynet har fått i oppdrag å opprette en slik "nettnemnd", og det antas at den skal være tilgjenglig for allmennheten innen kort tid.[35] En slik nettnemnd skal gi veiledning til personer som har blitt krenket på nettet, i hovedsak vil nettnemnda ha liten betydning opp mot opphavsretten, da opphavsmennene har organisasjoner som IFPI til å ivareta sine rettslige interesser. En slik nettnemnd vil nok heller tiltale personer som er blitt utsatt for personvernkrenkelser fra slike interesseorganisasjoner som IFPI, i den grad det skjer. Nettnemnda vil bare kunne gi råd, ikke rettskraftige avgjørelser.

## 3.3 Er ip-adresser å anse som personopplysning etter personopplysningsloven?

En ip-adresse er som vist ovenfor, under kapittel 2.1, en kompleks teknisk aktiva, som ut fra sin funksjon er vanskelig juridisk å kategorisere. Personopplysning er et vidt begrep. Spørsmålet her er hvorvidt ip-adresser omfattes av lovens ordlyd.

---

[33] Jfr. NOU 2009:1 s. 122,123. Argumentasjonen er hentet herfra, og reflekterer Personvernkommisjonen sitt syn, men også mitt syn på hvordan nettverter burde ha et ansvar for sine tjenester.

[34] Jfr. NOU 2009:1 Side 124

[35] Jfr. Datatilsynet.no

Begrepet ”personopplysning” er meget sentralt for anvendelsen av personopplysningsloven, jfr. formålsparagrafen § 1. Vurderingen av begrepet personopplysning kan være avgjørende for om loven kommer til anvendelse eller ikke. Begrepet er definert i personopplysningslovens § 2: ”Opplysninger og vurderinger som kan knyttes til en enkeltperson”. EUs direktiv om personopplysningsvern har lagt til grunn følgende definisjon: ””Personal data” shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”[36] Det er altså ikke typen av informasjon som er avgjørende for å identifisere en person, men informasjon som enten direkte, eller indirekte, kan knyttes til en identifiserbar person.[37]

Ut fra disse definisjonene kan vi dele begrepet i fire elementer[38]:

1) Enhver form for informasjon som 2) kan knyttes til 3) en identifisert eller identifiserbar 4) fysisk person. Nedenfor vil jeg gå gjennom de ulike elementene av definisjonen, selv om de ikke er uavhengige av hverandre. Deretter vil jeg ta for meg en pågående sak mellom Google Inc. og ”Working Party on the Protection of Individuals with Regard to the Processing of Personal Data” som belyser temaet videre.[39]

Direktivet har lagt til grunn en vid tolkning av begrepet, norsk lovgiver har også fulgt denne linjen og lagt til grunn en vid tolkning av begrepet. Den vide begrepsbruken gjenspeiles i betegnelsen ”enhver form for informasjon”. At det legges opp til en vid tolkning i norsk lovgivning følger også av forarbeidene.[40] Lovgiver ønsker å få til en fleksibel bruk av lovverket, slik at det omfatter viktige behandlingsformer, men er snevert nok til at ikke personvernregler brukes utenfor tiltenkt området. Begrepet omfatter altså

---

[36] Jfr. Direktiv 95/46/EF

[37] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s.107

[38] Denne drøftelsen bygger på NOU 2009:1 og Bygrave, Lee A. (2002), side 42-50

[39] Heretter henvist til som WP (Working Party), også kjent som ”the Art.29 Working Party.”

[40] Jfr. NOU 1997:19, punkt 10.1.1 og kapittel 21 og Ot.prp. nr. 92 (1998-1999), punkt 4.2.2 og kapittel 16

enhver form for informasjon. Dette må forstås som at både opplysninger og vurderinger er omfattet. Opplysninger er definert i NOU 2009:1 side 46, som: ”Faktabaserte former for data knyttet til en person, som for eksempel navn, adresse og alder. Med vurderinger forstås mer sammensatte former for data. … Det stilles ikke et krav om at opplysningene er sanne eller bevist på noen måte.” Det ligger også i begrepet at både individ/familie og arbeids informasjon faller inn under ”enhver form for informasjon”.

Det neste kriteriet i definisjonen er tilknytningskriteriet.[41] Dataene må kunne knyttes til en person. Noe som er et veldig viktig kriterium i forhold til internettilbydere sin identifisering av brukere. Det er her man knytter det som er ulike data opp mot et enkelt individ. Så hvilke relasjoner er relevante når man skal knytte data opp mot individet?

Her kan man på generelt grunnlag si at data regnes som relevante når opplysninger handler om individet. Ip-adresser referer i utgangspunktet til en maskin, og ikke til en person. Begrepet personopplysning omfatter både direkte og indirekte tilknytning til en person. En opplysning er indirekte når flere opplysninger må undersøkes før persontilknytningen kan stadfestes. Slik kan en si at en ip-adresse har en indirekte tilknytning til personen: Man kan finne ut abonnementsinformasjon gjennom ip-adressen, men navnet fremgår ikke av denne adressens spesifikke nummer. For å få denne opplysningen må man kontakte en internettilbyder. Det foreligger således en ”personopplysning”, selv om det er flere ledd mellom opplysningen og personen. Dette taler for at en ip-adresse kan behandles som en personopplysning. Ofte er det derimot ikke fullt så enkelt å fastslå hvorvidt dataene er knyttet til individet. Slik som i det overnevnte tilfellet, hvor dataene direkte knytter seg til fysiske objekter, slik som en ip-adresse. Disse dataene peker ikke mot et fysisk individ, og må da kunne knyttes til denne. Det må kunne oppstilles en kobling mellom det fysiske objektet og det fysiske individet. Eierskap vil her kunne gi en tilknytning og en god indikasjon på denne koblingen, altså abonnementet. I de fleste tilfeller vil det være noen som er satt opp som eier av det fysiske individet. En ip-adresse vil peke til et abonnement

[41] Avsnittet er hentet fra: Schartum, Dag Wiese og Bygrave, Lee A. (2004) kapittel 4.3.4, s. 111, og NOU 2009:1 s. 49

og abonnementet vil ha en oppført eier. Slik vil man kunne identifisere eieren av abonnementet og som oftest vil det by på små problemer å finne ut hvem som hadde tilgang til datamaskinen og internett på oppkoblingstidspunktet i en familiehusholdning.[42] Slik identifikasjon kan imidlertid også by på en del problemer, jfr. kapittelet ovenfor om statisk og dynamisk ip-adresser, særlig hvis bruken er i tilknytning til firmaer uten logg og lignende. Hvis det er stor usikkerhet med hensyn til hvilken person opplysningene gjelder, vil dette tale i mot å anse kravet om tilknytning til en enkeltperson for å være oppfylt. Kravet for at loven skal komme til anvendelse er at det er mulig å identifisere vedkommende, det er ikke et krav om at man må vite identiteten på et gitt tidspunkt. Det går derimot en skjønnsmessig grense for hvor stor innsats som kreves av internettilbydere for å tilknytte en bruker identitet. I fortalen til personverndirektivet (95/46/EF), nr. 26 står det at spørsmålet skal bedømmes ut i fra ”alle hjelpemidler ... som det er rimelig å ta i bruk for å identifisere vedkommende, enten av den behandlingsansvarlige eller av en annen person.” En tilsvarende reservasjon må kunne innfortolkes i den norske loven.[43] Dersom det kreves stor arbeidsinnsats for å knytte ip-adressen opp mot en person, kan dette derfor tale for at en ikke anser opplysningen for å være en ”personopplysning”. Tilsvarende gjelder dersom det er usikkerhet med henhold til hvilken person en opplysning er tilknyttet. Noe som kan være usikkerhet i forhold til hvem som er koblet opp på maskinen som benytter den aktuelle ip-adresse. Dersom flere personer i en husstand er brukere av samme ip-adresse, kan usikkerheten om hvilken person opplysningene gjelder tale for ikke å anse kravet om tilknytning til en enkeltperson for å være tilfredsstilt. Det er ikke mulig å gi en eksakt beskrivelse av hvor stor usikkerheten må være for at en opplysning ikke er å anse som ”personopplysning”. Det kan imidlertid antas at det vil bli godtatt større usikkerhet dersom de aktuelle personene tilhører samme hushold/familie enn dersom det ikke er slik tilknytning, jf. formålsbestemmelsen i personopplysningsloven § 1 annet ledd.
På en arbeidsplass e.l. er det mulig at grensen vil gå ved 4-5 personer. Generelt må kravet om tilknytning til enkeltperson vurderes i relasjon til formålsbestemmelsen. Jo mer alvorlig de mulige personvernkrenkelsene er, jo større ressursinnsats og usikkerhet kan være knyttet

[42] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004)112-113

[43] Jfr. NOU 2009:1, fotnote 8, side 47

til identifiseringen av personer, uten at opplysningen av den grunn faller utenfor begrepet ”personopplysning”.[44]

Det neste av de fire elementene er hvorvidt dataene kan sies å være relatert til et identifisert, eller identifiserbart individ.[45] Dette følger av personverndirektivets artikkel 2 litra a: ”’personal data’ shall men any information relating to an identified or identifiable natural person.”[46] Her stilles det opp et identifikasjonskrav. Et tilsvarende krav følger av forarbeidene i norsk rett: ”Med ’personopplysninger’ menes opplysninger og vurderinger som direkte eller indirekte kan knyttes til en identifiserbar, fysisk person.”[47] For at identifikasjonskravet i norsk rett skal være oppfylt må en person kunne skilles ut fra en større masse. Personen må være identifiserbar, den må kunne skilles fra andre individer i større grupper, selv om det ennå ikke er gjennomført noen slik identifisering.

Individer kan identifiseres på flere måter. Politiet kan identifisere personer gjennom beskrivelse av høyde, utseende, vekt, hårfarge osv. Andre identifikasjonsmuligheter vil være yrke eller navn. Navn kombinert med adresse, bilde og lignende er å regne som direkte, konkret identifikasjon. En direkte identifikasjon som ikke vil være like konkret, vil være navnet i seg selv.

Indirekte identifikasjon vil f. eks være ip-adresser og samlinger av data som gjør det mulig å snevre inn og peke ut det konkrete individet opplysningene relaterer seg til.[48]

Identifikasjonen vil naturligvis være situasjonsbetinget. I større forsamlinger vil ikke et vanlig navn som f. eks Pedersen være tilstrekkelig for å identifisere en person. I slike sammenhenger vil sammenholding av informasjon kunne føre til at Pedersen vil kunne identifiseres: Navnet sammen med fødselsdato, opphav, og adresse vil være eksempler på informasjon som sammen kan peke ut et enkelt individ.[49] Igjen vil det være nødvendig å

---

[44] Jfr. Schartum, Dag Wiese (2009)a

[45] Jfr. Bygrave, Lee A. (2002) s. 47

[46] Jfr. 95/46/EF

[47] Jfr. NOU 1997:19, kapittel 21, merknad til lovens § 2

[48] Coll, Line (2000) s. 53-54

[49] Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 113

sette en begrensing i forhold til hvor omfattende tiltak som skal til før man oppnår sikker identifisering. En hypotetisk mulighet vil ikke være tilstrekkelig for å fastslå dataene som identifiserbare. Med dette menes at en kun ubetydelig sannsynlighet for identifisering, vil ikke være nok til å anse individet for "identifiserbart". Dataene vil da ikke være å regne som "personopplysninger" etter loven. Momenter i denne vurderingen vil igjen være ressursbruk og kostnadene ved å gjennomføre en eventuell identifisering, formålet internettilbyderen/(brukeren av dataene) har med behandlingen, hvordan denne behandlingen av dataene er lagt opp og fordeler og ulemper for både brukeren (den behandlingsansvarlige) og den som identifiseres. Tilgjenglige teknologi vil også spille inn som et moment i vurderingen. Her vil lagringstiden og relasjoner til en mulig identifikasjon i fremtiden tale for eller i mot om dataene skal regnes som personopplysninger.[50]
Opplysninger som fremstår som anonymiserte kan også være "personopplysninger" etter loven. Kravet er at det finnes referanser eller andre tilknytningspunkter som gjør identifisering mulig. Et eksempel fra forarbeidene til personopplysningsloven er en internettilbyder som registrerer en anonym elektronisk identitet som bare kan knyttes til en identifiserbar enkeltperson dersom man har tilgang til opplysninger som vedkommendes internettilbyder har tilgjenglig.[51]
Det fjerde og siste elementet i definisjonen er at dataene må kunne relatere seg til en fysisk person. Person begrepet er knyttet til levende individer; begynner ved fødsel, slutter ved død. Juridiske personer (selskaper, stiftelser, foreninger og lignende) omfattes ikke av loven.
Denne gjennomgangen av elementene i definisjonen av personopplysningsloven § 2 har vist at det er en rekke kriterier knyttet til hvorvidt man kan bruke ip-adresser som personopplysninger. Noe som er en skjønnsmessig vurdering. Norsk lovgivning bygger her på EU's direktiv, og i en pågående tvist mellom Google og WP, strides det om hvorvidt ip-adresser er å anse som personopplysninger. Utfallet av denne tvisten vil kunne ha betydning for hvordan man anser personopplysnings begrepet i EU, som derav kan påvirke norsk rett og lovgivning. EF-domstolen har enda ikke tatt stilling til om ip-adresser er å

[50] Jfr. NOU 2009:1 s. 48

[51] Jfr. NOU 1997:19, kapittel 21, merknader til § 2

anse som personopplysninger. Den nærmeste bestemmelsen vi kommer er ”Lindqvist-avgjørelsen”.[52] Saken gjaldt en avgjørelse fra Göta hovrätt i Sverige om Bodil Linqvist, hvor EF-domstolen uttaler: ” The answer to the first question must therefore be that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes ‘the processing of personal data wholly or partly by automatic means’ within the meaning of Article 3(1) of Directive 95/46.” Det kan tolkes dit hen at telefonnummer er å anse som personopplysning etter direktivet. Denne uttalelsen kan dermed ha betydning for hvorvidt en ip-adresse vil passere kriteriene i den overnevnte definisjonen. Videre finnes en tilståelses dom i Oslo tingrett fra 2004-11-18, hvor det blant annet ble lagt til grunn tiltaltes ip-adresse for å knytte identitet og bevismaterialet i form av en chat-logg opp mot brukeren.[53] Denne dommen er ikke så relevant annet enn for å illustrere hvordan en ip-adresse kan brukes som en del av identifikasjonen av brukeren.

### 3.3.1 Google Inc. mot WP

WP har oppstått som en følge av artikkel 29 i EU’s direktiv om personopplysningsvern.[54] Det er et uavhengig organ i EU, hvis oppgaver er nedfelt i artikkel 30 i direktiv 95/46/EF, og artikkel 15 i direktiv 2002/58/EC, oppgavene omfatter personvern og data beskyttelse.[55] Det følger av direktivet at WP kun har rådgivningskompetanse.

Google Inc. er et selskap som er mest kjent for sin søkemotor, de operer utover dette med et bredt aspekt av tjenester, alt fra kart til oversettelser. Når man bruker Google sine tjenester,

---

[52] Case-101/02 Sweden vs. Lindqvist (2003)

[53] Jfr. TOSLO-2004-41422, 2004-11-18

[54] ”Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data”

[55] Jfr. 0737/EN/WP 148 s. 1

vil det bli lagret en hel del informasjon om brukeren, som Google igjen bruker til markedsføring av disse tjenestene. WP har på sin side bedt Google begrense lagringen av data om brukerne av tjenestene.[56] Google mener at markedsføring har informasjonsverdi i seg selv, og at reklame som er rettet mot forbrukerens interesser er noe alle tjener på, også forbrukeren.[57] For å oppnå dette lager Google en profil for hver bruker av deres tjenester. Søkene som brukeren foretar blir så lagret i en log ved hjelp av en server. I denne loggen lagres: Ip-adresser, dato og tid for søket, URL fil; som viser hva brukeren søkte og hvilken søkemotor, operativsystem og nettleser, og en Google cookie. (Cookie er i dette tilfelle en unik liten sporings fil, i form av tekst).[58] I denne oppgaven er det lagringen av ip-adressen som er relevant i forhold til hvorvidt den skal regnes som personopplysning.
Google kan ved hjelp av sine samlede data indirekte identifisere en bruker. De hevder at de, i motsetning til internettilbydere, ikke behandler personopplysningsdata. Dette begrunner Google med at en ip-adresse ikke kan anses som en personopplysning på grunn av deres stilling som tjeneste operatør. Selv om en ip-adresse skulle være å regne som personopplysning i EU, anfører Google at de ikke har en kontroll rolle i EU slik som en internettilbyder, da all behandling av personopplysninger skjer i USA.[59] I Europa er serverne deres kun for lagring av data. Videre anføres det at de kun har interesse i form av kommersiell drift, og ønsket om å selge velrettet reklame. Noe som etter min mening ikke kan regnes som et gyldig argument, jfr. drøftelse om formålsutglidning i kapittel 3.3.1.2.

#### 3.3.1.1 WP sitt perspektiv på hvorvidt ip-adresser kan oppfattes som personopplysninger.

WP gjør gjeldende at et individs søk på en søkemotor er å anse som personopplysning hvis individet det referer til er mulig å identifisere. Selv om Google ikke direkte kan identifisere

[56] Jfr. ibid. s. 3

[57] Jfr. Wojcicki, Susan (2009)

[58] Church, Peter & Kon, Georgina (2008) s. 462

[59] Fleischer, Peter (2008)

individet, kan identifikasjonen like fullt skje gjennom internettilbydere. Derfor vil data som Google samler inn anses som personopplysning, inkludert data som samles inn via en dynamisk ip-adresse. Internettilbydere på sin side må behandle all data som personopplysning med mindre de kan være absolutt sikker på at dataene ikke kan knyttes opp til brukeren.[60] Noe WP mener gjelder for Google også.[61] WP uttaler i dokument 37 at det er klart at en internettilbyder har en mulighet til å identifisere en bruker, og at dette må omfattes som personopplysning.[62] WP sitt synspunkt er i overensstemmelse med drøftelsen i kapittel 3.4 der det kommer klart frem at internettilbyderen har en mulighet til å identifisere brukeren som har fått en ip-adresse fra dem, gjennom tid og sted for oppkobling, og eventuelle cookies, hvis de overnevnte kriterier er oppfylt.

#### 3.3.1.2 Google's/Peter Fleischer sitt perspektiv på hvorvidt ip-adresser kan oppfattes som personopplysninger.

Google på sin side anfører at de alltid har sett på ip-adresser som høyst konfidensiell informasjon som trenger streng beskyttelse.[63] De mener derimot at ip-adresser ikke alltid kan regnes som persondata, ettersom hvor identifiserbart individet er. Google mener at hvis ip-adresser behandles av en internettilbyder vil adressene måtte anses som personopplysninger, fordi internettilbyderen har en reel mulighet til å identifisere brukeren. Google anfører at de på sin side ikke har en slik reell mulighet til å identifisere brukeren, og derfor kan ikke ip-adresser anses som personopplysning.[64] Google anfører altså at hvorvidt en ip-adresse er å anse som personopplysning vil fremgå av konteksten. Peter Fleischer som jobber som Google's Global Privacy Counsel har selv uttalt at ip-adresser må

---

[60] Jfr. 0737/EN/WP 148, s. 8 og 01248/07/EN WP 136, s. 17

[61] Jfr. argumentasjonen i 0737/EN/WP 148

[62] Jfr. 5063/00/EN/Final WP 37 s. 21

[63] Jfr. Fleischer, Peter (2008) s. 5

[64] Jfr. Fleischer, Peter (2008) s. 6

anses som anonyme så lenge en tredjepart som Google ikke mottar assistanse fra internettilbydere.[65] Igjen melder spørsmålet seg om formålsutglidning. I slike tilfeller vil det alltid være spørsmål om formålsutglidning. Det finnes allikevel et visst hold i denne argumentasjonen.

WP og Google sin argumentasjon vil ikke ha selvstendig betydning for norsk rett, annet enn i verdien av deres argumentasjon, og at saken kan ha påvirkning i en eventuell avgjørelse i EF-domstolen, som videre vil kunne ha betydning for norsk rett gjennom EØS. WP har kun rådgivningskompetanse. Det er derimot et organ i EU og man må anta at en del råd fra et slikt organ vil bli fulgt opp i EU. Ut over dette er det argumentasjonen i seg selv, og de verdier denne bærer som har betydning.

Jeg finner begge argumentasjons teoriene fornuftige, og det er vanskelig å si hvem som har rett da EF-domstolen ikke har gitt et klart svar på spørsmålet. Etter min oppfatning må derimot ip-adresser anses som personopplysninger, da de kan enten på lovlig, eller ulovlig vis misbrukes, og som vist, kan det forekomme uheldig formålsutglidning, hvor innsamlede data brukes til et annet formål en det tiltenkte, noe som kan få alvorlige konsekvenser for individets sfære og liv, jfr. eksempelet om SSB som samlet inn bostedsstatistikk, som senere ble brukt av nazister til å lokalisere jøder. Det ville være naivt å tro at innsamlede opplysninger kun vil brukes til ett formål i all overskuelig fremtid. Min oppfatning er i strid med juridisk litteratur.[66] Jeg vil nedenfor gå igjennom en del utenlandske dommer som bringer mer lys over argumentasjonen

[65] Fleischer, Peter (2007)

[66] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 116

#### 3.3.1.3 Utenlandske dommer som omhandler hvorvidt ip-adresser kan regnes som personopplysninger.

Jeg vil ta for meg tre tyske dommer som illustrer hvordan disse domstolene resonerer i forhold til problemstillingen.

Den første dommen taler i mot å anse ip-adresser som personopplysninger:
The District Court of Munich[67] anser ikke dynamiske ip-adresser for å være personopplysning, og går dermed i mot to tidligere dommer i Tyskland. Disse to dommene og deres begrunnelser vil bli omtalt senere i drøftelsen. Det er også interessant å merke seg at The District Court of Munich går i mot WP sin uttaleser.[68]
I denne saken hadde saksøker gjort gjeldende at den tiltalte, som drev en internett portal, lagret ip-adresser i logger, som ble brukt ut over endt sesjon for oppkoblingen. Altså ut over tiltenkt formål. Saksøker gjorde gjeldende at dette var en ulovlig måte å drive logginnsamling på, gjennom portalen, og at tiltalte avslørte ip-adressen til brukeren. Noe som ble gjort gjennom å lagre loggen lengre enn oppkoblingen varte. Saksøkeren ønsket en rettslig dom for at tiltalte skulle holde opp med den ulovlige aktiviteten. Saksøkte gjorde gjeldende at det å lagre en ip-adresse i en logg fil ikke ville bryte med personopplysnings lovgivning i Tyskland. Saken ble avvist på grunn av manglende søksmålskompetanse, men domstolen uttalte at saken også ville blitt avvist på annet lovgrunnlag. Domstolen ville avvise saken fordi den ikke anså dynamiske ip-adresser som personopplysninger etter personopplysningsloven i Tyskland. Noe som understreker viktigheten av konsekvensene dersom ip-adresser faller inn under personopplysningsbegrepet.
Ved avgjørelsen la domstolen vekt på hvorvidt en datalagrings operatør, som en web host, med sine vanlige, tilgjengelige verktøy har mulighet til identifisere/vurdere et individ ut fra hva operatøren har lagret om dette individet. Domstolen gikk så over til å vurdere hva som ligger i begrepet vanlige, tilgjenglige verktøy. De la vekt på at en dynamisk ip-adresse ble

[67] (AG München) 133 C 5677/08 "*Dynamische IP-Adressen*" publisert 30.09.2008

[68] Jfr. tidligere drøftelse, kapittel 3.3.1.1

gitt over et angitt tidsrom fra en internettilbyder, og at det bare var denne internettilbyderen som har mulighet til å identifisere brukeren, under/etter påloggingen. Her måtte altså saksøkte tatt kontakt med internettilbyderen for å få tilgang til informasjonen om saksøker. Videre er det kun med hjelp fra internettilbyderen at saksøkte ville hatt mulighet til å identifisere saksøker. Ut fra lovgivningen finnes det ikke grunnlag for internettilbyder eller web host og lignende til å utgi informasjon om vedkommende bruker. Da gjenstår det bare en teoretisk mulighet for at identifiseringen kan skje ved ulovlig aktivitet/samarbeid. Denne teoretiske muligheten anså ikke domstolen for å ligge til data lagrings operatørens vanlige, tilgjengelige verktøy. Dermed kom ikke definisjonen om personopplysning til bruk, fordi en dynamisk ip-adresse ikke kunne anses som personopplysning når den ble brukt av en datalagrings operatør.
Hva som lå i begrepet personopplysning drøftet ikke domstolen i forhold til ip-adresser, kun hvilke muligheter en datalagrings operatør hadde til å lovlig identifisere en bruker av sine tjenester.

The Amtsgericht and Landericht Berlin[69] er en annen tysk domstol, hvor den aktuelle rettssaken fikk motsatt utfall. I denne saken gjorde saksøker gjeldende at saksøkte ved hjelp av lagrede data kunne opprette en søke historikk over vedkommende, og dermed finne og beskrive saksøkers interesser. Disse interessene kunne omfatte politiske og religiøse oppfatninger. Saksøkte gjorde gjeldende at ip-adresser ikke lagret personlige data, og at lagringen av ip-adresser var av sikkerhets årsaker. Domstolen kom her til at en dynamisk ip-adresse omfatter person opplysninger. Dette er uavhengig av om det lagres hos en datalagrings operatør, eller hos en internettilbyder. Domstolen sin begrunnelse for resultatet bygde på at det var mulig, ved hjelp av en tredjepart (internettilbyderen), å innhente tilstrekkelig med data. Hvis man ikke godtok ip-adresser som personopplysning, ville ikke loven komme til anvendelse, og noe som ville kunne føre til omstendigheter hvor ip-adresser fritt kunne gis til en tredjepart. Domstolen anførte videre at loven måtte beskytte

[69](Amtsgericht Berlin-Mitte) 5 C 314/06, publisert 27.03.2007.

mot både lovlige og ulovlige omstendigheter som kunne oppstå. Loven måtte ha som mål å hindre all misbruk av data, lovlig eller ulovlig.

Den siste avgjørelsen er fra Landgericht Darmstadt[70]. Forskjellen fra de tidligere nevnte sakene er at her tilbød saksøker ikke bare internett tjenester, men også internett tilgang. Som i Norge er det i Tyskland bare lov til å lagre ip-adresser til faktureringsformål. Domstolen slo fast at det etter tysk lov ikke var hjemmel for å lagre ip-adresser på generelt grunnlag, kun til identifiseringsformål. Domstolen brukte ikke begrepet personopplysning, men dommen kan tolkes dit at ip-adresser er noe som tilhører det enkeltes individs personlige sfære, og man kan derfor ikke lagre ip-adresser på generelt grunnlag, annet enn med hjemmel i lov.

Alle de overnevnte dommene fokuserer kun på det juridiske grunnlaget i en spesifikk sak for lagring av data, dette viser en viss vegring for å drøfte ip-adresser opp mot personopplysning generelt.

En dom fra vårt naboland viser en lignende tendens: I Stockholm's Lænsrætt[71] måtte domstolen ta stilling til om ip-adresser omfatter persondata. Domstolen kom til samme resultat som Amtsgericht og Landgericht domstolene, at det avgjørende for å anse ip-adresser som persondata er hvorvidt en internettilbyder har mulighet til å identifisere et individ ut fra sine lagrede data. Den svenske domstolen tok derimot opp et tema som de tyske ikke hadde berørt, at det er tilstrekkelig å kunne identifisere den juridiske eieren av abonnementet, og ikke nødvendigvis den faktiske, fysiske brukeren. Denne kontraktrettslige forbindelsen gjør at ip-adresser må anses som personopplysning etter svensk rett.

De ovenfor nevnte domsavgjørelser viser at det ikke er "svart-hvitt" bilde på om ip-adresser kan anses som personopplysning. Resonnementet til Amtsgericht and Landericht

[70] (Landgericht Darmstadt) 25 S 118/2005, publisert: 07.12.2005

[71] (Lænsrætten i Stockholms Læn) 593-2005, publisert 08.06.2005

Berlin om at alle muligheter må tas i betraktning når man ser på hva en lov skal beskytte brukerne mot taler etter min oppfatning tyngst for å anse ip-adresser som personopplysning. Rettstilstanden vil etter min oppfatning ikke være holdbar i forhold til personvern hensyn hvis ip-adresser ikke skulle regnes som personopplysninger, jfr. Amtsgericht and Landericht Berlin avgjørelsen, hvor dette tilfelle ble beskrevet som at hvis man ikke godtok ip-adresser som personopplysning, ville ikke personopplysningsloven komme til anvendelse, og noe som ville kunne føre til omstendigheter hvor ip-adresser fritt kunne gis til en tredjepart. Etter norsk rett vil en slik situasjon kunne bli tilfelle i Norge. Amtsgericht and Landericht Berlin avgjørelsen er forøvrig i samsvar med min oppfattelse i drøftelsen under kapittel 3.3.1, om WP vs. Google.

### 3.3.2 Påtalemyndigheten og politiets adgang til å innhente informasjon om trafikkdata og bruker identifikasjon.[72]

Politiet har hjemmel til å hente ut abonnements/person opplysninger fra internettilbyderen etter ekomloven § 2-8. Internettilbyderen er etter ekomlovens § 2-8 forpliktet til å tilrettelegge nett og tjeneste slik at "lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres". Med dette menes politiets adgang til kommunikasjonskontroll, herunder informasjon via ip-adresser. Det er to typer trafikkdata som kan hentes ut etter straffeprosessloven: Lagrede trafikkdata, og sanntidstrafikkdata. For de lagrede trafikkdata er hjemmel strpl. § 210 om utleveringspålegg. Det følger av denne bestemmelsen at retten, og i hastetilfeller også påtalemyndigheten, kan kreve å få utlevert "[t]ing som antas å ha betydning som bevis". Med ting omfattes ip-adresser, jfr. Rt 1992 904. Kjennelsen gjaldt påtalemyndighetens beslags rett hos Televerket i utskrift av

[72] Kapittelet er skrevet på bakgrunn av notater fra samtaler med Rune Ljostad, og Svein Willassen.
Rune Ljostad er partner i advokatfirmaet Simonsen DA.
Svein Y. Willassen er utdannet sivilingeniør i informasjonssikkerhet ved Norges Teknisk Naturvitenskapelige Universitet. Han regnes av mange som en av Norges fremste ekspert på databevis og dataetterforskning. Han er ofte brukte av Høyesterett som rådgiver på databevis og dataetterforskning.

telefonoppringninger registrert til og fra siktedes mobiltelefonnummer. Retten uttaler: ”Beslagsadgangen og utleveringsplikten omfatter ikke bare legemlige gjenstander, men også opplysninger som lagres på data og som i tilfelle må gjøres tilgjengelig ved utskrifter, som f eks opplysninger om bankkonti.” Etter min oppfatning kan det utledes av denne uttalelsen at ip-adresser omfattes som ting. Denne kjennelsen er også fulgt opp av senere avgjørelser.[73]
Formuleringen ”antas å ha betydning som bevis” innebærer at en rimelig mulighet er tilstrekkelig. [74]

I kjennelse, Rt 1999 1944, har Høyesterett satt som vilkår til den nå opphevde telekommunikasjonsloven av 23. juni 1995 nr. 39 § 9-3 tredje ledd, at politi og påtalemyndigheten må spesifisere utleveringspålegg, slik at mottakeren (internettilbyderen) skal vite hva som skal legges frem av informasjon. Politiet må altså gi internettilbyderen tilstrekkelig med opplysninger om individet til at internettilbyderen lett kan finne disse opplysningene. Saken gjaldt hvorvidt politi og påtalemyndigheten kunne kreve opplysninger om en abonnents navn, adresse, telefonnummer eller datakommunikasjonsadresse, jfr. de nå opphevede bestemmelsene om taushetsplikt i telekommunikasjonsloven av 23. juni 1995 nr. 39 § 9-3 tredje ledd.
Videre omhandlet kjennelsen hvorvidt det var tilstrekkelig med en dynamisk ip-adresse og eksakt tidspunkt for oppkoblingen for å få tilgang til opplysning om navnet til vedkommende fra internettilbyderen, et datterselskap av Telenor i dette tilfelle.
Her uttalte Høyesterett at det viktigste for identifikasjonen ikke er en fast oppkobling, men at opplysningene ”entydig” må utpeke vedkommende individ. ”Entydig” kan tolkes ut fra ordlyden på den måten at det bare kan være en bestemt bruker knyttet til den oppgitte ip-adresse på et bestemt tidspunkt. At det her ikke kan være tvil om tilkoblingen. En dynamisk ip-adresse vil lettere kunne skape tvil rundt den faktiske identiteten til brukeren enn en statisk ip-adresse, ettersom den dynamiske kan forandre seg fra hver gang brukeren logger

[73] Jfr. Rt 1992 928

[74] Bjerke, Hans Kristian og Keiserud, Hans Kristian s. 725

på. Høyesterett legger til grunn i slike tilfeller at brukeren må kunne identifiseres på et slikt grunnlag at det er entydig hvem som er den faktiske brukeren.

Internettilbyderen har derimot ikke et ansvar for overføring og lagring av data med opphavsrettsbeskyttet materiale. De har ikke en generell plikt til å overvåke den informasjonen de overfører eller lagrer. Samtidig som de ikke har en plikt til å søke etter brukere som foretar ulovlig nedlastning, eller aktiviteter som indikerer ulovlig nedlastning. Plikten til ikke å overvåke brukerne følger av ehandelsloven § 19 som er implementert i ehandelsdirektivet (2000/31/EF) artikkel 15.

Etter strpl. § 210 kan utleveringsplikten bare gis personer som har vitneplikt. Retten kan etter strpl. § 218 ikke motta forklaring fra et vitne hvis dette medfører at han/hun bryter sin lovbestemte taushetsplikt. Ekomloven § 2-9 første ledd fastsetter taushetsplikt for ”innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter”. Loven omfatter dermed både trafikkdata og andre former for data. Taushetsplikten er likevel ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse, jf. ekomloven § 2-9 tredje ledd.
Bevisforbudet etter straffeprosessloven § 118 er derimot ikke ubetinget. Etter bestemmelsens første ledd første punktum kan departementet samtykke i at vitnet gis anledning til å forklare seg uten hinder av taushetsplikten. Samtykke kan bare nektes dersom forklaringen: ”vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold”, jf. strpl § 18 annet punktum. Samferdselsdepartementet har i vedtak 23. juni 1995 nr. 39 delegert samtykkekompetansen til Post-og teletilsynet. En tilbyder har dermed plikt til å utlevere elektronisk lagrede data etter § 210 i den utstrekning Post-og teletilsynet samtykker. På visse vilkår kan retten bestemme at underretning om utleveringspålegg kan utsettes, jf. straffeprosessloven § 210a.

Hjemmel er strpl. § 216b annet ledd, litra d) for tilfeller hvor man ønsker sanntidsinformasjon. Det kreves "skjellig grunn" til mistanke etter strpl. 216b. Jeg vil ikke gå videre inn på drøftelsen av skjellig grunn da dette faller utenfor oppgavens problemstilling.
Etter ekomloven § 2-8, plikter internettilbyderen å tilrettelegge nett og tjeneste "slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres". Det er viktig å merke seg at begjæring om kommunikasjonskontroll skal fremsettes av politimester eller visepolitimester.[75]

Ved all bruk av tvangsmidler gjelder det et prinsipp om forholdsmessighet[76]. Det må tas i betraktning den straffbare handlingens art. Man må altså se hvor grovt lovbruddet er. I følge åvl. § 54 er det ulovlig å laste ned en sang, men det vil i dette tilfellet være temmelig urealistisk å iverksette etterforskning med kommunikasjonskontroll for å innhente identifikasjon via ip-adresser og konstantere tidspunkt osv. Bruken av kommunikasjonskontroll vil stå i misforhold til den straffbare handlingens art. Det økonomiske perspektivet og det tidsmessige sammen med ressursbruken til etterforsking vil være uforholdsmessig i forhold til den straffbare handlig.
For det andre må en ta i betraktning hva som kan oppnås ved å iverksette tiltaket. I tilfeller ved ulovlig nedlastning er eneste måte å knytte brukeren opp mot den ulovlige handlingen å identifisere denne ved hjelp av informasjon fra internettilbyderen som kan knytte brukeren opp mot ip-adresse og tidspunkt. Her oppnår man altså som regel en identifisering, selv om dette også kan være vanskelig.
For det tredje må det legges vekt på hva siktede har å tape i forhold til at tiltaket settes i verk. Her kommer en rekke synspunkt inn i forhold til brukeren, helse, jobb, forsørger osv. En må vurdere skadevirkningene for siktede. I det overnevnte eksemplet vil det som nevnt være et tiltak som ikke står i forhold til den straffbare handlingens art og man vil muligens belaste brukeren med et stempel som kriminell for å ha foretatt en enkelt ulovlig nedlastning. Her er det skjønnsmessige vurderinger som må overveies.

[75] Jfr. Strpl. § 216 d (2)

[76] Jfr. Strpl. § 170a

Et siste punkt i forhold til kommunikasjonskontroll og forholdsmessighetsprinsippet er hjemlet i strpl. § 216c: " Tillatelse til kommunikasjonskontroll kan bare gis dersom det må antas at slik avlytting eller kontroll vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort."
Det må altså være av vesentlig betydning, eller i vesentlig grad vanskeliggjøre oppklaringen. Her er kravet om at det ikke skal være uforholdsmessige inngrep kommet konkret til uttrykk. [77]

Det kan være viktig å merke seg at det i gjennomsnitt er ca en domfellelse per år innenfor ulovlig fildeling. Noe som kan tyde på at politiressurser alene ikke er nok, men at etterforskning av brudd på åndsverksloven er nedprioritert. Et eksempel på dette er et ulovlig nettverk kalt Lysehubben, som naturlig nok er en hub på Lyse sitt nettverk. Lyse er en internettilbyder. De leverer fiberoptisk nettverk, noe som gir rask ned- og opplastning. I en artikkel hos Stavanger Aftenblad kommer det frem at politiet ikke ønsker å prioritere denne typen kriminalitet: "Det skal mye til for at politiet skal etterforske den såkalte Lysehubben. Det er snakk om prioritering," sier John Arild Jåsund ved Rogaland politidistrikt til Aftenbladet.[78] Samtidig sies det også at det er et spørsmål om ressurser.

Etter min oppfatning har politiet og påtalemyndigheten tilstrekkelig med hjemmel for å bekjempe den ulovlige fildelingen. Politiet sin faktiske mulighet til å innhente ip-adresser og identitet, for dermed å bekjempe ulovlig fildeling er et spørsmål om ressurser, og lagringstid hos internettilbyder (jfr. drøftelsen under). Det må derimot en holdningsendring til hos politikerne i Norge, og en omprioritering av ressurser, eller bevilgning til ekstra ressurser. Så lenge det ikke er tilstrekkelig med ressurser, er det etter min oppfatning ikke forsvarlig å omprioritere slik at ulovlig fildeling får forrang foran f. eks grov legemsbeskadigelse. Det må mer ressurser til politiet for å bekjempe den ulovlige fildelingen.

---

[77] Hov, Jo, kapittel 2, nr 10, side 81

[78] Aasland, Jarle (2009)

### 3.3.3 Sivile parters adgang til å innhente informasjon om trafikkdata og bruker identifikasjon

Dette avsnittet bygger i sin helhet på fremstillingen i Schartum & Bygrave (2004) Kapittel 4.7 – 4.8. Jeg vil i dette kapittelet gå igjennom de krav som stilles til en sivil part sin behandling av personopplysninger.

Personopplysningsloven (pol) er den sentrale loven i forhold til private parters adgang til å innhente trafikkdata og brukeridentifikasjon. Loven gjennomfører Norges forpliktelser etter personverndirektivet 95/46/EF og gjelder for "behandling av personopplysninger". Noe som betyr at loven kun gjelder i den grad opplysninger kan knyttes til et identifiserbart individ. Loven retter seg mot den "behandlingsansvarlige", som vil si den som bestemmer formål og virkemidler for behandlingen. Den behandlingsansvarlige må således følge visse materielle og prosessuelle grunnkrav for at behandlingen skal være lovlig.[79]

Disse grunnkravene må være oppfylt før behandling av personopplysninger kan skje. Disse kravene er oppstilt i pol. §§ 8-15. Informasjon vedrørende flere av kravene skal meldes inn til Datatilsynet minst 30 dager før behandling av personopplysninger. Slik behandling skal konsesjonsbehandles. Oppfyllelse av grunnkravene må angis i konsesjonssøknaden. Personopplysningsloven § 9 angir rammene for Datatilsynets kompetanse til å gi konsesjon for behandlingen av personopplysninger. For videre drøftelse om konsesjonsvilkår se kapittel 3.4.1.
Det er verdt å nevne at Simonsen Advokatfirma DA er det foreløpig eneste advokatfirmaet som har hatt en konsesjon fra Datatilsynet til å drive overvåkning av ip-adresser, og tilhørende brukere som driver med ulovlig fildeling og nedlastning (anti-pirat virksomheten). Advokatfirmaet opptrådte på vegne av rettighetshaverne som var og er

[79] Jfr. NOU 2009:1 s. 289

krenket av den ulovlige opp og nedlastningen. Disse rettighetshaverne er samlet i organisasjoner som Tono og IFPI.

#### 3.3.3.1 Grunnkrav

Dette kapittelet bygger på fremstillingen i Schartum, Dag Wiese og Bygrave, Lee A. (2004) kapittel 4.7, s. 130.

Etter pol. § 8 skal det foreligge et alminnelig krav til rettslig grunnlag for at det skal være lovlig å behandle personopplysninger. Etter pol. § 9 stilles det krav til særlig rettslig grunnlag for å behandle personopplysninger. Kravene må oppfylles uavhengig av hverandre, men har samme terskel for oppfyllelse. Det må enten foreligge, samtykke, en lovhjemmel eller så må behandlingen av personopplysninger anses for å være nødvendig for visse formål, angitt i loven. Det må etter pol. § 9 særskilt grunnlag for å behandle sensitive opplysninger.

Hovedpunktene i loven vil basere seg på en fremstilling av pol. § 8, men har også relevans i forhold til pol. § 9. Det er viktig å merke seg at spørsmålene om nødvendighet ikke er like systematisk samlet i lovens § 9, og at § 9 mangler en tilsvarende bestemmelse som lovens § 8 litra f).

Samtykke etter loven er et strengt krav. Samtykket må være ”frivillig”, ”utrykkelig” og ”informert”. At samtykke skal være frivillig antas å bety at det ikke skal være knyttet negative konsekvenser til det å ikke gi samtykke. Et eksempel vil være at samtykke aldri er å anse som frivillig hvis det er knyttet sanksjoner til det.

I kravet om at samtykket skal være ”uttrykkelig” ligger det at ingen tvil kan oppstå om hvorvidt samtykket er gitt eller ikke. Det foreligger derimot ingen formkrav. Samtykket kan gis skriftlig og muntlig.

Kravet om at samtykket skal være ”informert” innebærer at den som gir sitt samtykke skal ha informasjon om de faktiske forhold. Eksempel: Informasjon om relaterte kostnader og lignende.

Samtykket etter personopplysningsloven forutsettes å være individuelt. Samtykke i grupper eller organisasjoner, vil bare unntaksvis være i samsvar med personopplysningsloven. Hvis samtykke gis til organisasjonen om at samtykke kan gis på individets vegne, kan dette tenkes å oppfylle lovens vilkår. Det må derimot stilles et krav om at organisasjonen holder hvert medlem fullt informert og at medlemmene uten hindring kan trekke samtykket tilbake.

Et samtykke kan trekkes formfritt tilbake når som helst. Den behandlingsansvarlige mister i så fall retten til videre behandling, med mindre det finnes et annet hjemmelsgrunnlag. I enkelte avtalegrunnlag gjelder det derimot visse modifikasjoner på hvorvidt opplysningene vil bli slettet med en gang.

Dersom samtykket mangler kan opplysningene behandles på grunnlag av lovhjemmel. Den aktuelle loven må da gi en direkte hjemmel til behandlingen, eller klart forutsette en slik behandling.

Et siste alternativ loven oppstiller er at personopplysninger kan behandles dersom dette er ”nødvendig” for å understøtte visse konkrete angitte formål eller virkninger. Jeg vil gjennomgå det generelle i denne drøftelsen og gi en mer inngående drøftelse nedenfor i oppgaven.
Formålene som er oppgitt i pol. § 8 er til dels svært vide og vurderingspregede. I forhold til problemstillingen på oppgaven er det pol. § 8 litra f som er mest aktuell. Denne bestemmelsen krever at behandlingen er nødvendig for ” at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og

hensynet til den registrertes personvern ikke overstiger denne interessen"[80]. I motsetning til de andre nødvendighetskriteriene inneholder denne bestemmelsen en interesseovervekt. Det er ikke tilstrekkelig at behandlingen er nødvendig. Nødvendighetsgrunnen må være viktigere enn hensynet til individets personvern. Her må det en vurdering av interessemotsetningene til, og dersom denne vurderingen ikke er å anse tilstrekkelig, vil den behandlingsansvarlige kunne bli erstatningspliktig etter pol. § 49 pga uaktsomhet.

Det kan ikke leses ut av loven i hvilken grad det eksisterer en prioriteringsrekkefølge for de tre nødvendighetsgrunnlagene. Samtykke er det ideologiske og systematiske utgangspunktet for personopplysningsloven. Derimot er samtykke også ansett som vanskeligst for den behandlingsansvarlige å innhente i forhold til å påberope seg nødvendig grunn. Samtykke alternativet er så vidt formulert at nesten enhver situasjon vil passe inn i et av alternativene i litra a-f. Hvis det ikke kreves konsesjon fra Datatilsynet av den behandlingsansvarlige, er det også et moment som taler for at samtykke ofte kan bli unngått, fordi den behandlingsansvarlige selv skal vurdere hvorvidt behandlingen av personopplysningene er "nødvendig".
Det er vanskelig å skulle gi et klart svar på denne problemstillingen, da den ikke er avklart i lov eller forarbeider. I teorien er det lagt frem en tredelt tilnærming til forholdet mellom pol. § 8 litra a-f.[81]
I litra d ("allmen interesse") og litra f (berettiget interesse), er det grunnlag for å kreve innhenting av samtykke før man påberoper seg "nødvendig" grunn. Årsaken er at det i litra d og f er tale om så vage kriterier, så de vil nesten alltid kunne påberopes. Dette ville være i dårlig overensstemmelse med lovens intensjoner. Hvis man legger til grunn at innhenting av samtykke må prøves først, bør en legge til en tilsvarende reservasjon som i pol. § 20 andre ledd litra b.[82] I tilfeller hvor samtykke ikke blir innhentet på grunn av at det er umulig eller uforholdsmessig vanskelig, skal den registrerte likevel motta varsel etter pol. §

[80] Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 134

[81] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 135

[82] Bestemmelsen unntar den behandlingsansvarlige fra informasjonsplikt hvis det er "umulig eller uforholdsmessig vanskelig" å varsle vedkommende.

19 eller § 20. Den registrerte har da en mulighet til å hevde at den behandlingsansvarlige er uberettiget til å behandle personopplysninger, jfr. bestemmelsene om sletting i pol. § 27. Spørsmålet om en eventuell plikt til å innhente samtykke kan bringes inn for Datatilsynet og eventuelt Personvernnemda og domstolene.

Under pol. § 8 litra a (avtaler) og litra c("nødvendig for å ivareta den registrertes vitale interesser") kan den behandlingsansvarlige påberope seg de nødvendighetsgrunner i loven som inneholder et samtykke element, uten å gå veien om et separat samtykke etter § 8. Her faller det naturlig å innfortolke et krav om at den registrerte ville ha gitt sitt samtykke dersom vedkommende ble spurt.[83]

I noen tilfeller kan det være forsvarlig av den behandlingsansvarlige å la være å innhente samtykke, f. eks for at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse etter § 8 litra b. Det må i så fall være en udiskutabel rettslig forpliktelse. Hvis det er knyttet tvil til den rettslige forpliktelsen, vil det være større grunn til å innhente samtykke fra den registrerte. Tilsvarende vil gjelde for litra e (utøvelse av offentlig myndighet).

Å behandle personopplysninger ut fra et nødvendighetsgrunnlag kan også by på problemer i forhold til legalitetsprinsippet[84] og EMK artikkel 8. Hvis behandlingen av personopplysninger er av en inngripende art, kan det altså tenkes at den bare kan utføres hvis det foreligger tilstrekkelig lovhjemmel.[85] Selv om det foreligger lovhjemmel kan det også motsatt etter artikkel 8 kreves en nødvendighetsgrunn. Saken Klass med flere mot Tyskland av 6. september 1978 kan brukes til å illustrere et eksempel.[86] Her var det tale om

---

[83] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 136

[84] Legalitetsprinsippet er prinsippet om at den utøvende makt aldri å gripe inn i borgernes sfære og dømme dem uten hjemmel i lov.

[85] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 137

[86] Sag 2 EHRR 214 Klass and others v Federal Republic of Germany

overvåkning av individers post og telefon. EMD[87] måtte først avklare hvorvidt individene var ofre eller ikke. Dette var fordi tyske myndigheter ikke ønsket å gi uttrykk for om individene var blitt overvåket. Domstolen slo fast at måten det tyske systemet var organisert på, ledet til mulig inngrep i rettighetene borgerne. Avlytting av telefonsamtaler ble sett på som et inngrep i retten til privatliv og korrespondanse. EMD slo fast at det forelå lovhjemmel og relevant formål, og spørsmålet var så hvorvidt inngrepet i rettigheten var nødvendig i et demokratisk samfunn. Her gikk EMD inn i en konkret vurdering av hvilke adekvate og effektive garantier som var oppstilt for å forhindre misbruk av overvåkningshjemmelen, satt opp mot den trusselen fra terrorvirksomhet og spionasje. Selv om det ikke fantes rene rettslige mekanismer, var det tilstrekkelig med de administrative og parlamentariske kontrollmekanismene som var etablert. Jeg vil ikke gå videre inn i diskusjonen rundt artikkel 8, da jeg anser denne for å falle utenfor oppgavens problemstilling.

#### 3.3.3.2 Formål

Avsnittet bygger på Schartum, Dag Wiese og Bygrave, Lee A. (2004) kapittel 4.7.3

Etter pol. § 11 litra b kreves det at den behandlingsansvarlige skal fastsette et formål for hver behandling av personopplysninger han fremlegger. Formålet skal stå i samsvar med den behandlingsansvarliges virksomhet, og formålet skal være saklig begrunnet. I internettilbyders tilfelle vil dette formålet være fakturering, jfr. drøftelsen under. I utgangspunktet er behandlingen av de innsamlede opplysningene knyttet til formålet. Formålet kan likevel endres, dersom det ikke er ”uforenelig med det opprinnelige formålet”, jfr. pol. § 11 litra c.

[87] Den Europeiske Menneskerettighets Domstolen

#### 3.3.3.3 Sikring og internkontroll

Avsnittet bygger på Schartum, Dag Wiese og Bygrave, Lee A. (2004) kapittel 4.7.5

Etter pol. er det oppstilt krav til informasjonssikkerhet (pol. § 13) og internkontroll (pol. § 14). Disse må sees i sammenheng med hverandre fordi de innholdsmessig og systematisk er nært beslektede. Pol. § 13 regulerer særskilt sikring av personopplysningenes konfidensialitet, integritet og tilgjenglighet.[88] Etter § 14 har den behandlingsansvarlige en plikt til å vurdere om tiltak må igangsettes for å oppfylle kravene til å behandle personopplysninger etter loven, eller i medhold av lov. Loven gir ikke eksempler på tiltak, så her er det ingen begrensing i form av hvilke typer tiltak som kan iverksettes. Spørsmålet så er med hvilket omfang og på hvilket nivå tiltakene skal gjennomføres. Etter § 13 kreves det "tilfredsstillende informasjonssikkerhet", og etter § 14 kreves det tiltak som er på et "nødvendig" nivå for å oppfylle kravene til behandlingen. Det kreves etter § 13 at den behandlingsansvarlige gjennomfører sikringstiltak, i henhold til konsesjon eller lignende, og andre tiltak som gir tilfredsstillende sikkerhet sett opp mot personverntruslene. Kravet i § 14 kan tolkes på tilsvarende måte, at tiltakene må være "tilfredsstillende". Internkontroll bestemmelsen legger opp til at loven følges på en lojal måte, og at tilstander som balanserer på kanten til det ulovlige må unngås. Begrepet "nødvendig" stiller således opp et krav om vurderinger som fører til handlinger, og kan ikke tolkes som en tillatelse til å gjøre minst mulig.[89]

Hvis det er klart at lovens bestemmelser ikke blir overholdt, må det iverksettes adekvate tiltak fra kompetent myndighet (Datatilsynet, Personvernnemda.) Hvilke tiltak som skal iverksettes og hvor omfattende disse skal være, avhenger av skjønnsmessige avveininger der en vurderer risikoen for personvernkrenkelser (pol. § 1) opp mot risiko og kostnadsvurderinger. Ønsket ved tiltaket er å redusere risikoen til et akseptabelt nivå, ikke avslutte behandlingen av personopplysninger.[90]

---

[88] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 140

[89] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 141

[90] Ibid. s. 142

Tiltak som planlegges skal etter loven dokumenteres, systematiseres og være tilgjengelige for Datatilsynet og Personvernnemda.

Som fremstillingen viser, beror det på om kravene som loven oppstiller om private parter vil få tilgang til å behandle personopplysninger. Forutsatt at ip-adresser er å regne som personopplysninger, vil disse da kunne behandles, hvis den behandlingsansvarlige får en konsesjon fra Datatilsynet. I de fleste tilfeller vil den sivile parten måtte ha hjelp fra en tredjepart, internettilbyderen, for å kunne identifisere en person som bedriver ulovlig fildeling.

## 3.4 Problemstillinger knyttet til internettilbydere

Under dette kapittelet vil jeg gjennomgå særlige problemstillinger som knytter seg opp mot internettilbydere sitt ansvar i forhold til identifisering ved ulovlig nedlastning.

### 3.4.1 Kan en internettilbyder lagre logg over sine brukere?

Den første problemstillingen er spørsmålet om en internettilbyder i det hel tatt kan lagre en logg over brukerne sine og deres identitet m.m?
Hjemmel her er lov om elektronisk kommunikasjon (ekomloven) av 25. juli 2003. Ekomloven gjennomfører blant annet direktiv 2002/58/EF om elektronisk kommunikasjon og personvern (kommunikasjonsdirektivet).
Det følger av ekomlovens § 1-2 at ”loven gjelder virksomhet knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner.” Dette omfatter internettilbydere og deres tjenester som tilbyder av internett-oppkobling til private.

Det fremgår av Ot.prp. nr 58. punkt 13.3.3: ” Ved en vurdering av mulig lagringsplikt for trafikkdata må det foretas en nøye avveining av to motstridende hensyn, hensynet til

kriminalitetsbekjempelse og hensynet til personvernet." Dette er hensyn som ble lagt til grunn ved utformingen av ekomloven, og gir en føring for ekomlovens § 2-7.

Ekomlovens § 2-7 angir kommunikasjonsvernet og herunder internettilbyderen sin sletteplikt. Første ledd angir kommunikasjonsvernet. Her er internettilbyderen lovpålagt å gjennomføre nødvendige sikkerhetstiltak for "vern av kommunikasjon i egne elektroniske kommunikasjonsnett og –tjenester". Hvis det knytter seg en særlig høy risiko til tjenesten plikter internettilbyderen å informere brukeren, jfr. første ledd annet punktum.
Lovens § 2-7 annet ledd angir internettilbyderen sin sletteplikt. All trafikkdata skal slettes når de ikke lenger er nødvendig for "kommunikasjons- eller faktureringsformål". For trafikkdata som knytter seg til fysiske personer er det gitt spesifiserte bestemmelser om sletting og behandling av trafikkdata og lignende, i Datatilsynets standard konsesjonsvilkår, gitt med hjemmel i forskrift 15. des. 2000 nr. 1265 § 7-1.[91]
Med trafikkdata menes i denne paragrafen data som er nødvendig for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller for fakturering av slik overføring.[92]
Behandling av trafikkdata hos internettilbyder kan bare foretas av personer som arbeider med fakturering, trafikkstyring, kundeforespørsler, markedsføring av elektronisk kommunikasjonstjeneste eller avsløring av urettmessig bruk av elektronisk kommunikasjon. Disse personene må ha fullmakt for utførelsen av arbeidet fra internettilbyderen. Behandlingen skal begrenses til det som er nødvendig for utførelsen av nevnte arbeidsoppgaver.[93]
Annen behandling av trafikkdata enn den som er nevnt i ekomloven § 2-7 annet ledd første punktum, herunder behandling til markedsføringsformål, krever samtykke fra brukeren, jf. ekomloven § 2-7 annet ledd annet punktum.[94]

---

[91] Jfr. Rønnevig, Leif-Henrik (2009)

[92] Jfr. Ekomforskriften § 7-1

[93] lc.

[94] lc.

Faktureringsformålet er negativt avgrenset, og omfatter altså retten til å lagre informasjon om ip-adresser og lignende i et begrenset tidsrom. Unntaket er om det er hjemmel i lov, eller i medhold av lov.

Internettilbyderen har taushetsplikt om innholdet av elektronisk kommunikasjon og andres bruk av denne kommunikasjon, jfr. § 2-9. Taushetsplikten er derimot ikke til hinder for at det gis abonnementsopplysninger som ip-adresser til påtalemyndighet, jfr. § 2-9 tredje ledd. Slike anmodninger fra politiet skal etterkommes med mindre "særlige forhold gjør det utilrådelig", jfr. fjerde ledd. Reglene om taushetsplikt for internettilbyder, og andre som utfører arbeid eller tjeneste for tilbyder, følger av ekomforskriften kapittel 7, jf. ekomloven § 2-9.

Konklusjonen er at internettilbyderen kan lagre logg for nødvendig kommunikasjons- eller faktureringsformål, med mindre annet er bestemt i eller i medhold av lov.

### 3.4.2 Hva kan loggen til en internettilbyder inneholde?

Trafikkdata skal altså kun lagres til kommunikasjons- eller faktureringsformål, jfr. foregående drøftelse. Dette vil si at internettilbyderen må kunne påvise tidspunkt for bruk av internett, noe som typisk vil kunne omfatte oppkoblingstidspunkt, varighet og lignende. Til dette formålet er det ikke nødvendig med andre trafikkdata, som hvilke internett sider som er besøkt og lignende. Internettilbyderen har ikke hjemmel for å lagre slik data, fordi det ikke vil være omfattet under kommunikasjons- eller faktureringsformål. I følge Svein Willassen forekommer det likevel en del lagring som faller utenfor lovens formål.

### 3.4.3 Hvor lenge kan en internettilbyder lagre en logg.[95]

[95] Avsnittet bygger på samtaler med Svein Willassen og Rune Ljostad.

Det er altså klart at en internettilbyder kan lagre logger til kommunikasjon og faktureringsformål. Spørsmålet er så hva som omfattes av begrepet ” kommunikasjons- eller faktureringsformål” i ekomlovens § 2-7 annet ledd.

Kommunikasjonsformålet knytter seg til mobiltelefonsamtaler, e-mail kommunikasjon og lignende kommunikasjon. Når denne kommunikasjonen avsluttes og det ikke er behov for å benytte data i faktureringsformål skal altså data slettes. Det følger av Ot.prp. nr 58 (2002-2003) s.92 at skjæringstidspunktet for når en kommunikasjon er ansett avsluttet vil bero på hva slags elektronisk kommunikasjonstjeneste som benyttes.

Internettilbyderen kan også velge å anonymisere innholdet av trafikkdataene. Å anonymisere trafikkdata innebærer at alle entydige kjennetegn blir fjernet slik at det er umulig å finne tilbake til den brukeren dataene kan knyttes til. Det skal heller ikke være mulig å foreta koblinger og på den måten identifisere hvem brukeren er.[96]

I forhold til sletteplikten i § 2-7 annet ledd er det i Ot.prp. nr 58 (2002-2003) en del synspunkter gjort gjeldende fra de forskjellige instanser og grupper som har uttalt seg om ekomlovens § 2-7. Disse knytter seg til fristen for lagring av data og sletteplikt.97 Hovedargumentet i disse uttalelsene er at det blir umulig for internettilbydere å bistå politi og påtalemyndighet i ettertid med å utlevere trafikkdata, og at bestemmelsen ikke gir tilstrekkelig hjemmel til å fastsette unntak fra kravet om sletting. Det kommer til uttrykk en del bekymring ovenfor bekjempelse av kriminalitet. Det er på det rene at politiet og påtalemyndigheten må ha tilgang til trafikkdata for å kunne knytte personer opp mot for eksempel distribusjon av barnepornografi. Det vil være et alvorlig problem om internettilbyderen ikke kan utgi denne informasjonen pga at loggen er slettet. Dette gjelder likedann for private parter som Simonsen Advokatfirma DA, den gang de hadde konsesjon. Alle parter er avhengig av informasjon fra en internettilbyder for å få knyttet brukeren som laster ned ulovlig opp mot ip-adressen, for å identifisere personen. Rune Ljostad i

[96] Jfr. Ekomforskriten § 7-1

[97] Jfr. Ot.prp. nr 58 (2002-2003) s.71

Simonsen advokat firma DA påpeker at dette er et problem, da internettilbyderen ofte ikke har logg tilgjengelig på grunn av sletteplikten etter ekomlovens § 2-7.

Konklusjon er at trafikkdata kan lagres innenfor det tidsrom det trengs til fakturering eller etter at kommunikasjonen er avsluttet.

### 3.4.4 Kan internettilbydere kontakte brukerne ved lovbrudd?

Problemstillingen her knytter seg til internettilbydere sin rolle som tilbyder av internett og innehaver av nødvendig trafikkdata. I en rettsstat er det politi og påtalemyndighet som etterforsker og straffeforfølger. En internettilbyder kan risikere å få en mellomstilling hvor de må overvåke sine kunder, og iverksette tiltak for å forhindre ulovlig fildeling. Utgangspunktet ifølge e-handelsloven § 16 er en internettilbyder ikke er strafferettslig ansvarlig for innholdet i den overførte informasjonen, men at dette er ikke til hinder for at retten likevel kan opphøre eller hindre overtredelsene etter § 20 i samme lov.

Kan internettilbyder kontakte sine kunder med en oppfordring om å avslutte den ulovlige nedlastningen?
Spørsmålet reguleres av personopplysningsloven § 11 litra c, som sier at bruk av personopplysninger som er uforenelig med formålet ikke er tillatt, med mindre kunden samtykker.[98] For det andre skal opplysninger slettes når formålet er oppfylt, jf personopplysningsloven § 28.

Behandling etter nytt formål skal tilfredsstille kravene i personopplysningsloven §§ 8 og 9, jfr. § 11.[99] Behandlingen av slike opplysninger faller inn under pol. § 9, behandlingen krever derfor konsesjon fra Datatilsynet, jfr. personopplysningsloven § 33, 1.ledd. Personopplysningsloven § 9 angir rammene for Datatilsynets kompetanse til å gi konsesjon

[98] Se drøftelse om samtykke i kapittel 3.3.3.1

[99] Se drøftelse om formål i kapittel 3.3.3.1

for behandlingen av personopplysninger. Personopplysningsloven § 9 henviser videre til pol. § 8, hvor den endrer karakter fra å være en pliktnorm som direkte regulerer internettilbyders plikter, til å bli en kompetansenorm som setter grenser for Datatilsynets konsesjonsadgang.[100]

Grunnkravet for konsesjon er at den kan gis når betingelsene i pol. § 8 er oppfylt og dersom i tillegg minst ett av de ytterligere vilkårene i pol. § 9, 1.ledd litra a-h er oppfylt. Etter pol. § 8 er det en grunnforutsetning at ett av de tre vilkårene paragrafen oppstiller må foreligge.[101]

Spørsmålet er så hva som ligger i at behandlingen av personopplysninger må være nødvendig.

Nødvendighetskravet skal vurderes av internettilbyder selv, men Datatilsynet kan etter § 46 overprøve denne vurderingen[102]. Av ordlyden er det uklart om en internettilbyder kan nøye seg med å konstatere at kravet til nødvendighet er tilfredsstilt og derfor la være å innhente samtykke fra de personer opplysningene gjelder. Utformingen av paragrafens ordlyd gjør at nesten ethvert av de opplistede formålene kan legitimeres på denne måten.[103] Ot. prp. Nr. 92 (1998-1999) kap. 16 s. 108 angir at: ”Behandling av personopplysninger bør i størst mulig utstrekning baseres på samtykke fra den registrerte, selv om den også kan hjemles i de grunnlagene som oppstilles i bokstavene a-f.” Personvernnemnda har videre satt opp retningslinjer for vurderingen av spørsmålet i klagesak nr. 2004/1 (STAMI): ”For at man skal kunne gjøre et avvik fra hovedprinsippet, må det … foreligge en begrunnelse. Denne begrunnelsen kan … ikke bare være en ren hensiktsmessighetsbetraktning, f.eks. å unngå kostnader, spare tid eller lignende – selv om slike begrunnelser selvsagt også må vurderes konkret i forhold til den enkelte sak.”104 I litra a kommer spørsmålet i en særstilling i forhold til internettilbydere, fordi litra a må sies å inneholde et samtykkeelement. Dersom

---

[100] Jfr. Personvernnemdas klagesak 2004/01 (STAMI) avsnitt 6.1

[101] For vilkår og drøftelse om samtykke, se kapittel 3.3.3.1

[102] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) kapittel 4.7.2.4

[103] ibid. kapittel 4.7.2.5

[104] Jfr. Personvernnemdas klagesak 2004/01 (STAMI)

samtykke er forsøkt innhentet og samtykke nektet, må vurderingstemaene i nødvendighetsalternativene trolig skjerpes. Dette gjelder særlig dersom det er viktige personvernspørsmål som kan bli berørt, jfr. formålsbestemmelsen i lovens § 1. Innsamling og videre behandling av personopplysninger kan i henhold til legalitetsprinsippet kreve hjemmel i lov dersom innsamlingen må anses å være inngripende.[105] Offentlige myndigheter kan i slike tilfelle ikke vise til nødvendighetsalternativene som "grunnlag", men må ha eksplisitt lovhjemmel.

Loven stiller opp en begrensning om at opplysningene ikke kan behandles til formål som er «uforenlig» med det opprinnelige formålet, jfr. § 11. Er den opprinnelige behandlingen basert på en lovhjemmel, kan internettilbyderen ikke behandle de samme opplysningene for et nytt formål som er uforenlig med det opprinnelige, under ny henvisning til nødvendig grunn. Dersom behandlingen for det nye formålet er basert på samtykke, oppstår det ikke noe problem. Dette fordi brukeren kan samtykke til at behandling for et nytt formål kan skje. Bestemmelsen får altså bare betydning dersom en internettilbyder påberoper seg en nødvendig grunn to ganger for samme behandling. Noe som også gjelder dersom man først har påberopt seg lovhjemmel og deretter påberoper seg en nødvendig grunn for det endrede formålet.[106] Det avhenger av en konkret vurdering om hva som skal anses å være "uforenlig" med det opprinnelige formålet.
Spørsmålet er hva som ligger i begrepet "uforenelig" etter personopplysningsloven.[107] Utgangspunktet i begrepet følger av ordlyden: Også behandling i forhold til et nytt formål skal tilfredsstille kravene etter §§ 8 og 9: Det skal foreligge samtykke, lovhjemmel eller nødvendig grunn. Lovens § 11 litra c har betydning når det fra før blir behandlet opplysninger på grunnlag av lovhjemmel eller nødvendig grunn, og den behandlingsansvarlige ønsker å behandle allerede innsamlede opplysninger til et nytt formål på grunnlag av nødvendighet. Loven stiller her opp en begrensning om at opplysningene ikke kan behandles til formål som er "uforenlig" med det opprinnelige

[105] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s.136-137

[106] Hentet fra Schartum, Dag Wiese (2009)b

[107] Fremstillingen om hva som er "uforenelig" bygger på Schartum, Dag Wiese (2009)b

formålet. Er den opprinnelige behandlingen basert på en lovhjemmel, kan ikke internettilbyderen dernest behandle de samme opplysningene for et nytt formål som er uforenlig med det opprinnelige, under ny henvisning til nødvendig grunn.
Det kan være grunn til å skjerpe prøvingen av hjemmelsgrunnlaget dersom formålene vedrørende de to lovhjemlene er uforenlige. Hvis internettilbyderen sin personopplysningsbehandling for det nye formålet er basert på samtykke, oppstår intet problem fordi brukeren uansett kan samtykke til at behandling for et nytt formål kan skje. Bestemmelsen får altså betydning for to grunnlag: Dersom internettilbyderen påberoper seg en nødvendig grunn to ganger for samme behandling. Eller dersom han først har påberopt seg lovhjemmel og deretter påberoper seg en nødvendig grunn for det endrede formålet. Hva som skal til for at det nye formålet skal anses å være "uforenlig" med det opprinnelige formålet er avhengig av en konkret vurdering. Virker den nye bruken av opplysningene mot de interesser som den opprinnelige bruken skulle fremme, f.eks. om det opprinnelige formål var å gi fordeler for den registrerte, for så å endre det til å kontrollere lovligheten av den brukeren, vil terskelen for "uforenlighet" trolig være overskredet. Etter min oppfatning kan jeg ikke se at det vil være lov først å behandle opplysninger fordi det er nødvendig for å ivareta den registrertes vitale interesser (jfr. litra c) og deretter behandle opplysningene fordi det er nødvendig for å utøve inngripende offentlig myndighet (jfr. litra e). I et slikt tilfelle må den behandlingsansvarlige enten innhente samtykke for å behandle i tråd med det nye formålet, eller skaffe lovhjemmel for den nye behandlingen.[108]

Personopplysningsloven § 11 annet ledd må leses i sammenheng med § 11 første ledd, litra c. Noe som innebærer at personopplysninger kan benyttes til historiske, statistiske, og vitenskaplige formål, selv om disse formålene ikke var blant de opprinnelige formålene i litra b, til tross for at disse formålene er å anse som uforenelige med det opprinnelige formålet. Her er det derimot et vilkår om at en klar interesseovervekt må tilsi at de nye formålene må aksepteres.[109] Personverndirektivet art. 6 nr. 1 bokstav c bestemmer

108 Jfr. Ot.prp. nr. 92 (1998-99) kap. 16 s. 112-113, og Gyldendal rettsdata, kommentarer til § 11, av Dag Wiese Schartum

[109] Jfr. Schartum, Dag Wiese og Bygrave, Lee A. (2004) s. 138

at personopplysningene ikke skal være «for omfattende i forhold til de formål de er innsamlet for og/eller senere behandles for». Denne begrensningen må leses inn i kravet til relevans, jfr. Ot.prp. nr. 92 (1998-99) s. 114.[110]

Etter min oppfatning må konklusjonen bygge på en formålsbetraktning hvorvidt brukerne kan kontaktes av sin internettilbyder om lovbrudd.

#### 3.4.4.1 Rettspraksis om internettilbyderes adgang til å utestenge brukere angående ulovlig fildeling.

I Norge er det kommet en kjennelse fra Asker og Bærum Tingrett som omhandler internettilbyder sin adgang til å stenge ute brukere fra visse internettsider.[111] Det er en sak mellom Telenor og film- og platebransjen i Norge. Norsk film- og platebransje ba om midlertidig forføyning, for å få Telenor til å blokkere nettsiden The Pirate Bay for sine kunder. Asker og Bærum Tingrett avslo denne forføyningen. For at en begjæring om midlertidig forføyning skulle kunne tas til følge, måtte film- og platebransjen sannsynliggjøre så vel krav som sikringsgrunn, jfr. tvisteloven § 34-2. For at hovedkravet skulle vært sannsynliggjort måtte Telenor gjennom uaktsomhet eller forsett rettsstridig ha medvirket til opphavsrettskrenkelsene. Telenors aktive handlinger bestod i å tilby den nødvendige infrastrukturen og nødvendige tjenesten for å overføre datatrafikk slik at rettighetskrenkelsen kunne finne sted.
Retten fant at Telenors «aktive handlinger i seg selv innebærer en fysisk medvirkning til krenkelsene», siden nettverket er en forutsetning for rettighetskrenkelsene. Men siden Telenor handlet på samme måte uansett om deres tjeneste brukes til et lovlig eller ulovlig formål, anså de ikke medvirkningen som rettsstridig.
Retten viser til at en internettilbyder ifølge e-handelsloven § 16 ikke er strafferettslig ansvarlig for innholdet i den overførte informasjonen, men at dette er ikke til hinder for at

[110] Schartum, Dag Wiese (2009)c

[111] TAHER-2009-96202 publisert 06.11.2009

retten likevel kan opphøre eller hindre overtredelsene etter § 20 i samme lov. I kjennelsen heter det at de praktiske konsekvensene ved å gi film- og platebransjen medhold, ville vært store. Retten begrunnet kjennelsen ved ikke å ta forføyningen til følge, med at en motsatt avgjørelse ville lede til "en vanskelig håndterbar situasjon i praksis". Retten fant ikke at Telenor ut fra eksisterende lovverk har en plikt til å kontrollere eller undersøke hva kundene driver med på nettet.

I Danmark har dansk Høyesterett uttalt seg om en lignende sak.[112]
TDC som er en internett tilbyder i Danmark, var i underinstansen blitt pålagt å blokkere trafikk på enkelte spesifiserte ip-adresser benyttet av kunder av selskapet. Bakgrunnen for forbudet var at det fra disse adressene ble bedrevet ulovlig fildeling. Høyesterett fant at forbudet ikke utgjorde noen uforholdsmessig belastning overfor TDC, og at det var liten risiko for at TDC ville bli krevd for erstatning av sine kunder.
TDC mente angivelsen av stengningen var mer problematisk. ip-adressene var dynamiske, og ville kunne endre seg over tid. Høyesterett avviste dette under henvisning til at forbudet i realiteten var rettet mot de kunder som på det aktuelle tidspunkt hadde benyttet de angitte ip-adresser. Videre ble det lagt vekt på artikkel 8 tredje ledd i opphavsrettdirektivet, som forplikter statene til å innføre forføyningssanksjoner overfor tredjeparters urettmessige handlinger: "Medlemsstatene skal påse at rettighetshaverne har mulighet til å kreve rettslig forføyning overfor mellommenn hvis tjenester brukes av en tredjemann til å overtre en opphavsrett eller beslektet rettighet."
Forbudet ble derfor ansett ikke å være urimelig tyngende overfor TDC, og underinstansens resultat ble stadfestet.

Det er altså tolkningen av artikkel 8 som etter dansk rett er vesentlig for vurderingen av hvorvidt en internettilbyder kan kontakte og stenge internett forbindelsen til brukere som foretar ulovlig nedlastning og liknende. Direktivet tilsier at det er lovlig å foreta midlertidige kopier av materiale for å overføre det i et nettverk jf. artikkel 2

[112] Sak. 49/2005 (1. afdeling) publisert 10. februar 2006

Det interessante er at Asker og Bærum Tingsrett kom til motsatt resultat, men det er viktig å bemerke at Telenor argumenterte med at det var avgjørende forskjeller på dansk og norsk rett. Tingsretten sa seg enig i dette ved å avise forføyningen.

Konklusjonen må bli at etter norsk rettspraksis, som etter min oppfatning veier tyngst, både i argumentasjon og i teori, har internettilbydere ikke en plikt til å utestenge brukere fra ip-adresser som utelukkende driver med ulovlig fildeling. Dette kan etter min oppfatning tyde på at personvernhensyn stiller sterkt i Norge, og at tingsretten ser på det som en lovgiveroppgave å forandre rettstilstanden. Hvordan Høyesterett ville stilt seg til samme spørsmål blir ren spekulasjon.

## 3.5 Datalagringsdirektivet

EU-direktiv 2006/24/EF om lagring av trafikkdata, forkortet til datalagringsdirektivet[113], ble vedtatt i EU av Rådet for den Europeiske union og Europaparlamentet den 15. mars 2006 foranlediget av terrorangrepet 11. september 2001 i USA og Madrid og London-bombene i 2004 og 2005. Direktivet trådte i kraft den 15.9.2007. Direktivet er antatt å være EØS-relevant, men det foreligger ennå ikke forslag til hvordan direktivet skal implementeres i norsk rett. Datadirektivet tar sikte på å skape et felles regelverk på europeisk nivå for lagring av data. Direktivet angir en tvungen lagring av trafikkdata. Det er usikkerhet med hensyn til hvor lenge dataene skal pålegges lagret. Direktivet gir et valg for nasjonale myndigheter innenfor 6 og 24 måneders lagringstid.[114] Det er unntak for gjennomførelsen av lagring av kommunikasjonsdata vedrørende internettadgang, e-mail og telefoni via internettet i artikkel 15 nr 3. Her er fristen for gjennomførelse satt til 15.3.2009. Datalagringsdirektivet sier ikke noe om når man kan få tilgang til ip-adresser, kun om lagringstiden.[115]

---

[113] Jeg vil bruke betegnelsen ”direktivet” i dette kapittelet.

[114] Jfr. NOU 2009:1, s. 189

[115] Jfr. NOU 2009:1, s. 189

Direktivets overordnete formål er oppklaring av alvorlig kriminalitet, jfr. artikkel 1 første ledd. Begrepet alvorlig kriminalitet er ikke definert, dette er overlatt til nasjonale myndigheter. Rettstilstanden i dag, i Norge, på et lavere nivå for innsamling av ip-adresser enn det direktivet stiller opp til. Politiet har i dag tilgang til ip-adresser dersom det anses å ha betydning for etterforskningen av enhver kriminalitet, ikke bare alvorlig kriminalitet.

Direktivet vil ha omfattende betydning innen lagring og tilgjengligheten av data hos internettilbydere ved at det øker lagringstiden for trafikkdata hos internettilbyder fra 6-24 måneder, i motsetning til rettstilstanden i dag, hvor internettilbyder sletter trafikkdata etter faktureringsformål, som ofte kan være noen dager eller uker. Den mulig økte lagringstiden vil blant annet medføre at direktivet vil ha direkte betydning for identifiseringen av brukere ved ulovlig nedlastning, da politiet vil ha større sjanse for å kunne identifisere individer som laster ned ulovlig. Per i dag er det som oppgaven viser vanskelig for politiet å innhente informasjon om brukere, pga. internettilbydere sin mulighet til å slette data etter fakturering. [116]

Det er en sterk debatt pågående omkring direktivet både nasjonalt og internasjonalt. Grunnen til dette er selvsagts direktivets innhold og omfang. Direktivets artikkel 5 nummer 1 angir de kategorier av data som skal lagres. I forhold til lagring av ip-adresser er det litra c) som er aktuell.
Opplysningene som skal lagres etter direktivets artikkel 5 litra c) er:
”1.
Litra c): data som er nødvendige for at fastslå kommunikasjonens dato, tidspunkt og varighet:

For fast- og mobiltelefoni:

- dato og klokkeslett for start- og sluttidspunkt

[116] Jfr. kapittel 3.3.2

For e-post, ip-telefoni og internett-tilgang:

- dato og klokkeslett for inn- og utlogging av internett-tilgang, basert på en bestemt tidssone, og den tildelte dynamiske eller statiske ip-adressen, sammen med brukeridentitet på abonnent eller registrert bruker.
- Dato og klokkeslett for inn- og utlogging av e-post og ip-telefoni på en bestemt tidssone."

Data som avslører innholdet av kommunikasjonen kan ikke lagres i medhold av direktivet. Etter direktivet er det abonnementsdata som skal lagres, altså data som knytter brukeren til ip-adressen. Internettilbyderen har i oppgave å lagre disse data. Det kommer ikke klart frem fra direktivet hvem som skal ha tilgang til de overnevnte opplysningene. Det fremgår derimot klart av artikkel 1, annet ledd, at kommunikasjonsinnhold ikke skal lagres. Artikkel 4 i direktivet sier at opplysninger som ip-adresser kun skal utleveres til "kompetente nasjonale myndigheter".

Artikkel 6 angir lagringstiden på minst seks måneder og høyst to år fra datoen for kommunikasjonen. Innenfor denne rammen er det derimot opp til nasjonal myndighet å bestemme tidsrammen.

Artikkel 5 er en omfattende liste over kommunikasjon som skal lagres. Det er en del av listen som taler i mot en vedtakelse av datalagringsdirektivet. Det kanskje viktigste å merke seg er at lokasjonsdata skal lagres. Dette vil kunne ha stor betydning for personvernet, da mobiltelefoner er så utbredt, og nesten hver nordmann har en mobiltelefon. Jeg vil ikke gå videre inn på diskusjonen om datalagringsdirektivet, jeg ønsket kun å påpeke hva som vil skje i forhold til internettilbyder sin lagringsplikt, hvis direktivet blir vedtatt og implementert i norsk rett, jfr. fremstillingen ovenfor.

## 3.6 Om utviklingen av den ulovlige nedlastningen i samfunnet (de lege ferenda).

Først vil jeg sitere Peter Sunde fra The Piratebay saken i Sverige: ”For eller mot fildeling er som å diskutere om man er for eller mot grønt. Uansett hva man syns, kommer det ikke til å forsvinne.”

Det vil alltid være en del mennesker der ute som aldri vil, og som aldri kommer til å betale for nedlastning av film og musikk. De vil gå store omveier og selv om man går til rettslige skritt vil disse ikke være villige til å betale for disse tjenestene.

Et eksempel på dette er nettopp Peter Sunde. Det man burde fokusere på er å begrense tilgjenglighet for allmennheten. Dette er det flere løsninger på: Selskaper som Telenor kan blokkere tilgangen til ip-adresser, altså blokkere tilgangen til internett sider som thepiratebay.org, jfr. den tidligere nevnte dommen fra Asker og Bærum Tingrett.[117] Tingretten har derimot avslått en slik løsning, enn så lenge. I følge Gisle Hannemyr ved Institutt for rettsinformatikk kan rettspålagt blokkering av The Pirat Bay være en bedre kamel å svelge enn å overvåke internettrafikken for å straffe enkelt personer. ”Det vil løse dette dilemma med at vi ikke ønsker at nettet skal være et arnested for ulovligheter på en bedre måte som de personvernkrenkelsene som måtte følge ved å gå etter enkeltpirater.”[118] Her er altså en løsning, som kan vise seg å være til det beste for den enkelts personvern. På den annen side, kan man spørre seg om det er internettilbyderen sin oppgave å filtrere internett. Da må det trekkes opp grenser for hva som skal filtreres, og hvilke sider. Noe som fremstår som et enkelt valg for nettsteder som thepiratebay.org som har en klar overvekt av ulovlig fildeling. Spørsmålet er så hvor grensen skal trekkes etter dette. Etter mitt syn må hvert enkelt tilfelle hvor en interesse organisasjon ønsker å stenge en internettside inn for retten, og så får det være opp til retten å bestemme hvilke internett sider som og om de skal stenges for allmennheten. Dette må være løsningen i et slikt tilfelle, helt til lovgiver kommer på banen, og vi eventuelt får en lov som ipred-loven i Sverige. Et slikt scenario kan være en fremtidsløsning, hvor brukerne blir utestengt. Dette er en form for statlig kontroll over private selskaper som mange finner uheldig i dagens samfunn.

---

[117] TAHER-2009-96202

[118] Sitatet er hentet fra: http://nrk.no/magasin/spiller/1.6813158#articlecomments

Det kan derimot argumenteres med at staten griper inn og tar overordnet valg i en rekke sammenhenger, på bakgrunn av folkets ønsker. I dette tilfelle, som i andre, er det et ønske om å forhindre straffbar handling.

Et annet scenario vil være å bruke de midler som markedet selv sitter med: å selge seg inn på en mer fornuftig måte til brukerne. For det finnes en vilje til å betale for film og musikk. IFPI og andre sitt mål må være å utnytte denne før den forsvinner. Det å få på plass lovlige tjenester og la de være like gode som pirattjenestene vil være et eksempel på hvordan man kan bruke markedet og etterspørselen etter enkle løsninger til sin fortjeneste. Hvis markedet ikke satser ensidig på å selge eksemplarer, men knytter nedlastingen til abonnement og sosiale nettsteder vil dette med all sannsynlighet gi et godt alternativ. Et eksempel på en slik tjeneste er iTunes som knytter seg opp til diverse andre tjenester og hardware.
En annen strategi vil være å gi rabatter, spesielt til barn. Noe som vil bygge lojalitet. Når de først har betalt: La brukerne boltre seg i materialet. Restriksjoner på materialet, som antall tillatte nedlastninger osv, vil gi en negativ opplevelse for mange brukere.

Hvilken løsning som er mest suksessrik vil tiden vise.

# 4 KONKLUSJON

Jeg vil i dette kapittelet prøve å oppsummere resultatene jeg har kommet frem til i oppgaven, og fra dette komme med en form for konklusjon.

Oppgaven gir et nyansert bilde av hvorvidt ip-adresser burde omfattes av personopplysningsloven. I noen tilfeller vil det være mer naturlig at ip-adresser omfattes, som ved internettilbyder sin behandling av persondata. Her har internettilbyderen en reell mulighet til å identifisere brukeren. I andre tilfeller vil en bruker måtte samarbeide med internettilbyderen for å få tilgang til personopplysninger gjennom ip-adresser. Dette vil ofte

forekomme gjennom ulovlig aktivitet. Et annet argument som trekker i retning av å omfatte ip-adresser under personopplysningsbegrepet er den mulige formålsutglidningen som kan forekomme i slike tilfeller. Etter min oppfatning burde loven ta høyde for *all* mulig identifikasjon og ip-adresser burde være å anse som personopplysninger.

Når det gjelder hvilke identifiseringsprosesser som er tillatt for politiet, kommer det klart frem av kapittel 3.3.2 at politiet har tilstrekkelig med hjemmel til å bekjempe ulovlig fildeling. Spørsmålet om en effektiv bekjempelse av den ulovlige fildelingen står på ressurser, noe som er en politisk avgjørelse.

For sivile stilles det en rekke krav til behandling av personopplysninger. En eventuell behandling vil bero på hvorvidt kravene er oppfylt, herunder om formålet står i samsvar med behandlingen.

Konklusjonen i forhold til internettilbydere må etter min oppfatning bli at de ikke har en plikt til å utestenge brukere fra ip-adresser som utelukkende driver med ulovlig fildeling, jfr. "Telenor avgjørelsen".[119]

Oppgaven viser at i hovedsak at opphavsretten har trukket mer og mer inn i personvernets sfære, på bakgrunn av sivile parters ønske om en mer effektiv håndhevelse av åndsverksloven. Det blir stadig mer press på personvernet, i forhold til private parters ønske om identifisering av brukere.

# 5 KILDEKRITIKK

I denne oppgaven bruker jeg en del artikler fra diverse nettsteder, man kan sette spørsmålstegn ved troverdigheten, objektiviteten, nøyaktigheten, og egnetheten til disse.

[119] TAHER-2009-96202 publisert 06.11.2009

Jeg ville derimot ikke valgt å bruke noen sider eller kilder som jeg ut fra mitt eget skjønn fant tvilsomme eller som på et faglig nivå var uakseptabelt etter Universitetets standard, slik jeg vurderer den. Under en del emner kommer det frem subjektive synspunkt til forfattere eller organisasjoner, jeg vil da gjøre klart hvem sine meninger dette er og hvilke kilder disse meningene er hentet fra. Det vil alltid kunne settes spørsmålstegn ved kilder, om troverdigheten, objektiviteten, nøyaktigheten, og egnetheten, innen det juridiske området vil derimot kildekritikken fortone seg annerledes enn i f.eks historisk sammenheng. I dommer er det dommeren som legger til grunn det han/hun anser som faktum, og det er opp til jurister å tolke dommen. Jus er preget av tolkning og skjønn, og det er også kildekritikken.

# 6 Litteraturliste

## 6.1 Litteratur


Bing, Jon *Personvern i faresonen*. Oslo, 1991

Bygrave, Lee. A *Data Protection Law – Approaching its Rationale, Logic and Limits*. Kluwer Law International, 2002

Coll, Line *Innsyn I Personopplysninger I Elektroniske Markedsplasser*. (Complex 2/2002, Institutt for Rettsinformatik). 2002

Church, Peter & Kon, Georgina *Data Protection and search engines-Google at heart of a data protection storm*. (Publisert i Computer Law & Security Report, 2008) 2008

Hov, Jo *Rettergang II, straffeprosess. 2007*

Hugenholtz, P. Bernt, *Copyright and electronic commerce : legal aspects of electronic copyright management* . 2000

Koktvedgaard , Mogens *Lærebog i Immaterialret: Lærebog i immaterialret : ophavsret, patentret, brugsmodelret, designret, varemærkerett* 7 utgave, revidert av Schovsbo, Jens. 2005

Schartum, Dag Wiese & Bygrave, Lee A. *Personvern i informasjonssamfunnet* 2. opplag. 2004

## 6.2 Dommer, kjennelser og avgjørelser

Lovdata Rt 1992 904

Lovdata Rt 1992 928

Lovdata Rt 1999 1944

Lovdata TFRED-2006-177576, Pitbullterje

Lovdata LB-2007-10-11

Lovdata TAHER-2009-96202 publisert 06.11.2009

Lovdata TOSLO-2004-41422, 2004-11-18 (Oslo tingrett)

(Dansk høyesterettsdom) Sag 49/2005 (1. afdeling) 10. februar 2006

B 13301-06 (Stockholms tingsrätt) 17.04.2009

EMD Case 101/02 Sweden v Lindqvist (6 November 2003)

EMD Case 2 EHRR 214 Klass and others v Federal Republic of Germany (6 September 1978)

(AG München) 133 C 5677/08 ”Dynamische IP-Adressen” publisert 30.09.2008

(Amtsgericht Berlin-Mitte) 5 C 314/06, publisert 27.03.2007.

(Landgericht Darmstadt) 25 S 118/2005, publisert: 07.12.2005

(Lænsrætten i Stockholms Læn) 593-2005, publisert 08.06.2005

Personvernnemdas klagesak 2004/01 (STAMI)

## 6.3 Lovregister

1961 Lov om opphavsrett til åndsverk m.v. (Åndsverksloven) av 12. mai 1961 nr. 2.

1981 Lov om rettergangsmåten i straffesaker (Straffeprosessloven) av 22.05 nr 25.

1999 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21.05 nr 30

2000 Lov om behandling av personopplysninger (Personopplysningsloven) av 14.04 nr. 31

2003 Lov om elektronisk kommunikasjon (Ekomloven) av 4.juli 2003 nr 83.

2003 Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (Ehandelsloven) av 25.03 nr 35.

2004 Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (Ekomforskriften) av 02-16 nr 401.

## 6.4 Forarbeider

Ot.prp. nr. 31 (2002-2003) Om lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester

Ot.prp. nr. 46 (2004-2005) Om lov om endringer i åndsverkloven m.m.

Ot.prp. nr 58 (2002-2003) Om lov om elektronisk kommunikasjon

Ot.prp. nr. 92 (1998-99) Om lov om behandling av personopplysninger

NOU 1997:19 Et bedre personvern – forslag til lov om behandling av personopplysninger

NOU 2007:2 Lovtiltak mot datakriminalitet Delutredning II

NOU 2009:1 Individ og integritet Personvern i det digitale samfunnet

St.meld. nr 21 (2007-2008) *Samspill*

## 6.5 Konvensjoner, traktater og direktiver

Direktiv 95/46/EF Om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger

EU-direktiv 2006/24/EF Om lagring av trafikkdata

## 6.6 Artikler og elektroniske dokumenter

01248/07/EN WP 136 *Article 29 data protection working party, Opinion 4/2007 on the concept of personal data.* 2007
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf (Sitert 03.05.2008)

0737/EN/WP 148 *Article 29 data protection working party, Opinion 1/2008 on data protection issues related to search engines.* 2008
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf (Sitert 13.09.2008)

5063/00/EN/Final WP 37 *Working Document Privacy on the Internet - An integrated EU Approach to On-line Data Protection-.* 21.11.2000
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf (Sitert 12.11.2008)

Aasland, Jarle, *Vil ikke etterforske ulovlig fildeling*. 2009
http://aftenbladet.no/lokalt/1000730/Vil_ikke_etterforske_ulovlig_fildeling.html (Sitert 25.08.2009)

Blaker, Magnus *Slutten for dagens internett* 19.05.08
http://www.nettavisen.no/it/article1919504.ece (Sitert 15.11.08)

Conradi, Christopher, *Hva er egentlig Internett og hvordan fungerer det?* 05.10.2008 http://www.klikk.no/teknologi/data/article335697.ece (Sitert 05.10.08)

Erling Moe, *Juridisk Ordliste.* 21.09.2009, http://www.domstol.no/DAtemplates/Words.aspx?id=3547&epslanguage=NO (sitert 16.november 2008).

Fleischer, Peter *Are IP-adresses "Personal Data"?.* 2007 http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html (Sitert 01.04.2008)

Fleischer, Peter *Google Response to the Article 29 Working Party Opinion On Data Protection Issues Related to Search Engines 09/2008.* 2008 http://www.scribd.com/doc/5625427/google-ogb-article29-response (Sitert 19.02.2009)

Hagen, Anders W. *Fire av 182 saker etterforsket.* Oslo 2008. http://avis.dn.no/arkiv/?articleId=200818569 (Sitert 19.oktober 2008)

Moe, Erling, (ansvarlig redaktør). *Juridisk ordliste.* Trondheim 2009. http://www.domstol.no/DAtemplates/Words.aspx?id=3547&epslanguage=NO (Sitert 22.januar 2009)

Rønnevig, Leif-Henrik, *Rettsdata, Note 32 (til ekomloven).* 2009 http://abo.rettsdata.no/propub/template.htm?view=browse&doc_action=setDoc&doc_keytype=gadests&bid=direct&s_terms=ekomloven&doc_key=gL20030704z2D83&hash=gL20030704z2D83 (Sitert 15.10.09)

Schartum, Dag Wiese (a) *Rettsdata, Note 3 (til personopplysningsloven § 2).* 2009 http://abo.rettsdata.no/propub/template.htm?view=browse&doc_action=setDoc&doc_keyty

pe=gadests&bid=direct&s_terms=personopplysningsloven&doc_key=gL20000414z2D31&hash=gL20000414z2D31 (Sitert 12.09.09)

Schartum, Dag Wiese (b) *Rettsdata, Note 53 (til personopplysningsloven § 11).* 2009 http://abo.rettsdata.no/propub/template.htm?view=browse&doc_action=setDoc&doc_keytype=gadests&bid=direct&s_terms=personopplysningsloven&doc_key=gL20000414z2D31&hash=gL20000414z2D31 (Sitert 07.07.09)

Schartum, Dag Wiese (c) *Rettsdata, Note 56 (til personopplysningsloven § 11).* 2009 http://abo.rettsdata.no/propub/template.htm?view=browse&doc_action=setDoc&doc_keytype=gadests&bid=direct&s_terms=personopplysningsloven&doc_key=gL20000414z2D31&hash=gL20000414z2D31 (Sitert 07.07.09)

Wojcicki Susan,*The Official Google Blog: "Making ads more interesting".* 11.2009 http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html (Sitert 19.11.2009)

## 7 Lister over tabeller og figurer m v

Figur 1: Tekniske spesifikasjoner i InternettExplorer.

Bildene/illustrasjonene i oppgaven har jeg selv laget.