IP-ADRESSE SOM BEVISMIDDEL I STRAFFESAKER

Kandidatnummer: 671

Leveringsfrist: 27.04.2009

Til sammen 17981 ord

27.04.2009

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn

Da World Wide Web (www) ble presentert for offentligheten i 1993, besto Internett av omtrent 50 datamaskiner – et regionalt nettverk for de helt spesielt interesserte. Microsoft gründer Bill Gates skal ha uttalt: *"The Internet? We're not interested in it?"*.[1] I 2008 ble det anslått at over 1,4 milliarder mennesker var aktive brukere av Internett, og veksten mellom 2000-2008 var på hele 305,5 %.[2] Det som på slutten av 1960-tallet ble dannet som et kommunikasjonsnett for forsvars-, universitets- og forsknings institusjoner, har på få tiår opplevd eksponentiell utvikling og i stor grad revolusjonert måten vi organiserer våre samfunn på.[3] Internett er et uvurderlig verktøy og en globaliserende kraft som legger føringer for sentrale samfunnsområder som media, myndigheter, kommunikasjon, informasjon, næringsliv og handel.

Men utviklingen har også ført med seg nye utfordringer for det moderne samfunnet. Internett har gitt grobunn for nye kriminelle adferdsmønstre, og presset myndigheter til å utvikle nye bekjempelsesmetoder. Ulovlig fildeling har rammet platebransjen hardt.[4] Barnepornografi spres via Internett i et volum som tidligere ikke var mulig.[5] Økonomisk kriminalitet har vokst i omfang og blitt mer sofistikert.

Internetts virtuelle vesen har gjort det enklere både fysisk og psykologisk å begå lovbrudd, enn i det praktiske liv. Terskelen for å laste ned en film ulovlig, er trolig lavere enn å stjele den fra butikken. Risikoen for at det samme straffbare forholdet blir oppdaget ansees også å være lavere ved bruk av Internett.

---

[1] http://www.quotesandsayings.com/gbillgates.htm [sitert 24.04.2009]
[2] www.internetworldstats.com/stats [sitert 24.11.2008].
[3] ISSA (2000)
[4] St.meld. nr. 21 (2007-2008) pkt. 3.3.
[5] Kripos (2003) s. 7 og Sunde (2006) s. 217.

1.2 Valg av tema

Oppgavens tema er valgt ut i fra flere forskjellige hensyn og interesser.

Internettkriminalitet er et stort og voksende problemområde, og IP-adresse et av få gode instrumenter påtalemyndigheten har til rådighet i møte med et Internett som ikke enkelt lar seg overvåke, hverken praktisk eller juridisk. [6] IP- adresse fungerer som ledd i etterforskningsarbeid og som bevismiddel i hovedforhandling, og tolkningen av rekkevidden og vekten av IP-adresse som bevismiddel er derfor av stor betydning i slike saker.

Spørsmål knyttet til bevisbedømmelse og beviskrav står sentralt i den praktiske strafferett, men har etter mitt skjønn ikke fått den samme sentrale plass i det juridiske studium. I straffesaker er det ofte bevistemaet som er sakens stridende kjerne, ikke den materielle jussen, og jeg har derfor ønsket å benytte meg av muligheten i å fordype meg i temaet her.

Det kan stilles spørsmål ved om det er hensiktsmessig å vurdere IP-adresse isolert som bevismiddel. Normalt bygger retten sin avgjørelse på en rekke bevismidler, og avgjør gjennom sin bevisvurdering om bevisene, samlet sett, oppfyller beviskravet. Jeg vil likevel argumentere for at en teoretisk vurdering av IP-adresse som enkeltbevis vil være både interessant og praktisk relevant av flere årsaker. Først og fremst vil en generell bevisvurdering kunne gi veiledning om hvilken vekt og relevans IP-adresse bør ilegges i den enkelte straffesak, også der flere bevismidler foreligger. IP-adresse er også et bevismiddel der flere tekniske momenter har betydning for bevisverdien, og dette gjør at behovet for kunnskap om de rettslig relevante momentene ved beviset er større enn ved tradisjonelle bevis.

[6] Willassen (2008)

1.3 Problemstilling

Oppgavens problemstilling er om IP-adresse er et godt bevismiddel i straffesaker.

Innholdet i utrykket *"godt bevismiddel"* er ikke gitt i seg selv og trenger en nærmere presisering. I norsk rett er det er ingen skrevne regler for hvilke kriterier som er relevante for vurderingen av hvor godt et bevismiddel er og hvilken vekt momentene eventuelt har. En drøftelse av hvorvidt et bevismiddel er godt eller ikke må derfor bero på tolkning av lovverket, juridisk teori og rettspraksis. Dette vil etablere grunnlag for å trekke ut kriterier for hva som utgjør et godt bevismiddel – i rettslig forstand. Oppgavens omfang krever at kun de mest relevante momenter drøftes, selv om andre momenter naturligvis kunne ha vært trukket inn. I det følgende vil jeg forsvare mine valg av momenter.

Formålet til et bevismiddel i straffesaker er å overbevise retten om en rettslig relevant omstendighet.[7] I vurderingen av om et bevismiddel er godt eller ikke, er det naturlig å vurdere hvor godt bevismidlet er egnet til å oppfylle sitt formål. Momentet her blir med andre ord hvor stor overbevisningskraft bevismidlet har. Hvilke kriterier som igjen bestemmer overbevisningskraften er flere. De mest sentrale er bevismidlets evne til å kunne gi en entydig beskrivelse av hendelsesforløpet, og troverdigheten til de opplysningene som kan trekkes ut.

Et annet moment som er relevant er bevismidlets tilgjengelighet for påtalemyndighet og retten. Det følger av straffeprosessloven[8] § 305 at retten bare skal ta i betraktning bevis som blir lagt frem i hovedforhandling. For at beviset skal oppnå sitt formål må beviset kunne fremlegges for retten i hovedforhandling. Tilgjengeligheten kan begrenses av praktiske, økonomiske og juridiske hindringer. Hindringene kan føre til at avgjørende bevis for sakens opplysning ikke kommer for retten. Er hindringene et symptomatisk trekk ved en type bevismiddel, mister det verdi.

[7] Strandbakken (2003) s. 45.
[8] Lov 22. mai 1981 nr. 25 om rettergangen i straffesaker (strpl.)

Ytterligere et moment i vurderingen er i hvilken grad bevismidlet griper inn i borgerens sfære og krenker den personlige integritet. Lovgiver har vedtatt en rekke bestemmelser som beskytter borgerne mot inngrep, og at inngrep kun kan foretas på gitte vilkår.[9] Det er naturlig å se dette som at lovgiver mener at inngrep bør unngås og at bevis bør bli innhentet på andre måter. Høyesterett har også uttalt at den personlige integritet har høy verdi i strafferetten.[10] Inngrep i borgerens sfære vil som oftest oppleves som en krenkelse. Betinger innhenting av beviset et slikt inngrep, kan dette trekke i retning av å ikke anse det som godt.

I et samfunn der teknologien er i rask utvikling, vil også stadig nye typer bevismidler presenteres for retten. Teknisk kompliserte bevismidler vil kunne skape usikkerhet for retten om hvilken vekt og rekkevidde beviset skal ha. På bakgrunn av det vil det være et moment om retten lett kan få innsikt i rekkevidden og vekten av bevismidlet.

I min drøftelse av de momenter som fremgår ovenfor vil det bli lagt særskilt vekt på kriteriene *overbevisning* og *tilgjengelighet*.[11] De øvrige momenter vil det bli knyttet noen kommentarer til.[12]

1.4 Avgrensning

Oppgavens tittel og problemstilling favner meget vidt. Dette er gjort bevisst, og formålet er å skape rom for å kunne behandle IP-adresse fra innhentning til vurdering som bevismiddel i hovedforhandling. Oppgavens art og omfang tillater likevel ikke at alle emner knyttet til problemstillingen tas med. Jeg vil derfor her foreta en generell avgrensning mot de temaer som ikke vil bli behandlet i oppgaven. Avgrensninger vil også forekomme underveis i oppgaven der det er naturlig.

---

[9] For eksempel i straffeprosessloven kapittel 16
[10] Rt. 1996 s. 1116 (1122)
[11] I avsnitt 3.2 til 3.6.
[12] I avsnitt 4.4 og 4.5.

Kriteriene i problemstillingen om hvilken overbevisningskraft IP-adresse har, vil bli vurdert der bevismidlet blir lagt frem i en hovedforhandling i en straffesak. IP-adresse som bevismiddel for å gjennomføre tvangsmidler i etterforskningssammenheng faller utenfor. IP-adresse på etterforskningsstadiet vil kun behandles i lys av tilgjengelighetskriteriet.

Kriminalitet på Internett reiser mange problemstillinger i forhold til jurisdiksjon. Problemet er både aktuelt og relevant i forhold til kriteriet om tilgjengelighet. Jeg har likevel funnet det mer hensiktsmessig å fokusere på de regler som begrenser tilgjengeligheten i forhold til personvernhensyn. Problemstillinger knyttet til jurisdiksjon vil derfor ikke bli berørt i oppgaven.

1.5 Rettskildebruk

Oppgaven bygger på tradisjonell juridisk metode, og vil bli besvart på bakgrunn av de rettskildeprinsipper og faktorer som er gjeldende for norsk rett. Besvarelsen av de juridiske spørsmål som oppgaven reiser har primært blitt søkt funnet i formell lov, forskrifter, forarbeider, etterarbeider og rettspraksis. Andre rettskilder som juridisk teori og reelle hensyn blir trukket inn der de nevnte rettskilder ikke gir et klart svar.

I 1999 ble den Europeiske menneskerettskonvensjon (EMK/konvensjonen) inkorporert i norsk lov, og skal ved motstrid gå foran norsk lov.[13] Tolkningen av konvensjonen har derfor betydning for fastleggelsen av norsk rett. Den europeiske menneskerettighetsdomstol (EMD) sin praksis og tolkning av konvensjonen vil også bli trukket inn som rettskildefaktor.

Oppgaven er en deskriptiv fremstilling av rettstilstanden. Enkelte ganger vil det være naturlig å si noe normativt om de rettstema som behandles. Dette vil da fremgå ettertrykkelig i teksten.

[13] Lov 21. mai 1999 nr. 49 om styrking av menneskerettighetenes stilling i norsk rett (mnskrl.) §§ 2 og 3.

1.6 Oppgavens oppbygning

Etter problemstillingen vil spørsmål knyttet til IP-adresse fra innhenting til det skal vurderes som bevismiddel i hovedforhandling i en straffesak, besvares.

Jeg har funnet det hensiktsmessig å dele drøftelsen av problemstillingen inn i tre hoveddeler. I første del, oppgavens kapittel 2, vil jeg behandle de generelle regler i strafferetten om beviskrav, bevisbedømmelse og bevisføringsplikt. Beviskravet i strafferetten vil bli spesielt grundig behandlet, da retten på bakgrunn av beviskravet skal ta stilling til om de faktiske forhold er tilstrekkelig belyst for å idømme en straff i det foreliggende tilfellet.[14] Dette er sentralt for oppgaven da spørsmålet om IP-adressen er et godt bevismiddel eller ikke må vurderes på bakgrunn av de generelle regler om bevis i strafferetten.

I andre del, oppgavens kapittel 3, vil jeg drøfte spørsmål knyttet til IP-adresse i tilknytning til kriteriet om tilgjengelighet. Her vil jeg også drøfte hvilken overbevisning IP-adresse kan ha som bevismiddel.

I siste del, oppgavens kapittel 4, er temaet *effektivitetshensyn kontra rettssikkerhetsprinsippet*. Her vil jeg drøfte det generelle beviskravet i straffesaker i lys av den spesielle bevisvurderingen av IP-adresse. Kan IP-adresse stå alene som eneste bevismiddel for en fellende dom, eller bør, eventuelt må, andre bevis til for at tiltalte kan dømmes, jfr. det strenge beviskravet? I denne delen av oppgaven vil jeg også drøfte de resterende kriteriene i problemstillingen om i hvilket omfang inngrep IP-adresse som bevis gjør i borgerens sfære, og rettens forutsetninger for bevisvurdering av IP-adresse. I tillegg drøfte de kryssende hensyn som gjør seg gjeldende for kriteriene. Avslutningsvis vil jeg oppsummerer hovedtrekkene i oppgaven, før jeg konkluderer problemstillingen.

[14] Strandbakken (2003) s. 58.

2 Bevis i strafferetten

2.1 Bakgrunn

Vurderingen av IP-adresses overbevisningskraft som bevis i straffesaker må sees i sammenheng med det generelle beviskravet i stafferetten. Der beviskravet er høyt, stilles det strengere krav til bevisenes overbevisningskraft for at et faktum kan legges til grunn.[15]

I det følgende vil jeg gi en innføring i hva bevis er, hvordan bevisbyrden virker og hvordan bevis bedømmes juridisk. Hovedfokuset vil være å drøfte beviskravet i strafferetten, og nærmere gjøre rede for dets innhold.

2.2 Hva er bevis?

Formålet med å legge frem bevis er å underbygge grunnlaget for den anførte påstand for retten.[16] I juridiske sammenhenger brukes begrepet *"bevis"* i to forskjellige betydninger: *"bevismiddel"* og "*overbevisningsgrunn"*.

Bevismiddel defineres som en opplysningskilde som bidrar til å fremskaffe dommerens overbevisning om faktum i en rettssak, uten betydning til styrken.[17]
"Overbevisningsgrunn" eller også "*bevisresultat"* brukes om resultatet bevismidlene samlet sett oppnår.[18] Begrepet bevis i denne oppgaven brukes i betydning bevismiddel.

[15] Hov I (2007) s. 266-267.
[16] Strandbakken (2003) s.45.
[17] Hov I (2007) s. 266 og Strandbakken (2003) s. 45.
[18] Hov I (2007) s. 266 og Strandbakken (2003) s. 46.

2.3 Bevisbyrden, bevisføring og bevismidler

2.3.1 Bevisbyrden

Begrepet *"bevisbyrde"* brukes til å løse rettslige tvister der faktum er usikkert.[19] Meningsinnholdet i begrepet deles i juridisk litteratur inn i to: *"beviskravet"* og *"bevisføringsplikten"*. Beviskravet defineres som reglene for hvilken grad av sannsynlighet som kreves for at det faktum som hevdes kan legges til grunn. Bevisføringsplikten angir hvem av partene som har plikt til å føre bevis for sin påstand. [20] Noen egentlig plikt til å føre bevis er det ikke, da unnlatelse av å oppfylle plikten ikke har noen virkninger i form av sanksjoner, men kan resultere i at påstanden ikke blir lagt til grunn.

Beviskravet og bevisføringsplikten er forskjellig i sivile – og straffesaker. Bakgrunnen for denne forskjellen er de ulike hensyn som gjør seg gjeldende i de to typer rettergangsprosesser.

I sivilprosessen er hovedregelen til beviskravet *"overvektsprinsippet"*. Hjemmelen er ulovfestet, men må anses å ha vunnet allmenn oppslutning. Hensynet bak regelen er at med overvektsprinsippet vil flest saker bli pådømt riktig.[21] Beviskravet kan også følge av spesiallovgivningen.[22]

Hovedregelen i straffesaker er at påtalemyndighetene har bevisbyrden.[23] I forhold til beviskravet betyr det at beviskravet må settes høyt, jfr. nedenfor i avsnitt 2.4. Det følger implisitt av at beviskravet i straffesaker settes høyt at påtalemyndighetene har bevisføringsplikten. Hjemmelen for at bevisbyrden pålegges påtalemyndighetene følger av langvarig praksis i straffesaker.[24] Det følger i tillegg av uskyldspresumsjonen som har blitt

[19] Strandbakken (2003) s. 48.
[20] Strandbakken (2003) s. 49 og 58.
[21] Hov I (2007) s. 350.
[22] Se blant annet lov 3. mars 1972 nr. 5 om arv m.m. (al.) § 57 (2) der beviskravet satt til "tvillaust" eller lov 6. aug. 1984 nr. 59 om fordringshavernes dekningsrett (deknl.) § 5-2 (2), jfr. "utvilsomt".
[23] Andenæs I (2000) s. 177.
[24] Se blant annet Rt. 1990 s. 319 (322)

lovfestet i EMK art. 6 nr. 2.[25] De rettslige følgene av at påtalemyndighetene har bevisføringsplikten, er at tiltalte ikke trenger å føre bevis for sin uskyld for å unngå å bli dømt.

At bevisføringsplikten påhviler påtalemyndighetene i straffesaker kan også sies å følge på bakgrunn av sammenhengen i lovverket. Lovgiver pålegger unntaksvis en bevisføringsplikt for den bestemmelsen retter seg mot, jfr. strpl. § 249 nr. 3 og lov 29. mai 1981 nr. 38 om viltet (viltl.) § 34 (1) 3. punktum.[26] Dette innebærer at bevisbyrden snus. Hovedregelen er allikevel at bevisføringsplikten påhviler påtalemyndigheten.

I sivilprosessen er bevisføringsplikten lagt på partene, jfr. lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvl.) § 11-2 (2) første punktum.

2.3.2 Bevisføring

Bevisføring er fremleggelse av bevismidler for retten. Hovedregelen i straffeprosessen er at partene fritt kan føre de bevis som de finner ønskelig. Prinsippet følger ikke av noen lovregel, men har kommet til utrykk i en rekke Høyesterettsdommer.[27] I Rt. 1990 s. 1008 (1010) uttalte Høyesterett seg om rettstilstanden:

"Etter norsk straffeprosess har partene i utgangspunktet anledning til å føre de bevis de ønsker vedrørende saken. Denne forutsetning er ikke direkte kommet til uttrykk i loven, men hovedregelen er likevel klar."

I dette ligger et prinsipp om fri bevisførsel, og hensynet bak prinsippet er at saken skal være best mulig opplyst, og at grunnlaget for avgjørelsen blir mer solid.[28] I sivilprosessen er dette slått fast i tvl. § 21-3 (1).

---

[25] Strandbakken (2003) s. 340.
[26] "Bevisbyrden" i viltl. omfatter både beviskrav og bevisføringsplikt, jfr. Rt. 1957 s. 950 og Rt. 1957 s. 1132.
[27] Se blant annet Rt. 1996 s. 1114 (1115) og Rt 2004 s. 858 (pkt. 18)
[28] Strandbakken (2003) s. 61 og 181.

Det finnes unntak fra prinsippet om fri bevisførsel. Bevis kan nektes ført og bli avskåret på bakgrunn av lovfestet og ulovfestet hjemmel. For eksempel kan bevismidler som omfattes av taushetsplikten til bestemte yrkesgrupper, som utgangspunkt, ikke legges frem for retten, jfr. strpl. § 119. Det følger av fast Høyesterettspraksis at heller ikke resultat av løgndetektortest kan brukes som bevis.[29]

2.3.3 Bevismidler

Et bevismiddel er en opplysningskilde som bidrar til å klargjøre de rettslige relevante omstendighetene ved en sak.[30] Det er på bakgrunn av de bevismidler som blir ført i hovedforhandling, at retten kan ta stilling til hvilket faktum som skal legges til grunn, jfr. strpl. § 305. Bestemmelsen er likevel ikke til hinder for at retten kan bygge på kjensgjerninger eller faktiske sammenhenger på grunnlag av sin alminnelige livserfaring.[31]

I juridisk teori har man funnet det hensiktsmessig å dele bevismidler i kategorier, blant annet etter overbevisningskraft, form og innhold. Noen bevismidler egner seg til å slå sikkert fast at tiltalte er gjerningspersonen, mens andre fastslår det motsatte. Disse typer bevis omtales gjerne som sikkert bevis og utelukkelsesbevis. De færreste bevis faller inn under disse kategoriene. Bevis vil som oftest trekke i varierende styrke i retning av at tiltalte er gjerningspersonen eller ikke. Slike bevis omtales som sannsynlighetsbevis.[32]

IP-adresse tilhører kategorien elektronisk bevis. Elektroniske bevis er bevismidler som lagres elektronisk og som kan gi rettslig relevante opplysninger. Slike bevis skiller seg fra personlige bevis ved at de ikke har noen subjektive motiv. Eksempler på elektroniske bevis kan stamme fra innholdet av en mobiltelefon, harddisk eller videoovervåkning.

---

[29] Se blant annet i Rt. 1990 s. 1008 (1010) og Rt. 1996 s. 1114.
[30] Strandbakken (2003) s. 45.
[31] Hov I (2007) s. 335.
[32] Bratholm (2008) s. 175-176.

2.4 Beviskravet i strafferetten

2.4.1 Beviskravets rettslige utgangspunkt

Etter alminnelig juridisk metode ville det vært naturlig å ta utgangspunkt i en generell lovregel for å bestemme hvilket beviskrav som må legges til grunn. Norsk lovgivning har ingen slik lovbestemmelse som etter ordlyden beskriver hvilket beviskrav som skal legges til grunn.[33]

Beviskravet har blitt slått fast i en rekke Høyesterettsavgjørelser, og kan utrykkes ved at *"enhver rimelig tvil skal komme tiltalte til gode"*.[34] Tradisjonelt sett har beviskravets rettslige forankring i norsk rett vært langvarig rettspraksis og teori.[35]

EMK er inkorporert i norsk rett og skal ha forrang annen lovgivning, jfr. mnskrl. § 3. Det er derfor av betydning for fastleggelsen av beviskravet i norsk rett hvorvidt det følger et beviskrav av EMK. Uskyldspresumsjonen er et grunnleggende universalt rettsstatsprinsipp for straffesaker. Uskyldspresumpsjonen var i norsk rett ulovfestet, inntil den ble nedfelt i EMK art. 6 nr. 2. Prinsippet kan uttrykkes som at *"enhver skal anses uskyldig inntil det motsatte er bevist"*.[36] I EMK art. 6 nr. 2 har prinsippet fått ordlyden:

"Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law."

Etter ordlyden er det naturlig å forstå prinsippet slik at påtalemyndighetene har bevisføringsplikten.[37] Hvorvidt et beviskrav følger av prinsippet går ikke klart frem av ordlyden.

---

[33] Strandbakken (2003) s. 345.
[34] Se blant annet Rt. 2001 s. 44 (46) og Rt. 2004 s. 1063 (pkt. 9).
[35] Andenæs I (1994) s. 162-163.
[36] Strandbakken (2003) s. 27.
[37] Strandbakken (2003) s. 340. Om bevisføringsplikten, jfr. avsnitt 2.3.1 i denne oppgaven.

Den juridiske metode som skal legges til grunn for tolkningen av rekkevidde av EMK skiller seg ut fra den alminnelige metode norsk rett. Dette ble drøftet i Rt. 2000 s. 996 (Bøhlerdommen). De prinsipper som ble slått fast der, har blitt fulgt opp i flere Høyesterettsdommer.[38] Etter denne praksis skal norske domstoler foreta en selvstendig tolkning av konvensjonen. Tolkningen skal være i samsvar med den metoden EMD benytter ved håndhevelsen av EMK. Norske domstoler må dermed basere seg på konvensjonsteksten, alminnelige formålsbetraktninger og EMDs avgjørelser.[39]

I Rt. 2007 s. 1217 behandlet Høyesterett problematikken om hvorvidt det følger et beviskrav av EMK art. 6 nr. 2. Dommen ble avsagt under dissens.

Høyesteretts flertall og mindretall la til grunn forskjellige deler av ordlyden i bestemmelsen til støtte for sitt synspunkt. Mindretallet la til grunn at beviskravet fulgte av *"according to law"*, som var en henvisning til beviskravet i konvensjonsstatens nasjonale rett.[40] Flertallet ved førstvoterende la vekt på en annen del av ordlyden:

"Selv om ordlyden i artikkel 6 nr. 2 ikke gir noe klart svar, er det etter min mening mest naturlig å forstå den slik at bestemmelsen oppstiller et beviskrav (« until proved guilty ») [41]

Det som ble avgjørende for både flertallet og mindretallet var EMDs egen praksis. Grunnen til at retten ble splittet kommer av en tolkning av EMDs dommer. Førstvoterende som representant for flertallet tok utgangspunkt i en plenumsdom fra 1988 i saken Barberà mfl. mot Spania. Der ble det uttalt at *"any doubt should benefit the accused"*. Oversatt blir det *"enhver tvil skal komme tiltalte til gode"*. Førstvoterende uttalte at:

[38] Rt. 2002 s. 557 (565), Rt. 2003 s. 359 og Rt. 2005 s. 833 (pkt. 45).
[39] Rt. 2005 s. 833 (pkt. 45).
[40] Rt. 2007 s. 1217 (pkt. 77).
[41] ibid. pkt. 51.

"Denne uttalelse kan etter min oppfatning vanskelig forstås på noen annen måte enn at artikkel 6 nr. 2 ikke bare angir hvem som har bevisbyrden, men at den også oppstiller et beviskrav - enhver tvil skal komme tiltalte til gode." [42]

De lege lata følger det etter Rt. 2007 s.1217 at det er hjemlet et beviskrav i EMK art. 6 nr. 2. Rettsvirkninger av dette er at domstolene er bundet av den tolkning av beviskravet som oppstilles i EMD. EMDs praksis er dermed bindende for norske domstoler i fastsettelsen av beviskravet i norsk rett.

2.4.2 Hva skal bevises?

Det som skal bevises i en straffesak omtales som bevistema.[43] I en straffesak er det flere omstendigheter som må bevises for at tiltalte skal kunne dømmes. Bevistema vil ikke bare omfatte spørsmålet om tiltalte har utført ugjerningen, men også andre spørsmål.

I en straffesak er det to hovedspørsmål retten må ta stilling til; *skyldspørsmålet* og *straffespørsmålet*. Skyldspørsmålet består av å ta stilling til de forutsetninger som stilles for å ilegge straff, det vil si om de fire straffbarhetsvilkår er oppfylt.[44] For å idømme straff må det bevises at tiltalte har overtrådt en straffesanksjonert lovregel, utvist den nødvendige skyld, vært juridisk tilregnelig og at det er fravær av straffrihetsgrunner.

Under straffespørsmålet hører det med å avgjøre reaksjonsfastsettelsen, det vil si hvilken type straff som skal ilegges. Dette kan også utgjøre bevistema i en straffesak.[45] Det viktigste spørsmålet som retten skal besvare er skyldspørsmålet.[46] Det er klart at feil avgjørelse i disfavør av tiltalte i skyldspørsmålet gagner mer ulykke enn i straffespørsmålet. Dette har fått betydning for hvor strengt beviskrav som skal legges til grunn.

---

[42] Rt. 2007 s. 1217 (pkt. 54.)
[43] Hov I (2007) s. 266 og Strandbakken (2003) s. 47.
[44] Hov I (2007) s. 41.
[45] I.c.
[46] Andenæs I (2000) s. 177.

2.4.3 Beviskravet etter bevistemaets art

Beviskravet i strafferetten kan variere i forhold til hvilke spørsmål retten tar stilling til.[47] Hensynet bak beviskravet i strafferetten er at *"ingen uskyldige skal bli dømt"*. Det uttrykkes gjerne som at det er større ulykke at en uskyldig blir dømt enn at ti skyldige går fri.[48] Når det gjelder staffespørsmålet gjør ikke dette hensynet seg gjeldende i full styrke. Etter Høyesterettspraksis og teori kan beviskravet settes noe lavere, men det hersker strid om i hvilken grad beviskravet kan senkes.[49]

Når det gjelder beviskravet for skyldspørsmål, er heller ikke beviskravet her konstant. I Rt. 1998 s. 1945 (1947) uttaler Høyesterett seg generelt om beviskravet for skyldspørsmålet:

"Det er enighet i strafferettsteorien om at det ikke kan stilles de samme beviskrav med hensyn til alle straffbarhetsbetingelser. Det kan f eks ikke stilles like strenge beviskrav til tilregnelighet og subjektiv skyld som når det er spørsmål om tiltalte har begått den handling det er tale om."

Høyesterett presiserer at det her tales om nyanseforskjeller.[50] Hensynet bak at beviskravet kan senkes bygger på følgende hensyn: Det antas å være en mindre ulykke å dømme tiltalte når han faktisk har utført handlingen, men ikke har vært tilregnelig etter loven, enn om tiltalte ikke har hatt noen tilknytning til handlingen over hodet.

I lys av oppgavens tema vil ikke de nyanser i beviskravet som finnes for de enkelte straffbarhetsvilkår bli nærmere behandlet. IP-adresse er relevant i forhold til å bevise om tiltalte har overtrådt den objektive gjerningsbeskrivelse. Bevistema knyttet til de andre vilkårene for straff, lar seg ikke belyse av IP-adresse.

---

[47] Andenæs I (2000) s. 178.
[48] Hov I (2007) s. 349 og Andenæs I (2000) s. 177.
[49] Se blant annet Rt. 1992 s. 833 (834) og Hov I (2007) s. 364-365.
[50] Rt. 1998 s. 1945 (1947).

2.4.4 Beviskravets nærmere innhold

Når man skal angi det nærmere innhold av beviskravet i norsk rett, ville det vært naturlig å ta utgangspunkt i en lovregel. EMK art. 6 nr. 2 hjemler et beviskrav, men en nærmere beskrivelse av hva beviskravet inneholder kommer ikke frem av bestemmelsen.[51] Det nærmere innholdet i beviskravet må dermed klarlegges på bakgrunn av andre rettskilder.

De sentrale rettskilder for en slik vurdering er Høyesterettspraksis, juridisk teori, og EMDs praksis.

2.4.4.1 Høyesteretts praksis

Det følger av strpl. § 306 annet ledd at anke til Høyesterett ikke kan fremmes grunnet feil ved bevisbedømmelsen under skyldspørsmålet. Høyesterett er dermed avskåret fra konkret å vurdere bevisenes styrke opp mot beviskravet. Beviskravet kan likevel bli behandlet av Høyesterett etter anke vedrørende om feil beviskrav er lagt til grunn av underinstansen og derved gi veiledning i forhold til formuleringen av beviskravet.

I Rt. 1978 s. 882 (883) satt kjæremålsutvalget til side en dom på bakgrunn av feil formulering av underinstansen. Underinstansen fant det *"overveiende sannsynlig og således bevist"* det faktum som betinget skylden. Kjæremålet uttalte at det var *"uklart"* om underinstansen hadde stilt riktig krav til beviskravet. Kjæremålet uttalte videre at beviskravet først er oppfylt når det føres *"fullt bevis for det faktiske forhold"*, og slik at *"rimelig tvil skal komme tiltalte til gode"*. Overveiende sannsynlighet er altså ikke tilstrekkelig for å oppfylle beviskravet.

Formuleringen *"fullt bevis"* er ikke spesielt presis, og det er ikke lett å trekke noe konkret ut av utrykket. Utrykket utgjør likevel den positive angivelsen av beviskravet. Kjæremålsutvalget trekker også frem at *"rimelig tvil"* må komme tiltalte til gode. Dette er den negative angivelsen av beviskravet.

---

[51] jfr. avsnitt 2.4.1

At rimelig tvil skal komme tiltalte til gode er fulgt opp i en rekke avgjørelser i Høyesterett, blant annet i Rt. 1998 s. 1945 (s. 1947). I dommen uttaler Høyesterett at *"prinsippet om at rimelig tvil skal komme tiltalte til gode er et gammelt grunnleggende rettssikkerhetsideal"*.

Andre formuleringer av beviskravet enn at tiltaltes skyld må bevises utover *"rimelig tvil"* er tatt i bruk av Høyesterett, for eksempel at *"forstandig tvil"* skal komme tiltalte til gode.[52] Dette er ikke ment som en realitetsforskjell, men som en presisering av beviskravet.[53]

Formuleringene *"enhver"*, *"all"* og *"bevist utover"* er flere ganger tatt i bruk foran *"rimelig"* og *"forstandig"* tvil av Høyesterett.[54] Det er ingen grunn til å tro at ordbruken innebærer noen realitetsforskjell.[55]

2.4.4.2 Juridisk teori

I juridisk teori er beviskravet nærmere behandlet og definert. Utgangspunktet er tatt i samme ordlyd som Høyesterett har lagt til grunn, om at rimelig tvil skal komme tiltalte til gode.[56] Bratholm presiserer at enhver teoretisk og filosofisk tvil ikke omfattes.[57] En gjennomgående oppfatning av beviskravet er at dommeren må være sikker, og føle seg overbevist om tiltaltes skyld for å idømme straff.

Et beviskrav kan også utrykkes på andre måter enn semantisk. I juridisk litteratur har det vært drøftet om det kan oppstilles et numerisk beviskrav i straffesaker. I sivilprosessen følger et numerisk beviskrav naturlig etter ordlyden. Det numeriske beviskravet til sannsynlighetsovervekt vil være over 50 % sannsynlighet for å kunne legge faktum til grunn.

---

[52] HR-2008-2063-A pkt. 17.
[53] Rt. 2007 s. 744 (pkt. 24.)
[54] Blant annet i Rt. 2002 s. 599 (604).
[55] Eskeland (2006) s. 510 fotnote 16.
[56] Se Andenæs I (2000) s. 178, Mæland (1999) s. 143, Bratholm (1980) s. 95, Slettan (1997) s. 29.
[57] Bratholm (1980) s. 95.

Etter ordlyden til beviskravet i straffesaker er det ikke så lett å angi dette i prosent, slik som i sivilprosessen. Likevel er det mange i rettsteorien som omtaler beviskravet i prosent.[58] Ut i fra hensynet bak beviskravet i strafferetten om at *"det er bedre at ti skyldige går fri en at en uskylig blir dømt"*, kan man matematisk regne frem til at beviskravet må være 90 %.[59] En slik løsning er en meget forenklet og teoretisk tilnærming av problemstillingen. I juridisk litteratur strekker spredningen av hvilken prosent som skal legges til grunn fra 90 % og opptil 100 %.[60]

Mange forfattere har motforestillinger mot at det angis et presist numerisk beviskrav, blant annet Strandbakken og Andenæs.[61] Begrunnelsen går blant annet i at selv om beviskravet var angitt numerisk, er virkeligheten så sammensatt at man hverken vil kunne tallfeste bevistemaet eller beviskravet. Pedagogisk sett kan et numerisk beviskrav være en *"hjelp for tanken"*.[62]

2.4.4.3 EMDs praksis

Mange av EMDs avgjørelser som berører beviskravet etter EMK. art. 6 nr. 2 inneholder formuleringen "*any doubt should benefit the accused" – "enhver tvil skal komme tiltalte til gode"*.[63] Etter ordlyden vil dette innebære et vesentlig høyere beviskrav etter EMK, enn det beviskravet som er lagt til grunn i Høyesterett og juridisk teori. Det kan etter dette se ut som det er motstrid mellom beviskravet etter norsk rett og EMDs praksis av EMK.

Etter Høyesteretts syn må beviskravet som har kommet til utrykk i EMDs praksis tolkes på tvers av ordlyden; "*enhver tvil"* kan ikke nødvendigvis komme tiltalte til gode.[64] Et beviskrav der "*enhver tvil"* skal komme tiltalte til gode, vil i praksis være meget vanskelig

[58] Strandbakken (2003) s. 367.
[59] ibid. s. 368.
[60] Andenæs I (2000) s. 178 og Strandbakken (2003) s. 368.
[61] Strandbakken (2003) s. 370 og Andenæs I (2000) s. 178.
[62] Strandbakken (2003) s. 370.
[63] Rt. 2007 s.1217 pkt. 64.
[64] I.c.

å oppfylle.[65] Høyesterett mener beviskravet må sees i sammenheng med det mer nyanserte beviskravet som følger av Geerings v. the Netherlands.[66] I dommen oppstilte det et beviskrav med ordlyden *"beyond a reasonable doubt" – "utover rimelig tvil"*. Dette er samme formulering av beviskravet som Høyesterett i en rekke avgjørelser har lagt til grunn etter norsk rett. Etter ordlyden er det grunn til å tro at beviskrav i norsk intern rett oppfyller beviskravet etter EMK, noe rettsteorien også har lagt til grunn.[67]

EMD har forøvrig aldri satt til side et nasjonalt beviskrav.

2.4.5 Kan beviskravet variere etter lovovertredelsens art?

Om beviskravet er det samme ved alle typer straffbare handlinger er en omdiskutert problemstilling i rettslæren. I strafferetten står hensynene til rettsikkerhet og prevensjon/effektivitet sterkt, men vektingen vil variere.[68] Altså vil hensynene gjøre seg gjeldende i forskjellig grad i ulike typer straffesaker. I alvorlige straffesaker, der det potensielle straffeansvaret er høyt, vil hensynet til rettssikkerhet veie tungt, og vektingen i forhold til prevensjonshensynet være tyngre enn det som er tilfelles i mindre alvorlige saker som for eksempel trafikkforseelser. Dette synspunktet er også blitt støttet i rettsteorien.[69]

Det er ikke tvilsomt at *"rimelig tvil"* skal komme tiltalte til gode uansett straffesakens alvorlighetsgrad. Spørsmålet som har blitt reist, spesielt i juridisk litteratur, er om hva som er rimelig tvil skal bero på lovovertredelsens art.[70] Bakgrunnen for at spørsmålet reises, er at de legislative hensyn (rettssikkerhet og prevensjon/effektivitet) som begrunner beviskravet, til en viss grad varierer etter sakens art, jfr. første avsnitt.

---

[65] Andenæs (2000) s. 178.
[66] EMD-2003-30810.
[67] Eskeland (2006) s. 101.
[68] ibid. s. 509.
[69] Andenæs I (2000) s. 178.
[70] Andenæs I (2000) s. 178 og Hov I (2007) s. 362.

Høyesterett har ikke tatt stilling til spørsmålet. Flere juridiske forfattere, blant annet Andenæs og Hov, mener at det i praksis eksisterer en variasjon av beviskravet etter sakens art.[71] Det har også blitt hevdet at på de områder der det er vanskelig å innhente bevis, må beviskravet lempes. Det har blant annet blitt hevdet fra påtalemyndighetens side at ved økonomisk kriminalitet bør beviskravet lempes.[72]

2.5 Bevisbedømmelsen

Bevisbedømmelse er en psykologisk prosess der dommeren skal ta stilling til hvilket faktum som skal legges til grunn.[73] Formålet med bevisbedømmelsen er å vurdere hvor sannsynlig et faktum er ut i fra de bevismidler man har til rådighet. Det er på bakgrunn av en bevisbedømmelse at rettsanvenderen kan slå fast om beviskravet er oppfylt eller ikke.

Bevisbedømmelsen er fri i begge prosessformene. I sivilprosessen er dette utrykkelig slått fast i tvl. § 21-2 (1). I lov 1. juli 1887 om Rettergangsmaaden i Straffesager (strpl. av 1887) § 349 andre punktum ble det utrykkelig slått fast at bevisbedømmelsen var fri. Når den nye strpl. av 1981 skulle vedtas ble bestemmelsen om fri bevisbedømmelse ikke tatt med. Det kom da til uttrykk i forarbeidene til loven at prinsippet var så grunnleggende at noen lovfesting ble vurdert som unødvendig.[74]

Hensynet til at bevisvurderingen skal være fri, er at retten på den måten best vil finne sannheten om faktum i saken.[75]

Bevisbedømmelsen var tidligere legal, og ikke fri. I NL 1-13-1 var det lovfestet at hvis to uavhengige vitnesbyrd var i samsvar med hverandre, skulle retten legge det faktum til grunn.

---

[71] Andenæs I (2000) s. 178 og Hov I (2007) s. 362.
[72] Hov I (2007) s. 363.
[73] Strandbakken (2005) s. 59.
[74] Instillingen (1969) s. 197 første spalte og s. 308 andre spalte.
[75] Andenæs I (1994) s. 166-167.

Selv om retten står fri til å vurdere bevisene i saken, forutsettes det at bevisvurderingen gjøres ut i fra rasjonelle standpunkter. Som det fulgte av strpl. av 1887 § 349 annet punktum at bevisvurderingen skulle gjøres på *"en samvittighetsfull prøvelse av de fremførte bevisligheter"*. Det må også kunne sies at det følger av uskyldspresumsjonen at tiltalte må være vernet fra vilkårlig bevisbedømmelse, jfr. EMK art 6.[76]

3 IP-adresse som bevismiddel

IP-adresse er, sammenlignet med andre bevis, et nytt og sjeldent anvendt bevismiddel i konkrete straffesaker.[77]

I det følgende vil jeg drøfte en rekke spørsmål knyttet til IP-adresse som bevismiddel i straffesaker. Det ble under problemstilling, i avsnitt 1.3, oppstilt fire kriterier for vurderingen av om et bevismiddel er godt. I denne delen vil jeg gå nærmere inn på de to mest sentrale kriteriene: *"tilgjengelighet"* og "*overbevisning"*.

Bevismiddels tilgjengelighet kan begrenses av praktiske, økonomiske og juridiske hindringer. Etter oppgavens art, vil de juridiske bli særskilt nøye behandlet. I forhold til kriteriet om overbevisning, kreves det at det gjøres en bevisvurdering. Målet med bevisvurderingen er å drøfte hva, nøyaktig, IP-adresse kan kaste lys over i straffesaker, og vurdere med hvilken sikkerhet IP-adresse utpeker gjerningspersonen.

En forutsetning for drøftelsen er at leseren har grunnleggende kjennskap til hva en IP-adresse er, og dette vil jeg derfor kort gjøre rede for, i lys av de juridiske spørsmål som skal besvares.

---

[76] Strandbakken (2003) s. 213.
[77] Den eldste dom der IP-adresse er omtalt i lovdata er fra 1998, se LH-1998-892. Totalt 12 dommer er publisert i lovdata.no der IP-adresse er ført som bevis (per april 2009).

3.1 Bakgrunn

3.1.1 Hva er en IP-adresse?

En IP-adresse er en numerisk adressekode som elektroniske enheter bruker for entydig adressere kommunikasjonen dem imellom via Internett. Alle enheter som er knyttet til Internett må ha en IP-adresse, og all data som sendes over Internett må være adressert til en sådan.[78] IP-adressen er unik for hver enhet som er knyttet til Internett. Dette er helt essensielt for at strømmen av informasjon skal komme frem utelukkende til rett enhet.

En IP-adresse består av en tallkombinasjon på inntil tolv tall, delt inn i fire deler. Eksempelvis har hjemmesiden til VG, www.vg.no denne IP-adressen: 193.69.165.21. Alle IP-adresser som er tilknyttet Internett må nødvendigvis være unike, og under dagens IP-adresse system ligger kapasiteten på over 4 milliarder mulige adresser.[79]

Selv om Internett er basert på bruken av IP-adresser, er det uvanlig at brukere av Internett selv benytter seg av IP-adressen i kommunikasjonen. IP-adressen til en konkret nettside kan også brukes for å få tilgang til siden. For å komme inn på siden www.vg.no, kan man i stedet taste in IP-adressen 193.69.165.21 i adressefeltet på internettleseren.

Grunnen til at man til daglig ikke trenger å hverken huske eller taste inn IP-koden, er at programvarer som kommuniserer via Internett *"omformulerer"* konvensjonelle internettadresser eller linker til IP-adresser. Når en bruker besøker et nettsted og taster inn domenenavnet til nettsiden, oversettes domenenavnet til en IP-adresse av en DNS-server (Domaine Name System).[80]

Vanlige enheter som kommuniserer over Internett er datamaskiner, servere, routere, og siden for nylig, mobiltelefoner.

---

[78] Teknologirådet (2005) s. 47.
[79] Sunde (2000) pkt. 4.1. En ny versjon av IP-adresser er under oppseiling, slik at kapasiteten øker ytterligere, jfr. http://no.wikipedia.org/wiki/IP-adresse [sitert 20.04.2009]
[80] NOU 2007:2 Del II s. 34 (pkt. 3.5.13)

3.1.2 Hvilken informasjon kan IP-adresse gi?

IP-adresse kan gi informasjon om hvem som har foretatt seg en handling via Internett. Den vil kunne brukes som bevis i forhold til om tiltalte har begått handlingen eller ikke, det vil si om tiltalte har overtrådt den objektive gjerningsbeskrivelse i straffebudet.

En IP-adresse gir informasjon om hvilken enhet som har vært del i en kommunikasjon på samme måte som et telefonnummer angir hvilket abonnement det ringes fra. Når en enhet kobler seg til en internettside, vil IP-adressen som loggføres indikere hvilken enhet som har vært inne på siden.

IP-adressen vil etter dette gi informasjon om hvilke enheter som har kommunisert og til hvilken tid. Siden all kommunikasjon over Internett foregår via IP-adresser, kan som utgangspunkt alle praktiske handlinger spores. Det må presiseres at det er ikke all kommunikasjon over Internett som blir loggført. Det kan være tilfeller der loggføring bevisst ikke skjer, med hensyn til personvern eller kriminalitet. Generelt lagres IP-adresse ved sending av e-post og på servere som driver internettsider.[81]

Det som er viktig og essensielt for besvarelsen av oppgavens problemstilling er at IP-adresse ikke direkte gir informasjon om hvem som er brukeren bak handlingen. IP-adressen identifiserer kun enheten som er brukt i kommunikasjonen, på samme måte som elektroniske spor av et mobiltelefonnummer kun identifiserer abonnenten og ikke personen som ringer.[82]

[81] Teknologirådet (2005) s. 49.
[82] Se også bemerkninger i NOU 2009:1 pkt. 4.5.3.2 på s. 47.

Fordi IP-adressen identifiserer den enheten som har kommunisert via nettet, kan IP-adressen gi geografisk informasjon om hvor handlingen er blitt utført. Slik informasjon betegnes som lokasjonsdata.[83]

Et elektronisk spor fra IP-adresse tidfestes, på den måten kan IP-adressen gi informasjon om når kommunikasjonen fant sted. Dette har sentral betydning i forhold til identifisering av adressen, og dermed bevisets verdi, noe jeg vil komme tilbake til senere i oppgaven.[84]

3.1.3 IP-adresse i rettspraksis – typetilfellene

IP-adresse som bevismiddel er, som nevnt innledningsvis, primært aktuelt ved kriminalitet foretatt via Internett. En gjennomgang av rettspraksis viser at det er en bestemte typer straffesaker der IP-adresse føres som bevis.[85] Drøftelsen her vil kun ta utgangspunkt i de typetilfeller som omhandler IP-adresse som nevnt nedenfor. Her er IP-adressen knyttet til handlinger foretatt via en datamaskin.

IP-adresse er ført som bevis i flere saker som gjelder hacking eller datainnbrudd, jfr. lov 22.mai 1902 nr. 10, Almindelig borgerlig Straffelov (strl.) § 145 annet ledd. Bestemmelsen annet ledd retter seg mot den som *"uberettiget skaffer seg adgang til data"*.[86]

Et stort problem for film og musikkbransjen er den omfattende fildelingen som foregår over Internett. IP-adresse er derved relevant som bevismiddel i flere saker som omhandler brudd på åndsverkloven.[87] Deling av materiale som dekkes av strl. § 204a (barnepornografi) er også typiske straffesaker der IP-adresse er bevismiddel.[88]

---

[83] Teknologirådet (2005) s. 11.
[84] Se avsnitt 3.3.
[85] Gjennomgangen av rettspraksis er basert på de dommer som er tilgjengelige i lovdata.
[86] Blant annet i TSTVG-2002-634, LA-2003-83 og LB-1997-1527.
[87] Lov 12. mai 1961 nr. 2 om opphavsrett til åndsverk m.v." (åvl.)
[88] Blant annet TOSLO-2004-94328 (ulovlig fildeling etter åndsverkloven) og LG-2008-150465 (barnepornografi).

I rettspraksis har IP-adresse også blitt ført som bevis i bedragerisaker (strl.§ 270) og sosial trakassering (strl.§ 390a).[89]

3.2 Etterforskningssituasjonen – innhenting av IP-adresse

Bevismiddels tilgjengelighet kan som nevnt begrenses både juridisk, praktisk og økonomisk. Etter oppgavens problemstilling og tema er det ikke naturlig at det gås i dybden på hvordan IP-adresse teknisk innhentes og på hvordan etterforskningssituasjonen foregår. En kort innføring i hvordan beviset kan innhentes anses likevel nødvendig for vurderingen av tilgjengelighetskriteriet. Vurderingen her er tilknyttet etterforskningsstadiet.

3.2.1 Anmeldelse fra fornærmede

Etterforskning av internettkriminalitet åpnes normalt på bakgrunn av anmeldelse av det straffbare forhold.[90] Anmeldelse vil også som regel komme fra den fornærmede i saken, som vanligvis besitter den datamaskin som har vært en del av kommunikasjonen. Fordi fornærmedes datamaskin har vært en del av kommunikasjonen, vil vanligvis IP-adressen til den enhet som noen har foretatt den straffbare handling ved hjelp av, ligge registrert på denne maskinen. En e-post med anonym adresse vil normalt inneholde avsenders IP-adresse,[91] og IP-adressen til den enhet som noen begikk datainnbruddet ved hjelp av vil også normalt kunne innhentes.[92]

Utgangspunktet for innhenting av IP-adresse er at det er et inngrep i borgerens sfære og derav må ha hjemmel i lov, jfr. legalitetsprinsippet.[93] I de tilfeller der fornærmede eller andre som besitter IP-adressen frivillig utleverer informasjonen, kreves ikke hjemmel i lov.

---

[89] Blant annet TOSLO-2004-41422 (strl. § 390a) og TSTVG-2005-62640 (strl. § 270).
[90] Sunde (2000) pkt. 4.2.
[91] Teknologirådet (2005) s. 49.
[92] Slik tilfelle var i LA-2003-83.
[93] Legalitetsprinsippet er nærmere drøftet i avsnitt 3.2.3 nedenfor.

Fornærmede vil i utgangspunktet ønske å bistå i etterforskningen. Den såkalte *tilgjengeligheten* er i disse tilfeller å vurdere som god.

3.2.2 Politiet – og publikums rolle

I forbindelse med mange typer lovbrudd som begås via Internett, er fornærmede ikke en del av kommunikasjonen. Fornærmede er indirekte berørt, men er i mange tilfeller ikke klar over det straffbare forhold. Et eksempel på dette kan være rette opphavsmanns rolle i forbindelse med ulovlig fildeling. I tilfeller som dette besitter fornærmede ikke IP-adressen til enheten som er knyttet til det kriminelle forholdet, og IP-adressens tilgjengelighet er følgelig liten. Mulighetene for at forholdet blir oppdaget og rett person tiltalt og dømt er tilsvarende små.

Der fornærmede ikke er en del av kommunikasjonen, er det i hovedsak to *"veier"* som fører til at politiet oppdager forholdet og kan innhente IP-adresse. Det kan skje gjennom etterforskning og tips fra publikum.

En utbredt etterforskningsmetode av Internettkriminalitet, består i at etterforskere infiltrerer nettverk på Internett. Et slikt nettverk kan infiltreres ved at vedkommende kobler seg til IRC, en prate – eller samtalelinje, der medlemmene kommuniserer via Internett. Forholdet kan da både oppdages og IP-adresse innhentes hvis kommunikasjonen har skjedd direkte med infiltratoren.[94] Det kan tenkes at infiltratoren har opparbeidet et slikt tillitsforhold at han får tilbudt ulovlig materiale. Etterforskning som foregår på denne måten er meget ressurskrevende, og politiet er derved avhengig av publikum for å i større grad kunne bekjempe internettkriminalitet.[95] I tilfelle der publikum for eksempel blir tilbudt barnepornografi kan en enkeltperson og interesseorganisasjoner være behjelpelige ved å bringe nødvendig informasjon til politiet. Et enkelt tips om lovbrudd fra en tredjepart som

[94] Slik som tilfelle var i Rt. 1999 s. 1944 andre avsnitt.
[95] Kripos (2003) s. 13.

ikke er direkte del av kommunikasjonen, kan også være nyttig. Politiet kan da sette i gang nødvendig etterforskning slik at IP-adresse blir innhentet.

3.2.3 Ufrivillig utlevering av IP-adresse

Ufrivillig utlevering av IP-adresse utgjør et inngrep i borgernes sfære. Myndighetens inngrep i borgernes rettsfære trenger hjemmel i lov, jfr. legalitetsprinsippet. Legalitetsprinsippet er i sin generelle form ikke lovfestet, men flere sider av prinsippet er det.[96] Ved inngrep i borgernes sfære og personlige integritet følger prinsippet nå av EMK art. 8, jfr. nærmere nedenfor i pkt. 3.4.

Bruk av beslag og utleveringspålegg er nødvendig for at påtalemyndigheten og retten skal kunne innhente IP-adresse der besitteren ikke frivillig vil utlevere. IP-adresse lagres elektronisk, slik at de mest aktuelle gjenstandene for belag er elektroniske enheter som datamaskin og router.

En generell behandling av vilkårene for beslag og utleveringspålegg vil gå utenfor denne oppgavens rammer. Jeg vil her kun drøfte spørsmål knyttet til de spesielle spørsmål som knytter seg til IP-adresse, og de momenter som har betydning for vurderingen av tilgjengeligheten.

Hjemmelen for utlevering og beslag etter strpl. kap. 16 er av generell karakter.[97] Reglene skiller ikke mellom hvem eventuelt beslag eller utleveringspålegg retter seg mot, eller hvor alvorlig det straffbare forhold som er under etterforskning er.

Hva som kan være gjenstand for beslag fremgår av strpl. § 203. Etter bestemmelsen er det *"ting"* som *"antas"* å ha betydning som bevis som kan beslaglegges, inntil rettskraftig

[96] Lagt til grunn i NOU 2004:6 pkt 5.2.1.
[97] Rt. 1992 s. 904 (906)

dom foreligger. Etter Høyesterettspraksis er det blitt fastsatt at *"antas"* innebærer et krav om rimelig mulighet.[98]

Etter en naturlig tolkning av ordet *"ting"* er det ikke åpenbart om IP-adresse omfattes. Problemstillingen om hvorvidt elektronisk lagret data er *"ting"* kom opp i Rt. 1992 s. 904 (906). Der uttalte Høyesterett at:

"[ting] omfatter ikke bare legemlige gjenstander, men også opplysninger som lagres på data og som i tilfelle må gjøres tilgjengelig ved utskrifter."

Avgjørelsen ble fulgt opp i en Høyesterettsdom senere samme år i Rt. 1992 s. 928 (929) og Rt. 1997 s. 470 (471). IP-adressen lagres elektronisk og må klart omfattes av opplysninger som lagres på data.

Kompetansen til å beslutte beslag følger av strpl. § 205. Etter bestemmelsen kan en beslutning om beslag av *"ting"* som besitteren ikke vil utlevere frivillig besluttes av påtalemyndighetene. Dette fører til at påtalemyndigheten kan handle raskere enn der kjennelse fra retten er påkrevd.

Utleveringspålegg gis der påtalemyndigheten ikke vet hvor gjenstanden befinner seg, men bare hvem som er besitteren.[99] Utgangspunktet ved utleveringspålegg etter strpl. § 210 er at retten, ved kjennelse, kan gi slikt pålegg. Når det er fare for at *"etterforskningen vil lide"* ved opphold, kan beslutning av påtalemyndighetene tre i stedet for kjennelse fra retten, jfr. strpl. § 210 annet ledd.

[98] Rt. 1998 s. 1839, Rt. 1999 s. 1115 og Rt. 1999 s. 2063.
[99] Andenæs II (2000) s. 196.

Hva som er gjenstand for utleveringspålegg fremgår av § 210 første ledd. Der brukes *"ting"*, som er samme formulering som i § 203. Dette må forstås på samme måte som ved beslag.[100]

At bevis innhentes raskt er ofte viktig for oppklaring av det straffbare forhold. Tilgjengeligheten til IP-adresse er bedre der beslutning om innhenting kan skje av påtalemyndighetene uten å måtte innhente kjennelse fra retten.

3.3 Identifisering av IP-adressen – rettslig hjemmel

3.3.1 Bakgrunn

En IP-adresse har i seg selv liten verdi for etterforskningen og som overbevisningsgrunnlag i retten. En IP-adresses bevisverdi realiseres først når den knyttes til en enhet eller bruker. Identifiseringsprosessen inneholder en rekke hindringer, som igjen innskrenker bevismiddelets tilgjengelighet. Det er derfor av sentral betydning for oppgaven at disse rettslige hindringer blir drøftet.

Reglene om identifisering av IP-adresse bygger på lovgivers avveining mellom hensynet til privatlivet og en effektiv rettshåndhevelse.[101] Denne avveiningen treffer selve kjernen i vurderingen av oppgavens problemstilling, en vurdering som jeg vil jeg komme tilbake til i kapittel 4.

Identifikasjon av IP-adresse er i konflikt med hensynet til personvern. Det er et grunnleggende prinsipp i en rettsstat at borgerne har rett til fred i privatlivet. En identifikasjon av IP-adresse i strafferettslig henseende kan krenke denne retten. Prinsippet om privatlivets fred er nedfelt i EMK. art 8 nr.1, og gitt forrang norsk formell lov, jfr. avsnitt 2.4.1. Det er dermed potensielt motstrid mellom EMK og norsk lovgivning.

---

[100] Bjerke I (2001) s. 724.
[101] Rt. 1999 s. 1944 (1949).

3.3.2 Tilbyderens rolle

Når IP-adresse er innhentet må adressen knyttes til en tilbyder for den videre prosess med å identifisere brukerkontoen. Tilbyder er den som videreformidler Internett til brukere. Søkemotorer for slik sporing er allment tilgjengelige på Internett.[102]

Flere sider av tilbydernes rettsforhold berøres i lov 7. juli 2003 nr. 85 om elektronisk kommunikasjon (e-koml.), jfr. § 1-2 første punktum. Tilbyder defineres i e-koml. § 1-5 nr. 14 som *"enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller – tjeneste"*. Tilbyderen formidler internettilgang til sluttbrukeren, som defineres som den som bruker Internett til eget formål, jfr. e-koml. § 1-5 nr. 13.[103]

Ved opprettelse av et kundeforhold mellom brukeren og tilbyderen, oppgis det kundeopplysninger som knyttes til det som kalles brukerkonto. Slik informasjon gis på bakgrunn av faktureringsformål og inneholder typisk personalia.

Tilbyderne har et begrenset antall IP-adresser til rådighet. Av de IP-adresser som gis ut til kundene, skilles det mellom statiske og dynamiske adresser. Statisk IP-adresse er der sluttbrukeren bruker samme IP-adresse for hver tilkobling. Dette er vanlig for større bedrifter og institusjoner. Dynamiske IP-adresser er der sluttbrukeren får ny IP-adresse for hver oppkobling eller ved jevne mellomrom.[104] Dette er vanlig for private brukere. For at brukeren til en dynamisk IP-adresse skal kunne identifiseres, er påtalemyndighet avhengig av at slik informasjon er lagres hos tilbyder.

På bakgrunn av at tilbyder formidler kommunikasjon loggføres informasjon knyttet til kommunikasjonen. I bransjen er det variasjon med hensyn til hvilke data og hvor lenge data loggføres. I relasjon til IP-adresse og internettbruk lagres informasjon om hvilke IP-adresser som er disponert av brukerne til gitte tider og hvor lenge bruken varte. Også

---

[102] Se for eksempel www.whois.net [tilgjengelig den 20.03.2009]
[103] Heretter også betegnet som bruker.
[104] Teknologirådet (2005) s. 47.

informasjon knyttet til hvilke IP-adresser brukeren har kommunisert med lagres.[105] Det betyr at man kun trenger å knytte mottakers IP-adresse til en enhet for å vite hvem enhet brukerkontoen[106] kommuniserte med.

I e-koml. og ekomforskriften[107] er det ingen hjemmel for at tilbyderne har noen plikt til å lagre data om sluttbrukeres IP-adresser, selv om slik data vil være av stor interesse for en etterforskning av internettkriminalitet. Av personvernhensyn finnes det begrensninger i lov og forskrift om hvor lenge slik informasjon kan lagres og hvordan opplysningene skal behandles. I forhold til IP-adressens tilgjengelighet er tidselementet her spesielt viktig i etterforskningsøyemed. For at en dynamisk IP-adresse skal kunne identifiseres til rett bruker, må tilbyder ha lagret informasjon på det aktuelle tidspunktet.

Tilbyders sletteplikt følger av e-koml. § 2-7 annet ledd. Bestemmelsen pålegger tilbyder en plikt til å slette trafikkdata. Trafikkdata er ikke definert i loven, men det følger av forarbeidene at trafikkdata er *"data som er nødvendig for overføring av kommunikasjon i et elektrisk kommunikasjonsnett eller for fakturering av slik overføring."*[108] Slik data omfatter hvilken IP-adresse en brukerkonto har benyttet, til hvilken tid, hvor lenge og hvem IP-adresser brukeren har kommunisert med.

Etter e-koml. § 2-7 annet ledd plikter tilbyder å slette eller anonymisere trafikkdata *"så snart de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål"*. At opplysningene skal slettes eller anonymiseres volder ikke store tolkningsproblemer. Informasjonen skal enten fjernes, eller anonymiseres slik at alle entydige kjennetegn som kan identifisere brukeren fjernes.

---

[105] Teknologirådet (2005) s. 47.
[106] Brukerkonto er videre i oppgaven også brukt synonymt med abonnement.
[107] Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste av 16. feb. 2004. (ekomforskriften)
[108] Ot.prp.nr. 58 (2002-2003) s. 92.

Skjæringstidspunktet for plikten til å slette dataene er når de ikke lenger er nødvendig for faktureringsformål. Etter en naturlig tolkning av ordlyden må trafikkdata slettes i det betaling har funnet sted.[109] Skjæringspunktet for sletteplikten vil etter dette være avhengig av hyppigheten på tilbyders fakturering.[110]

Lagring av trafikkdata må sees i sammenheng med forskrift om behandling av personopplysninger[111] § 7-1. Bestemmelsen gjør det konsesjonspliktig etter personopplysningsloven å behandle *"personopplysninger for kundeadministrasjon, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett"*. En sletteplikt følger også av popplyl. § 28, og etter datatilsynet konsesjonspraksis skal trafikkdata slettes etter 3 til 5 måneder. Det foreligger altså en dobbelt hjemmel for sletteplikt av trafikkdata. Likevel viser praksis at rutinene for å slette eller anonymisere slike data kan svikte. Politiet har i enkelte tilfeller kunnet innhente slike data som er eldre enn 5 måneder.[112]

Det kan få uheldige konsekvenser for etterforskningen at lagring av data knyttet til IP-adresse kun kan lagres for faktureringsformål. Det kan tenkes at nye abonnementstyper oppstår der lagring ikke er nødvendig for faktureringsformål. Dette kan skje ved at kunden betaler forskuddsvis og ikke etter faktisk bruk. Da vil enhver lagring etter e-koml. § 2-7 være lovstridig og brukeren vil opptre helt anonymt på Internett.

Ved identifisering av en dynamisk IP-adresse har tilbyderne en avgjørende rolle. Tilbyder har eksklusiv informasjon som identifiserer brukerkontoen bak IP-adressen.[113] I forhold til tilgjengeligheten er politiet avhengig av at tilbyder har lagret trafikkdata, og at det ikke har gått for lang tid før tilbyders sletteplikt inntreffer. Politiet må dermed oppdage den straffbare handlingen og handle raskt for at ikke essensiell informasjon skal gå tapt.

---

[109] Ot.prp.nr. 58 (2002-2003) s. 92.
[110] Ved omtvistet faktura kan data lagres inntil betaling har funnet sted, men ikke utover den tid kravet kan kreves inn, for eksempel etter at kravet er foreldet. Det går frem i Ot.prp.nr. 58 (2002-2003) s. 92.
[111] Forskrift om behandling av personopplysninger 15 des. 2000 nr. 1265
[112] Høgtveit (2008) s. 332
[113] NOU 2009:1 s. 283.

Tidselementet har vist seg å være avgjørende i praksis for at identiteten til brukerkontoen ikke har blitt identifisert.[114]

En statisk IP-adresse kan spores direkte til en bruker via tilgjengelige søkemotorer på Internett.[115] Tilbyders medvirkning er ikke alltid nødvendig i slike tilfeller.

3.3.3 Tilbyders taushetsplikten knyttet til IP-adresse

Det påhviler taushetsplikt for tilbydere for informasjon tilknyttet IP-adresse. Dette følger av e-koml. § 2-9 første ledd. Etter bestemmelsens første ledd omfattes *"innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon"*[116] av taushetsplikten.

Taushetsplikten retter seg for det første mot *"innhold av elektronisk kommunikasjon"*. Det betyr at blant annet innholdet i SMS, telefonsamtaler og e-post omfattes. I forhold til IP-adresse er ikke dette relevant og vil ikke bli nærmere behandlet.

Videre omfattes også informasjon om *"andres bruk av elektronisk kommunikasjon"*. I det ligger det at trafikkdata anses som en del av det taushetsbelagte materialet. Etter e-koml. § 2-9 fjerde ledd kan *"myndigheten"* gi nærmere forskrifter om taushetsplikten.[117] At trafikkdata er taushetsbelagt følger nå også eksplisitt etter ekomforskriften § 7-1 gitt med hjemmel i § 2-9 fjerde ledd. Dermed vil informasjon knyttet til en brukers aktivitet på Internett være taushetsbelagt. Nærmere bestemt vil det si opplysninger om tidspunkt for av og pålogging og hvilke IP-adresser som brukeren har benyttet. Det samme gjelder også for opplysninger om når en e-post er blitt sendt og mottatt, samt hvilke IP-adresser kommunikasjonen kan knyttes til.

---

[114] Willassen (2009) og Høgtveit (2008) s. 333
[115] Teknologirådet (2005) s. 49.
[116] Se e-koml. § 1-5 nr. 1.
[117] Samferdselsdepartementet er "myndighet" etter bestemmelsen, jf. forskrift 4. juli 2003 nr. 881, I nr. 1.

Taushetsplikten er ikke til hinder når samtykke fra rette vedkommende er innhentet. Det følger direkte av lovens forarbeider.[118]

3.3.4 Fritak fra taushetsplikten etter ekomloven

Personvernet etter e-koml. § 2-9 første ledd er ikke ubeskåret. Etter e-koml. § 2-9 tredje ledd kan visse opplysninger unntas fra taushetsplikten. Etter bestemmelsen er det *"påtalemyndigheten eller politiet"* som kan få utlevert slik informasjon. Videre følger det at det samme gjelder for vitnemål for retten, jfr. bestemmelsens tredje ledd annet punktum.

I tredje ledd siste punktum kan også andre myndigheter enn påtalemyndigheten få utlevert taushetsbelagt informasjon når det fremgår av lov. Bestemmelsen ble inntatt for at det ikke skulle være motstrid mellom bestemmelsen og det øvrige lovverket.[119]

Etter ordlyden i § 2-9 tredje ledd kan opplysninger unntas fra taushetsplikten som gjelder:

"avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse".

I tillegg til at tilbyder kan utlevere informasjon om avtalebasert hemmelig telefonnummer, kan tilbyder oppgi *"andre abonnementsopplysninger"*. Slike opplysninger vil etter en naturlig forståelse av begrepet innebære personalia knyttet til et abonnement.

Videre følger det at unntak fra taushetsplikten omfatter *"elektronisk kommunikasjonsadresse"*. Rekkevidden av begrepet er nærmere omtalt i forarbeidene.[120] Der presiseres det at informasjon om *"navn, adresse og telefonnummer tilknyttet en*

[118] Ot.prp.nr. 58 (2002-2003) s. 93.
[119] Se for eksempel tvl. § 7-12 som hjemler utlevering av abonnementsopplysninger som er omhandlet i tredje ledd.
[120] Ot.prp.nr. 58 (2002-2003) s. 93.

elektronisk kommunikasjonsadresse" kan oppgis til påtalemyndighet og politi. At en statisk/fast IP-adresse omfattes av elektronisk kommunikasjonsadresse anses som klart.[121]

Hvorvidt en dynamisk IP-adresse omfattes av begrepet må etter forarbeidene sees på bakgrunn av Rt. 1999 s. 1944. Dommen gjelder den nå opphevede lov 23. juni 1995 nr. 39 om telekommunikasjon (teleloven) § 9-3 tredje ledd. Det fremgår imidlertid eksplisitt av forarbeidene at e-koml. § 2-9 er en *"videreføring av bestemmelsene i teleloven om taushetsplikt"*.[122]

I Rt. 1999 s. 1944 fremgikk det av Høyesterett at begrepet omfatter både personalia og telefonnummer tilhørende innehaver av en dynamisk IP-adresse.[123] En begrensning for unntak av taushetsplikten er at påtalemyndigheten kan angi et konkret oppkoblingstidspunkt. Høyesterett begrunner begrensningen med at ved politiets angivelse av et konkret tidspunktet for oppkoblingen gir dette en *"entydig anvisning på abonnentforholdet"*. På den måten blir det sikrere at rett abonnent, og bare den, blir identifisert. Høyesterett sin forståelse av daværende ordlyd i telelov. § 9-3 tredje ledd, datakommunikasjonsadresse, skal forstås på tilsvarende måte som e-koml. § 2-9 tredje ledd, elektronisk kommunikasjonsadresse.[124]

Etter ordlyden i e-koml. § 2-9 oppstilles det ikke noe krav til at opplysningene skal gjelde i forbindelse med etterforskning eller straffesak. Etter e-koml. § 2-9 fjerde ledd kan opplysninger som unntas taushetsplikten etter tredje ledd likevel ikke gis hvis *"særlige forhold gjør det utilrådelig"*. I forarbeidene trekkes det frem at vilkåret etter fjerde ledd kan være oppfylt når opplysningene ikke gjelder i forbindelse med en etterforskning.[125]

---

[121] Rt. 1999 s. 1944 (1947)
[122] Ot.prp.nr. 58 (2002-2003) s. 93.
[123] Rt. 1999 s. 1944 (1950-1952)
[124] Rønnevig (2009) note 42.
[125] Ot.prp.nr. 31 (1997-1998) s. 8.

Regelverket i e-koml. hjemler imidlertid ikke tilbyder noen plikt til å utlevere informasjon som er fritatt etter § 2-9 tredje ledd. Slik hjemmel må søkes i det øvrige lovverket. Mest aktuelt her er straffeprosesslovens bestemmelser, spesielt om beslag (strpl. § 203) og utleveringspålegg (strpl. § 210) i straffeprosesslovens kap. 16, jfr. ovenfor i pkt. 3.2.3.

3.3.5 Fritak fra taushetsplikten etter vedtak av Post – og teletilsynet

Informasjon knyttet til IP-adresse som ikke omfattes av unntaket i e-koml. § 2-9 tredje ledd, vil likevel på visse vilkår kunne utleveres av tilbyder. Informasjon som ikke kan leveres ut etter § 2-9 tredje ledd er trafikkdata. Trafikkdata omfatter hvilke IP-adresser brukeren har kommunisert med, til hvilken tid og hvor lenge. Utlevering av IP-adresse der politiet ikke har et konkret oppkoblingstidspunkt, men vil vite hvilke IP-adresser en brukerkonto har benyttet i en periode omfattes også.

Trafikkdata anses som mer sensitiv og omfattende informasjon enn den som omfattes av e-koml. § 2-9 tredje ledd. Av hensyn til personvern kreves en mer betryggende saksbehandling for at taushetsplikten kan settes til side.

Utgangspunktet er at *"enhver"* plikter å forklare seg for retten, men unntak av hva som følger av lov, jfr. strpl. § 108. Etter strpl. § 118 første ledd kan retten ikke *"uten samtykke fra departementet"* ta imot forklaring fra vitne som krenker lovbestemt taushetsplikt. I andre punktum går det eksplisitt frem at dette gjelder for *"tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste"*. Samtykke fra departementet er nødvendig hvis informasjon som faller innenfor strpl. § 118 skal frigis. Slik myndighet til å vurdere fritak er delegert fra Samferdselsdepartementet til Post- og teletilsynet (PT).[126]

[126] Delegasjonsvedtak av 15. september 1995 nr 39.

Hovedregelen er at så lenge departementet ikke har gitt samtykke, kan verken retten eller politiet få tilgang til opplysningene uten at tilbyder bryter taushetsplikten etter strpl. § 118.[127]

Etter strpl. § 108 er det oppstilt et ulovfestet konkretiseringskrav av det straffbare forhold. Det innebærer at *"forklaringen skal gjelde bestemte forhold som er under strafferettslig forfølgning"*.[128] Det er imidlertid ikke noe vilkår at en bestemt person er siktet eller mistenkt.[129] Konkretiseringskravet for vitneplikten gjelder også i forhold til taushetsbelagte opplysninger som har blitt gitt fritak etter strpl. § 118. Det har i praksis vært oppstilt varierende krav til hvor nøyaktig det straffbare forhold må konkretiseres.[130] Konkretiseringskravet innebærer at PT ikke kan gi fritak fra taushetsplikten der det ikke er satt i gang etterforskning av et straffbart forhold.

Vitneplikten etter strpl. § 108 gjelder kun overfor retten. I forhold til forklaring ovenfor politiet, er hovedregelen at ingen plikter å forklare seg, jfr. strpl. § 230 første ledd. Frivillig forklaring kan derimot finne sted, hvis ikke taushetsplikt er til hinder for det. Etter strpl. § 230 fjerde ledd gjelder reglene i strpl. § 118 første og andre ledd tilsvarende. Det betyr at tilsynet kan frita tilbyder for taushetsplikten etter de samme regler som gjelder for strpl. § 118.

Vurderingstemaet om fritak skal nektes av PT følger av strpl. § 118 første ledd siste punktum. Slikt samtykke skal bare nektes hvis opplysningene utsetter *"staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold"*. PT foretar en rimelighetsvurdering mellom de nevnte hensyn. Rimelighetsvurderingen er tilsvarende den i strpl. § 170a.[131]

---

[127] Hustad (2009) note 716.
[128] ibid. note 647.
[129] Bjerke (2001) s. 447-448.
[130] Hustad (2009) note 647.
[131] PT (2008)

En slik vurdering innbærer en helhetsvurdering av en rekke momenter. Et viktig moment er alvorlighetsgraden det straffbare forhold dreier seg om. Et annet moment er hva som kan oppnås ved å frita for taushetsplikten. Er det gode muligheter for at et fritak vil kunne føre til oppklaring i saken, taler det for at tilsynet opphever taushetsplikten. Det er også et moment hvilke skadevirkninger et eventuelt fritak av taushetsplikten vil kunne ha for den som fritaket går ut over.[132]

Spørsmålet som melder seg her er om det tilhørende konkretiseringskravet etter strpl. § 108 gjelder tilsvarende for frivillig forklaring ovenfor politi. I forhold til det spørsmålet har meningene vært delte. PT har uttalt at konkretiseringskravet må gjelde fullt ut, slik at tilsynet kun kan gi fritak fra taushetsplikten der det straffbare forholdet har blitt konkretisert.[133] Lovutvalget har tatt det motsatte standpunktet i forståelsen av sammenhengen mellom strpl. §§ 230, 118 og 108. De legger til grunn at:

"Lovavdelingen kan ikke se at denne henvisningen til straffeprosessloven § 118 innebærer at hovedregelen om vitneplikt etter straffprosessloven § 108, og dermed det tilhørende konkretiseringskravet, gjelder fullt ut også ved forklaringer til politiet, slik Post- og teletilsynet legger til grunn."[134]

Hva som ligger i at konkretiseringskravet ikke kan gjelde *"fullt ut"* fremgår ikke som klart. Lovutvalget påpeker at hensynene er annerledes ved forklaring for politiet sammenlignet med retten. Politiforklaringer avgis på et tidlig stadium, for å avgjøre om det i det hele tatt er grunnlag for videre etterforskning. Et konkretiseringskrav av det straffbare forholdet vil vanskeliggjøre politiets arbeid. Dette gjør seg ekstra sterkt gjeldene der saken innehar et hasteelement. På bakgrunn av begrunnelsen kan det se ut som lovutvalget mener at det ikke skal foreligge noe konkretiseringskrav.

---

[132] PT (2008). Momentene er knyttet til trafikkdata ved mobilbruk, men de samme hensynene bak vurderingen gjør seg i stor grad gjeldende for trafikkdata knyttet til IP-adresse.
[133] JD (2009)
[134] I.c.

PT har sterk interesse av å beskytte personvernet, og det er ikke unaturlig å tro at tolkningen av lovverket i denne sammenheng gjøres ut i fra dette hensyn.

Noen endelig avklaring på spørsmålet kan ikke sies å foreligge, selv om lovutvalget er klart i sine uttalelser. Det er ikke unaturlig å tro at det vil komme en avklaring av spørsmålet i rettspraksis. Hensynene til personvern og en effektiv etterforskning står igjen her mot hverandre.

For at tilbyder skal ha plikt til å utlevere data knyttet til IP-adresse må det finnes annet rettlig grunnlag. Vedtak av PT etter strpl. § 118 gir ikke slikt grunnlag. Mest aktuelt som er reglene i strpl. §§ 203 og 210.

3.3.6 Fritak fra taushetsplikten etter kjennelse fra retten

Taushetsbelagte opplysninger som PT ikke gir unntak fra, kan angripes ved kjennelse fra retten, jfr. strpl. § 118 annet ledd. Dette gjelder også etter § 230, jfr. henvisningen i fjerde ledd.

Hjemmel for utlevering av trafikkdata knyttet til IP-adresse kan også skje etter regelen i strpl. § 216b annet ledd d. I slike tilfeller er politi og påtalemyndighet ikke avhengig av å få PTs godkjennelse. Retten kan ved kjennelse oppheve taushetsplikten og hjemle utlevering av opplysningene, jfr. bestemmelsens første ledd.

Etter bestemmelsen kreves det at informasjon knyttet til den opplysningene retter seg mot, mistenkes på *"skjellig grunn"*. Etter Høyesterettspraksis er det blitt knesatt et krav om sannsynlighetsovervekt.[135] Dommene gjelder andre bestemmelser enn strpl. § 216b med ordlyden *"skjellig grunn"*. Det er ansett som sikker rett at samme krav til sannsynlighet gjelder etter 216b.[136]

---

[135] Rt. 1992 s. 1529, Rt. 1993 s. 1303 og 1995 s. 421.
[136] Bjerke I (2001) s. 745 med henvisninger.

Utgangspunktet er at den straffbare handlingen som mistenkes må medføre fengsel i 5 år eller mer, jfr. første ledd a.[137]. I tillegg til slike handlinger, omfattes også datainnbrudd (strl. § 145 annet ledd) og barnepornografi (strl. § 204a) som etter rettspraksis er typetilfeller der IP-adresse er anvendt som bevis, jfr. første ledd bokstav b.[138]

Omfanget av hva som kan utleveres følger av bestemmelsens annet ledd bokstav d.

"... opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som nevnt i bokstav a, og andre data knyttet til kommunikasjon."

Opplysningene som kan gis til politiet etter bestemmelsen er trafikkdata. Bestemmelsen gjelder ikke kun utlevering av trafikkdata knyttet til Internett bruk. Trafikkdata i tilknytning Internett omfatter hvilke IP-adresser som vedkomne har benyttet, hvilke IP-adresser som det ble kommunisert med, samt hvor lenge.

Bestemmelsen retter seg som utgangspunkt ikke mot innholdet i kommunikasjonen. På bakgrunn av at IP-adresser knytter seg til internettsider, vil trafikkdata kunne gi mye informasjon om innholdet i kommunikasjonen, for eksempel der en IP-adresse har kommunisert med IP-adresse som knytter seg til barnepornografisider eller politiske forum. Internettsider har faste IP-adresser, og identifisering av disse kan gjøres gjennom allment tilgjengelige søkemotorer på Internett.[139] Utlevering av slik informasjon kan likevel gjøres etter reglene om utlevering av trafikkdata, selv om kan sees på som innholdsdata.

---

[137] Ved beregningen tas ikke "forhøyelse ved gjentakelse eller sammenstøt" med, jfr. § 216b annet punktum.
[138] Begrunnelsen for at disse også skal omfattes, er at etterforskningen vil være særlig effektiv ved disse typer lovbrudd, se Ot.prp.nr. 64 (1998-1999) pkt. 23. og Bjerke (2001) I s. 745.
[139] For eksempel på http://cqcounter.com/whois/ [sitert 10.03.2009]

Opplysningene som skal utleveres må begrenses til å gjelde et *"bestemt tidsrom"*. Et bestemt tidsrom retter seg ikke bare mot historiske data, men også fremtidige.[140] Det fremgår av forarbeidene at det ikke ligger noen begrensning i tid for historiske data, mens det for fremtidige data, som hovedregel, ikke skal gis mer enn 4 uker om gangen, jfr. strpl. § 216f.

De alminnelige regler for utlevering av beslag i straffeprosesslovens kap. 16 overlapper til en viss grad bestemmelsen i strpl. § 216b annet ledd d. Når det gjelder utlevering av historiske trafikkdata kan det skje etter strpl. § 216b og etter de alminnelige regler om utlevering og beslag. Når det gjelder fremtidige trafikkdata må det skje etter reglene i strpl. § 216b.

Hovedregelen er etter strpl. § 216b første ledd er at retten, som ved kjennelse, kan gi pålegg om utlevering av trafikkdata. Etter strpl. § 216d kan beslutning gjøres av påtalemyndighetene dersom det ved opphold er *"fare for at etterforskningen vil lide"*.

3.4 EMK art. 8 – en begrensning av tilgjengeligheten?

Som redegjort for ovenfor, i avsnitt 3.1-3.3, er det en rekke hindringer som begrenser tilgjengeligheten til IP-adresse i forhold til innhenting og identifisering. EMK art. 8 omhandler borgernes rett til privatliv, og kan etter forrangsprinsippet i mnskrl. § 3 sette til side inngrep som er legale etter norsk intern rett. Dette kan føre til en ytterligere begrensning av tilgjengeligheten til IP-adresse. EMK art. 8 er dermed helt sentral i vurderingen om hvorvidt IP-adresse er et godt bevismiddel eller ikke.

Oppgavens omfang tillater ikke en vurdering av alle de inngrep ved innhenting og identifisering av IP-adresse som kan være i strid med EMK art. 8. Behandlingen i det følgende vil derfor bli noe generell.

[140] Ot.prp.nr. 64 (1998-1999) pkt. 23.

EMK art. 8 nr. 1 oppstiller et forbud mot inngrep i privatlivet fra staten, og har ordlyden:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

Et slikt prinsipp kan ikke gå foran alle andre hensyn som er nødvendig for et velfungerende samfunn. I bestemmelsens nr. 2 oppstilles det unntak, for når inngrep likevel kan skje. Bestemmelsen oppstiller tre kumulative vilkår for at inngrep som krenker privatlivets fred likevel kan forekomme. Forutsetningene er at det må finnes hjemmel lov, inngrepet må fremme et av de uttømmende formålene i bestemmelsen og inngrepet må være nødvendig i et demokratisk samfunn.

EMD har ikke tatt stilling til om norsk regelverk om identifisering av IP-adresse eller utlevering av trafikkdata har vært i strid med konvensjonen.[141] Grunnlaget for vurderingen om EMK art. 8 begrenser tilgjengeligheten kan derfor ikke trekkes direkte ut EMDs praksis.

Kravet om at inngrepet må følge *"accordance with the law"* volder ikke problemer i forhold til innhenting og identifisering av IP-adresse. De bestemmelser som gjør inngrep i borgerens private sfære er alle hjemlet i formell lov, og oppfyller utvilsomt kriteriet forutberegnelighet om at inngrepet må følge av den nasjonale rett i EMK art. 8 nr. 2.[142]

Videre følger det at inngrepet må være begrunnet i de nevnte formål. Et formål som spesielt gjør seg gjeldene i forhold til oppgavens tema er hensynet til *"the prevention of disorder or crime"*. Der innhenting og identifisering av IP-adresse har til formål å forebygge kriminalitet ved å etterforske straffbare forhold kan hensynet til privatlivets fred måtte vike.

---

[141] NOU 2009:1 pkt. 17.4.4.
[142] jfr. avsnitt 3.2 – 3.3.

Høyesterett har tatt stilling til om utlevering av informasjon som kan unntas av taushetsplikten etter e-koml. § 2-9 tredje ledd oppfyller kravet til formålet i EMK art. 8 nr. 2. Her uttalte Høyesterett at:

"Sterke reelle hensyn tilsier at politiet får slike opplysninger hurtig for å kunne bekjempe den stadig tiltakende kriminalitet som foregår via Internett".[143]

Hva som er formålet med inngrepet må selvfølgelig vurderes konkret i den enkelte sak. I forhold til de tilfeller der identifisering av IP-adressen er knyttet til et straffbart forhold, er Høyesterett klar på at formålet etter EMK art. 8 nr. 2 er oppfylt, jfr. den siterte dom ovenfor.

I forhold til formålsvilkåret kan jeg ikke se for meg praktiske tilfeller der innhenting og identifisering av IP-adresse i forbindelse med en straffesak der vilkåret til formål isolert sett etter EMK art. 8 nr. 2, ikke er oppfylt.

Siste vilkår er at inngrepet må være *"necessary in a democratic society"*. Dette må ses på som et krav om forholdsmessighet mellom inngrepets alvorlighet og den interessen som beskyttes. Dette vilkåret er skjønnspreget, og ordlyden gir ikke særlig veiledning. Kriteriet om hva som er *"necessary in a democratic society"* brukes i flere bestemmelser i EMK. Hva som ligger i begrepet følger av en rekke dommer i EMD.[144]

For at ikke den bestemmelse som gjør inngrep skal være i strid med EMK art. 8 må følgende momenter være oppfylt. Staten må påvise at inngrepet tilsvarte et tvingende samfunnsmessig behov (a pressing social need). Dette må stå i forhold til det legitime formål som skal ivaretas (her: hensynet til å bekjempe kriminalitet). I tillegg må de grunner som nasjonale myndigheter anfører være relevante og tilstrekkelige (relevant and

[143] Rt. 1999 s. 1944 (1948).
[144] Møse (2009) note 75 med henvisning til note 85.

sufficient). I vurderingen må man ta i betraktning offentlige interesser som er aktuelle i saken i forhold til de private interesser som er ønskes beskyttet.[145]

Av de regler som hjemler innhenting og identifisering av IP-adresse, er det vanskelig å se at noen av bestemmelsene i seg selv er i strid med EMK art. 8. Det er blant annet kommet til utrykk i dommer og forarbeider om bestemmelser om innhenting og identifisering. I forhold til fritak fra taushetsplikten i e-koml. § 2-9 tredje ledd har Høyesterett uttalt:

"Lovbestemmelsen er helt klar. Inngrepet er ikke uforholdsmessig. Sterke reelle hensyn tilsier at politiet får slike opplysninger hurtig for å kunne bekjempe den stadig tiltakende kriminalitet som foregår via Internett."[146]

I forarbeidene til strpl. § 216b om utlevering av trafikkdata går det klart frem at utvalget mener at reglene straffeprosesslovens kap. 16a i seg selv ikke er i strid med EMK art. 8. I alle praktiske tilfeller vil det heller ikke være i strid med EMK art. 8, selv om flere inngripende bestemmelser blir benyttet samtidig mot et enkelt individ.[147]

Etter dette må det antas at regelverket om innhenting og identifisering i seg selv ikke er i strid med EMK art. 8. Det kan imidlertid ikke utelukkes at det i den konkrete sak kan være det. De mest praktiske tilfeller der EMK art. 8 kan være til hinder er når inngrepet ikke skjer i forbindelse med etterforskning. Dette faller litt utenfor oppgaven siden tema er IP-adresse i straffesaker, og jeg vil ikke forfølge de problemstillinger som melder seg her.

[145] Møse (2009) note 75 med henvisning til note 85.
[146] Rt. 1999 s. 1944 (1948).
[147] Ot.prp.nr. 64 (1998-1999) pkt. 4.2

3.5 Den rettslige utviklingen

Det foreligger per april 2009 ingen lagringsplikt for tilbyderne. Av hensyn til å bekjempe kriminalitet på Internett er dette meget uheldig, da sjansene for oppklaring blir vesentlig mindre når ikke informasjon om bruker knyttet til IP-adressen lagres. I den Europeiske Union (EU) har man ønsket et regelsett som ikke er for sprikende i forhold til lagring av slike opplysninger. På den måten unngår man at noen land blir *"fristeder"* for internettkriminalitet på grunn av nasjonal lovgivning.

I EUs datalagringsdirektiv av 15. mars 2006 (2006/24/EF) pålegges medlemslandene å innføre datalagringsplikt for tilbydere.[148] Lagringsplikten omfatter informasjon som karakteriseres som trafikkdata. Lagringsplikten kan etter direktivet settes mellom 6 måneder til 2 år, jfr. direktivets art. 6. En slik lagringsplikt er begrunnet i hensynet til effektiv bekjempelse av kriminalitet.[149] Norge har ikke inkorporert direktivet, og det er blitt debattert for og imot hvorvidt Norge bør gjøre det med hensyn til personvernet.[150]

I relasjon til IP-adresser vil en inkorporering utvide lagringstiden fra 3-5 måneder til minimum 6 måneder og opptil 2 år. Omfanget av lagringsplikten dekker de opplysninger som blir betegnet som trafikkdata. Disse data lagres allerede av flere tilbydere for faktureringsformål. En inkorporering av direktivet vil ikke medføre vesentlig videre trengsel av det personvernet som eksisterer.

---

[148] Norge er gjennom EØS-avtalen forpliktet til å innføre direktiv som gjelder det indre markedet. Norge har imidlertid en reservasjonsrett, men som til i dag ikke har blitt benyttet, jfr. EØS-rett (2004) s. 181 flg.
[149] NOU 2009:1 s. 190.
[150] Blant annet Slettemark (2007) og Sunde (2007).

3.6 Bevisvurdering av IP-adresse

3.6.1 Premisser for drøftelsen

I norsk rett er bevisvurderingen fri, som tidligere beskrevet.[151] Det betyr likevel ikke at det ikke må stilles krav til hvordan en bevisbedømmelse når sitt resultat.[152] Det har blant annet blitt sagt at *"bevisbedømmelse er frihet under ansvar."*[153]

Et naturlig utgangspunkt i en vurdering av bevisverdien til IP-adresse ville være å ta utgangspunkt i hvordan IP-adresse blir vurdert i dommer. Rettspraksis er begrenset der IP-adresse er bevismiddel. I de dommer som er tilgjengelig vurderes ikke IP-adresse isolert, slik at bevisets vektlegging ikke entydig kan trekkes ut i fra vurderingen av de øvrige bevismidler i saken.

I juridisk litteratur er det flere teorier om hvordan en bevisvurdering kan foretas.[154] Målet med alle typer bevisvurderinger er imidlertid felles; det handler om å trekke slutninger fra hva som har skjedd i fortiden, til det som kan konstateres i ettertid.[155]

Bevisverdien kan også utrykkes på forskjellig måter, både numerisk og semantisk. Den bevisvurderingsmetode som vil bli lagt til grunn her vil ikke alene springe ut fra en bevisteori.[156] Metoden som vil bli lagt til grunn her vil bygge på rasjonelle vurderinger i forhold til hva IP-adresse kan fortelle om hendelsesforløpet og med hvilken sikkerhet.

Bevisverdien som vil bli lagt til grunn vil utrykkes semantisk. I juridisk teori er det blitt hevdet at det ikke er hensiktsmessig å legge til grunn en matematisk fremstilling av beviskravet.[157] Bratholm og Eskeland har i sin teori oppstilt tre hovedkategorier for

---

[151] Se avsnitt 2.5.
[152] Strandbakken (2003) s. 213.
[153] ibid. s. 213 note 2.
[154] ibid. kap. 8.
[155] Strandbakken (2003) s. 238.
[156] Elementer fra flere bevisteorier bør legges til grunn i praksis, jfr. Strandbakken (2003) s. 244.
[157] Strandbakken (2003) s. 244.

angivelse av bevisets styrke: sikkert bevis, utelukkelsesbevis og sannsynlighetsbevis. [158] I det følgende vil jeg vurdere IP-adresse etter disse.

3.6.2 IP-adresse som sikkert bevis

Et sikkert bevis er et bevis som med sikkerhet slår fast at tiltalte er gjerningspersonen, og at det ikke kan være noen andre.[159] En IP-adresse er unikt knyttet til en enhet på Internett, og det kan ikke være flere enheter som har samme IP-adresse til samme tid.[160] Dette gjør at IP-adressen er ideell for å identifisere en enhet på Internett. Enheten kan identifiseres enten direkte via offentlig tilgjengelig registre, eller gjennom tilbyder.[161] Som nevnt er det kun enheten som identifiseres, ikke brukeren.

En brukerkonto vil normalt kunne disponeres av et begrenset antall personer, ofte knyttet til en husstand eller arbeidsplass. Brukere som er knyttet til en slik brukerkonto, vil etter min terminologi bli omtalt som naturlige brukere.

I de tilfeller der IP-adressen knyttes til kun én naturlig bruker hviler mistanken mot vedkommende alene, men å konkludere med at det da må være sikkert at den naturlige brukeren er gjerningspersonen vil ikke holde juridisk mål. Andre legitime omstendigheter kan foreligge, selv om spor fra brukerens IP-adresse er funnet, jfr. avsnitt 3.6.5 nedenfor.

IP-adresse kan etter dette aldri benyttes som sikkert bevis.

---

[158] Kategoriene er lagt til grunn i Bratholm (2008) s. 175-176.
[159] Bratholm (2008) s. 175.
[160] Se avsnitt 3.1.1.
[161] Se avsnitt 3.2.3 og 3.3.2.

3.6.3 IP-adresse som utelukkelsesbevis

Et utelukkelsesbevis er et bevis som ikke er forenelig med en påstand om at tiltalte er gjerningspersonen.[162] Det samme usikkerhetsmomentet som utelukker at IP-adresse kan brukes som sikkert bevis, nemlig at den sporede enheten kan ha blitt brukt av andre enn den naturlige brukeren, umuliggjør at IP-adresse, alene, brukes som utelukkelsesbevis. Altså, hvis en IP-adresse, i seg selv, ikke er tilstrekkelig til entydig å *slå fast* at tiltalte er gjerningsmannen, er den heller ikke tilstrekkelig til å *utelukke* det samme.

På bakgrunn av at IP-adresse tidfestes, vil imidlertid andre bevis kunne utelukke at tiltalte er gjerningspersonen. Det kan tenkes at tiltalte satt i varetekt mistenkt for andre forbrytelser da handlingen ble begått, og at det dermed praktisk ikke er mulig at tiltalte er gjerningspersonen.

IP-adresse kan etter sin art ikke benyttes som utelukkelsesbevis alene.

3.6.4 IP-adresse som sannsynlighetsbevis

Sannsynlighetsbevis er i den kategorien bevis som ikke faller inn under sikkert eller utelukkelsesbevis. Bevis i denne kategorien trekker i varierende styrke i retning av at tiltalte er eller ikke er gjerningspersonen. De aller fleste bevis tilhører denne kategorien bevis, og det er også i denne kategorien IP-adresse befinner seg.

Det å plassere et bevismiddel innenfor de nevnte kategorier er som regel ikke problematisk. Utfordringen med bevismidler som havner i kategorien sannsynlighetsbevis er å slå fast med hvilken grad av sannsynlighet beviset utpeker gjerningspersonen.

[162] Bratholm (2008) s. 175.

3.6.5 Hvilken grad av sannsynlighet er det at IP-adressen utpeker gjerningspersonen?

Verdien av IP-adresse som bevismiddel må vurderes konkret i den enkelte sak. Bevisvekten vil variere i forhold til en rekke omstendigheter. Av plassmangelhensyn kan jeg ikke gå inn på alle situasjoner av betydning for bevisverdien her, heller ikke alle usikkerhetsmomenter som kan oppstå. I det følgende vil jeg berøre de momenter som etter praksis og teori er mest relevante.

IP-adresse brukes som bevis for å knytte en enhet til det straffbare forhold. En naturlig konsekvens av dette er at styrken med mistanke avhenger av tiltaltes forhold til enheten. En annen variabel er hvor sikkert det er at riktig IP-adresse er innhentet og identifisert.

I bevisvurderingen av IP-adresse er det disse to momentene som er avgjørende. Hvor sikkert er det at riktig IP-adresse er innhentet og identifisert? Og hvor stor sannsynlighet er det da for at tiltalte er brukeren og gjerningspersonen?

3.6.5.1 Innhenting av IP-adresse – en feilbarlig prosess?[163]

Når en IP-adresse som er knyttet til et straffbart forhold blir innhentet, vil det bevismessig være relevant å avgjøre med hvilken grad av sikkerhet rett IP-adresse er innhentet. Vurderingen om hvor sikkert det er at riktig IP-adresse er innhentet må vurderes konkret i den enkelte sak.

Ved funn av IP-adresse knyttet til et straffbart forhold, kan det spørres om adressen bak kommunikasjonen kan være forfalsket. For at kommunikasjon mellom enheter på Internett skal kunne skje, må begge enheter kjenne hverandres rette IP-adresse. Forfalsking er ikke en problemstilling der det har vært toveis kommunikasjon.

[163] Avsnittet er basert på e-post korrespondanse med Willassen (2009).

De aller fleste IP-adresser som benyttes er dynamiske. For at riktig IP-adresse kan identifiseres, må den tidfestes. Det er helt essensielt at tidfestingen er riktig, både hos enheten der kommunikasjonen ble loggført og hos tilbyder. Kvaliteten her må vurderes konkret i det enkelte tilfelle av fagpersoner.

I de fleste tilfeller kan det imidlertid slås fast med sikkerhet at riktig IP-adresse er innhentet. I praksis er usikkerheten knyttet til tidfestingen betydelig mer utfordrende enn om en IP-adresse er forfalsket eller ikke.

3.6.5.2 Type Internettilkobling

I dag har de fleste internettilgang via bredbånd/fast linje, som er tilknyttet et nettverk. Nettverk som benyttes er ofte trådløst, slik at flere enheter enkelt kan koble seg på samme internettforbindelse.

Internettilkobling via et trådløst nettverk utgjør en særskilt sikkerhetsrisiko på bakgrunn av flere omstendigheter. Et trådløst nettverk gjør det mulig å koble flere enheter sammen uten å bruke kabel, og å knytte flere enheter opp mot Internett samtidig. Et trådløst nettverk vil kunne ha en rekkevidde innendørs på mellom 20-100 meter og opptil 400 meter utendørs. Rekkevidden avhenger av hvilke fysiske hindringer som befinner seg i område mellom mottaker og nettverket, for eksempel vil godt isolerte dører og vegger begrense rekkevidden.[164]

Hvor sikkert et trådløst nettverk er, varierer i stor grad etter hvor godt brukeren velger å sikre seg. En rekke trådløse nettverk er ikke sikret i det hele tatt. Det betyr at enhver enhet som innholder et trådløst nettverkskort og befinner seg innenfor nettverkets rekkevidde, kan koble seg opp mot Internett.

[164] NorSIS (2008)

At et nettverk er sikret, er ikke ensbetydende med at det er umulig for uvelkomne å trenge seg inn og misbruke internettilkoblingen. Et sørgelig faktum er at de fleste private forbrukere ikke sikrer nettverket sitt godt nok. Det kreves ikke kyndig datakunnskap for urettmessig å bryte seg inn i et trådløst nettverk. Enkel programvare som gjør dette mulig ligger faktisk gratis tilgjengelig på Internett.[165]

Trådløse nettverk rekker ofte langt utenfor husets fire vegger, og en inntrenger kan derfor befinne seg i nabohuset eller i en parkert bil på gatenivå. Det at personer aktivt søker etter ubeskyttede eller dårlig sikrede nettverk har utviklet seg til å bli et eget fenomen. Det at inntregere søker nettilgang fra bil har til og med fått en egen betegnelse – *"wardriving"*.[166]

Trådløst nettverk øker muligheten for at andre enn den naturlige bruker er gjerningspersonen. Dette gjør seg spesielt gjeldende når nettverket er usikret.

Når en hacker trenger seg inn i ett trådløst nettverk med tilgang til Internett, vil inntrengerens IP-adresse bli knyttet opp mot brukerkontoen som er hacket. På den måten avleder den kriminelle mistanken fra seg selv til den som disponerer brukerkontoen.

Ved tilkobling til kabelnettverk vil en inntrenger være fysisk koblet til nettverket. Dette gjør det både vanskeligere og mindre attraktivt for utenforstående å koble seg til nettverket, fordi det krever at man fysisk må trenge seg inn i husstanden og koble seg til med kabel, i tillegg til at sannsynligheten for å bli oppdaget/avslørt av øker drastisk. Når oppkoblingen har skjedd gjennom kabeltilkobling, vil det med større sannsynlighet enn ved bruk av trådløst nettverk, være noen i husstanden som har foretatt den kriminelle handlingen.

---

[165] Teknologirådet (2005) s. 71
[166] Teknologirådet (2005) s. 34 og http://www.wardriving.com/about.php [05.03.2009]

3.6.5.3 Bruk av proxyservere

Bruk av proxyservere er blitt stadig mer vanlig på Internett, ikke bare for kriminelle, men også for de som av forskjellige grunner vil opptre anonymt på Internett. Formålet med bruk av proxyservere er å undertrykke og skjule brukerens egentlig IP-adresse.[167]

Anonymitet på Internett oppnås ved at brukeren knytter seg til proxyservere som videreformidler informasjon mellom brukeren og tjenester på Internett. På denne måten vil IP-adressen til proxyserveren etterlates som elektronisk spor, og ikke brukerens reelle adresse.

Leverandøren til proxyserveren kan finne ut av hvilken IP-adresse som ble benyttet. Brukeren av proxyserveren må kunne stole på leverandøren for at anonymiteten skal være sikret. Det tilbys også tjenester hvor kommunikasjonen passerer gjennom flere proxyservere. Anonymiteten er da ekstra godt ivaretatt, siden det da er tilstrekkelig at en av proxyserverene er til å stole på for å sikre anonymitet.[168]

Kriminelle som opptrer med en viss profesjonalitet vil dermed ha få problemer med å opptre anonymt på Internett. Tjenester av denne sort ligger offentlig tilgjengelig, og er ikke ulovlige å benytte seg av.[169]

Av dette følger at det er gode muligheter for å opptre anonymt på Internett. Dette gjelder både for profesjonelle kriminelle og alminnelig brukere.

Bevisverdien til en IP-adresse som er knyttet til en proxyserver vil ha liten eller ingen bevismessig verdi. IP-adressen som blir identifisert er ikke den egentlige adressen til

---

[167] NOU 2009:1 s. 284.
[168] Teknologirådet (2005) s. 89.
[169] Se blant annet www.torproject.org [sitert 10.03.2009]

brukeren. Ved videre sporing kan den egentlige IP-adresse identifiseres, noe som også har forekommet i praksis.[170]

3.6.5.4 Antall naturlige brukere

Antall naturlige brukere av brukerkontoen er relevant og av betydning for IP-adressens bevisverdi. Er det kun én naturlig bruker av brukerkontoen vil mistanken alene falle på vedkommende. I slike tilfeller har IP-adressen isolert sett størst bevisverdi. IP-adressen indikerer at det med klar sannsynlighetsovervekt er noen i den husstanden som er gjerningspersonen.[171]

Med tanke på at sporet fra IP-adressen tidfestes vil man på bakgrunn av videre etterforskning kunne eliminere mistanken mot enkelte av beboerne med hjelp av andre bevismidler.

Internett har i de siste årene i stadig større grad blitt tilgjengelig i det offentlige rom. Deriblant tilbyr mange caféer, restauranter, bibliotek og andre oppholdssteder usikret Internett for brukere. Det betyr at det ikke føres kontroll over hvem som er bruker. Hvis IP-adressen som er knyttet til den kriminelle handlingen knyttes til en slik brukerkonto, vil bevisverdien være minimal.[172] Siden tidspunktet for den kriminelle handlingen er registrert, vil det være mulig å identifisere mulige gjerningspersoner, da med støtte i andre bevis i saken.

[170] Dette var tilfelle i LA-2003-83.
[171] Willassen (2008)
[172] Sunde (2000) pkt. 4.2.2.

4 Effektivitetshensyn kontra rettssikkerhetsprinsippet

På bakgrunn av drøftelsene i pkt. 2 og 3 i oppgaven, om bevis i straffesaker og IP-adresse som bevismiddel, vil jeg her drøfte og vurdere kriteriene i problemstillingen om IP-adresse er et godt bevismiddel i straffesaker eller ikke. Innenfor de enkelte kriteriene vil jeg drøfte i hvilken utstrekning hensynene til rettsikkerhet og effektivitet gjør seg gjeldende, og om disse hensyn har innflytelse på IP-adressens bevismessige verdi.

Etter dette vil jeg oppsummere hovedpunktene i oppgaven og til slutt konkludere om IP-adresse er et godt bevismiddel eller ikke.

4.1 Bakgrunn

Effektivitets – og rettsikkerhetshensyn er helt grunnleggende hensyn i strafferetten og straffeprosessen, og de ilegges vekt både ved utformingen og ved tolkningen av rettsregler.[173] Hensynene er derved også sentrale for vurderingen av oppgavens problemstilling.

Effektivitetshensyn i strafferetten er hensynet til at lovverket blir effektivt håndhevet. Det kan skje ved at politiet får hjemmel til å benytte seg av ekstraordinære etterforskningsmetoder[174] eller at bevisføringsplikten snus.[175] Under kategorien effektivitetshensyn, faller hensynet til prevensjon, som også er et viktig hensyn i strafferetten.[176]

Rettsikkerhet er ikke et entydig begrep, og favner mange forskjellige hensyn. Det kanskje viktigste hensynet under gruppen rettsikkerhet er hensynet til at ingen uskyldige skal

[173] Eskeland (2006) s. 525.
[174] Det vil si metoder som griper inn i borgernes sfære, jfr. Ot.prp.nr. 64 (1998-1999) pkt. 3.3.
[175] Se for eksempel vilt. § 34 annet ledd.
[176] Eskeland (2006) s. 526

dømmes.[177] At borgerne er sikret mot vilkårlig inngrep i sine respektive sfærer, er et annet hensyn som også må sies å ligge i kjernen av begrepet rettsikkerhet.[178]

Det fremstår som åpenbart at disse hensyn i flere relasjoner kan kommer i sterk konflikt med hverandre i straffesaker.[179] Dette gjelder særlig saker som omhandler IP-adresse. IP-adresse er som nevnt et av få gode instrumenter i etterforskningsarbeid og som bevismiddel i saker som omhandler kriminalitet utført via Internett. Der hensynet til rettsikkerhet blir prioritet vil dette gå utover en effektiv håndhevelse av lovverket, og omvent.[180]

Hva som utgjør en det optimale balansepunkt mellom hensynene er ikke klart. Men det som er klart er at balansepunktet lovgiver og rettspraksis opererer med, varierer innefor det rettstema i strafferetten eller straffeprosessen som behandles. I det følgende vil disse avveiningene mellom hensynene bli belyst.

4.2 IP-adresse som bevis i lys av beviskravet

4.2.1 Metode

Et naturlig utgangspunkt for vurderingen av IP-adresse som bevismiddel i lys av beviskravet i straffesaker ville vært å undersøke rettspraksis, og sett hvordan retten vurderte dette. Av flere årsaker er ikke dette hensiktsmessig, hovedsakelig på bakgrunn av mangelen på rettspraksis.[181]

I vurderingen av hvordan IP-adresse står seg mot det strenge beviskravet i strafferetten, vil jeg basere drøftelsen på den induktive metode. Metoden er en bevisvurderingsmetode som har sin opprinnelse fra angloamerikansk rett.[182] Det er noe usikkert hvor anerkjent metoden

[177] Eskeland (2006) s. 509.
[178] Strandbakken (2003) s. 74.
[179] Se blant annet Eskeland (2006) s. 526.
[180] ibid. s. 528.
[181] Se avsnitt 3.6.1.
[182] Strandbakken (2003) s. 228.

er etter norsk rett, men blant annet Strandbakken har anerkjent at denne metoden bør legges til grunn i straffesaker.[183] Det er etter Strandbakkens synspunkt realistisk å tro at denne metoden anvendes i praksis.[184]

Utgangspunktet for den induktive metode er at det oppstilles en hypotese fra påtalemyndighetene om de faktiske forhold. Hypotesen må oppstilles på bakgrunn av rasjonelle og erfaringsmessige vurderinger av hva bevisene kan si om hendelsesforløpet. Hypotesen må deretter enten *valideres* eller *falsifiseres*.[185]

Hvorvidt påtalemyndighetenes hypotese skal bli lagt til grunn når den blir bestridt beror på følgende etter den induktive metode:

"every relevant reason for doubt has to be excluded"[186]

Dette innebærer at hypotesen må være bevist utover enhver rimelig tvil, noe som tilsvarer beviskravet i straffesaker etter norsk rett.

4.2.2 Innvendingene mot hypotesen må ikke skape rimelig tvil

Beviskravet i strafferetten formuleres som at *"enhver rimelig tvil skal komme tiltalte til gode"*.[187] Beviskravet krever en høy grad av sannsynlighet for at faktum skal kunne legges til grunn. Den legislative begrunnelsen for beviskravet uttrykkes gjerne, som også tidligere nevnt, med at det er større ulykke at en uskyldig blir dømt enn at ti skyldige går fri.[188] Et så høyt beviskrav fører utvilsomt til at tiltalte som med høy sannsynlighet er skyldige går fri på bakgrunn av at påtalemyndigheten ikke makter å oppfylle beviskravet.

---

[183] Strandbakken (2003) s. 256.
[184] ibid. s. 230.
[185] ibid. s. 228.
[186] ibid. s. 230.
[187] Se avsnitt 2.4 om beviskravet i strafferetten.
[188] Andenæs I (2000) s. 177.

At dette forekommer er ingen hemmelighet, og er en naturlig konsekvens av at hensynet til rettsikkerhet settes høyt.

Om hensynet til rettsikkerhet skulle få gjelde fullt ut ville beviskravet være *absolutt visshet*, der ingen teoretisk tvil kan foreligge. Så langt har ikke rettsikkerhetshensyn fått gjennomslag. Grunnen til det er hensynet til effektivitet. Et beviskrav som stilte så høye krav til sikkerhet ville føre til at alt for mange lovbrytere ville slippe fri, siden det nesten alltid kan oppstilles en teoretisk tvil.[189]

Etter den induktive metode må enhver rimelig tvil til hypotesen om at tiltalte er gjerningspersonen måtte fjernes. Ikke alle innvendinger mot hypotesen kan behandles her. Derfor vil jeg i det følgende kort drøfte de typetilfeller av rimelig tvil som må fjernes i forhold til anvendelsen av IP-adresse som bevismiddel for at tiltalte skal kunne domfelles.

4.2.2.1 Flere naturlige brukere

Som drøftet i avsnitt 3.6.4 utgjør det et usikkerhetsmoment at flere personer/brukere kan knyttes til en brukerkonto. Det kan tenkes at tiltalte påberoper seg at det var andre i husstanden som er gjerningspersonen og ikke han. En slik innvending vil vanligvis innebære en rimelig tvil til påtalemyndighetenes hypotese, og må fjernes for at tiltalte skal dømmes til straff.

Tvil knyttet til om det var andre i husstanden enn tiltalte som er gjerningspersonen, kan fjernes på bakgrunn av flere omstendigheter. Tidfesting av IP-adresse gjør at man på bakgrunn av andre bevismidler kan utelukke innvendingen fra tiltalte.

Handlingene kan også være av en slik art at innvendingen på hypotesen må forkastes. En innvending om at et profesjonelt datainnbrudd er begått av noen andre i husstanden, som på det rene ikke har slike ferdigheter, bør for eksempel ikke føre frem.

---

[189] Andenæs I (2000) s. 178.

Situasjonen kan være at handlingens art knytter seg like mye til alle i husstanden, og tidfestingen av IP-adresse ikke gir klare svar. I de tilfeller vil innvendingen på hypotesen utgjøre en relevant grunn til tvil. Tiltalte bør i slike tilfeller frifinnes.

4.2.2.2 Hacking

En innvending om at det er utenforstående som har benyttet seg av internettilgangen kan være utfordrende for retten å ta stilling til. Spesielt kan dette volde tvil ved bevissituasjonen når det er brukt trådløst nettverk, jfr. avsnitt 3.6.5.2.

Denne innvendingen mot hypotesen ble forelagt Oslo tingrett i 2004.[190] En mann var tiltalt for fire tilfeller av brudd på strl. § 390a. Tiltalte hadde via chattesteder på Internett gitt seg ut for å være andre og oppfordret folk til blant annet å sende seksuelt ladede eller perverse tekstmeldinger til dem han uriktig utga seg for å være. Etter utskrift fra loggen til internettsiden som formidlet chatten mellom tiltalte og tredjemenn ble det knyttet IP-adresser til samtalen. IP-adressen som ble funnet ble identifisert som tiltaltes.

I dommen gjør ikke retten nærmere rede for hvilken vekt den legger på de forskjellige bevismidlene. Den legger til grunn at den har *"lagt vekt"* på utskriftene som knytter IP-adressen til brukerkontoen til tiltalte. I tillegg legger retten blant annet vekt på at tiltalte hadde inngående kjennskap til de fornærmede, samt at tiltalte hadde innrømmet å være bruker av chattestedet.

Tiltalte oppstilte innvendingen til hypotesen at noen andre hadde *"brutt seg inn"* på hans maskin, og at det ikke var han som sto bak de straffbare handlingene. Det vil si at noen har hacket seg inn på maskinen hans. Tiltalte ble ikke trodd. Retten fant det bevist utover enhver rimelig tvil at tiltalte var skyldig.

---

[190] TOSLO-2004-41422

Hvilken vekt retten faktisk legger på IP-adresse som bevismiddel kommer ikke tydelig frem i dommen. Retten går ikke nærmere inn på hvilken betydning IP-adressen har for rettens utfall.

Retten fant at tiltaltes forklaring om at noen skal ha *"brutt seg inn"* på maskinen hans var oppkonstruert, og forekom som rent teoretisk. Etter omstendighetene ellers i saken kan dette forsvares, men en anførsel om at utenforstående kan ha *"brutt seg inn"* er generelt reell, og bør kunne støttes på andre faktiske forhold. Ved bruk av kabel vil en innvending om datainnbrudd lettere kunne forkastes. Andre bevismidler vil også enkelt kunne forkaste en slik teori.

4.2.3 Kan IP-adressen alene føre til domfellelse?

Som redegjort for, er det en rekke usikkerhetsmomenter knyttet til IP-adresse som bevismiddel. For å oppfylle beviskravet må *"enhver tvil"* elimineres for at tiltalte skal kunne dømmes. Etter min vurdering kan *ikke* IP-adresse alene føre til domfellelse.

4.2.4 Avveining mellom hensynene

I beviskravet er det klart at hensynet til rettssikkerhet er mer fremtredende enn hensynet til effektivitet. Når *"enhver rimelig tvil"* kommer tiltalte til gode, skal det i teorien hindre at uskyldige blir dømt. Et slikt beviskravet medfører antagelig at skyldige går fri grunnet at bevisene ikke utgjør en tilstrekkelig overbevisning.

I avsnitt 2.5.4 ble det drøftet om beviskravet i straffesaker kan bero på sakens art, grunnet at hensynet til rettssikkerhet og effektivitet i varierende grad gjør seg gjeldende. I teorien har dette blitt akseptert som en realitet, og man kan ut i fra de legislative hensyn i strafferetten begrunne en slik praktisering. Høyesterett har ikke tatt nærmere stilling til

spørsmålet. Det er enighet i juridisk teori at det kun er tale om nyanseforskjeller, og at beviskravet uansett må settes høyt.[191]

I saker som omhandler mindre alvorlige kriminelle handlinger via Internett, kan det hevdes at beviskravet kan senkes noe. På den måten kan man muligens ilegge IP-adresse større rettslig vekt som argument i en straffesak enn i alvorligere tilfeller. Dette er, som nevnt, svært omdiskutert.[192] Effektivitetshensyn taler for en slik løsning. I praksis er det usikkert hvorvidt dette er rettstilstanden. De lege ferenda bør etter min mening effektivitetshensynet tas vare på andre måter, for eksempel gjennom videre etterforskningsadgang.

Når det gjelder hensynet til at ingen uskyldige skal bli dømt, står dette som nevnt meget sterkt i strafferetten, og hensynet til effektivitet bør etter dette i stor grad vike.

4.3 IP-adresses tilgjengelighet

4.3.1 Hensynene

Hovedregelen om bevisføringsplikten i straffesaker medfører at påtalemyndighetene må føre bevis for at tiltalte er gjerningspersonen.[193] Påtalemyndighetene står ikke fritt til å innhente bevis. Hensynet til effektivitet tilsier at påtalemyndigheten skal ha vid adgang til å innhente de bevis som er ønskelig. Rettsikkerhets hensyn tilsier det motsatte, det vil si at slike inngrep bør skje i begrenset utstrekning og eller gitte vilkår.

Utlevering og identifisering av IP-adresse er i strid med prinsippet om personvern. Personvernhensyn faller i stor grad under paraplyen rettsikkerhet, som også er ment å beskytte borgernes integritet mot overgrep.[194]

---

[191] Se avsnitt 2.5.4.
[192] jfr. avsnitt 2.4.5.
[193] Se avsnitt 2.3.2.
[194] NOU 2009:1 pkt. 4.1.6.

4.3.2 Praktisk og økonomisk tilgjengelighet

Om et bevismiddel er tilgjengelig beror som nevnt på flere momenter. Praktiske, økonomiske, så vel som juridiske hindringer kan spille inn. I oppgavens pkt. 3.1-3.3 har disse temaene blitt gjennomgått.

IP-adresse er tilgjengelig for de enheter som er part i kommunikasjonen. Politiet er derfor avhengig av enten selv å være i kontakt med gjerningspersonen eller få hjelp fra publikum. Dette gjør at majoriteten av IP-adresser knyttet til kriminelle handlinger aldri blir kjent for politiet. De praktiske hindringene for at politiet effektivt skal kunne innhente IP-adresser for alle straffbare forhold er enorme i så måte, og urealistisk å oppnå. For å oppdage kriminelle handlinger på Internett er politiets mulighet stort sett knyttet til infiltrering og overvåkning. Slik aktivitet er veldig ressurskrevende og koster politiet betydelig beløp og arbeidskraft.[195]

Økonomiske hensyn setter grenser for hvor mye tid og ressurser som kan brukes på etterforskning, og det er liten tvil om at økonomiske hensyn er en vesentlig grunn for at ulovlig fildeling ikke blir prioritert av politiet. Det kommer klart til utrykk ved at Norsk Videogramforening (NVF) har engasjert advokatfirmaet Simonsen, for å samle inn IP-adresser og forfølge fildelere rettslig. For å gjøre dette har Simonsen fått konsesjon til å benytte seg av overvåkningsprogram, som kan innhente IP-adresser til fildelere.[196]

4.3.3 Juridisk tilgjengelighet – innhenting og identifisering

Beslag og utlevering av IP-adresse følger de alminnelige regler for beslag og utleveringspålegg, jfr. avsnitt 3.3. Innhentingen av IP-adresse er ikke underlagt større hindringer enn ved alminnelig innhenting av bevis.

[195] Kripos (2003) s. 13.
[196] NOU 2009:1 pkt. 17.4.2.

Den juridiske terskel for å identifisere IP-adresse er større enn ved innhenting av den. Tilbyder kan være avskåret fra å utlevere informasjon som etter de alminnelige regler om beslag og utleveringspålegg er hjemlet. Det følger av reglene om taushetsplikt for tilbyder. Tilbyder kan både være avskåret fra å bidra fordi hjemmel for å identifisere ikke foreligger, eller at informasjonen har blitt slettet grunnet sletteplikten. Disse begrensningene er begrunnet i hensynet til personvernet, og hindrer en mer effektiv bekjempelse av kriminalitet.

Sletteplikten utgjør en betydelig hindring, i tillegg til at tilbyder ikke plikter å lagre informasjon knyttet til en IP-adresse. En slik plikt finnes for tilbyder ved telefontjeneste, jfr. ekomforskriften § 6-2. En slik plikt begrunnes i hensynet til effektiv bekjempelse av kriminalitet.

Hjemmelen for utlevering i strpl. § 216b første ledd bokstav b) illustrerer hvordan hensynet til effektivitet får gjennomslag i lovverket. Etter den generelle regelen om vilkåret til alvorlighetsgrad i bokstav a kan utlevering kun foretas der den straffbare handling medfører fengsel i minst fem år. I bokstav b kan likevel slik utlevering og kontroll forekomme om det straffbare forhold gjelder enkelte straffebestemmelser som er typiske ved internettkriminalitet. I forarbeidene går det frem at unntaket er begrunnet med hensynet til at etterforskningen er særlig effektiv ved slike lovbrudd.[197]

At hensynet til rettsikkerhet og effektivitet er sentrale ved utlevering av personopplysninger knyttet til IP-adresse kommer klart til utrykk ved Post – og teletilsynets vurdering om hvorvidt taushetsplikten skal oppheves. Her vurderer PT direkte opp mot hverandre hensynet til effektivitet kontra hensynet til rettssikkerhet (personvern).[198]

[197] Ot.prp.nr. 64 (1998-1999) pkt. 23 under § 216b.
[198] Se avsnitt 3.3.5.

4.3.4 Avveiningen mellom hensynene

Det er tydelig at hensynet til effektivitet ved innhenting og identifisering av IP-adresse har fått større gjennomslag i utformingen av lovverket, enn i beviskravet. På bakgrunn av at hensynene mellom effektivitet og rettsikkerhet i stor grad er motstridene, er en naturlig slutning at hensynet til rettssikkerhet ikke er like godt ivaretatt som i beviskravet.

Hvorfor hensynet til effektivitet gis økt vekt i etterforskningssammenheng kan bero på inngrepets art. Frihetsstraff og bøter er i norsk rett det ultimative inngrep i borgerens sfære, og begrunner at rettssikkerhet settes høyt. Inngrep i etterforskningen er som regel mindre i omfang, og begrunner derfor ikke at rettssikkerhet vektes like høyt.

4.4 Identifisering av IP-adresse – et alvorlig inngrep?

Det tredje momentet i vurderingen om hvorvidt et bevismiddel er godt eller ikke, er i hvilken grad innhenting og identifisering krenker borgerens sfære. Det følger av lovverket at lovgiver ønsker å beskytte mot slike inngrep, og Høyesterett har uttalt at borgernes integritet er av høy verdi.[199]

Identifisering av IP-adresse og innsyn i en brukers trafikkdata er en krenkelse av privatlivets fred og korrespondanse. Selv om inngrepet gir resultater, er det like fullt et inngrep i den personliges sfære.

Inngrep kan krenke borgerens fysiske integritet så vel som den psykiske, og vil variere både i omfang og alvorlighetsgrad. Ofte vil inngrep kun krenke en av delene, slik som er tilfelle når det gjelder identifisering av IP-adresse og utlevering av trafikkdata; inngrepet krenker ikke den fysiske integritet, men den psykiske. Jeg ønsker i det følgende å vurdere inngrepet i dette tilfellet opp mot andre inngrep innenfor den psykiske integritet. En slik sammenlignende vurdering krever en målestokk, og jeg vil for enkelthetsskyld bruke følgende tredelte skala for å beskrive et spesielt inngreps alvorlighetsgrad.

[199] jfr. avsnitt 1.3.

1. Alvorlighetsgrad 1 – Lav
2. Alvorlighetsgrad 2 – Middels
3. Alvorlighetsgrad 3 – Høy

Disse er kun ment som veiledende for hvor krenkende inngrepet oppleves for borgeren, selv om denne vurderingen kan variere fra en konkret borger til en annen. Momentet som avgjøres inngrepets alvorlighetsgrad, og dermed hvilken kategori det plasseres i, er hvor mye informasjonen den kan gi om en person og dens handlemønster.

Utlevering av innholdet i en gitt kommunikasjon må anses å falle inn under Alvorlighetsgrad 3 - høy. Det faktiske innholdet i kommunikasjonen har størst potensial for å gi mest mulig informasjon om en person og dens handlemønstre og er dermed den groveste form for inngrep i denne sammenheng.

Trafikkdata gir ikke direkte innhold om kommunikasjonen, men kan kartlegge en persons handlinger på Internett. Slik informasjon har ikke like stort potensial til å si noe om en person. Det er naturlig å plassere dette inngrepet i Alvorlighetsgrad 2 – middels. Internettsider har fast IP-adresse, og det vil dermed på bakgrunn av trafikkdata være mulig å identifisere internettsider som har blitt besøkt. Trafikkdata knyttet til IP-adresse vil med hensyn til graden av inngrep befinne seg et sted mellom Alvorlighetsgrad 3 og 2.

Identifiseringen av IP-adresse knyttet et straffbart forhold, utgjør etter mitt skjønn den laveste for form krenkelse, relativt til de andre. På skalaen kan dette plasseres under Alvorlighetsgrad 1 – lav. Inngrepet har kun potensial til å gi informasjon om en persons handling på en konkret tidspunkt.

4.5 Rettens grunnlag for bevisvurderingen av IP-adresse

For at retten skal få avsagt materielt riktig dom er det et sentralt at bevisvurderingen gjøres ut i fra erfaringsmessige og rasjonelle vurderinger. En forutsetning for dette, er blant annet at bevisvurdereren har kunnskap om bevisets relevans og vekt. Er kunnskapen begrenset, kan et ellers godt bevis være vanskelig å tolke, og dermed muligens føre til feil avgjørelse, og i verste fall justismord.[200]

Når det gjelder vurderingen av IP-adresse som bevismiddel i norsk rett, på nåværende tidspunkt, er det flere tenkelig grunner til å anta at mangel på kunnskap kan eksistere i større eller mindre grad. For det første utgjør IP-adresse en ny type bevismiddel, og rettens erfaringsgrunnlag vil derfor være begrenset.[201] For det andre knyttes det mange tekniske aspekter til vurderingen av IP-adresse som bevis (vist i avsnitt 3.6). Sannsynligheten for at bevisvurdereren besitter en intuitiv forståelse av relevante tekniske egenskaper og sammenhenger, vil derfor være redusert.[202] Til slutt later det til å være en generell mangel på litteratur og veiledning rundt dette temaet, som igjen begrenser muligheten for å sette seg inn i tema.[203]

Når det er sagt, er det klart at påtalemyndighetene og forsvarere i praksis vil gjøre sitt beste i å gjøre rede for de omstendigheter som har betydning for bevisvurderingen, blant annet ved å hente inn sakskyndige. Dette reduser betydning av den potensielle effekten av de overnevnte punktene, i noen grad. Likevel er det å foretrekke at retten har den nødvendige kunnskap til selvstendig å vurdere beviset, og egenhendig kunne påpekte mangler ved partenes anførsler.

---

[200] Justismord er den alminnelige betegnelsen der tiltalte kjennes uskylidig dømt, jfr. Eskeland (2006) s. 513.
[201] jfr. avsnitt 3.
[202] Faktisk argumenterer Eskeland at en av hovedårsakene til justismord er nettopp mangel på kunnskap om tekniske bevis, Eskeland (2006) s. 515 flg.
[203] Willassen (2008)

Av de dommer der IP-adresse er ført som bevis, kan jeg ikke se at retten har vurdert IP-adresse feilaktig. Men etter hva som har kommet frem i domsgrunnene, er det tydelig at det er flere relevante rettslige usikkerhetsmomenter som ikke ble drøftet.[204]

4.6 Sammenfatning av oppgaven

DEL I – Bevis i strafferetten

I straffesaker er det påtalemyndighetene som har bevisføringsplikten og det må kreves et strengt beviskrav. Beviskravet i straffesaker er strengt, og utrykkes ved at *"enhver rimelig tvil skal komme tiltalte til gode"*. Hovedregelen i norsk rett er fri bevisvurdering og fri bevisførsel.

DEL II – IP-adresse som bevismiddel

Det er praktiske, økonomiske og juridiske hindringer for at IP-adresse kan bli brukt som bevis. For at IP-adresse skal bli innhentet, bør en med interesse i å melde fra om det straffbare forhold, være en del av kommunikasjonen. Det er økonomisk kostbart å drive etterforskning på Internett.

Selv om hovedregelen er fri bevisførsel, kan ikke retten ta bevis til vurdering som knytter seg til taushetsbelagt informasjon. Informasjon knyttet hvilken brukerkonto som innehaver en IP-adresse er taushetsbelagt i e-koml. § 2-9. Da realisasjonen av bevisets verdi avhenger av at IP-adressen blir identifiser, utgjør taushetsplikten en juridisk hindring. Disse hindringene kan omgås slik at informasjon knyttet til IP-adresse likevel kan føres for retten ved unntaksbestemmelsen i e-koml. § 2-9 tredje ledd, vedtak fra Post –og teletilsynet og kjennelse fra retten. Slike inngrep må sees i sammenheng med den generelle regelen i EMK art. 8, som begrenser myndigheter inngrep i den personligs sfære. Bestemmelsen har forrang annen norsk lovgivning.

[204] jfr. TOSLO-2004-41422

Tilbyder har ingen lagringsplikt, men sletteplikt. Det betyr at, som utgangspunkt, må informasjonen bli etterspurt innen 3-5 måneder fra den straffbare handling ble begått.

IP-adressen indikerer hvilken enhet som har vært en del av kommunikasjonen, og impliserer de naturlige brukerne av enheten. Rekkevidden av hva IP-adresse kan bevise, begrenser seg til den objektive gjerningsbeskrivelse. Hvilken vekt beviset skal ilegges, må vurderes konkret i den enkelte sak, på bakgrunn av en rekke momenter som har rettslig betydning for bevisverdien. De omstendigheter denne oppgave har satt fokus på er blant annet antall naturlige brukere og hvilken internettilkobling som ble benyttet.

DEL III – Effektivitetshensyn kontra rettssikkerhetsprinsippet

For å anslå i hvilken grad IP-adressen overbeviser retten, må bevisvurderingen settes opp mot beviskravet. Beviskravet i straffesaker er høyt, og etter min drøftelse, har det blitt vist at IP-adresse ikke alene er godt nok som bevis i straffesaker.

Mange sider av tilgjengeligheten har blitt drøftet. I forholdet mellom de praktisk, økonomiske og juridiske hindringer, har det blitt vist at de juridiske hindringer er minst. Identifisering av IP-adresse og utlevering av trafikkdata utgjør et inngrep i den psykiske integritet. Utlevering av trafikkdata anses som en middels grad av inngrep, mens identifisering har lav grad av inngrep.

For av bevisvurderingen skal være optimal, må bevisvurdereren ha god kjennskap til de momenter som har betydning for bevisvurderingen. Slik kunnskap er det naturlig å tro at ikke retten alltid besitter, og at retten i for stor grad må basere seg på hva partene anfører.

Hensynet til rettsikkerhet og effektivitet gjør seg i varierende grad seg gjeldene om man befinner seg i etterforskningssituasjon eller i retten for å vurdere bevis. I beviskraet er hensynet til rettsikkerhet helt avgjørende. I etterforskningssituasjonen har effektivitetshensyn fått mer gjennomslag i lovverket.

4.7 Hovedkonklusjon på problemstillingen

I problemstillingen ble det reist spørsmål om hvorvidt IP-adresse er et godt bevismiddel.[205] I vurderingen ble det oppstilt fire kriterier; overbevisning, tilgjengelighet, inngrepet det gjør i borgerens sfære og rettens forståelse av beviset. Av disse kriterier, er det *overbevisning* og *tilgjengelighet* som veier tyngst.

Etter min vurdering trekker overbevisningskraften til IP-adresse i retning av å anse det som godt. Bevisverdien til en IP-adresse varierer på bakgrunn av en rekke momenter, likevel begrenses antall mulige gjerningspersoner betydelig, i de mest praktiske tilfellene av saker. Mitt standpunkt gjelder, selv om IP-adresse som bevis alene ikke kan føre til domfellelse.

Tilgjengeligheten til IP-adresse trekker i retning av å *ikke* anse det som et godt bevismiddel. Det ligger store praktisk/økonomiske utfordringer i å innhente beviset. Dette selv om de juridiske forhold er lagt til rette for at beviset skal være tilgjengelig.

Realisasjon av bevisverdien til IP-adresse krever at borgerens sfære blir krenket, og dette trekker isolert ned i vurderingen. Krenkelsens alvorlighetsgrad i forhold til hensynene til effektiv bekjempelse av kriminalitet, er likevel avgjørende for at jeg mener dette *ikke* kan trekke ned i vurderingen. Kriteriet trekker opp i vurderingen.

IP-adresse som bevis krever kjennskap til en rekke tekniske faktorer som gjør det krevende å vurdere beviset. Dette utgjør en risiko for at feil materiell avgjørelse treffes, og selv om risikoen kan ansees som minimal, er kriteriet med på å trekke ned i vurderingen.

Jeg har i avsnittene ovenfor forsøkt å sette mine fire valgte kriterier i sammenheng, og vurdert hvordan de enten trekker opp eller ned i vurderingen av om IP-adresse er et *"godt"* bevismiddel. Selv om formuleringen *"å trekke opp/ned"* selvfølgelig er grov, og på mange måter upresis, så er det nyttig i en konklusjon å si noe *"ukvestet"* om hvordan vurderingen av hvert enkelt kriterium veier inn mot problemstillingen.

[205] jfr. avsnitt 1.3.

Det kan til slutt være fristende å besvare problemstillingen direkte og uttale med endelig autoritet at IP-adresse er, eller ikke er, et godt bevismiddel. Men en slik båssetting er både meningsløs og uten rettslig relevans. Formålet med min vide problemstilling, var ikke å nå frem til et endelig standpunkt, men å skape rom for å belyse en rekke relevante momenter og kriterier underveis. Problemstillingen har vært forsøkt belyst, ikke avklart. Jeg mener likevel det har vært rettslig relevant og interessant å drøfte de valgte tema.

Oppgavens tema og problemstilling er av et uvanlig slag i masteroppgavesammenheng. Utfordringene har vært mange, men blant de mest praktiske kan nevnes: tilgangen til litteratur, teknisk krevende bakgrunnsstoff, riktig avgrensning, vekting av de valgte temaer og hensynet til at leser vil ha praktisk nytte av arbeidet, uten krav om spesielt store forkunnskaper.

5 Litteraturliste

5.1 Forkortelser

St.meld.	Stortingsmelding.
Ot.prp.	Odelstingsproposisjon.
NOU	Norges Offentlige Utredninger.
Rt.	Norsk Retstidende.
I. c.	Loco citato – Samme fotnote som ovenfor.
Ibid.	Ibidem – Samme verk som fotnote ovenfor.

5.2 Lover

Kronologisk oppstilt. Forkortelse i parentes.

Kong Christian Den Femtis Norske lov af 15. April 1687 (NL)

Lov 1. juli 1887 nr. 5, om Rettergangsmaaden i Straffesager (strpl. av 1887)

Lov 22.mai 1902 nr. 10, Almindelig borgerlig Straffelov (strl.)

Lov 12. mai 1961 nr. 2, om opphavsrett til åndsverk m.v." (åvl.)

Lov 22.mai 1981 nr. 25, om rettergangsmåten i straffesaker (strpl.)

Lov 23. juni 1995 nr. 39, om telekommunikasjon (teleloven) (opphevet)

Lov 21. mai 1999 nr. 30, om styrking av menneskerettighetenes stilling i norsk rett (mnskrl.)

Lov 7. juli 2003 nr. 85 om elektronisk kommunikasjon (e-koml.)

Lov 17. juni 2005 nr. 90, om mekling og rettergang i sivile tvister (tvl.)

Lov 29. mai 1981 nr. 38 om viltet (vilt.)

5.3 Forskrifter

Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste 16. feb. 2004 nr. 401 (ekomforskriften)

Forskrift om behandling av personopplysninger 15 des. 2000 nr. 1265 (personopplysningsforskriften)

5.4 Forarbeider

5.4.1 Stortingsmeldinger

St.meld. nr. 21 (2007-2008) Samspill. Et løfte for rytmisk musikk.

5.4.2 Odelstingsproposisjoner

Ot.prp.nr.31 (1997-1998) Om lov om telekommunikasjon (teleloven)

Ot.prp.nr. 64 (1998-1999) Om lov om endringer i straffeprosessloven og straffeloven mv. (etterforskningsmetoder mv)

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

5.4.3 Innstilling

Instilling om rettergangsmåten i straffesaker fra Straffeprosesslovkomitéen, fra juni 1969. (Instilling 1969)

5.4.4 NOU'er

NOU 2003:27 Lovtiltak mot datakriminalitet. Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

NOU 2004:6 Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed.

NOU 2007:2 Lovtiltak mot datakriminalitet. Delutredning II.

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

5.5 Rettsavgjørelser

5.5.1 Høyesterettsavgjørelser

Rt. 1957 s. 950.

Rt. 1957 s. 1132

Rt. 1978 s. 884

Rt. 1990 s. 319

Rt. 1990 s. 1008

Rt. 1992 s. 833

Rt. 1992 s. 904

Rt. 1992 s. 929

Rt. 1992 s. 1529

Rt. 1993 s. 1303

Rt. 1994 s. 1521

Rt. 1995 s. 421

Rt. 1996 s. 864 (Ringvold)

Rt. 1996 s. 1114 (Løgndetektor)

Rt. 1997 s. 470

Rt. 1998 s. 1945

Rt. 1998 s. 1839

Rt. 1999 s. 1944

Rt. 1999 s. 1115

Rt. 1999 s. 2063

Rt. 2000 s. 996 (Bøhlerdommen)

Rt. 2001 s. 44

Rt. 2002 s. 557

Rt. 2003 s. 359

Rt. 2004 s. 1063

Rt. 2004 s. 858

Rt. 2005 s. 833.

Rt. 2007 s. 1217.

HR-2008-206

5.5.2 Underrettsavgjørelser

TSTVG-2002-634

LA-2003-83

LB-1997-1527

TOSLO-2004-41422

LG-2008-150465.

TSTVG-2005-62640

LH-1998-892

5.5.3 Europeiske menneskerettsdomstol (EMD)

Geerings v. The Netherlands, The European Court of Human Rights, Strasbourg, 1 Mars 2007.

Barberà, Messegué and Jabardo v. Spain, The European Court of Human Rights, Strasbourg, 6 December 1988.

5.6 EU direktiv.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. (datadirektivet)

5.7 Bøker

Andenæs I (1994)	Andenæs, Johs. Norsk straffeprosess. Bind I. 2. utg. Oslo, 1994
Andenæs I (2000)	Andenæs, Johs. Norsk Straffeprosess, Bind I, 3. utg. Oslo, 2000
Andenæs II (2000)	Andenæs, Johs. Norsk Straffeprosess, Bind II, 3. utg. Oslo, 2000
Bjerke I (2001)	Bjerke, Hans Kristian og Keiserud, Eirik. Straffeprosessloven Kommentarutgave. Bind I. 3. utgave, 2001.
Bratholm (1980)	Bratholm, Anders. Stafferett og samfunn. Alminnelig del. Oslo. 1980
Bratholm (2008)	Bratholm, Anders. Eskeland, Ståle. Justismord og rettsikkerhet. Oslo, 2008.
Eskeland (2006)	Eskeland, Ståle. Strafferett. 2.utgave. Oslo, 2006.
EØS-rett (2004)	EØS-rett. Frederik Sejersted ... [et al.]. 2.utg. Oslo, 2004.
Hov I (2007)	Hov, Jo. Rettergang I. Oslo, 2007
Hov II (2007)	Hov, Jo. Rettergang II. Oslo, 2007
Hov III (2007)	Hov, Jo. Rettergang III. Oslo, 2007
Mæland (1999)	Mæland, Henry John. Innføring i alminnelig strafferett. 2. utg. Bergen, 1999.
Strandbakken (2003)	Strandbakken, Asbjørn. Uskyldspresumsjonen. Bergen, 2003.
Sunde (2006)	Sunde, Inger Marie. Lov og rett i cyberspace. Bergen, 2006.
Slettan (1997)	Slettan, Svein og Øye, Torill M. Forbrytelse og straff. Oslo, 1997.

5.8 Lovkommentarer

Sitert dato i parentes.

Haugland (2009) Haugland, Geir Sunde. Kommentar til straffeprosessloven. I: Norsk lovkommentar nettversjon. [sitert 01.04.2009]

Hustad (2009) Hustad, Knut-Fredrik. Kommentar til straffeprosessloven. Norsk lovkommentar nettversjon. [sitert 01.04.2009]

JD (2009) Justisdepartementets tolknings uttalelse. Forholdet mellom taushetsplikten etter straffeprosessloven § 118, jf. § 230 fjerde ledd og vitneplikten etter straffeprosessloven § 108. [sitert 01.04.2009 på rettsdata.no under strpl. § 230.]

Møse (2009) Erik Møse og Jørgen Aall t.o.m. 2005, Ragnar Nordeide f.o.m. 2006. Norsk lovkommentar nettversjon. [sitert 15.04.2009]

Rønnevig (2009) Rønnevig, Leif-Henrik. Kommentar til ekomloven. Norsk lovkommentar nettversjon. [sitert 01.04.2009]

5.9 Artikler

Sitert sted og dato i parentes.

Høgtveit (2008) Høgtveit, Einar. Lagring av trafikkdata. Fra Økokrim. 2008. [sitert 03.03.2009]
http://www.okokrim.no/aktuelt_arkiv/artikler/TfS308_Hogetveit_datalagring.pdf

ISSA (2000) Elektronisk handel - visjon og virkelighet. Nettavis ved Institutt for sosiologi og statsvitenskap" april 2000. [sitert 12.12.08]
www.svt.ntnu.no/iss/issa/0004/000406.shtml

Kripos (2003) Huuse, Arne. Kripos. Overgrep samfunnet ikke aksepterer. 2003. [tips.kripos.no 10.03.2009]

NorSIS (2008) Norsk senter for informasjonssikring. Trådløst nettverk. 2008. [sitert 12.12.2008]
http://www.norsis.no/veiledninger/teknisk/Tradlost_nettverk.html

PT (2008) Post – og Teletilsynet. Begjæring om fritak fra tilbyders lovpålagte taushetsplikt. 2008. [http://www.npt.no 20.02.2009]

Slettemark (2007) Slettemark, Guro. Hele folket under mistanke. I: Lov & Data nr. 89. April 2007. [www.lovdata.no 20.03.2009]

Sunde (2000) Sunde, Inger Marie. IKT-kriminalitet: Etterforskningsmetoder og personvern, Nordisk Tidsskrift for Kriminalvidenskab, nr. september. 2000. [sitert 10.02.2009]
http://www.okokrim.no/aktuelt_arkiv/artikler/Etterforskingsmetoder_og_personvern.html

Sunde (2007) Sunde, Inger Marie. Jeg vet jeg ikke er paranoid. I: Lov&Data nr.89 September 2007. [lovdata.no 01.04.2009]

Teknologirådet (2005) Teknologirådet. Elektroniske spor og personvern. 2005. [sitert 20.02.2009]
www.teknologiradet.no/dm_documents/Elektroniske_spor_og_personvern_web_GvB9r.pdf

5.10 Personlige meddelelser

Willassen (2008) Willassen, Svein Yngvar. Epost 09.10.2008.
Willassen (2009) Willassen, Svein Yngvar. Epost 01.04.2009.

5.11 Internettsider

Sitert dato i parentes.

www.internetworldstats.com/stats (24.11.2008).
http://no.wikipedia.org/wiki/Internett#Web (01.04.2009)
http://no.wikipedia.org/wiki/IP-adresse (20.04.2009)
http://cqcounter.com/whois/ (10.03.2009)
www.wardriving.com/about.php (05.03.2009)
www.torproject.org (10.03.2009)
www.whois.net (20.03.2009)
www.quotesandsayings.com/gbillgates.htm (24.04.2009)