UNIVERSITETET I OSLO
Institutt for informatikk

Elektroniske dokumenter som bevismateriale

Masteroppgave

(60 studiepoeng)

Robert Didriksen

1. august 2008

SAMMENDRAG

Problemstillingen i denne oppgaven er todelt: (P1) Hvordan kan man på best mulig måte sikre autentisiteten til elektroniske dokumentbevis? (P2) Kan man gjøre noe spesifikt for å ivareta personvernhensyn i møte med elektroniske dokumentbevis? Det første spørsmålet blir forsøkt besvart ved å foreta en grundig redegjørelse for begreper, teori, praksis og gjeldende lover og regelverk som er knyttet til elektroniske dokumentbevis. I tillegg reises to delspørsmål som omhandlet hvorvidt metadata og hashverdier kan brukes som ledd i autentifisering. For å prøve å besvare dette gjennomføres noen enkle tester i analyseverktøyet Metaviewer for å sjekke autentisiteten til et utvalg av elektroniske dokumenter etter hvert som disse blir utsatt for ulike lagrings- og kopieringsmåter. Oppsummert ser det ikke ut til å eksistere noen måter som sikrer en hundre prosent autentifisering. Det foreligger heller ikke klart definerte rutiner for sikring av autentifisering. Likevel gir testene holdepunkt for at man bør fortrekke hashverdier over metadata når man skal undersøke ekthet på de typer dokumenter som ble testet. Manipuleringstesten ga holdepunkt for at hashverdier er en god indikator på hvorvidt det har skjedd endringer i metadata. Det bør likevel nevnes som en begrensning at man på forhånd må kjenne hashverdien fra originaldokumentet for at en eventuell autentifisering kan skje. Det ser uansett ut for at enkelte metoder er bedre enn andre, og at det er mulig å komme frem til slike konklusjoner bare på grunnlag av noen få enkle tester. Fremover er det svært viktig at forskningen på dette feltet etterstreber tydeligere retningslinjer for prosedyrer på autentifisering. Det andre spørsmålet blir behandlet ved en gjennomgang av problemstillinger som henger sammen med personvern, så vel som en gjennomgang av personvernteori og sider ved personopplysningsloven som angår innhenting av elektroniske bevis. Konklusjonen på (P2) er at man i dag står overfor mange utfordringer i forhold til personvern som følge av en lovgivning som enda ikke er tilpasset elektroniske bevis. Det mest spesifikke man kan gjøre for å ivareta personvernhensyn må på overordnet nivå bli å utarbeide et oppdatert lovverk. I den enkelte sak er det viktig å følge det gjeldende lovverket når man innhenter personopplysninger. Avslutningsvis i oppgaven følger et forslag til sjekkliste for best mulig innhenting, sikring og lagring av elektroniske dokumentbevis. Her er både tekniske og juridiske hensyn inkludert.

Innhold

Figurer

FORORD

Denne oppgaven ble skrevet som en del av min mastergrad ved Institutt for Informatikk ved Universitet i Oslo. Denne oppgaven kan være et bidrag til det tverrfaglige samarbeidet mellom IKT og jus. Gjennom arbeid med oppgaven har jeg fått mulighet til å sette meg inn i mange nye og spennende områder der det juridiske og personvernmessige møter informasjonsteknologi, og jeg har lært mye om hvilke utfordringer det fører med seg.

Jeg ønsker å takke veilederen min ved Universitet i Oslo, Odd Aurmo og ekstern veileder Kjell Thorvaldsen ved Devoteam daVinci for gode og konstruktive innspill. Jeg vil i tillegg takke Frank Almås, Kine Steinsvik og Lars Berntsen for innspill og diskusjon på den juridiske delen.

Vil også takke familien og til slutt en kjempestor takk til Kristin som har vært en god støttespiller gjennom hele prosessen.

Trondheim, juli 2008
Robert Didriksen

1. INTRODUKSJON

Helt siden oldtiden har det vært behov for å kunne sikre at informasjon er autentisk. Både internasjonal handel og etter hvert også regnskapsføring skapte et behov for andre kommunikasjonsmåter enn muntlig overføring. Dette løste man ved å nedtegne informasjonen som symboler på leirbrikker. I boken "landskap med tegn" skriver Jon Bing om hvordan man kunne sikre autentisiteten til viktig informasjon langs oldtidens karavaneruter:

"Avtrykk av brikkene ble presset inn i en våt leirkonvolutt, deretter ble brikkene lagt ned i konvolutten som så ble presset sammen slik at det formet en hul ball. De originale brikkene raslet rundt inne i den tørkede leirkonvolutten. Var man i tvil om avtrykkene på utsiden virkelig stemte med de lagrede brikkene, var det bare å bryte i stykker bullaen. Man hadde funnet en enkel måte å garantere autensitet og samtidig det vi jurister av og til kaller uavviselighet: Det kunne konstateres med sikkerhet om det hadde skjedd noe tukling med representasjonen av brikkene på utsiden av konvolutten. Bullaen fungerte som et slags fraktbrev eller konnossement langs oldtidens karavaneruter (Bing, 1998).

Mye har skjedd i utviklingen av metoder for å sikre informasjon siden "bullaens" tid. Bare i løpet av de siste tiårene har den raske utviklingen innen IKT ført med seg et mangfold av nye informasjonskanaler og lagringsformer. Elektronisk kommunikasjon har etter hvert tatt over for mange andre former for kommunikasjon. E-post er et eksempel på en uformell, elektronisk kommunikasjonskanal som har blitt stadig mer vanlig. Andre eksempler er elektroniske dokumenter og kommunikasjonsformer som for eksempel såkalte *øyeblikksmeldinger*, slik som msn eller sosiale nettverk som facebook . Man kan gjennom flere ulike elektronisk baserte tjenester, som blant annet Google docs, skrive og legge ut dokumenter på nettet og dele disse med andre slik at flere personer kan skrive i og redigere de samme dokumentene. Den elektroniske informasjonen kan kopieres og kommuniseres hurtig, og derfor vil det i mange tilfeller eksistere flere kopier av et dokument. Disse er som regel identiske i utgangspunktet, men kan lett endres (Thorvaldsen, 2006). Muligheten for å distribuere dokumenter ut til flere

personer bare ved noen enkle tastetrykk gjør det uoversiktiglig å kontrollere hva som er de originale dokumentene, hva som er kopier og hvilken av kopiene har blitt redigert.

I dag foregår det meste av interaksjonen mellom mennesker, bedrifter og offentlig forvalting gjennom elektronisk kommunikasjon. Det kan for eksempel være gjennom usikret e-post og ubeskyttede vedlegg som Word dokumenter, Excel regneark eller andre typer tekstbehandlingsdokumenter. Et problem det vies stadig mer oppmerksomhet til, er at disse dokumentene med enkelhet kan manipuleres og tas utskrift av (Føyen, 2006). Særlig når elektroniske dokumenter skal brukes som bevismateriale i retten skaper slike forhold komplikasjoner. Elektronisk informasjon har andre egenskaper enn vanlige, papirbaserte dokumenter, noe som gjør at de elektroniske bevisene skiller seg fra vanlige bevis. Forandring av egenskapene til elektroniske dokumenter kan skje utilsiktet ved at for eksempel noen åpner et digitalt dokument for så å lagre det igjen. Da kan egenskaper som er usynlige for et utrent øye (for eksempel såkalte metadata) ved dokumentet ha blitt endret. Det har i takt med den økte tilgang på digital informasjon reist seg et stadig større behov for at det utarbeides standarder og rutiner for fremlegging av elektroniske bevis i retten. Elektroniske dokumenter som bevis vil være et hovedanliggende i denne oppgaven.

Det meste av informasjonen blir i dag lagret elektronisk. Ifølge organisasjonen Cybex, et spansk firma som spesialiserer seg på elektroniske bevis, foreligger hele 90 prosent av alle dokumentene i et selskap i elektronisk form og bare 30 prosent av disse er skrevet ut i papirformat. Når det gjelder elektroniske bevis i retten ser man konsekvenser av denne utviklingen. Tradisjonelle bevis slik som papirdokumenter er i ferd med å forsvinne, eller i hvert fall bli langt mindre vanlige. Derfor er det også et økende behov for nye prosedyrer i behandlingen av digitale dokumenter. (Cybex, 2008).

I dagens rettspraksis er det nok å legge frem en papirkopi av det elektroniske beviset, noe som faktisk innebærer at informasjon som kan være viktig i saken ikke kommer frem. Dette kan dreie seg om såkalt *metadata* som for eksempel forteller når dokumentet sist ble endret, sendt eller mottatt (Thorvaldsen, 2006). Det kan også dreie seg om informasjon i form av hashverdier

av dokumentet, som for eksempel kan brukes for å bevise kopiens originalitet (Losey, 2007). Både metadata og hashverdier blir testet og forklart grundigere lenger ut i oppgaven.

Den vanligste måten å oppbevare dokumenter på i dag er elektronisk oppbevaring. Dette medfører at stadig mer digitalt materiale blir knyttet til rettstvister, og etterforskere sikrer, analyserer og presenterer elektroniske materiale oftere enn for noen år siden. Ettersom digitale bevis representerer helt nye former for bevismidler er også kunnskapsnivået blant dommere og advokater begrenset (Riise, 2006). Det gjør at norsk lovgivning ikke har rukket å tilpasse et regelverk som gir retningslinjer for hvordan man skal håndtere digitalt materiale(Larsen, 2007). På grunn av dette er heller ikke lovgivningen utformet på en slik måte at det per i dag eksisterer klare retningslinjer for hvordan man skal håndtere digital informasjon (Thorvaldsen, 2006).

For å belyse hvilke problemstillinger som kan følge i kjølvannet av den raske utviklingen innen IKT, skal jeg innledningsvis bruke to konkrete eksempler fra media. Det første omhandler forfalskning og det andre omhandler ulovlig innsyn i e-post. Det første omhandler en sak som fikk mye medieomtale i januar 2008, der Morgan Andersen sto tiltalt for å ha forfalsket kontraktspapirer til fotballspilleren John Obi Mikel. iflg straffelovens § 182 første ledd første straffealternativ: *"for i rettsstridig hensikt å ha benyttet som ekte eller uforfalsket et ettergjort eller forfalsket dokument".* I dette tilfellet sto Andersen tiltalt for å ha forandret datoen på når kontrakten med fotballspilleren ble skrevet. I tillegg skal han ha byttet om noen sider i kontrakten og skrevet under med falsk underskrift (Nybøe, 2007). I Andersen-saken var det dataanalyse gjort av Kripos som avslørte at datoen var endret to uker frem i tid (Mæland, 2008). Andersen ble på bakgrunn av bevisene i saken dømt den 26.mars 2008. Det er verd å merke seg at dette var en straffesak, og at påtalemakten dermed hadde mulighet til å beslaglegge bevismateriale som pc og telefon for å kunne foreta en grundig analyse av bevisene. I sivilsaker har man ikke denne muligheten. Problemstillinger knyttet til lovverket rundt beviservervelse vil bli nærmere drøftet senere i oppgaven.

Det andre eksempelet jeg skal nevne dreier seg om ulovlig ervervelse av elektronisk materiale, nemlig e- post saken i redningsselskapet der Monica Kristensen Solås ble suspendert som generalsekretær i Norges Redningsselskap i 2005, på grunn av at hun beordret ulovlig innsamling av bevis mot egen personalsjef (Aftenposten, 2005). Den enkle tilgjengeligheten på digital informasjon skapte en ny nisje for å begå innsyn i private opplysninger. Disse sakene representerer bare to av mange eksempler relatert til manipulering og ulovlig innsyn i elektroniske dokumenter og e-post.

Det som er nevnt til nå belyser noen av utfordringene rundt innsamling, lagring og validering av elektroniske bevis. Som følge av den nevnte utviklingen reises det en rekke nye spørsmål av juridisk, etisk, og samfunnsmessig art (Coll & Schartum, 2004), i tillegg til mange tekniske utfordringer. I oppgaven omhandles også spørsmål om hvordan menneskelige hensyn blir ivaretatt gjennom personvernet når innsamling av elektroniske bevis skal gjøres og i hvilken grad arbeidsgivere kan tillate seg å gjøre dette. Progresjonen innen IKT- feltet er i dag med på å trekke nye grenser i forhold til mange etiske spørsmål, som for eksempel hvordan man bør stille seg til arbeidsgivers krav om innsyn i private mapper og e-post. personvernhensyn tas opp i kapittel 5.

Elektroniske bevis i seg selv er ikke ”rettslig bindene bevis”, men har beviskraft av ulik grad. Det er opp til advokatene på begge sider å overbevise dommerne om hvilken beviskraft en bestemt dokumentasjon skal ha i den aktuelle saken, hva som bør vektlegges i hver enkelt sak, og hvordan man skal håndtere konkrete elektroniske dokumenter for at det skal få størst mulig bevisverdi (Føyen, 2006). Dette er en stor oppgave som det enda er knyttet mye usikkerhet til, men det er i dag flere prosjekter som på internasjonalt nivå som tar sikte på å øke forståelsen av hvordan elektroniske bevis må håndteres og legges frem slik at man kan få en tilfredsstillende beviskvalitet. Det er nødvendig å etablere nye rutiner og systemer for strukturert behandling. Det vil si innsamling og lagring av elektroniske dokumenter med formål om i etterkant å kunne dokumentere hva som faktisk har foregått (Føyen, 2006).

1.1 Motivasjon

At det i dag heftes en del usikkerhet til bruken av elektroniske bevis i retten er grunnlag og motivasjon for denne oppgaven. Det finnes svært mange typer elektronisk informasjon som kan brukes som bevis, som for eksempel: e-post, loggfiler, sms, og dokumenter. Fordi det eksisterer mange varianter av elektronisk informasjon, og at det er relativt lett å manipulere slik informasjon, har jeg i løpet av studietiden utviklet en spesiell interesse for hvordan man bør håndtere elektroniske bevis i rettssaker. Jeg har i denne oppgaven valgt å fokusere på *elektroniske dokumenter* og i hvilken grad man kan ivareta autentisitet til dokumentene. På grunn av sakens kompleksitet og denne oppgavens tidsbegrensning kan man ikke tillate seg å se på alle typer elektronisk informasjon. Selv om jeg skriver om elektroniske dokumentbevis vil mye være relevant i forhold til håndtering av andre typer elektroniske bevis.

Jeg vil sette søkelys på hvordan man kan bevare dokumentenes autensitet i den såkalte *forvaringskjeden*. Det vil si bevisets gang fra det blir sikret og lagret til det blir lagt frem som bevis i retten. Man kan også undersøke *verdikjeden* til det digitale beviset, noe jeg har valgt å fokusere litt mindre på. Med verdikjeden menes livsløpet til et elektronisk bevis. Motivasjonen bak å velge hovedsakelig å se på forvaringskjeden heller enn verdikjeden virker for meg mest naturlig sett ut fra oppgavens problemstilling.

I tillegg til selve håndteringen av elektroniske bevisdokumenter er jeg i oppgaven interessert i å belyse *personvernet* i sammenheng med innhenting av elektroniske bevis. Dette fordi det oppstår nye utfordringer i sikringen av enkeltindividets rettigheter som følge av den raske utviklingen innen IKT. Utvikling av stadig nye former for informasjon reiser nye spørsmål knyttet til personvern. Jeg ønsker å se elektroniske dokumentbevis i et personvernperspektiv, fordi nesten all behandling av slike bevis skjer i nær sammenheng med overveielser i forhold til personvern. Langt på vei kan man si at det er nettopp personvernet som legger føringer på hvordan man kan forholde seg til elektroniske bevis. Derfor vil det etter min mening være unaturlig å skrive en oppgave om elektroniske bevis uten å berøre de spørsmål som reiser seg i forhold til enkeltmenneskets rettigheter og privatsfære.

1.2 Problemstilling

Problemstillingen i denne oppgaven er todelt. Man kan si at den har en teknisk og en juridisk del:

(P1): hvordan kan man på best mulig måte sikre autentisiteten til elektroniske dokumentbevis?

Jeg vil i forbindelse med (P1) prøve å besvare følgende delspørsmål:

- I hvilken grad klarer man ved hjelp av metadata og hashverdier å sikre autentisiteten til et elektronisk dokument ved forskjellige kopierings- og lagringsmåter?
- Er bruk av både metadata og hashverdier nødvendig for å bevare autentisitet tilelektroniske bevis, eller er en metode å foretrekke over den andre?

(P2): Kan man gjøre noe spesifikt for å ivareta personvernhensyn i møte med elektroniske dokumentbevis?

Målet med oppgaven er blant annet å utarbeide en sjekkliste for sikring, lagring og validering av digitale bevis. Tanken bak en slik sjekkliste er å bidra til å legge grunnlag for best mulig å kunne ivareta autentisiteten til de elektroniske bevisene, slik at man kan få en mest mulig rettferdig og korrekt vurdering av dokumentene i en rettssak.

1.3 Avgrensning og disposisjon

I oppgaven skal jeg se på mulige metoder for behandling og testing av elektroniske dokumentbevis, og i hvilken grad de involverte parter best mulig kan ivareta integriteten til de digitale bevisene slik det kan ses i problemstillingen er dette en oppgave som fokuserer på tverrfaglighet. De spørsmål som skal besvares krever innsikt i to store og nokså ulike fagfelt; teknologien og jussen. Kompleksiteten dette fordrer gjør det nødvendig å gå igjennom flere ulike områder. Som et supplement til gjennomgangen av teori, praksis og relevant forskning på området vil jeg teste noen ulike dokumenters metadata og hashverdier for å finne ut i hvilken grad de elektroniske dokumentene klarer å beholde sin integritet ved forskjellige former for behandling. Jeg vil også foreta manipulasjon av metadata som en del av testingen.

Denne oppgaven har i tillegg til introduksjonsdelen (1) åtte videre deler, eller kapittel. Disse omhandler: (2) elektroniske bevis, (3) autentisitet, (4) rettsprosessen, (5) personvern, (6) dataetterforskning, (7) testing av elektroniske dokumenter, (8) drøfting og forslag til sjekkliste, og (9) en avslutnings- og konklusjonsdel.

I delen som omhandler elektroniske bevis vil jeg først gi en redegjørelse for bevis, bevisregler og elektroniske bevis. Deretter tar jeg for meg ulike utfordringer av teknisk og juridisk art som følger på grunn av tilgangen på elektroniske bevis. Denne delen, sammen med det neste kapittelet om autentisitet vil fungere som grunnlag for de neste oppgavedelene.

I kapittelet om rettsprosessen vil jeg gi en innføring i sivil- og straffesaker. Neste kapittel omhandler utfordringer knyttet til personvern og i hvilken grad personvernet virker inn på håndteringen av elektronisk informasjon.

I kapittel 6 tar jeg for meg dataetterforskning. Her vil jeg se på prosedyrer som blir brukt i dag, så vel som tekniske utfordringene man kan møte ved håndtering av elektroniske bevis.

I del 7 vil jeg utføre testing av elektroniske dokumenter. Dokumentene jeg skal teste er: MS Word 2007, MS Word 2003 og OpenOffice dokumenter. Årsaken til at MS Word og OpenOffice blir brukt i testingen er at disse er noen av de vanligst brukte tekstbehandlingsprogrammene. Disse verktøyene blir brukt i både offentlige og private organisasjoner i Norge så vel som i internasjonal sammenheng. Metoden for testing av metadata og hashverdier, samt manipulasjon av metadata blir beskrevet i underkapittelet om testmetode i del 5. Resultatene vil også bli presentert i denne delen. Analyseverktøyet ble brukt for å undersøke hvilke metadata og hashverdier som ble generert når dokumentene ble utsatt for forskjellige lagrings- og kopieringsmåter. I tillegg ble det utført en metadatamanipulasjon i MS Word 2003. Dette ble gjort for å undersøke hvilke aktører som kan endre, manipulere og slette metadata.

Del 8 er drøftingsdelen. Jeg vil her trekke sammen tråder fra de foregående delene av oppgaven. Resultatene fra testene vil bli brukt her, i forbindelse med diskusjon om hvorvidt

metadata og hashverdier kan sikre validiteten til digitale dokumentbevis. Drøftingsdelen inkluderer et forslag til sjekkliste for sikring, lagring og validering av elektroniske bevis.

Den niende og siste delen inneholder en kort avslutning på oppgaven, og en konklusjon som blant annet understreker viktigheten av videre arbeid på feltet.

Før jeg går inn på de overnevnte delene i oppgaven følger henholdsvis en begrepsavklaring og et kort avsnitt om fremgangsmåten som er brukt i arbeidet med å besvare problemstillingen.

1.4 Begrepsavklaring

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

Dokument er en logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting framvisning eller overføring. Et dokument kan være på papir, elektronisk medium, eller virken som helst annet medium som kan være bærer av informasjon. Dokumentet kan inneholde tekst, tegninger, grafikk, fotografier, video, tale m.m. Et dokument kan bestå av et flere dokument som for eksempel vedlegg (*Noark-5 Norsk arkivsystem*, 2007; *Uten penn og blekk*, 2001)

Dokumenthåndtering er behandling av alle typer dokumenter; både uferdige og ferdige arbeidsdokumenter og arkivdokumenter (*Uten penn og blekk*, 2001).

Bevis er et middel som skal dokumentere et påstått faktum.
Beviset kan være personlig (vitnebevis) eller såkalt tinglig, dvs. reelle bevis f eks et åsted, gjenstander og dokumenter (("Juridisk ordliste," 2008)).

Autentisk er noe som er ekte eller pålitelig. Det vil si at dokumentet er hva det gir seg ut for å være. Et eksempel er at identiteten til partene i en elektronisk kommunikasjon er riktig ("authentic," 2008; *Noark-5 Norsk arkivsystem*, 2007).

Autentisering er en prosess som har som mål å bekrefte en påstått identitet (*Uten penn og blekk*, 2001)**.**

Dataintegritet er en tilstand som eksister når data er uforandret og ikke har blitt modifisert, endret eller ødelagt på en utilsiktet eller ondartet måte (CNSS, 2006)

Hashverdi er et tall som er et resultat av å bruke hash-algoritme på elektroniske dokumenter. Hash- algoritme er en matematisk funksjon som lager et elektronisk ”fingeravtrykk” av et sett med data. Fingeravtrykket er alltid den samme for like data og alltid forskjellig for ulik data. Hash algoritmen blir ofte brukt til å sikre integriteten på data. Hvis for eksempel et dokument har forskjellig fingeravtrykk før og etter en overføring kan det ha blitt feil i overføringen eller at noen har endret dokumentet ("Informasjonsteknologi
Adminstrasjon av informasjonssikkerhet ", 2001). Hashverdien er et unikt ”digitalt fingeravtrykk” som er med på å gjøre dokumentet unikt(*Uten penn og blekk*, 2001).

Digital signatur er et dataelement som følger en elektronisk melding eller et dokument og som knytter dokumentet til et individ, maskin eller datasystem(*Uten penn og blekk*, 2001). Dette tillater mottakeren å bevise hvor dokumentet kommer fra og om dokumentet er forfalsket. Man kan også si at digital signatur er en kryptografisk prosess brukt til å sikre meldingens opprinnelse, autensitet og integritet (CNSS, 2006)

Metadata er data som beskriver eller definerer andre data. I for eksempel et elektronisk dokument vil det være informasjon om dokumentets struktur, innehold og kontekst (*Noark-5 Norsk arkivsystem*, 2007)

Digital etterforskning er praktisk bruk av metoder, rammeverk og verktøy for bevaring, innsamling, validering, identifisering, analyse, tolkning, dokumentasjon og presentasjon av digital informasjon(Larsen, 2007).

1.5 Fremgangsmåte

Spørsmålene i problemstillingen ble besvart ved hjelp av litteratursøk og informasjonsinnhenting på internett. Det ble blant annet foretatt søk i databaser som IEEE, ACM, Google Scolar, Google og Informatikkbiblioteket. For å innhente informasjon fra det praktiske feltet ble det gjort ustrukturerte intervju i form av e-post- korrespondanse med advokat og en Practice Area Manager, som jobber med arkiveringsrutiner i en stor bedrift. Informert samtykke ble innhentet. Jeg valgte ustrukturert intervjuform da dette er et felt det er gjort lite forskning på. Jeg ønsket derfor ikke å legge føringer på informantenes svar

I tillegg ble det utført tester på elektroniske dokumenter. Målet med testingen var å se på om metadataene og hashverdiene kunne være med på å sikre integriteten til elektroniske dokumenter ved forskjellige lagrings- og kopieringsmåter. Undersøkelse av metadata og hashverdier ble basert på MS Word 2003, MS Word 2007 og Open Office dokumenter (ODF), og et utfyllende metodekapittel knyttet til testingen følger i oppgavens kapittel 7.

2. ELEKTRONISKE BEVIS

I denne delen vil jeg foreta en gjennomgang av oppgavens mest sentrale begrep; bevis. Jeg vil se på de ulike lover og bestemmelser som legger føringer på håndteringen av bevis i retten.

2.1 Hva er bevis?

Bevis kan defineres som et middel for å godgjøre en saks rettslige relevante omstendighet (Coll & Schartum, 2004). Bevis kan også bety to ting; For det først kan det bety "bevismidler" som dokumentbevis og vitneprov. For det andre kan bevis bety "bevisresultat". Eksempel på det kan være at man kan si at det ikke forligger tilstrekkelig bevis for at tiltalte er skyldig, eller at en avtale er inngått selv om det foreligger en mengde bevismidler. *Bevistema* er det forhold som er formålet med bevisføringen. Det vil si de faktiske forhold som har rettslig betydning eller begrunner den rett en krever dom for. (Hov, 2007).

Bevisreglene er viktige, det hjelper ikke om en part har et faktisk grunnlag for det krav som fremmes, dersom retten ikke kan bygge på dette. Dette vil kunne oppstå i situasjoner hvor for eksempel partene er rettslig avskåret fra å føre bevis for det faktiske forholdet på grunn av reglen om bevisforbud. Det kan for eksempel være et dokument, som motparten sitter med og ikke opplyser om det, kanskje fordi han ikke er pliktig å gjøre det. Det er også mulig at reglen om bevisbedømmelsen kan føre til at retten bygger på et annet faktum enn det korrekte, selv om det er i samsvar med bevis som er ført (NOU:32, 2001).

Rettsreglen om bevis kan føre til at det blir lagt et annet faktum til grunn for avgjørelsen enn det som er korrekt. Idealet om bevisregelen som sikrer bevisgrunnlag og en korrekt bevisbedømmelse, må til en viss grad bøye av for andre viktige hensyn man må ivareta i prosessen. Dette kan gjelde *bevisforbud* ut fra personvernhensyn eller andre viktige hensyn (NOU:32, 2001)For at det skal være lovlig for private å behandle personopplysninger må det være et alminnelig rettslig grunnlag, jf pol 8.

2.2 Bevismidler og bevisføring

Fremføring av forskjellig bevismidler overfor retten kalles *bevisføring*. Bevismidlene kan deles inn i flere kategorier:

- Realbevis
- Vitnebevis
- Partsforklaringer som bevis
- Sakkyndige
- Personundersøkelse og mentalobservasjon (bare i straffesaker)

Realbevis utgjør den viktigste bevisfaktoren i denne oppgaven med hovedvekt på elektroniske dokumenter og andre former for elektronisk lagret informasjon. Realbevis er definert i tvl. § 26 - 1:

"Realbevis er personer og gjenstander (fast eiendom, løsøre, dokumenter, elektronisk lagret materiale mv.) hvor personen eller gjenstanden, eller dens egenskaper, tilstand eller innhold, inneholder informasjon som kan ha betydning for det faktiske avgjørelsesgrunnlaget i saken."

Hov (Hov, 2007) mener i den sammenheng at definisjonen av realbevis ikke er spesielt vellykket. Han sier det ikke virker naturlig språklig sett at en person eller fast eiendom "innholder informasjon". Men at det typiske for realbevis er å observere eller undersøke en gjenstands eller personers fysiske egenskaper og ut fra det kan man trekke slutninger om faktiske eller relevante forhold. Skriftlige bevis som papirdokumenter og elektronisk lagrede dokumenter (skrift)skiller seg fra andre realbevis ved at det er innholdet som tillegges betydning og ikke deres rent fysiske egenskaper (Hov, 2007)

Straffeprosessloven har ikke særlige bestemmelser vedrørende realbevis verken om dokumentbevis eller andre reelle bevismidler.

Partenes rett til å føre de bevis de måtte ønske er fastslått i tvl § 21-3 (1). I straffesaker er det ingen tilsvarende lovfesting av regelen, men det hersker liten tvil om at det samme gjelder her

(Hov 2007). Både i sivil og straffesaker kan partene legge frem de bevis som de mener er til deres fordel, men de er ikke pliktig til å legge frem bevis. Tvl. § 21.4 omfatter en prinsipiell begrensning Det skal være et overkommelig forhold mellom betydningen av saken og omfanget av bevisførselen. Hvis retten synes bevisførselen er for omfattende kan det besluttes at bevisføringen skal begrenses (Hov, 2007).

Hensikten med *bevisbedømmelse* er å fastslå hvilke fakta som skal legges til grunn for en dom. At bevisbedømmelsen er fri betyr at det ikke er regler for hvor mye man skal vektlegge hvert enkelt bevis. Tidligere var det bestemte regler på hvordan bevis skulle føres, men i dagens rettsvesen gjelder prinsippet om fri bevisbedømmelse (Hov, 2007).

Bevisbedømmelse er ofte vanskelig i en sak og de faktiske forhold kan være belyst ved en rekke bevis. Det kan være dokumentert i form av brev mellom de involverte før tvisten eller det kan være uklare eller motstridende vitneforklaringer. *Vitneforklaringer* kan være dårlige bevis, menneskets hukommelse kan svikte eller den kan være selektiv, selv om den enkeltes forklaring blir fremført klart og sikkert. *Dokumentbevis* kan være gjort en posisjonering fra partenes side med tanke på en mulig fremtidlig tvist og kan være utformet på basis av dette (*Uten penn og blekk*, 2001). Retten står fritt i sin bevisbedømmelse, men det er ikke alle bevis den har rett til å ta til vurdering. Bevisene må gå frem av de dokumenter eller rettsmøter som skal danne grunnlaget for dommen. Hov kaller dette for ”det formelle avgjørelsesgrunnlaget” for dommen (Hov, 2007, 335). Men retten kan også legge til grunn kjensgjerninger selv om det ikke fremgår av det formelle avgjørelsesgrunnlaget (tvl. 21.2 (3)). Med det mener man at det fremgår av loven at dommeren kan bygge på faktiske sammenheng, eller kjensgjerninger han har kunnskap om på grunnlag av sin alminnelige livserfaring. Det gjelder også den kunnskap han har tilegnet seg gjennom sitt arbeid (Hov, 2007).

Angående elektroniske bevis og fri bevisbedømmelse så bygger det på den forståelse at dommeren skal best kunne finne frem til sannheten i saken gjennom å vurdere bevisene uten å være fastlåst av lovregler. Det er vanskelig å angi noen retningslinjer, hverken prosessuelt eller empirisk for hvordan man kan vektlegge elektroniske bevis. Dette kommer av manglende

kunnskap om rettpraksis koblet sammen prinsippet om fri bevisbedømmelse. Elektroniske bevis spenner seg over et vidt felt og derfor vil også slike bevis befinne seg i ulike bevismessige sammenheng. Derfor er det grunn til å anta at intensiteten for å prøve elektroniske bevis vil variere avhengig av om det er utelukkende elektroniske bevis i en sak eller om det inngår i en rad av flere andre bevis (Coll & Schartum, 2004).

Bevisavskjæring blir brukt når bevis blir ervervet på ulovlig eller kritikkverdig måte. I noen tilfeller kan partene i en sak innhente bevis uten hensyng til de regulering som ligger i loven. I vid forstand kan bevisavskjæring gjelde alle bevis som ikke kan fremlegges fordi lovens betingelser for å føre beviset ikke er til stede, dette kan for eksempel gjelde en person som skal vitne blir nektet fordi hans forklaring vil krenke yrkesmessig taushetsplikt eller på grunn av personopplysningsloven har innhentet bevis på ulovlig vis (Hov, 2007). Også bevis som ikke har betydning for en sak skal avskjæres. I sivile saker bedømmes bevis ut fra partenes krav om beviset er relevant for saken eller ikke (Hov, 2007).

I tilfeller der en av partene mener at bevis er innhentet på ulovlig eller kritikkverdig måte, kan det protesteres under hovedforhandlingene. Når innsigelsen er fremlagt vil retten ta stilling til protesten og beviset blir enten avskåret eller tillatt brukt (Larsen, 2007).

2.3 Elektroniske bevis

To termer blir ofte brukt til å beskrive et dokument i andre formater enn papir. De kan beskrives som elektroniske dokumenter eller digitale dokumenter. Begge termene er viser til det samme (Mason & Barrister, 2006), og vil videre i oppgaven bli brukt om hverandre. Når det dreier seg om hva som defineres som elektronisk lagrede materiale er det ingen annen avgrensning enn at *materiale må være lagret på et elektronisk lagringsmedium*.

Hovedsaklig kan man si at all aktivitet på datamaskinen blir lagret men omfanget av hva man kan finne igjen varierer i stor grad. Det vil si at mye av informasjonen som blir generert blir også lagret automatisk (Monsen, 2007). I mange applikasjoner blir sensitiv informasjon lagret som

loggfiler, ofte på upålitelige maskiner (Schneier & Kelsey, 1999) Også når brukerne anvender programfiler som Microsoft Outlook, Microsoft Excel, Microsoft Word eller andre typer tekstbehandlingsprogram vil man lagre dette som datafiler på en server eller på datamaskinens hardisk. Disse filene kan også inneholde informasjon som ikke fremkommer av utskriften. Det vil si informasjon som man legger inn i for eksempel et Word dokument som ikke vil fremkomme på utskriften. Her vil man kunne legge inn kommentarer eller annen informasjon om dokumentet. Dette kalles også metadata, det er strukturert informasjon som forteller når dokumentet ble opprett og sist gang det ble lagret. Man kan også finne informasjon om forfatteren av dokumentet og når det sist ble skrevet ut på papir. Det som kommer inn under definisjonen elektroniske og digitale dokumenter inkluderer blant annet:

- Skannet bilder av et fysisk dokument
- Filer i naturlig format slik som tekstbehandlings dokument som Microsoft Word format, regneark i Lotus 1-2-3 format, presentasjon i Microsoft Powerpoint format , PDF dokumenter og flere andre formater (osv).
- Nettverkskommunikasjon slik som e-post og øyeblikksmeldinger som for eksempel MSN.
- Digitalt genererte bilder og digitalt kodet audio og video.
- Arkiv, indekser logger og filer
- Databaser
- Arkiv av transaksjoner, spesielt finansielle transaksjoner.
- Nettsider

Denne listen illustrerer den enorme mengden av digitale bevis som blir produsert daglig muligens hvert sekund over hele kloden[1] (Mason & Barrister, 2006).

[1] *I 2004 ble ca 31 milliarder e-post sendt hver dag. Dette forventes å doble i 2006. (harvard Business review gjengitt*

Digitale bevis kan også være video fra overvåkingskamera, opplysninger om passering i bomring, bilder som er knipset i fartsbokser, utskrift fra adgangslogger, e-post og databaselogger, mobiltelefoner, datamaskiner, printere,. PDA, backup tape, CD'er DVD, nettverksrutere og i programvare og kommunikasjonsprotokoller.

Dokumenter i elektronisk format betyr at de har en rekke forskjellige kjennetegn som presenterer spesielle utfordringer som vanlig papirdokumenter ikke har. Data i elektronisk format er avhengig av spesifikke maskinvare og programvare for at man skal kunne ha tilgang til det. Det er også klart at et dokument i elektronisk format krever andre mekanismer for autentisering enn vanlige papirdokumenter. Det er også knyttet større grad av kompleksitet til et elektronisk dokument enn et fysisk dokument. Det er lett å manipulere digitalt lagret data, de kan bli kopiert, forandret, oppdatert og slettet ved noen enkle tastetrykk (Mason & Barrister, 2006).

Elektroniske bevis omfatter i utgangspunktet svært mange forskjellige former for opplysninger, men begrepet kan defineres som "et hvert digitalt materiale som er samlet for å underbygge en håndgripelig omstendighet som antas å være rettslig relevant" (Coll & Schartum, 2004). Innsamling av slikt materiale kan deles inn i to kategorier. Den første kalles *direkte innsamling* av bevis. Dette innebærer at man samler opplysninger med det formål å underbygge og dokumentere at noen har overtrådt rettsreglene det er knyttet sanksjoner til. Denne kategorien dekker tilfeller av kriminelle handlinger som er avdekket eller klart forventet. I slike sammenhenger kan en arbeidsgiver for eksempel ta beslag i arbeidstakeres filer med ulovlig innhold, eller sette opp et videokamera for å avdekke mulig kriminalitet. Den andre kategorien kalles *indirekte innsamling* av bevis. Denne formen for innsamling av digitale bevis kan gjøres uten at formålet i seg selv trenger å være å få tak i bevis. Et eksempel på slike innsamlingsmetoder er at opplysninger om biler som har passert en bestemt bomring, senere kan brukes i etterforskningen av et bestemt ran. (Coll & Schartum, 2004).

2.3.1 Analoge og elektroniske dokumentbevis

Under skal jeg gi en oversikt over forskjellene på analoge og digitale bevis.

Analoge dokumenter har ofte underskrevet dato for opprettelse, i tillegg til at man ofte vil finne informasjon om hvem forfatteren er i topp eller bunntekst, som regel er det en bekreftende signatur nederst på dokumentet. Denne informasjonen har flere funksjoner, signaturen bekrefter avsender i tillegg til at avsender vanskelig kan nekte å ha opprettet eller sendt dokumentet. I tillegg blir det trykket på papir som gjør det vanskeligere å gjøre endringer på dokumentet i etterkant, dette er igjen med på å øke integriteten til dokumentet.

Elektroniske bevis er materiale samlet inn for å underbygge de rettslige relevante omstendighetene. Elektroniske dokumenter har ofte andre egenskaper enn analoge dokumenter. Eksempler på dette kan være metadata som ikke vil komme til syne hvis man skriver dokumentet ut og arkiverer det som en papirutskrift (Coll & Schartum, 2004; Larsen, 2007).

I norsk rettsprosses har man hatt lang erfaring med bruk av analog bevis, derav også strenge rutiner for innsamling og bevaring av denne type bevis. Derimot er elektroniske bevis en utfordring rettsvesenet har måttet ta stilling til i den senere tid. Utfordringen er blant annet knyttet til prosessreglene som ikke er tilstrekkelig tilpasset denne type bevis. Derfor er det behov for å ha metoder slik at man best mulig kan analysere hvilke egenskaper digitale dokumenter har og i hvilken grad man best mulig kan svare på om bevisets ektehet(Larsen, 2007).

2.4 Relatert forskning

Det har etter hvert blitt generert en del forskning innefor området elektroniske bevis, selv om dette er et relativt nytt felt med mange ubesvarte spørsmål. Jeg skal i denne delen foreta en kort gjennomgang av noen av de forskningsprosjektene som eksisterer både i Europa og USA.

I Norge er det opprettet et datakrimutvalg som etter mandat skal utrede lovtiltak mot datakriminalitet. Den første del utredningen ble publisert i Norges offentlige utredninger (NOU) 2003:27 ”Lovtiltak mot datakriminalitet – Delutredning 1”. Her har utvalget tatt for seg Europarådets konvensjon som omhandler bekjempelse av kriminalitet. Utvalget tok i denne delutredningen for seg Europarådets konvensjon om bekjempelse av kriminalitet knyttet til informasjons og kommunikasjonsteknologi. I hovedsak omhandlet utredningen hvilke endringer i norsk rett som var nødvendig for å kunne ratifisere Europarådets datakrimkonvensjon fra 2001. Slutningen av den første delutredningen var at konvensjonen trådde i kraft i Norge med virkning fra 1.oktober 2001. Det har i senere tid vært flere utredninger men skal ikke gå noe nærmere inn på det i denne oppgaven (Larsen, 2007).

”The admissibility of electronic evidence in court: Fighting against high- tech crimes” er et forskningsprosjekt som tar sikte på å gi svar på hva elektroniske bevis er for noe som for eksempel er elektroniske bevis regulert i Europeiske jurisdiksjoner, hvilke problemer møter etterforskere, advokater og dommere som er involvert i sikring, analyse, evaluering og presentasjon av elektroniske bevis og hvordan de utfører arbeidet i de forskjellige fasene. Dette prosjektet var i regi av Cybex, et spansk firma som spesialiserer seg på elektroniske bevis. Prosjektet pågikk i 2006 der representanter fra 15 EU i tilegg til Romania deltok i prosjektet.

I den første delen av prosjektet analyserte de den eksisterende lovgivningen i forhold til elektroniske bevis i de ulike deltagerlandene. Deretter ble det gjennomført åtte intervjuer med sivile, kriminelle, offentlige og private advokater, ledere innen advokatforeninger og den høyeste påtalemakten i hvert av deltagerlandene. Etter en gjennomgang av lovgivningen i de forskjellige landene viste det seg at det ikke eksisterer en klar referanse til elektroniske bevis, utrykket var heller ikke definert på noe bestemt måte. Men det ble imidlertid funnet at det i deltagerlandene forekommer reguleringer med forskrifter som på en eller annen måte henviser til elektroniske bevis. Etter en analyse av lovgivningen viste det seg at elektroniske bevis blir håndtert på lik linje med tradisjonelle bevis i de forskjellige landene også et flertall av dommerne i deltagerlandene ser på elektroniske bevis som det samme som tradisjonelle bevis

det vil også si at de ser på elektroniske bevis på lik linje med dokumentbevis (Insa, 2006; Larsen, 2007).

Det finnes i flere prosjekter innen emnet elektroniske bevis men komme ikke til gå gjennom disse i denne oppgaven.

2.5 Noen utfordringer knyttet til elektroniske bevis

Hele denne oppgaven handler i stor grad om hvilke utfordringer man kan møte ved behandling av elektroniske bevis. Jeg vil likevel gi en systematisk gjennomgang av noen av de typiske utfordringene under.

Elektroniske bevis er forholdsvis nye former for bevismidler. Når man skal sammenligne de nye formene for bevismidler med de mer tradisjonelle, er grensene flytende (Coll & Schartum, 2004). Dagens anvendelse av elektronisk informasjon i retten er i all hovedsak papirutskrift av e-post og andre elektroniske formater som blant annet tekstbehandlingsdokumenter. I rettslig sammenheng tillates det per i dag å fremlegge elektroniske bevis i henhold til svært varierende krav til kvalitet og sikkerhet (Thorvaldsen, Skomedal, 2006). I tillegg knyttes det ofte stor usikkerhet til hvem som har opprettet og sendt det aktuelle elektroniske dokumentet, og om dokumentet er ekte.

Elektronisk informasjon som arkiveres blir sjelden organisert slik som papirdokumenter i et vanlig (fysisk) arkiveringssystem. Det kan kopieres og distribueres svært kjapt slik at det ofte finnes flere utkast eller versjoner av dokumentene som er lagret. (Thorvaldsen, 2006). Det sier seg selv at dette skaper utfordringer i under bevisførsel.

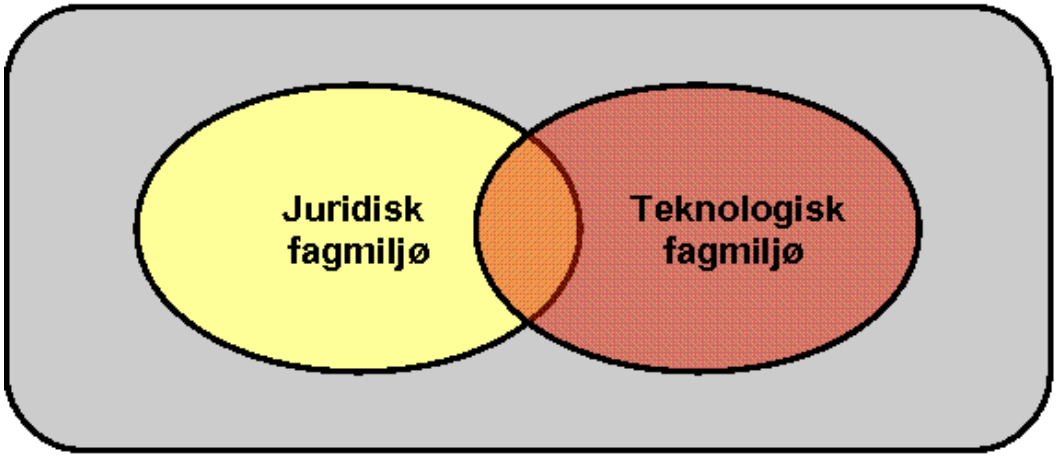
Et beslektet problem er at det er lett å feiltolke eller manipulere digitalt lagrede bevis. Det er sjelden bevisene bestrides, og det ville for eksempel være mye hjelp i å få utarbeidet rutiner for at en e-post eller andre former for elektroniske lagrede dokumenter blir elektronisk verifisert i en rettsammenheng. For eksempel bemerker Thorvaldsen (gjengitt i Gangnes, 2006) at i dag er det papirutskriften av e-post og andre digitale formater som blir lagt frem som bevis i retten. Når man legger frem papirbevis av digitalt lagrede dokumenter vil man ikke kunne få frem de

dataene som verifiserer om beviset er ekte eller ikke, for eksempel vil man bare ved å datere klokken på datamaskinen tilbake i tid hevde at e-posten ble opprettet og sendt ved det tidspunktet klokken ble stilt til eller at et tekstdokument ble opprettet og lagret på et annet tidspunkt enn det egentlig ble. Dermed kan man se at behovet er til stede for spesialisert kompetanse når slike bevis skal tolkes i retten.

Selv om man rettslig sett kan forplikte seg til å inngå avtaler via e-post og at domstolene vil ta dette i betraktning som relevant bevis, er det likevel et spørsmål om hvilken beviskraft e-postene skal ha. (Panzer). Det er derfor både viktig og nødvendig å komme fram til en måte å validere bevisene på før de blir brukt i retten.

En annen utfordring går på advokater og dommeres kunnskap om elektroniske bevis. Det er funnet at kunnskapsnivået blant dommere og advokater i dag ikke er godt nok, noe som øker risikoen betydelig for at databevis kan feiltolkes i retten (Riise, 2006). Ellefsen (gjengitt i Riise, 2006) argumenterer for at databevis er en akilleshæl i det norske rettsystemet, og at det er problematisk at mesteparten av datalagrede bevis godtas slik de legges frem. Ellefsen og Willasen (gjengitt i Riise, 2006) peker på at hovedårsaken til dette problemet er manglende kunnskap om hva slags informasjon databevis kan gi, og hvilken informasjon det ikke kan gi.

Det kreves økt kompetansebygging både innefor det tekniske og juridiske området, og i dag er det svært begrenset samarbeid mellom disse to fagmiljøene. Økt samarbeid er en utfordring, og en forutsetning for å utvikle gode og anvendelige teorier og prosedyrer som kan fungere i skjæringspunktet mellom det tekniske og det juridiske (se fig 1). For å få dette til må det skapes et miljø der man tar for seg både det juridiske og tekniske perspektivet slik at personer som arbeider i feltet lettere kan skaffe seg større innsikt i begge disse områdene (Larsen, 2007).



FIGUR 1. To overlappende fagmiljø

Det kreves at domstolene har god kompetanse på egenskapene til og bruken av elektroniske bevis. Resultatet kan bli at bevisene blir vektlagt feil og eller at man aksepterer manipulert data og dermed kan få uriktige rettsavgjørelser (Thorvaldsen, 2006)

En stor utfordring er at man ofte ikke har tilgang til de originale elektroniske dokumentene, eller at de elektroniske bevisene ikke er sikret på en slik måte at man kan ha tillit til om det er det ekte beviset man har å forholde seg til (Thorvaldsen, 2006).

De tekniske utfordringene knyttet til elektroniske bevis er mange, et av de viktigste spørsmålene i denne sammenheng er hvor lett elektroniske bevis kan manipuleres, spesielt hvis det gjøres på en slik måte at det blir vanskelig å gjennomskue(Thorvaldsen, 2006). Andre utfordringer relatert til det tekniske er hvordan organisasjonene skal behandle informasjon som kan bli bevismateriale, i forhold til det som lagres og hva som slettes Det kan være alt fra hvem og hvor ble informasjonen laget, og i hvilken grad har informasjonen blitt behandlet på en slik måte at den ikke har endret sin opprinnelige form (Thorvaldsen, 2006)

Mason peker på tre kategorier elektroniske bevis som kan være en utfordring i en rettpraktisk sammenheng (Mason, 2007). Den første kategorien er elektroniske bevis som kan være et register av aktiviteter skrevet av en eller flere personer, dette kan for eksempel inkludere e-post, tekstbehandlingsfiler som Word dokument, og øyeblikksmeldinger (instant messages). Om

man ser på disse forskjellige formene for elektroniske bevis fra et bevismessig hensyn, kan det være nødvendig å påvise at dokumentets innehold er pålitelig under vitneforklaringen.

Den andre kategorien Mason (2007) peker på er de dataene som blir generert av en datamaskin og som ikke har hatt noe input eller innmating fra mennesker. Eksempel på denne type datagenerering er datalogger, telefontilkobling og minibank transaksjoner. Hovedutfordringen med denne type datagenerering som bevismateriale kan være at man må påvise at det dataprogrammet som laget dataene fungerte normalt når dataene ble generert.

Den tredje kategorien Mason (2007) nevner er en form for datagenerering der man får en blanding av menneskelig input og kalkuleringer generert og lagret av en datamaskin. Et eksempel på dette er et finansielt regneark som inneholder input i regnearket gjort av mennesker, i tillegg til dataprosessering (det vil si matematiske kalkulasjoner gjort av regnearkprogrammet). Fra et bevismessig hensyn kan det oppstå tvil rundt hvem og hvor mye som er laget av mennesker og hvor mye har datamaskinen produsert. I slike tilfeller kan det bli sådd tvil rundt autentisiteten til data prosesseringen.

Man kan utfordre ekteheten til elektroniske bevis på mange måter, i flere tilfeller indikeres det at advokater ikke stoler på påliteligheten eller autentisiteten til denne type bevis. Her vil de digitale bevisene blir utfordret på mange måter; Det kan bli påstått at dokumentene har blitt endret, manipulert eller skadet mellom det tidsrommet de ble laget og frem til den dagen det skal legges frem som bevis i retten. Det vil også kunne påstås at dataprogrammet som laget disse dataene kan bli stilt spørsmålstegn ved. En annen utfordring kan være hvem som er dokumentets forfatter. En person som har hatt ansvar for å lage dokumentet i et tekstprogram kan bestride at han har skrevet teksten eller at han eller henne har nekter på å ha tasten en pin kode, passord eller klikket ”jeg aksepter” ikonet (Mason, 2007; Panzer) .

Til nå har vi sett at det knytter seg både juridiske og tekniske problemstillinger til håndtering av elektroniske bevis. Senere går jeg inn på henholdsvis juridiske og tekniske tema hver for seg..

3. AUTENTISITET

Autentisitet betyr det å være "autentisk, ekte."[2] Autentisk betyr "fullt ut ekte og pålitelig"[3]. Om informasjon er unøyaktig, utdatert, inkonsistent eller uklar er den ikke autentisk, og den må dermed forkastes som potensielt bevismateriale (Martin J Eppler, 2004). Derfor er det viktig å ta for seg hva som definerer god informasjonskvalitet. Et kjernepunkt i denne oppgaven er autentisiteten, eller ektheten, til digitale dokumentbevis. Selv om dette temaet allerede har blitt viet mye oppmerksomhet, vil jeg nå gå nærmere inn på hva det vil si at et dokument er autentisk. I tillegg vil jeg vurdere hvilke forhold man må se på når man vil prøve å sikre elektroniske bevismaterialers autentisitet. I denne sammenheng trekker jeg inn Bygraves (1996) modell for datakvalitet.

Papir har vært den viktigste informasjonsbæreren i vår kultur gjennom hundrevis av år. I løpet av denne perioden har papir opparbeidet seg tillit og autoritet som et troverdig materiale som ikke blir borte over natten. Mange omstendigheter i samfunnet krever fremdeles dokumentasjon i form av en underskrift på papir. Papir har også troverdighet fordi vi vet at informasjonen er tilgjengelig når vi har papiret fysisk i hånden. Tilliten til elektronisk informasjon er på langt nær like stor, derfor skriver vi ofte ut dokumenter som er viktig på papir. Men samfunnet er i en endringsprosess der bruken av elektronisk informasjon øker, og det stilles stadig høyere kvalitetskrav til lagring og bearbeiding av slik informasjon. For å kunne bruke informasjon til noe nyttig er det viktig at vi kan stole på at den har høy nok kvalitet i forhold til bruksområdet (Gulbrandsen, 1997).

Den enkleste måten å bekrefte autentisiteten til et elektronisk bevis er å ha et vitne til å stadfeste at dokumentet er hva man påstår det skal være. Denne bevisformen ble i sin tid utviklet for analoge dokumenter og har ikke tatt i betrakting eksistensen av elektroniske dokumenter(CLAES GRÄNSTRÖM et al., 2002).

---

[2] Bokmålsordboka http://www.dokpro.uio.no/ordboksoek.html

[3] Bokmålsordboka http://www.dokpro.uio.no/ordboksoek.html

3.1 Vurdering og sikring av autentisitet og kvalitet

Hva definerer autentisiteten til et elektronisk dokument? Når kan man si at et elektronisk dokument har god kvalitet? Jeg skal i dette avsnittet se på hva som kan være med på å definere og sikre autentisitet og ulike former for kvalitet på data og informasjon. Jeg vil både se på teoretiske begreper og metoder for sikring som er utviklet til bruk for vurdering av kvalitet på elektronisk informasjon. I denne sammenheng gjennomgås også noen teoretiske modeller og dimensjoner for måling av informasjonskvalitet. Det er i ut fra oppgavens problemstilling relevant å ta for seg hvordan autentisiteten til elektronisk informasjon blir forsøkt definert. På grunnlag av en detaljert terminologi kan man igjen skaffe seg utgangspunkt for å gjøre kvalitetssikring.

Et autentisk dokument er i hovedsak et som utgir seg for å være ekte og det ikke er klusset med (Glick & Sloma, 2002). Autentisiteten er truet når dokumentene blir overført gjennom ”rom”, det vil si sendt mellom personer, systemer eller applikasjoner. Også ”tid” er en avgjørende faktor for å avgjøre ekteheten, enten det blir lagret frakoblet (offline), eller når maskinvare eller programvare som er med på å prosessere, kommunisere eller vedlikeholde de elektroniske dokumentene blir oppgradert eller erstattet. For å identifisere om et elektronisk dokument er ekte eller ikke, er det vanlig å bruke *digital signatur*. Dette er en teknologi som har blitt utviklet på basis av behovet for sikker elektronisk kommunikasjon via åpne nettverk slik som internett. Digital signatur som identifiserer senderen av dataobjektet og verifiserer at det ikke har blitt forandret underveis kan støtte autentifikasjonen men er ikke nok til å fastslå identiteten og påvise integriteten til det elektroniske dokumentet over lang tid.

3.1.1 Sikre autentisitet ved bruk av hashverdier

For å kunne sikre autentisiteten til et dokument kan man bruke hashverdier. Disse verdiene er med på å sikre integritet til et dokument ved at det opprettes et slags ”digitalt fingeravtrykk” på dokumentet i form av den unike hashverdien. Jeg vil videre forklare mer om hva en hashverdi er.

Når man har opprettet en hashverdi analyseres først en datafil, og deretter kalkuleres det et unikt identifikasjonsnummer for filen. Det er dette som kalles en hashverdi. Sannsynligheten for at to elektroniske dokumenter har lik hashverdi er ekstremt liten (Boland & Fisher, 2000). Derfor blir hashverdier kalt ”digitale fingeravtrykk” av elektroniske dokumenter. Fordelene med å bruke hashverdier er at de automatisk vil gjøre de nødvendige forandringene om en fil eller et dokument endrer seg. Derfor kan også hashverdier tilføre dokumenter objektiv struktur og bevise ektheten til et ubegrenset antall dokumenter (Losey, 2007).

For å forklare hashverdi nærmere skal jeg gi en kort innføring i hva en hashingalgoritme er. Ordet hash betyr ”å dele inn i små biter”. Hash er en matematisk funksjon eller en serie av funksjoner; mer presist er hash en krypteringsalgoritme. Hash generer en unik alfanumerisk verdi for å identifisere det totale antallet bits og bytes som utgjør en bestemt datafil, gruppe av filer eller en hel hardisk(Losey, 2007). Hensikten med en hashfunksjon er å lage et ”digitalt fingeravtrykk” av en fil, melding eller en blokk med data (Stallings, 2006). Det er også viktig å forstå at beregningen av hashverdiene går hurtig å utføre i praksis, og kan med enkelhet bli implementert i moderne datamaskiner (Boland & Fisher, 2000). Losely (2007) viser til et eksempel fra ”The Libary of Congress”, som man estimerer inneholder ca 136 terabytes med data. Dersom dette hadde vært lagret i elektronisk format ville man kunne hashe denne informasjonen i løpet av noen timer. Skulle man ha gitt disse papirene vanlig, manuelt stempel på hver side for å sikre autentisiteten ville det ha gått flere generasjoner før man har blitt ferdig (Losey, 2007). Dette illustrer hvor effektivt et digitalt stempel kan være når man skal sikre autentisitet i mange digitale dokumenter samtidig.

Teknisk sett er hashing basert på innsetting av data ved matematiske formler, derfor blir prosessen kalt hashing (nøkkeltransformasjon). Hashing er en måte å koke sammen en fil til essensielle nummer. Hashverdien er vanligvis representert ved en kort streng av tilsynelatende tilfeldige bokstaver og nummer men som er binære data skrevet i heksadesimale notasjon og som vanligvis blir kalt filens ”fingeravtrykk” fordi den representerer noe unikt og eget (Losey, 2007; Sangchul & Joseph, 2007; Stallings, 2006). Om to datafiler er helt identiske så vil de også

ha den samme hashverdien. Selv om filene har forskjellige navn vil disse filene ha samme verdi, dersom innholdet i filen er det samme. Hvis noe i filen endres, det kan være noe så lite som et enkelt komma i en tusen siders tekst, vil dokumentet få totalt forskjellige hashverdier fra det originale dokumentet (Boland & Fisher, 2000; Losey, 2007). På denne måten kan man verifisere om integriteten er i behold ved å sammenligne den lagrede hashverdien med en nylig beregnet hashverdi (Sangchul & Joseph, 2007). En mulig begrensning av denne ellers svært så effektive valideringsstrategien er at den forutsetter at man innehar opplysninger om den originale hashverdien på et gitt dokument. Dersom man mistenker at dokumentet er endret, eller at to elektroniske dokumenter ikke er like, kan man sjekke om hashverdien er sammenfallende med originalverdien.

Det finnes flere typer hashfunksjoner som er i bruk. De mest vanlig er: MD5, SHA-1, og SHA-256. ”*Secure Hash- Algoritmen*” (SHA) ble utviklet av The National Institute of Standard And Technology (NIST) ved det amerikanske handelsdepartementet. Den originale spesifikasjonen av algoritmen ble publisert i 1993 (*SHA hash functions*, 2008; Stallings, 2006). SHA kommer også som SHA-224, SHA-256, SHA-384 og SHA-512. De fire siste versjonene blir ofte omtalt som SHA-2. Sikkerheten i SHA-1 har til en viss grad blitt kompromittert av forskere innefor kryptografimiljøet men ingen kritikk av SHA-2 har blitt rapportert (*SHA hash functions*, 2008).

SHA-1 er en forbedret utgave av den originale SHA versjonen. SHA-1 produserer en 160-bit (20 byte) fil gjengivelse. Selv om den er tregere enn MD5 har den en større verdi i gjengivelsen av dataene som igjen gjør den mer pålitelig og mer effektiv mot forsøk på å knekke kryptografikoden (Losey, 2007).

MD5 eller ”*Message Digest 5*”, ble utviklet og publisert i 1992 av Professor Ronald L. Rivest ved MIT. MD5 -algoritmen tar en inputmelding av tilfeldig lengde og produserer et 128bits ”fingeravtrykk” eller en ”meldingsgjengivelse” av inputmeldingen. Den 128 bit (16 byte) meldingsgjengivelsen i MD5 sammenlignet med de 160 (20 bytes) til SHA-1 -algoritmen gjør den raskere å implementere og sammen med dens pålitelighet er den en vanlig brukt hash algoritme i data etterforskning(Losey, 2007).

Jeg kommer til å bruke disse formene for hashverdier senere i oppgaven, under testingen av elektroniske dokumenters autentisitet. Også metadata, beskrevet under, vil brukes her.

3.1.2 Metadata bruk ved autentifisering

Metadata er strukturert informasjon som beskriver, forklarer, eller på andre måter gjør det enklere å gjenfinne, bruke eller behandle informasjonsressurser. Metadata blir ofte kalt data om data. Hos et elektronisk dokument kan for eksempel metadata si noe om når det ble opprettet, hvem opprettet det og når det sist ble endret(NISO, 2004).

Slik data kan brukes som informasjon når man undersøker et dokuments autentisitet. Hvor godt dette er som autentifiseringsverktøy vil jeg undersøke i kapittel 7.

3.1.3 Standarder for autentifisering

I mange land har forsøk på å forbedre data- og kommunikasjonssikkerhet tradisjonelt sett fokusert på beskyttelse av konfidensialiteten av informasjonen. Det vil si at man har lagt vekt på å forsikre seg om at informasjonen ikke kommer i hendene på uautoriserte personer.

Relativt liten oppmerksomhet har blitt viet det å beskytte andre aspekter ved sikkerheten. Dette kan for eksempel være det å forsikre seg om at informasjonen er korrekt, fullstendig og relevant, samt at informasjonen er beskyttet fra og bli endret, skadet eller ødelagt av uvedkommende (Bygrave, 1996). Ifølge National Archives of Australia må et digitalt dokument kunne innbefatte informasjon om dokumentinnhold, kontekst og struktur. Det betyr at et digitalt dokument for å være autentisk bør holde informasjon som er, og fortsetter og være, en korrekt refleksjon av hva som har skjedd ved et bestemt tidspunk. Man bør også kunne plassere informasjonen i en kontekst, slik at omstendighetene rundt dokumentets opprettelse kan bli forstått i forbindelse med informasjonsinnholdet. Dersom disse kravene til autentisitet oppfylles kan man til en hver tid klare å rekonstruere dokumentet elektronisk når man har behov for det (Australia, 2004).

Videre vil jeg nevne en standard som er utarbeidet for vurdering av autentisitet. International Organization for Standardization (Warren, George, Sarah, Mark, & John) har publisert ISO 15489-1, Information and documentation – Record Managment. Standarden ble utviklet slik at beskyttelse av alle typer dokumenter skulle bli viet den rette oppmerksomhet, og at bevisene og informasjonen disse inneholdt kunne bli gjenopprettet eller gjenfunnet mer effektivt gjennom standardiserte metoder. Standarden definerer autentisitet som

Et autentisk dokument er et som kan bli bevist ved:

a) at det er hva det utgir seg for å være
b) det har blitt opprettet eller sendt av den personen som påstår han har opprettet og sendt det
c) At det har blitt sendt ved det tidspunktet det hevdes å ha blitt sendt

For å forsikre seg om ekteheten til dokumentet burde organisasjoner implementere og konstatere fremgangsmåter og prosedyrer som kontrollerer etableringen, mottakelse, overføringen, vedlikeholdet og ordningen av dokumenter for å forsikre seg om at de som lager dokumentene blir beskyttet mot uautorisert tilføyelser, sletting, endringer, bruk og hemmeligholdelse (CLAES GRÄNSTRÖM et al., 2002). Om integriteten eller autentisiteten til et elektronisk dokument blir satt i tvil i retten ved antydninger om at det har blitt klusset med, eller at det foreligger feilaktig systemfunksjonalitet eller maskinsvikt, vil man kunne redusere eller eventuelt miste verdien av beviset og skade saken (CLAES GRÄNSTRÖM et al., 2002).

For å påvise identitet må man se forskjell på de unike karakterene og attributtene ved et dokument. Slike attributter burde inneholde: dokumentets forfatter, adressat, opphavsmann, datoen det ble opprettet og datoen dokumentet eventuelt ble overført, en indikasjon på når det ble laget og eventuelt endret og mottatt (Glick & Sloma, 2002).

Videre skal jeg se på informasjonskvalitet og datakvalitet. Dette er to ulike betegnelser på kvalitet som ofte refereres til i litteraturen. Fordi det er snakk om informasjonskvalitet og datakvalitet skal jeg først og fremst definere begrepene data og informasjon. *Data* blir ofte sett

på som en samling av symboler som viser den virkelige verden systemets status eller tilstand, og blir brakt sammen fordi de blir oppfattet som relevant i forhold til noen meningsfulle aktiviteter. *Informasjon* er en objektiv tjeneste som er utført av symboler og relaterer til hvem som produserer det, hvorfor og hvordan det ble produsert og dets forhold til den virkelige verdens tilstand (Xu, 2003). *Datakvalitet* og *informasjonskvalitet* blir ofte sett på som synonyme begreper både i litteratur og i praksis (Melkas, 2004; Slone, 2006; Xu, 2003). Senere vil jeg presentere en modell laget av Bygrave(1996), som skiller mellom disse begrepene og legger til en tredje kategori for kvalitet (informasjonssystemkvalitet). Jeg vil for øvrig ikke gjøre et videre poeng av skille mellom disse begrepene senere i oppgaven.

Som tidligere påpekt er elektroniske dokumenter er lett å manipulere. Likevel kan man ikke uten videre argumentere for at elektroniske systemer produserer bevis av dårligere kvalitet enn tradisjonelle. De problemene som ofte oppstår i forbindelse med elektroniske bevis dveler i mange tilfeller på manglende tradisjon, kultur og rettspraksis (Brattsberg, 1994). Det å bevise ektheten av elektroniske dokumenter har vist seg å være en vanskelig oppgave. Slike dokumenter beskrives som ustabile om de ikke blir lagret korrekt. Dette har ført til et økende behov å utarbeide reliable metoder for å teste elektroniske dokumenters ekthet (Mason & Barrister, 2006).

Tradisjonelt sett har det ikke blitt utarbeidet eksplisitte kvalitetstermer for elektronisk informasjon. Både innefor jussen og informatikkfeltet har det vist seg å være lite litteratur på dette området. Kristo Ivanov (sitert i Bygrave, 1996) skriver i sin doktoravhandling i 1972 at litteraturen i data- og informasjonsvitenskap viser liten interesse for emnet data- og informasjonskvalitet. Litteraturen avslørte også lite enighet om hvordan man skulle definere data- og informasjonskvalitet og hvordan man skulle måle det (Bygrave, 1996). Det har siden den gang blitt foreslått mange forskjellige definisjoner på datakvalitet. Generelt sett kan man definere datakvalitet som ”fitness for use”, eller ”brukbarhet” (Kerr, 2006; Scannapieco, 2004; Xu, 2003). En andre definisjon på datakvalitet er ” forskjellen mellom den dataen som er presentert i et informasjonssystem og den samme dataen i den virkelige verden” (Scannapieco,

2004). Den første definisjonen er fremhever den subjektive karakteren ved datakvalitet, mens den andre definisjonen er en mer anvendelig definisjon selv om det å definere datakvalitet ved å sammenligne med den virkelige verden er en vanskelig oppgave (Scannapieco, 2004).

Tradisjonelt har datakvalitet blitt beskrevet ut fra et nøyaktighetsperspektiv, men i dag viser både forskning og praksis at definisjonen på datakvalitet burde gå lengre enn nøyaktighet og i stedet bli definert multidimensjonalt (Kerr, 2006; Scannapieco, 2004; Xu, 2003). En datakvalitetsdimensjon er identifisert av Wang (gjengitt i Kerr, 2006) som et sett av kvalitetsattributter som de fleste databrukere oppfatter på en rimelig forenelig måte. Disse dimensjonene er:

- Nøyaktighet (accuracy) som oppstår når den registrert verdien er i overensstemmelse med den reelle verdien.
- Tidsriktighet (timeliness) oppstår når den registrerte verdien ikke er gått ut på dato.
- Fullstendighet (completeness) oppstår når alle verdiene for en spesiell variabel blir lagret.
- Konsistens (consistency) som oppstår når representasjon av dataverdiene er den samme i alle tilfellene (Xu, 2003, Kerr, 2006).

Denne bruken av flere dimensjoner er konsistent med tidligere empirisk forskning (Kerr, 2006)

3.1.4 Bygraves modell for datakvalitet, informasjonskvalitet og informasjonssystemkvalitet

Bygrave (1996) har gjort en studie som bygger på en rekke tidligere analyser av kvalitetskrav til data og informasjon. På grunnlag av studien har han utviklet en modell for kvalitet. Denne modellen kan være med på å belyse hva som definerer autentisitet, så vel som hvilke faktorer man kan bruke som utgangspunkt når man skal vurdere autentisiteten til et elektronisk dokumentbevis. Bygrave skiller mellom begrepene datakvalitet, informasjonskvalitet og informasjonssystemkvalitet (Bygrave, 1996). Jeg vil under forklare disse tre begrepene nærmere.

Datakvalitet består av en gruppe egenskaper eller karakteristikker som omhandler graden av hvordan data korresponderer med de personer, fakta, konsepter, instruksjoner og prosesser som det er meningen at dataen skal representere. Disse egenskapene kan også beskrives som Real world objects (RWO) eller på norsk ”objekter i den virkelige verden”. Korrespondansen mellom et sett med data og RWO kan bli oppsummert med betegnelsen gyldighet eller validitet av dataene. Det er tre hoveddimensjoner av slik validitet. Den første er *nøyaktighet*, det vil si hvor presist dataene beskriver eller definerer RWO. Den andre dimensjonen er *fullstendighet* det vil si i hvilken grad alle data som er nødvendig for å representere RWO er tilstede i et gitt informasjonssystem. (Bygrave, 1996). Den tredje dimensjonen er *integritet. Med* dette mener man i hvilken grad dataene forblir uforandret ved innsamling og lagring. Et viktig moment med den tredje dimensjonen er hvor håndgripelig og hvor oppdatert dataen er. Det vil si alderen på dataen målt i perioden fra dataen blir samlet inn og lagret og til det tidspunktet det blir brukt for en gitt årsak (Bygrave, 1996).

Informasjonskvalitet vil si nytteverdien til informasjonen, eller hensikten med å samle inn, lagre og bruke opplysningene. Det er to sentrale faktorer som er viktig for at vi skal ha nytteverdi av informasjon: fullstendighet og relevans. *Fullstendighet* referer til i hvilken grad all relevant informasjon er presentert i relasjon til en bestemt bruk. *Relevans* dreier seg om et gitt sett av informasjon som er relevant til et gitt behov eller anvendelse. Relevansen må vurderes i forhold til hver konkrete sak, noe som igjen gjør det vanskelig å gi en generell definisjon på hva som er relevante personopplysninger (Bygrave, 1996; Lind, 2001). Hypotetisk sett kan man si at informasjonen er relevant til et gitt bruk ut fra om utfallet hadde blitt annerledes om den ikke hadde blitt tatt med i betrakting. Det er flere faktorer som er med på å avgjøre relevansen til informasjon. En av disse er informasjonens kognitive autoritet, det vil si hvor mye informasjonen blir ”vektlagt” i form av dens tilsynelatende troverdighet og pålitelighet. En annen faktor er legalitetsprinsippet; det vil si i hvilken grad bruken av informasjon for en bestemt sak er i samsvar med loven. (Bygrave, 1996; Lind, 2001).

Sist skal vi se på *informasjonssystemkvalitet,* som først og fremst er relatert til kvaliteten på systemene som er konstruert og brukt til å samle, lagre prosessere og spre data. Slike attributter inkluderer påvirkelighet, robusthet, tilgjengelighet, pålitelighet og forståelighet. *Påvirkelighet* omhandler den ønskelige måten et gitt informasjonssystem skal samhandle med andre systemer. Dette i form av styring, administrasjon og vedlikeholding. Informasjonssystemet skal også tilordne ansvar for å definere, registrere, lagre, korrigere og spre dataen som behandles av systemet. Systemets *robusthet* tar for seg hvorvidt systemet er sårbart for inngrep utenfra, mens tilgjengligheten relateres til hvilken grad et informasjonssystem tillater at data blir lokalisert og hentet. *Påliteligheten* til et informasjonssystem henviser til hvorvidt systemets funksjoner er i overensstemmelse med de forventinger brukerne har. Denne karakteristikken tar for seg kapasiteten systemet har for å beskytte integriteten og de muligheter systemet har til å innhente eller gjenfinne data. Den siste egenskapen Bygrave nevner er *forståelighet*. Det han mener med det er om informasjonssystemet fremmer eller hindrer forståelse av hvordan det fungerer. Det er ikke bare nok å forstå personene eller organisasjonen som er ansvarlig for å betjene systemet, men også forstå de personene og organisasjonene som blir påvirket av systemet (Bygrave, 1996).

Etter at Bygraves modell er gjennomgått ser man at modellen inneholder mange nyttige konseptualiseringer som kan fungere som sjekkpunkter når kvaliteten og autentisiteten til et elektronisk dokumentbevis skal vurderes.

4. RETTSPROSESSEN

Jeg har til nå presentert to viktige begreper: bevis og autentisitet. I dette kapittelet vil jeg gi en oversikt over rettprosessen, som jo er konteksten elektroniske dokumentbevis befinner seg i. Når oppgavens problemstilling skal besvares, er det en forutsetning at man legger til grunn kunnskap om prosessen et elektronisk bevis følger i retten. Nedenfor ser jeg både på saksgangen i sivile saker og straffesaker. Det er nødvendig å stifte kjennskap til disse to former for saksgang fordi elektroniske bevis blir brukt i begge tilfeller.

4.1 Rettsprosessen i norsk sivil- og straffrett

Jeg vil prøve å gi et oversiktsbilde over dagens prosessordning og se på noen av de prosessuelle reglene i saksgjennomføringen. Dette vil omhandle både sivil- og strafferettsprosessen.

I det juridiske faget beskrives "prosess" vanligvis som regler for hvordan saker behandles for domstolen. Det finnes to hovedfelt innenfor prosessfaget; sivil- og straffrettsprosess.

I hovedsak er en prosesshandling de skritt en part må ta for å iverksette et søksmål og bringe det fremover mot en avslutning. Prosesshandling vil gi utrykk for en begjæring eller en beslutning angående saksbehandlingen. Dette gjelder om en sak skal reises eller frafalles, eller hvilke bevis som skal føres.

Prosesshandlingen må ofte være avgitt innen bestemte frister for å få virkning. Derfor er reglene for når en frist begynner å løpe og hvordan fristen skal beregnes er meget viktig praktisk sett. Spesielle formkrav gjelder for enkelte typer prosesshandlinger, i den sammenheng har loven regler hva en ankeerklæring skal inneholde (tvl. §§ 9-2 og 29-9).

Prosesshandlingen kan man enten foreta gjennom prosessskrift eller man kan gjøre det muntlig (tvl kap12). Straffelovsprosessen har ikke regler for prosessskrift. Dette medfører at partenes kontakt med hverandre og retten skjer gjennom brev.

Prosesskrifter har frem til i dag vært vanlige papirdokumenter men det er fastsatt en ny regel i dstl. § 197a som gir kongen hjemmel til å gi regler om at kommunikasjon mellom partene og

domstolen skal kunne gjøres elektronisk (Hov, 2007)Justisdepartementet la frem denne proposisjonen i 2002. Der de argumenterte med at prosesslovgivningen var gammel og ikke tilpasset moderne kommunikasjonsformer med og i domstolen ("IKT Strategi for justissektoren", 2004).

Formålet med reglen er å sikre teknologinøytralitet ved skriftlig kommunikasjon med domstolene. Reglen vil også gå foran de enkelte lover som angår domstolenes saksbehandling. Denne bestemmelsen vil gi en mulighet men ingen rett eller plikt til å kommunisere med domstolene elektronisk.

Bakgrunnen for dette høringsbrevet er at regjeringen ønsker å likestille elektronisk kommunikasjon med papirbasert så langt det er mulig. Derfor ble eRegelprosjektet satt i gang for å fjerne unødige og rettslige hindringer for elektronisk kommunikasjon. I denne sammenheng ble prosesslovgivningen utelatt fordi kommunikasjon med domstolene krever løsninger som må vurderes særskilt. Dette går på helhetlige rettslige løsninger.(str.prop 2002). Det ble samtidig gitt en regel om fristavbrytelse i dstl. § 146 (2) 3. Pkt: *Hvis frist avbrytes ved elektronisk kommunikasjon, anses fristen avbrutt når det utsagn som avbryter fristen, er sendt til riktig elektronisk adresse ("IKT Strategi for justissektoren ", 2004).* Regelen i domstolloven gir ikke i seg selv hjemmel for å stanse en frist gjennom for eksempel e-post. (Hov, 2007).

Jeg vil nå forklare gangen henholdsvis i en sivil rettssak, og deretter i en straffesak.

4.1.1 Gangen i en sivil rettssak

En sivil sak gjelder tvist mellom to parter. En part kan være en privatperson, et firma, en organisasjon, en offentlig etat eller en offentlig virksomhet. En sivil sak begynner med at to eller flere personer er uenige om noe i rettsforholdet seg imellom. En sak mellom to private parter begynner i forliksrådet, men i saker mot stat og kommune og de tilfeller der begge partene har vært representert ved advokat, går direkte for retten og starter ikke i forliksrådet. Når stevningen kommer til retten undersøker dommeren om det oppfyller kravene i loven, deretter sendes stevningen til den saksøkte, her får den saksøkte tre uker på seg til å levere tilsvar og må

imøtegå de kravene som er reist. Når man har fått inn tilsvar blir det som regel satt en dato for hovedforhandlingen. Når saken er sendt til retten, må det fremlegges domstolen innen et år. Dette gjøres ved at man leverer en stevning tilegg til å betale et rettsgebyr. Hvor stort gebyret blir, er avhengig av hvor mange dager som går med i retten.

I sivile saker har retten som regel bare en fagdommer. Partene kan kreve to fagkyndige meddommere og i noen saker skal det være fagkyndige meddommere. Hovedforhandlingene begynner med at prosessfullmektige til saksøkte holder et innledningsforedrag hvor han redegjør for saken, dokumenterer de bevisene han vil føre og tar en kjapp gjennomgang av de juridiske spørsmålene i saken. Til slutt legger han ned en påstand om hva han mener sakens resultat bør bli. Det samme gjør den prosessfullmektige til den saksøkte. Etter man er ferdig med denne delen blir hver av partene avhørt. Det er den prosessfullmektige til parten som spør først, deretter er det motpartens prosessfullmektig som kan stille spørsmål. Når partene har forklart seg blir mulige vitner avhørt, i det tilfelle er det den som fører vitnet som avhører først, deretter har motparten mulighet til å stille spørsmål. I noen tilfeller drar retten på befaring etter vitneavhøret for å se på det saken dreier seg om. Når bevisføringen er ferdig holder de prosessfullmektige en prosedyre. I denne delen summerer de opp fakta og framstiller jussen i saken, slik de ser det. Når både prosedyrene og mulige replikkrunder er avsluttet, er hovedforhandlingen over og saken blir tatt opp til dom. Når rettsaken er over skriver dommeren dommen og dommen blir så uttalt for partene i saken. Den som taper må i mange tilfeller også betale saksomkostninger(domstoler, 2008).

I hovedsak er domstolens oppgave å løse rettslige konflikter mellom partene og avgjøre spørsmål om skyld og straff. Et viktig krav til prosessordningen er at man treffer en avgjørelse på best mulig grunnlag. Det er ikke gitt at domstolene har de beste kvalifikasjonene for å avgjøre hva som faktisk har skjedd. Det vil ofte være nødvendig å øke rettens kompetanse ved å bruke oppnevnte sakkyndige. Grunner til det er at antall kompliserte saker har økt og der retten helst bør ha god kjennskap til for eksempel medisinske, tekniske eller økonomiske områder (Hov, 2007).

4.1.2 Gangen i en straffesak

En straffesak er en sak staten fører mot privatpersoner, som har begått et straffbart lovbrudd. I straffesaker gjelder spørsmål om den tiltalte er skyldig, om tiltalte skal straffes og i hvor stor straffen skal være- skyldspørsmål, straffespørsmål og straffeutmåling.
en straffesak starter med en etterforskning, dette for å få tilstrekkelig opplysning for å avgjøre spørsmålet om tiltale. Under etterforskningen kan det være behov for å varetektsfengsle mistenkte personer for å motvirke bevisforspillelse.
Tiltalespørsmålet kommer opp etter en tilstrekkelig etterforskning. Da blir avgjørelse på om det skal reises tiltale på grunnlag av dokumentene fra etterforskningen. Det er påtalemyndigheten som avgjør tiltalespørsmålet. Påtalemyndighet er en egen organisasjon med riksadvokaten på toppen, etterfulgt av, statsadvokaten og politimestre og visse andre polititjenestemenn.
En straffesak som i en sivilsak kan også løses utenfor domstolene, det kan skje ved at saken blir henglagt. Dette kan påtalemyndigheten gjøre hvis det er mest hensiktsmessig. Saker kan også avgjøres ved forelegg. Et forelegg er å avgjøre saken med bot. Påtalemyndigheten kan også overføre saken til konfliktrådet. En slik overføring forutsetter at den fornærmede og den siktede samtykker i dette. Saker som egner seg for konfliktrådet kan være tyveri og skadeverk. Det er ofte unge lovbrytere som havner i konfliktrådet. Påtaleunnlatelse skjer ved at påtalemyndigheten avstår fra å reise tiltale selv om straffeskyld er bevist(2008.).

4.2 Saksforberedelser

Saksforberedelser har man både i sivil og straffesaker. Man må forberede en sak før en domstol kan ta stilling til sakens. I tvl. § 9-4 (1) er formålet med saksforberedelsene angitt:

"Retten skal aktivt og planmessig styre saksforberedelsen for å oppnå en rask, prosessøkonomisk og forsvarlig behandling" (tvl. §9-4 (1).

Dette gjelder i prinsippet også for straffesaker.

Hvis sakens de faktiske forhold skal behandles i en hovedforhandling er det viktig at hovedforhandlingen kan føre til avslutning uten avbrytelser. Dette gjelder både i sivil og straffesaker. Dersom man må avbryte hovedforhandlingene vil det kunne føre til mye av bevisføringen som har blitt fremlagt, må gjentas. Dette kan igjen føre til økte utgifter og problemer for alle de involverte (Hov, 2007).

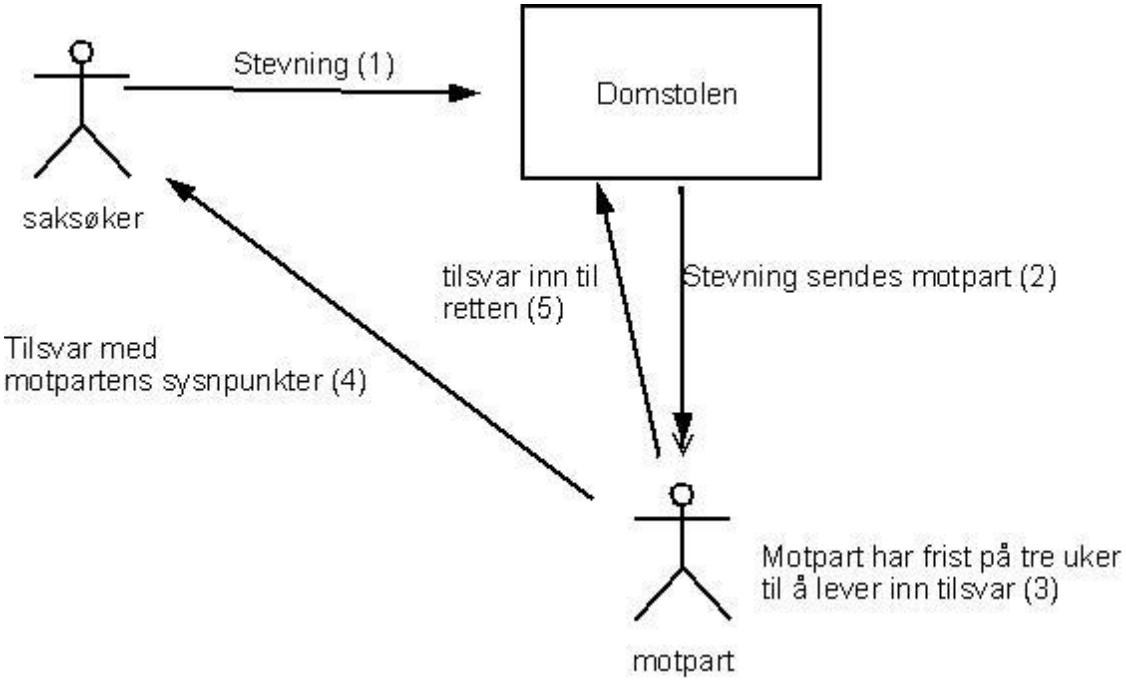
4.2.1 Saksforberedelser i sivile saker

Før en sak reises har tvisteloven innført noen nye regler om partenes plikter. Disse reglene står i tvl. Kap 5. Her har tanken vært hvis partene blir pålagt en viss dialog før en eventuell sak bringes videre, kan det være en mulighet for at noen tvister bilegges, eller at man får en viss avklaring i hvilke synspunkter motparten har.

Den som ønsker å gå til sak er pliktig å informere motparten. Her skal man varsle om hvilke *krav* man gjør gjeldende og grunnlaget for dette. Kravet skal som hovedregel være skriftlig. Den som har planlagt å gå til sak skal oppfordre motparten til ta stilling til kravet som har blitt fremsatt. Begge partene er pliktige å gi hverandre beskjed om hvilke bevis, både elektroniske og analoge, som de måtte være i besittelse av. Disse reglene gjelder også før en sak bringes inn for forliksrådet. Når det gjelder bevisplikten gjelder ikke dette mer enn at man varsler om hvilke bevis man sitter inne med, man har heller ingen plikt å legge frem bevisene på dette stadiet av saken. Før saken bringes inn for tingsretten skal det undersøkes fra begge partene om det er grunnlag for en forsonlig ordning (tvl. §5-4). Ifølge loven kan dette gjøres på tre måter. Ved at partene prøver megling utenom retten, eller ved at bringes inn for forliksrådet eller en utenrettslig tvisteløsningsnemnd.

I sivile saker skal saken reises ved *stevning* til retten (tvl. 9-2 (1). En stevning skal inngis skriftlig eller muntlig. Stevningen skal hovedsakelig individualisere det rettsforhold som saken omhandler. Stevningen skal være med å trekke en ramme for forhandlingen på en slik måte at domstolen får innholdet i saken avgrenset. Stevningen må også innholde hvilke rettforhold man krever en dom for. Personen som saksøker må også melde fra hvilke påstander han nedlegger.

Man skal også angi hvilke bevis man skal fremføre i stevningen men har mulighet til å frembringe nye bevis senere. dommeren skal ta en foreløpig prøvelse av stevningen når den kommer inn til retten(Hov, 2007). Figuren under viser en forenklet skjematisk oversikt over hvordan prosessen med stevningen foregår (se fig 2).



Figur 2. Sivil sak etter tvisteloven

4.2.2 Saksforberedelser i straffesaker

I straffesaker vil det ha foregått en etterforskning før tiltalebeslutning og det er på bakgrunn av denne etterforskningen at påtalemyndighet og den siktede har en god oversikt over hvordan saken ligger an. Dette medfører at behovet for en påfølgende saksforberedelse blir mindre viktig enn i sivile saker (Hov 2007). Når man har ferdigbehandlet tiltalebeslutningen skal påtalemyndigheten sende en kopi til retten sammen med en oppgave (oversikt) over de bevis de ønsker å føre. I norsk straffrett hovedregelen at påtalemyndigheten sitter med bevisbyrden i en straffesak. Så lenge det finnes rimelig tvil om skyldspørsmålet skal tvilen komme tiltalte til

gode. Andenes (sitert i Larsen, 2007 s 12) skriver at en dom kan bare begrunnes med de bevis som har kommet frem under den muntlige hovedforhandlingen. Det vil si at man ikke kan dømme noen på grunnlag av å ha studert saksdokumenter og man kan ikke supplere muntlige utsagn i hovedforhandlingene med dokumentinnhold som ikke er nevnt under den muntlige forhandlingen (Larsen, 2007).

4.3 Sakkyndige

I en del sammenhenger vil retten ha behov for bistand fra sakkyndige. Av og til trenger dommeren kunnskap om et område som blir brakt opp i retten som ligger utenfor dommerens kunnskapsfelt. Da vil det være naturlig for retten å oppnevne en sakkyndig som har grundig kjennskap til temaet. Dette kan gjelde for eksempel økonomiske, medisinsk, eller tekniske forhold(Larsen, 2007). Tema i denne oppgaven er elektroniske bevis, og det er for eksempel lett å tenke seg at behovet for spesialistbistand er til stede i saker der elektroniske bevis er viktige for sakens utfall. Selv om partene oppnevner sakkyndig er det ingen plikt at retten følger synet til den sakkyndige, men det er vanlig at den sakkyndiges vitneprov blir fulgt(Hov, 2007) Den sakkyndiges erklæring skal gjelde rent faktiske forhold. Partene kan både protestere mot oppnevnte sakkyndige og selv foreslå sakkyndig men det er retten som tar den endelige avgjørelsen, dette skaper også klare ansvarsforhold. I straffesaker kan også påtalemyndigheten oppnevne sakkyndige under etterforskningen (Hov, 2007). For at man skal ha plikt til å være sakkyndig er den første betingelsen, er at det virkelig er et sakkyndighetsspørsmål som skal utredes. I sivile saker har vi to hovedtyper av sakkyndige; faste og ikke faste. Forskjellen på disse to er at de faste er oppnevnt uten tilknytning til noen bestemt sak, og gjennom oppnevnelse er forpliktet til å stå til rettens disposisjon, dersom innhabilitet eller andre grunner ikke hindrer dette. Selv om det forventes at sakkyndige skal ha inngående kunnskap om teamet hun/han skal vitne om, er det ingen formelle krav til hvem som skal vitne som sakkyndig(Larsen, 2007).

I neste kapittel går jeg inn på personvern, som i mange tilfeller der elektroniske dokumentbevis er aktuelle påvirker gangen i rettsprosessen.

5 PERSONVERN

Man kan på mange måter betrakte personvern som et ideal. *Personvernidealet* er slik som andre idealer; det vil si at det representerer en rendyrket tilstand eller det høyeste målet vi streber mot. Idealer kan dessverre ikke oppfylles fullt ut (Schartum og Bygrave, 2004). Det er særlig to grunner til et slikt mismodig syn. Personvernidealet er ikke "alene" i verden. Dette fører til at andre idealer vil komme i konflikt med personvernidealet, noe som igjen fører til at man ikke kan realisere ett eller flere av idealene fullt ut. Disse konfliktene skaper behovet for avveininger, for eksempel konflikt med behovet for bevis i en rettssak. En annen grunn til at personvernidealene ikke kan oppfylles fullt ut, er av en mer praktisk art. Personvernidealet ville vært umulig å sette ut i livet på en måte som sikrer full oppfølging av det som formelt sett har blitt bestemt, selv om den skulle få fullt gjennomslag i avveiningen i konkurranse med andre idealer. Selv om det for eksempel er fastsatt at personopplysningene skal sikres mot uautorisert innsyn på en omfattende og trygg måte er det med stor sannsynlighet at disse tiltakene vil en eller annen gang rammes av teknisk eller menneskelig svikt (Schartum & Bygrave, 2004).

Når det er snakk om innsamling og behandling av elektroniske dokumenter er det avgjørende at vi også vender blikket mot personvern. Man må blant annet forholde seg til spørsmål knyttet til personvern for å få til en adekvat informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet når personopplysninger behandles (Johansen, Kaspersen, & Skullerud, 2001). En konsekvens av den massive utviklingen av elektroniske verktøy og kommunikasjonsmidler er at nye spørsmål dukker opp i forhold til hvordan den enkeltes privatliv kan og bør vernes. Jeg har valgt å fokusere på slike spørsmål i det følgende kapittelet.

Først vil jeg ta for meg relevant, overordnet teori, deretter følger en redegjørelse for de personvernmessige utfordringer man står overfor ved bruk av elektroniske dokumentbevis spesielt.

5.1 Personvernteori

Personvernteori utdyper og identifiserer tradisjonelle konfliktlinjer i den delen av norsk politikk og lovgivningsvirksomhet som har særskilt relevans for personvernet (Schartum & Bygrave, 2004). Dagens personvernteori er i stor grad orientert mot forhold som gjelder anvendelse av elektronisk informasjon og kommunikasjonsteknologi.

Det moderne personvernet har siden 1970-årene vært knyttet til datamaskinbehandling og personopplysninger i ulike "registre" (Schartum & Bygrave, 2004). Det var de datamaskinbaserte registrene som var av interesse, særlig fordi sjansene for manipulering, samkjøring, gjenfinning og utveksling av personopplysninger var mange og betydningsfulle. Siden den gang har den teknologiske utviklingen gått videre, og det er to relevante trekk ved denne utviklingen som er merkbare. For det første er det ikke bare den elektroniske behandlingen av skrift som er aktuell, men også i større grad behandling av bilder og lyd. For det andre innebærer utviklingen at personopplysningene registreres i elektroniske medier på flere måter enn tidligere. Noen eksempler på dette er ulike type sensorer som registrerer personers vekt, en bils hastighet, oppholdssted, biometriske forhold som skanning av iris, samt fingeravtrykk. (Schartum & Bygrave, 2004)

5.1.1 Tre ulike perspektiver på personvern

Det har blitt formulert tre hovedperspektiver på personvern: Integritetsperspektivet, beslutningsperspektivet og maktperspektivet. Personvernperspektivene tar for seg noen klassiske konfliktlinjer i moderne samfunnsliv og viser hvordan personvern har nær sammenheng til områder som forvaltningsrett, arbeidsmiljørett og forbrukerrett (Schartum & Bygrave, 2004). Videre følger en gjennomgang av de overnevnte perspektivene, med et hovedfokus på integritetsperspektivet. Det er nødvendig med en slik gjennomgang da disse perspektivene vil danne et viktig grunnlag for den senere drøftingsdelen.

Integritetsperspektivet representerer på mange vis den klassiske måten å se personvern på. Dette perspektivet er nært knyttet opp mot "sfæreteori", som deler opp menneskers liv i sfærer

med forskjellige grader av intimitet eller sensitivitet for den enkelte. Disse ”sfærene” blir sett på som nokså statiske. Om sfærene bør beskyttes mot inntrengere utenfra, er først og fremst avhengig av hvor sensitive og personlige de er. Hovedproblemet med teorien er at den fremstiller sensitivitet og intimitet som faste, objektivt gitte og kontekstuavhengige størrelser (Schartum & Bygrave, 2004)

Dette er på mange måter den eldre oppfatningen av personvern. Med sfæremodellen tenkte man seg nærmest en form for magisk sirkel eller kuppel rundt hjem og familie, en form for sosialt gjerde hvor man selv bestemte hvem man skulle slippe innenfor. Det er åpenbart mange personlige eller huslige forhold som den enkelte i gitte situasjoner er nødt til å redegjøre for (Bing, 1991)I denne sammenheng kan man bare tenke seg alle opplysningene man formidler til for eksempel skatteadministrasjon og trygdevesen.

Det man tar utgangspunkt i når det gjelder integritetsperspektivet er frie, ”ukrenkelige” mennesker. Under dette punktet skiller vi mellom territorial integritet, som omhandler andres respekt for enkeltmenneskets private, geografiske områder. Et eksempel på dette er hjemmene våre. Kroppslig integritet er et annet diskusjonspunkt innenfor integritetsperspektivet, som kan knyttes til personvern. For eksempel kan undersøkelse av kroppens hulrom og forskjellige typer biometriske tester komme inn under personvernsbegrepet. Det vil si forhold som måling av alkoholpåvirkning, puls, blodtrykk og arvelige egenskaper. Slike undersøkelser kan oppfattes som måter å krenke kroppens integritet på, og angår dermed personvernet.

En annen kategori for integritet som kommer inn under personvernet er psykologisk integritet. Enkelte spørsmål vedrørende psykologisk integritet bør og kan ses i lys av personvern. Noen eksempler på dette er svært lange ventetider for asylsøkere, eller en handling som krenker en annens rett til uforstyrret refleksjon (Schartum & Bygrave, 2004).

Beslutningsperspektivet på personvern har fokus på hvordan korrekte avgjørelser blir tatt på basis av hvordan behandlingen av personopplysningene foregår (Engebretsen, 2002). Opplysninger om enkeltpersoner baseres ofte på et grunnlag av beslutninger som har blitt tatt

av andre (Schartum & Bygrave, 2004). Man kan finne mange eksempler på at ulike beslutningsinstanser treffer avgjørelser om oss. Banker samler inn opplysninger om oss når de skal vurdere en lånesøknad, ligningskontoret benytter opplysninger om selvangivelse og oppgavepliktige tredjemenn for å fastesette skatt og skolemyndighetene behandler opplysninger om karakterer for å avgjøre opptak til videregående skole (Skauge et al., 1997), eller systemer som automatisk genererer beslutninger på bakgrunn av data i en database, som for eksempel hvor mye vi får i trygd eller restskatt.

Disse beslutningene kan være avgjørende for folks livssituasjon og velferd, derfor er det viktig å peke på at beslutningene treffes både innenfor offentlig og privat sektor. Det vil igjen si at velferdssamfunnet har både en offentlig og privat dimensjon der den offentlige dimensjonen dekker myndighetsutøvelse som er med på å etablere plikter for den enkelte. Dette skjer da gjennom å betale skatter og avgifter. Den offentlige dimensjonen er også med på å dekke tildelingen av ulike typer rettigheter som trygdeytelser og andre former for støtteordninger. Når det gjelder den private dimensjonen av velferdssamfunnet kan den forklares med samfunnsviktige institusjoner som arbeidsgivere, banker, forsikringsselskaper, fagforeninger og ulike interesseorganisasjoner. Disse private institusjonene tilbyr funksjoner og tjenester som ofte kan anses som å ha stor velferdsmessig verdi (Skauge et al., 1997).

Til slutt presenteres *maktperspektivet* i personvernet. Dette perspektivet betrakter maktrelasjonen mellom den offentlige myndighet og det enkelte. I denne sammenheng er man opptatt av hvilke virkninger behandling av personopplysninger kan ha på forholdet mellom det offentlige og privatpersoner(Schartum & Bygrave, 2004). Offentlig myndighet eller juridiske personer kan for eksempel være Brønnøysundregistrene hvor databasen skal ha absolutt troverdighet.

5.2 Personvern og innsyn i elektroniske dokumenter

Jeg vil nå fokusere på sider ved retten til innsyn i elektroniske bevis. For å illustrere dette nærmere velger jeg å bruke arbeidsgivers innsyn i ansattes elektroniske dokumenter som et

eksempel. Ved å se på dette eksempelet kan man skaffe seg innsikt i utviklingen på området, og det blir tydelig at man står overfor mange potensielle konfliktområder når "private" elektroniske opplysninger etterspørres som bevismateriale. Problemer kan på grunn av hensyn til personvernet og individets rettigheter oppstå lenge før dokumentet foreligger som bevis i retten. Temaet om innsyn er altså nært knyttet til personvern og personopplysningsloven, noe jeg kommer til å gjennomgå i neste underkapittel.

Det er knyttet mange spørsmål til personvern og innsyn i e-post og andre typer elektroniske dokumenter. Innsynsreglene har til tider vært vanskelig å skjønne, og arbeidsgivere har i flere tilfeller foretatt innsyn uten at det har vært saklig eller rettslig grunnlag for dette. Datatilsynet har i denne sammenheng mottatt en rekke henvendelser fra både arbeidstakere og arbeidsgivere med spørsmål om hvor grensen for lovlig innsyn går (høringsnotat, 2007).

Ved *personopplysningsloven* er EU's personverndirektiv implementert i norsk rett. Hensikten med loven er:

"å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger"(jf § 1, personopplysningsloven).

Det er i denne loven lagt vekt på de grunnleggende personvernhensynene som behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene (Administrasjonsdepartementet, 2007)

Gjennom høyesteretts kjennelse av 22.november 2002 er det fastslått at innsyn i e-post innebærer behandling av personopplysninger og dermed faller det inn under personopplysningslovens virkeområde. Verken personopplysningsloven eller personopplysningsforskriften har noen spesielle bestemmelser som gjelder innsyn i elektroniske verktøy arbeidsgiver har stilt til de ansattes disposisjon. Dette gjelder også innsyn i e-post(Administrasjonsdepartementet, 2007)

I enkelte situasjoner er det likevel mulig å foreta innsyn i ansattes e-post. I de tilfeller dette er mulig er det snakk om å hente ut nødvendig, virksomhetsrelatert e- post. Dette er e-post som er knyttet til gjennomføring av arbeidsoppgaver. I de tilfeller innsyn er nødvendig skal dette alltid være saklig begrunnet (Dagslet, 2006). For at arbeidsgiveren skal kunne ha innsyn i arbeidstakers e- post, må arbeidsgiver oppfylle grunnkravene til behandlingen av personopplysninger i personopplysningsloven § 11.

I følge datatilsynets erfaring viser det seg at det er problemer knyttet til tolkningen av § 11b om at personopplysninger som blir behandlet skal:

"bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet" (personopplysningsloven § 11b).

Det dukker ofte opp uenigheter mellom arbeidsgiver og arbeidstaker i forhold til om innholdet i e-posten er virksomhetsrelatert eller ikke, slik at arbeidsgiver kan ha en saklig begrunnelse for innsyn. Hva som er privat e- post eller hva som er tilstrekkelig for at arbeidsgiveren skal kunne foreta innsyn er avhengig av situasjonen. I tillegg til grunnkravene i § 11 må også arbeidsgiver ha behandlingsgrunnlag i personopplysningslovens § 8. I denne paragrafen legger man til rette for de vilkårene som må være til stede for behandling av personopplysninger (Administrasjonsdepartementet, 2007)

Ifølge datatilsynets praksis viser det seg at grunnlag for behandling som ofte påberopes er henholdsvis samtykke og interesseavveining etter personopplysningsloven § 8 bokstav f:

"At *den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen" (personvernloven § 8 bokstav f).*

Den enkeltes samtykke er vektlagt stor verdi i forhold til behandling av personopplysninger. For at samtykke skal være gyldig må den gis frivillig. Utfordringene med forutsetning om frivillig samtykke blir satt på prøve når samtykke gis fra arbeidstaker på forespørsel fra arbeidsgiver.

Datatilsynet anbefaler at virksomheter utarbeider egne instruksjoner som omfatter blant annet regler for innsyn i e- post. Skal det da være behov for innsyn er det viktig at man følger de fremgangsmåter instruksen beskriver. Hvis man følger instruksen vil interesseavveiningen som regler favorisere arbeidsgiver, forutsatt at man følger personopplysningsloven og instruksene ikke gir større rett til innsyn en hva loven sier, da vil i så fall interesseavveiningen falle ut til fordel for arbeidstaker.

I de tilfeller det ikke forligger en instruks eller at det oppstår en situasjon som ikke instruksen dekker, vil det bli sett an hvilke andre tak som er gjort for å begrense inngrepet i den ansattes personvern (Administrasjonsdepartementet, 2007).

Personvern er et omfattende område. Hva som er den ”private sfære” og hva som kan gis innsyn i er ofte tema for diskusjon. For å skape retningslinjer og hjelpe frem enighet omkring dette spørsmålet har det nylig kommet et forslag til en e-postlov som vil fastsette regler for arbeidsgivers tilgang til ansattes e-post. Forslaget omfatter arbeidstakernes vern mot innsyn i IT verktøy som arbeidsgiver har stilt til arbeidstakers disposisjon. E-post står sentralt i dette utkastet, men de samme vurderingene vil i stor grad gjøre seg gjeldene for andre kommunikasjonsmedium som for eksempel mobiltelefoner og innsyn i arbeidstakers internettbruk og private filer (Administrasjonsdepartementet, 2007). Dette vil i stor grad gjøre det vanskeligere for arbeidsgiver å vinne frem med sine bevis i arbeidsrettssaker.

Den store veksten i virksomheters og institusjoners bruk av elektroniske kommunikasjonsmidler har vært med på å skape større mulighet for at bedrifter kan overvåke de ansatte. Den teknologiske utviklingen fremskaffer også stadig nye programmer og verktøy som muliggjør overvåkning. Ledelsen har for eksempel mulighet for å loggføre hvilke internettsider medarbeiderne besøker i løpet av en arbeidsdag, og med ip telefoni er det også mulig å

overvåke telefonbruken. Med lett tilgjengelige programmer kan man lagre og deretter gjennomgå telefonsamtaler og e-post. Det viktigste regelverket Norge er bundet opp mot, er den europeiske menneskerettighetskonvensjonen (EMK). Den slår fast at "enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse" (Høringsnotat, 2004 s2). Hvordan dette tolkes er avhengig av hvilken forståelse som legges til grunn for begrepet privatliv. Er det for eksempel rimelig å kreve en privat sfære på arbeidsplassen? Dette og lignende spørsmål kan diskuteres i lys av integritetsperspektivet. Lesing av e-post og overvåkning av internettbruk kan oppfattes som et inngrep i arbeidstakerens private sfære.

Det finnes også mange argumenter for at bedriftene bør ha klare retningslinjer for de ansattes informasjonshåndtering, samt rutiner for oppfølging av misbruk. Uforsvarlig bruk av e-post og IT systemer kan blant annet øke faren for å eksponere bedriften for sikkerhetsrisiko. Med enkle hjelpemidler kan elektronisk kommunikasjon forfalskes og endres på en slik måte at det gjør det vanskelig å oppdage uten at man har den rette kunnskapen. Personer med adgang til e-post vil kunne endre innholdet i denne uten at det vil fremkomme i en senere utskrift. I slike tilfeller blir det nødvendig at man kan etterprøve opplysninger som er fremskaffet gjennom innsyn i e-post og annen elektronisk kommunikasjon. Dette for å kontrollere at informasjonen er korrekt og ikke har vært utsatt for endringer.

I høringsnotatet argumenteres det for at innsyn i e-post kanskje ikke er så godt egnet til å samle bevis i straffesaker og personalsaker. Som et argument for dette nevnes det at arbeidsgiver sjelden har tilstrekkelig kunnskap om innhenting av gyldig bevis, noe som vil vanskeliggjøre at bevisene kan etterprøves og der gjennom være gyldige i eventuelle rettssaker. (Administrasjonsdepartementet, 2007). Som et eksempel på en slik utfordring kan utskrift av e-post nevnes. Ved en utskrift vil man ikke kunne se når og hvor e-posten ble opprettet. Personverninteressene må kunne balanseres mot arbeidsgivers interesser mot det å beskytte seg mot skadelige konsekvenser (Borchgrevink, 2006).

5.3 Personopplysningsloven ved innsamling og behandling av elektroniske bevis

I denne delen skal jeg se nærmere på rutiner og sentral lovgiving som omhandler innsamling og behandling av personopplysninger.

Personopplysninger er opplysninger og vurderinger som kan knyttes til en identifiserbar enkeltperson jf personopplysningsloven § 2 nr 1. Tilknytningen kan være både direkte eller indirekte. *Direkte* tilknyttede opplysninger kan være for eksempel navn, personnummer, og fingeravtrykk. *Indirekte* tilknytning kan være opplysninger om bostedsadresse, telefonnummer eller yrkestittel (Coll & Schartum, 2004).

5.3.1 Innhenting

Felles for all innhenting av digitale bevis er at de opplysningene som innhentes svært ofte vil inneholde personopplysninger. Både informasjon fra elektroniske spor på Internett, anropslogger og informasjon om passering av bomringer kan inneholde personlige opplysninger. Opplysninger om enkeltpersoners handlinger vil komme inn under det man definerer som personopplysninger, men opplysninger om regnskap og om virksomhet uten særlig tilknytting til enkeltpersoner vil *ikke* komme under personopplysningsloven. I forhold der man ønsker opplysninger om *juridiske personer,* omfattes dette som hovedregel ikke av personopplysningsloven. Dette betyr igjen at innsamling av bevis som er knyttet til juridiske personer i utgangspunktet vil falle utenfor personopplysningsloven. Eksempler på det kan være skatteunndragelse eller korrupsjon hos en bedrift. Dette må nyanseres, der grensen mellom personopplysninger og virksomhetsopplysninger i mange tilfeller kan være vanskelige å trekke (Johansen et al., 2001)

I tilfeller der privat virksomhet eller enkeltpersoner samler inn elektroniske bevis og selv avgjør på hvilken måte det skal foregå, vil de betraktes som *behandlingsansvarlige*, her vil også en rekke plikter etter loven være gjeldende. Hvis innsamling av bevis skjer ved avtale med politi eller andre vil disse kunne oppfattes som behandlingsansvarlige, eller at det er et delt behandlingsansvar (Coll & Schartum, 2004; Jansen & Schartum, 2005).

De *strafferettslige sider* er spesielt sentrale i forbindelse med den offentliges innhenting av elektroniske bevis (Coll & Schartum, 2004). I strafferetten og strafferettsprosessen finner man en rekke bestemmelser for bevisinnhenting som er av personvernmessig karakter. I straffelovens § 390 og § 390a har vi klare personvernrettslige bestemmelser som verner om privatlivet. I § 390 straffes den som krenker privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold. Flere av handlingene som er straffebelagt i straffeloven, for eksempel § 145 som setter straff for brevbrudd og § 145a som regulerer ulovlig telefonavlytting, er med på å beskytte den personlige integriteten og den private sfæren. Det kan i spesielle tilfeller likevel være lovlig for politiet å utføre for eksempel telefonavlytting som en del av en etterforskning ved innsamling av bevis. Det er verdt å merke seg at lovligheten avhenger av en rekke vilkår for at politiet skal kunne utføre både telefonavlytting og åpning av brev. Disse handlingene, som rammes av *straffeloven*, er det bare politiet som kan gjennomføre og kan ikke utføres av privatpersoner som ønsker å sikre digitale bevis (Coll & Schartum, 2004).

For at det i det hele tatt skal være lovlig for private å samle inn personopplysninger, blant annet i form av elektroniske bevis, må man ha et rettslig grunnlag for innhentingen, jf. personopplysningsloven (senere omtalt som ”pol”) § 8. Denne loven bygger på EU- direktivets artikkel 7. Ved innhenting av sensitive personopplysninger er det krav til særlig rettslig grunnlag. Dette står i pol § 9. Og er basert på EU- direktivets artikkel 8 nr 1-5. Hva som regnes som sensitive opplysninger er fastsatt i pol § 2 nr 8. Kravene i § 8 og 9 er bygget opp under samme modell og skal være oppfylt hver for seg. Det vil si at man må ha samtykke fra den registerte, innsamlingen må ha hjemmel i lov og må anses som nødvendig i samsvar med det som er angitt i loven.

I pol § 11 står *grunnkravene til innsamling av personopplysninger*. Denne bestemmelsen inneholder grunnkrav til gjennomføring av selve innsamlingen av personopplysningene. Dette gjelder både for sensitive og ikke sensitive opplysninger. I § 31 gjelder *meldeplikten*. Den inneholder blant annet bestemmelser som melding til datatilsynet før behandlingen av personopplysninger med elektroniske hjelpemidler. Etter personopplysningsloven § 33 kreves

det *konsesjon* for tilgang på sensitive personopplysninger. Konsesjonspliktet betyr hovedsakelig at den behandlingsansvarlige må innhente forhåndstillatelse fra Datatilsynet før man kan sette i gang en behandling av personopplysninger (se fig 3) (Johansen et al., 2001; Schartum & Bygrave, 2004).

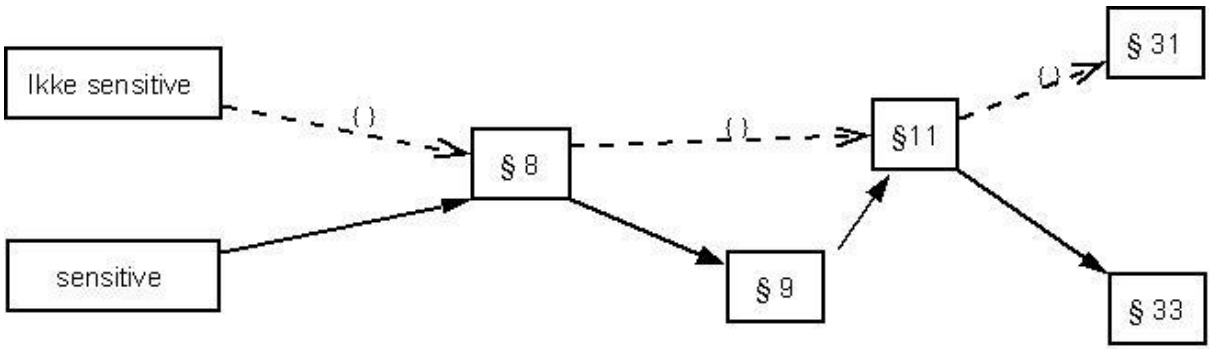


Fig 3 innhenting av personopplysninger (Johansen et al., 2001)

5.3.2 Behandling

Begrepet *behandling* dekker alt som kan tenkes å bli gjort med personopplysningene etter at de er innhentet, som for eksempel innsamling, lagring, retting og sletting. (Coll & Schartum, 2004).

Personopplysningsloven (pol) ble nevnt over, i forbindelse med innhenting. Loven omfatter også all behandling av personopplysninger. Denne loven med tilhørende forskrifter trådde i kraft første januar i 2001. Denne loven gjelder i utgangspunktet alle virksomheter og personers behandling av personopplysninger; også informasjonsopplysninger som kan være aktuelle som digitale bevis (Coll & Schartum, 2004). Bruk av personopplysninger reguleres for øvrig av en rekke *særlover*, som i hovedsak gjelder visse typer personopplysninger. Særlovgivningen kan innenfor enkelte saksområder av ulik grad komme foran i rang enn personopplysningsloven. Dette gjelder hovedsaklig for helseinstitusjoners behandling av helseopplysninger.

Personopplysningsloven skiller mellom *generelle* og *sensitive* personopplysninger. Det stilles strengere krav til behandling av sensitive personopplysninger enn for andre

personopplysninger. At personopplysningene er *sensitive* betyr generelt sett at den har et innhold som den registrerte personen ønsker å beskytte. I pol § 2 nr 8 er sensitive opplysninger definert som opplysninger om rasemessige, eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person er har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger. Det er i hovedsak opplysningstypen som avgjørende for om en opplysning skal sees på som sensitiv eller ikke. Om en behandlingsansvarlig setter opp en loggrutine som registrer opplysningstypen som viser klart staffbare forhold (disposisjoner) vil disse loggopplysningene være sensitive, men dersom det kun gjelder uønskede disposisjoner som ikke er straffbare vil ikke opplysningene være sensitive. Ved behandling av sensitive personopplysninger gjelder det skjerpede krav til det rettslige grunnlaget for behandlingen. Det er i utgangspunktet bare behandling av sensitive opplysninger som er konsesjonspliktig se pol § 33 (Coll & Schartum, 2004; Schartum & Bygrave, 2004).

Den *behandlingsansvarlige* er den som har bestemmelsesrett over formålet med behandlingen av personopplysningene og hvilket hjelpemiddel som skal benyttes, jf § 2 nr 4 (Jansen & Schartum, 2005). En behandlingsansvarlig er pålagt en rekke plikter ved behandling av personopplysninger og er den ansvarlige for at grunnlaget for behandlingen er lovlig og at behandlingen skjer i henhold til lover og regler og kan saksøkes ved overtredelser av lovens bestemmelser.

5.4 Informasjonssikkerhet

Behovet for å sikre informasjons verdier i en organisasjon har blitt viktigere nå som dataressurser har blitt mer komplekse. Dataressurser har blitt en del av den moderne driften i foretningsvirksomhet, offentlig sektor, militæret og det akademiske miljøet. Derfor er det nødvendig med data og nettverksikkerhet og at organisasjoner opprettholder full kontroll over dataressursene sine(Figg & Zhou, 2007).

For å sikre at lovens bestemmelser oppfylles av den behandlingsansvarlige medarbeider i virksomheten pålegger personopplysningsloven den behandlingsansvarlige å etablere rutiner

for informasjonssikkerhet (Personopplysningsloven § 13 og personopplysningsforskriften kapittel 2)(Coll & Schartum, 2004). Man er altså pliktig å oppbevare elektronisk lagret informasjon på en forsvarlig måte.

Utfordringene dukker opp når personopplysninger skal være tilgjengelig for mange offentlige etater gjennom effektivisering i offentlig forvaltning. Både den enkelte og samfunnet generelt kan ha nytte av viktige helseopplysninger om oss. På den måten kan vi oppnå en sikrere og raskere behandling (Jansen & Schartum, 2005). Utfordringene knyttet til pasientjournalsystem (EPJ) har vist seg å være et problem når det kommer til personvernhensyn. I flere tilfeller har man oppdaget sniking i journaler til både ansatte og pasienter. Et av hovedproblemene er at elektroniske pasientjournalene ikke er forsvarlig sikret mot innsyn fra de ansatte som ikke har legitimt behov for opplysningene (Dommerud, 2007). Man kan på mange måter sammenligne dette med innsyn i e post og private dokumenter som man lager på arbeidsplassens servere. Hvem har tilgang og kan disse dokumentene brukes i en eventuell arbeidstvist. Derfor har også Informasjonssikkerhet en viktig verdi for en organisasjon på lik linje med andre virksomhetsaktiva. Informasjonssikkerhet beskytter mot en lang rekke trusler med det formålet å sikre drifts kontinuitet, redusere skader og maksimere utbyttet av investeringer og forretningsmuligheter (BSI, 2001).

Samtidig som kryptering beskytter innholdet i en fil, en melding eller annen form for kommunikasjon, beskytter det ikke identiteten til den som kommuniserer og hvem han eller hun kommuniserer med. Skal man analysere mulige trusler sett fra et brukerperspektiv kan man skille mellom brukerens interaksjon med systemet, overføring av data gjennom nettverket og behandling i et sentralt datasystem. Det er også krav til hvordan man skal sikre personopplysningen. Dette er viktig blant annet fordi sikkerhetsbestemmelsene i forskriften til personopplysningsloven er forholdsvis omfattende og detaljerte. Derfor kan forskriftene komme til å få innvirkning på tenkningen rundt sikring av informasjonssystemer i en mer generell kontekst.(Jansen & Schartum, 2005). Krav til sikring av personopplysninger er fastslått i lov om behandling av personopplysninger. Loven har kun en bestemmelse som direkte

regulerer informasjonssikkerheten (§13). Det ligger også en bestemmelse om internkontroll (§14). Det er også en del andre bestemmelser som man kan sies å gjelde Informasjonssikkerhet (Jansen & Schartum, 2005). Informasjonssikkerhet beskytter informasjon mot en rekke trusler mot det formålet å sikre driftskontinuitet, redusere skader og maksimere utbyttet av investeringer og foretningsmuligheter (BSI, 2001). Informasjon forekommer i mange former, det kan trykkes, skrives på papir, lagres elektronisk, overføres via e- post eller annen elektroniske media. Informasjonssikkerhet omfattes i denne sammenheng beskyttelse av: a) konfidensialitet, det vil si at informasjonen bare er tilgjengelig for de med autorisert tilgang. b) Integritet, som omhandler nøyaktig og fullstendig informasjon om behandlingsprosessen c) Tilgjengelighet, som omfatter at bare autoriserte brukere har tilgang til informasjon og tilhørende tjenester når de har bruk for dem (BSI, 2001).

Sikring av informasjonssystemer er nødvendig i stadig større grad, ettersom organisasjoner og deres informasjonssystemer står overfor en rekke sikkerhetstrusler. For eksempel kan dette være sabotasje, spionasje, spredning av datavirus, datakriminalitet og tjenesteblokkering. Vanskelighetsgraden rundt sikkerhetskontroll er stadig økende ettersom sammenkoblingen av både offentlige og private nettverk samt deling av informasjonsressurser gjør det vanskeligere å sikre tilgangskontroll. I mange tilfeller er ikke informasjonssystemet utformet med tanke på sikkerhet, i tillegg er sikkerheten som kan oppnås med tekniske virkemidler begrenset og bør suppleres med passende styring og prosedyrer. Håndtering av sikkerhetstiltak i bedriften krever deltagelse fra alle ansatte i organisasjonen. I tillegg kan det være lurt å ta med leverandører, kunder eller andre interessenter (BSI, 2001). Gjennom en metodisk vurdering av sikkerhetsrisikoen fastsettes krav til sikkerhet. En risikovurdering består av en systematisk gjennomgang av sannsynlige skader for organisasjonen som følge sikkerhetsvikt. Da ser man på følgene av svekket konfidensialitet, integritet, eller tilgang på informasjon. I tillegg ser man på sannsynlighet for at en slik svikt skal forekomme sett i lys av eksisterende trusler og svakheter. (BSI, 2001.

6 DATAETTERFORSKNING

Man har som vi nå har sett ofte behov for å sikre digital informasjon. I tilfeller der det er spørsmål om hvorvidt det har skjedd noe lovstridig, for eksempel under en rettssak, kan behovet for å etterforske hvor troverdig den elektroniske informasjonen er. Man kan også ha behov for å anvende elektronisk lagret og sikret informasjon som ledd i en gitt etterforskning. I dette kapittelet vil jeg konsentrere meg om slik etterforskning.

På mange måter har datateknologien bidratt til at sikkerheten kan ivaretas på en bedre og mer effektiv måte nå enn før, men på den andre siden har teknologien også gjort oss mye mer sårbare og tilgjengelige for datainnbrudd eller datakriminalitet. Konsekvensene av uønskede hendelser kan være dramatiske (Jansen & Schartum, 2005).

I dette kapittelet vil jeg gå gjennom det man kaller dataetterforskning og de metoder man bruker i sikring, analyse og evaluering av elektroniske bevis.

Dataetterforskning er en samling av teknikker og verktøy som brukes for å finne bevis på en pc. (Caloyannides, 2004). Det kan også defineres som praktisk bruk av tekniske metoder og verktøy for bevaring, sikring, identifisering, analyse, dokumentering og presentasjon av elektronisk informasjon (Larsen, 2007).

Dataetterforskning er en ny praksis, eller disiplin, som ble viktig etter hvert som datamaskiner ble vanlig både i hjemmet og innenfor foretningsvirksomheter (Willasen & Stig Frode Mjølsnes, 2005)(Willasen & Stig Frode Mjølsnes, 2005)(Willasen & Stig Frode Mjølsnes, 2005)[63](Willasen & Stig Frode Mjølsnes, 2005). Elektronisk etterforskning ble etter hvert vanlig for politiet, fordi det å komme over datamaskiner som inneholdt elektronisk lagrede bevis etter hvert ble mer dagligdags. Til slutt ble det nødvendig å etablere spesialenheter som skulle håndtere elektroniske bevis. Her var USA først ute med å etablere en slik enhet da FBI opprettet ”Computer Analysis and Response Team”(CART) i 1984. Senere ble lignede avdelinger opprettet i Storbritannia i regi av Scotland Yard (Willasen & Stig Frode Mjølsnes, 2005). I Norge jobbes det med digital etterforskning både innenfor det private og det offentlige. I 1995 opprettet

ØKOKRIM en gruppe som jobbet med datakriminalitet, som i 2002 fikk navnet Politiets datakrimsenter (PDS). De har som oppgave å ta seg av digital etterforskning på nasjonal basis i politiet. På den kommersielle siden har vi IBAS AS som har utført oppgaver både innenfor privat sektor og på oppdrag fra statlige institusjoner innen digital etterforskning siden slutten av 1990 tallet (Larsen, 2007).

Dataetterforskere kan samle inn og bruke mange former for elektroniske bevis. Digitale spor i en datamaskin kan være filer, dokumenter, cookies , cache-minne, internetthistorikk og e-post kommunikasjon. Elektronisk informasjon har begynt å spille en viktig rolle som bevis i en økende andel av saker som involverer for eksempel urettmessig tilegnelse av verdier, bedrageri, seksuell diskriminering, tyveri av intellektuell kapital, sporing av aktiva, innsidehandel og aksjemanipulering. Mer tillit har blitt tilegnet elektroniske bevis i rettstvister, derfor er det viktig å innhente bevis gjennom metoder som allerede er brukt eller testet i retten (Williams, 2006).

Det en dataetterforskning oftest går ut på, er å gjenfinne informasjon som potensielt kan anvendes som elektroniske bevis. På harddisken lagres data automatisk, og i tillegg registreres internettrafikken. Når det gjelder slettet informasjon kan man også finne dette på datamaskinen. Selv om filene tilsynelatende er slettet for brukeren er det likevel mulig for en dataetterforsker å finne filen (Nysæter, 2006). Jeg vil forklare dette nærmere. Det man egentlig gjør når man lagrer en fil, er at filnavnet, størrelse og lagringssted blir lagret i ”file allocation table”(FAT) ,eller i New Technology File System (NTFS). NTFS har etter hvert erstattet FAT og nå er standard filsystemet til til Windows. Når filen blir slettet, blir ingen data direkte påvirket av dette. Det er bare oppføringen i FAT eller NTFS, som blir fjernet. Oppføringen i FAT eller NTFS er bare en markør, eller et flagg, som forteller operativsystemet at plassen kan brukes om igjen til å skrive over ny data. Dette betyr ikke at data nødvendigvis blir skrevet over(Zetterstrom, 2002)

Det er bare nylig at det vitenskaplige miljøet har blitt interessert i digital etterforskning, som et resultat av det er digital etterforskning en ”ad-hoc -praksis” som ennå mangler det vitenskaplige fundamentet. Men på grunn av offentlige behov, direkte forespørsler fra regjerings autoriteter,

har ICT sikkerhetsmiljøet nå vist en interesse i å tilføre digital etterforskning en vitenskaplig tilnærming, og i 1998 ble Scientific Work Group on Digital Evidence (SWGD) opprettet i USA og forskningsmiljøet etablerte The International Journal on Digital evidence i 2002(Willasen & Stig Frode Mjølsnes, 2005).

Forskning med et mål om å klargjøre terrenget eller å trekke nye grenser innenfor et spesielt felt blir ofte gjort uavhengig av praksis. Innefor dataetterforskning er det veldig viktig at forskere kjenner til hva forskningen deres blir brukt til i felten. Dette gjelder spesielt når forskning fører til utvikling av et nytt etterforskningsverktøy som skal brukes innefor sivil- og kriminaletterforskning. I slike tilfeller kan verktøy utviklet for å prosessere digitale bevis komme under undersøkelse, eller bli "gått etter i sømmene". Svakheter kan føre til at bruken av verktøyet må bli begrenset. (Mocas, 2004).

Som vi ser her er det i dag et stort behov for ytterligere forskning på feltet om dataetterforskning, samt et mer utstrakt samarbeid mellom forskere og pragmatikere.

6.1 Forvaringskjeden: sikring, analyse og evaluering

De digitale etterforskingsmetodene sikring, analyse og evaluering av elektroniske bevis vil bli grundig gjennomgått nedenfor. Metodene beskrevet her skal bidra til å danne grunnlaget for min senere presentasjon av en sjekkliste for hvordan man best mulig kan ta vare på elektroniske dokumentbevis.

Dataetterforskning kan deles inn i tre trinn eller faser (Carrier, 2003; Willasen & Stig Frode Mjølsnes, 2005). Disse er som følger:

1. Sikre bevis
2. Analysere bevis
3. Evaluere bevis (resultat)

Figur 4 gir en skjematisk oversikt over disse tre trinnene, og hvordan de står i sammenheng med hverandre (figur 4).

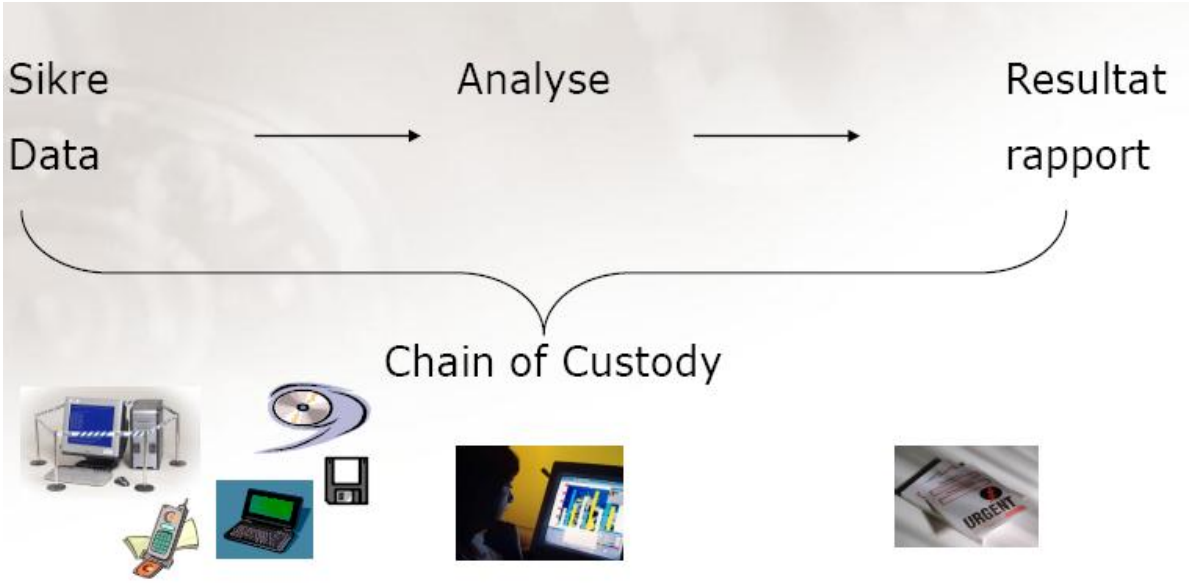


Fig 4. Forvaringskjeden(Nysæter, 2006)

Jeg vil videre ta for meg hvert trinn i kronologisk rekkefølge.

6.1.1 Sikring av bevis

Prosessen med å sikre bevisene innebærer at man produserer eksakte kopier av det beslaglagte digitale mediet. Dette kalles speilkopiering, som illustreres i figur 5 (fig 5). Målet med det er å sikre all data. Man bruker da hashingteknikk for å bevise at innholdet i kopien er den samme som i den originale, noe som følgelig er med på og sikre dataens integritet. Denne delen av etterforskningen langs forvaringskjeden er viktig, og må gjøres før analysedelen (Larsen, 2007; Mason, 2007). Grunnen til at det er viktig å være påpasselig med elektroniske bevis er at slike bevis er lette å endre på.

Fig 5. speilkopi av harddisk (Nysæter, 2006).

6.1.2 Analyse av bevis

I den andre fasen av bevisets forvaringskjede skal de elektroniske bevisene analyseres. Denne fasen er noe mer komplisert og tidkrevende med tanke på at man må gjennomgå hvert enkelt bevis. Utfordringene ligger i at det ofte er store datamengder som må behandles og det er sjelden klarlagt hvilken deler av datainformasjonen som kan ha status som bevis i en rettsprosess (Willassen & Stig Frode Mjølsnes, 2005). Analysen av bevisene må innebære en gjennomgang av både teksten i dataene og dataens egenskaper. Det vil også kunne inkludere det å se etter og gjenopprette slettede filer eller anen data som kan være skjult på disken samt sjekke logger for aktivitet og ikke allokerte områder på disken for restdata (Mason, 2007)

Casey (gjengitt i Mason, 2007) foreslår flere underkategorier i analysedelen:

a) Bedømmelse av innhold og kontekst: digitalt bevis som blir betraktet eller lest av et menneske, med tanke på å vurdere spørsmål som hensikt, motivasjon og mulighet.
b) Eksperimentering: det er her at uortodokse eller uprøvde metoder og teknikker må vurderes brukt under en etterforskning. Om nye metoder blir brukt er det viktig å dokumentere eksperimentet riktig. Ved å eksperimentere vil en ny teknikk enten bli akseptert eller avvist.
c) Fusjon eller korrelasjon: sammenføring av de digitale og ikke digitale bevisene for å hjelpe til med å forstå helheten.

d) Validering: denne delen skal analysen representere funnene gjort under den digitale etterforskningen basert på sunn fornuft.

Mislykkes man med å bedømme de elektroniske bevisene kan det føre til falske antagelser (Mason, 2007). Det er derfor viktig at man etterstreber en grundig analysefase.

For å kunne utføre analyse av elektroniske bevis er det som regel nødvendig å bruke spesialeverktøy, denne programvaren er ofte proprietær, det vil si programvare der opphavsrett brukes til å beskytte produsentens eierskap. Den senere tid har det kommet "open source" -alternativer som har sammenlignbare trekk som de proprietære. Fordelen med "open source" -verktøyene er at kildekoden er tilgjengelig og dette gjør analyseverktøyene mer pålitelig slik at man kan vurdere verktøyene på mer troverdig måte enn hvis kildekode er lukket. Carrier(2007; 2003) konkluderer med at hvis verktøyene skal få troverdighet er det viktig at prosedyrene som har blitt brukt blir offentliggjort, vurdert og debattert. (Carrier, 2003)

6.1.3 Evaluering av bevis

Den tredje fasen i forvaringskjeden til et elektronisk bevis er å evaluere bevisene. I denne fasen lager man en konklusjon basert på de funn gjort i sikrings- og analysefasen. Uansett om man forbereder en strafferettsprosess eller en sivilsak er det viktig at rapporten inneholder en mengde informasjon som er relevant for saken, det kan for eksempel omfatte:

a) Notater klargjort under undersøkelsesfasen av etterforskningen;
b) Detaljer om hvordan etterforskningen ble utført;
c) Detaljer om forvaringskjeden;
d) Validiteten til prosedyrene brukt; og
e) Detaljer om funnene i analysen av de elektroniske bevisene:

i. Karakteristiske filer eller data som var direkte relatert til etterforskningen;
ii. Ytterligere filer og analyse av eventuelle grafiske filer;
iii. Type søk som har blitt utført, som for eksempel, søk etter nøkkelord, og hvilke program som har blitt undersøkt;

iv. Relevant bevis funnet på internett, slik som e-post, analyse av nettider som er besøkt og loggfiler;

v. Indikasjoner på navn som kan påvise eierskap til programvare som for eksempel, hvem er programvaren registrert på; i tillegg

vi. Se om det har vært forsøk på å skjule data, hvis så hvilke metoder ble brukt.

(Mason, 2007)

Det er viktig at rapporten fra evalueringsfasen reflekterer hvordan undersøkelsen ble utført og hvilken data som ble gjenopprettet. Det er avgjørende at den som undersøker kan påvise hvilke metoder som ble brukt i undersøkelsen og brukbarheten til prosedyrene og verktøyene brukt. Grunnen til at man må være grundig i denne delen er at noen vil kunne stille spørsmålstegn ved validiteten og utfordre legitimiteten og konklusjonene til de elektroniske bevisene som er samlet inn, analysert og evaluert (Mason, 2007).

Det er verd å merke seg at det ikke finnes noen spesielle rutiner i norsk sivil eller strafferettsprosessen for hvordan evaluering av elektroniske bevis skal utføres (Larsen, 2007).

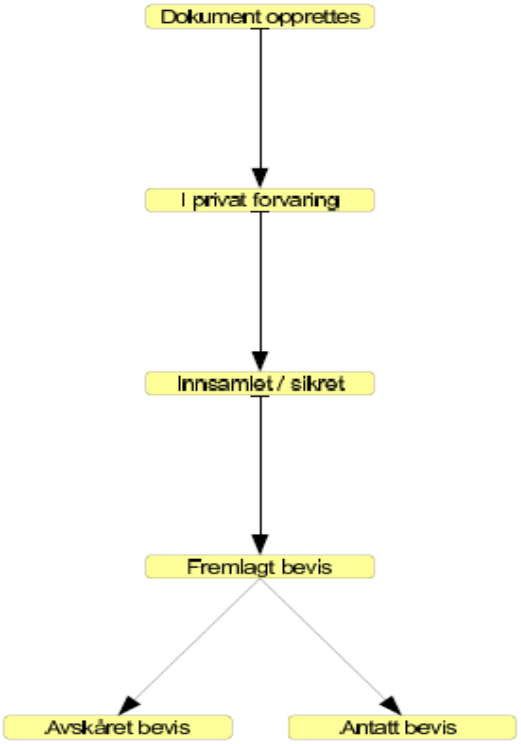
6.2 Verdikjeden til elektroniske bevis

I tillegg til de tre nevnte fasene i forvaringskjeden er det også mulig å sjekke *verdikjeden* til de elektroniske bevisene. Selv om jeg konsentrerer meg mest om forvaringskjeden, er det interessant å gi en kort framstilling av bevisets bevegelse gjennom verdikjeden.

Verdikjeden beskriver hele livsløpet til et bevis. Når livsløpet er til det elektroniske beviset er kartlagt vet man også mer om egenskaper som brukbarhet, integritet og troverdigheten til beviset. Det finns i dag ingen rutiner for kartlegging av bevisets verdikjede verken i sivil eller strafferetten. Men likevel er det viktig at det elektroniske bevisets validitet er dokumentert når en dommer skal vurdere det. Validiteten og autentisiteten til et elektronisk bevis bygger på tre egenskaper; brukbarhet, integritet og troverdighet. Derfor er det viktig at påtalemyndigheten vektlegger disse egenskapene når de skal sikre, analysere og presentere bevis, slik at bevisfremleggingen blir så nøyaktig som mulig (Larsen, 2007). I sivile saker vil det også være

viktig at bevisene validitet og autensitet er troverdig selv om det er andre beviskrav som gjelder. I straffesaker har påtalemyndigheten bevisbyrden og må føre bevis for tiltaltes skyld og til enhver tvil skal komme tiltalte til gode, mens sannsynlighetsovervekt er hovedregelen i sivile saker.

Verdikjeden til et bevis kan hovedsakelig deles opp i fire stadier: privat forvaring, innsamlet og sikret, fremlagt som bevis og antatt eller avskåret som bevis. Disse er skissert i figur 6 (Figur 6).



Figur 6. Verdikjeden til et digitalt dokumentbevis (Larsen, 2007)

I den *første* delen av verdikjeden befinner det elektroniske beviset seg i privat forvaring. Det vil si at dokumentet ikke har fått noe status som bevis. Det har heller ikke blitt gjennomført noe tiltak for å sikre dokumentet. Når dokumentet er opprettet, er det kommet inn i den første fasen i verdikjeden. Når digitale dokumenter som for eksempel et MS Word dokument blir opprettet, er det hovedsaklig enkeltpersoner som har gjort dette ved å starte

tekstbehandlingsprogrammet og opprettet et dokument. Det opprettet automatisk et tidsstempel som man kan finne i dokumentets *metadata*. Det kan i tillegg opprettets metadata som forfatternavn og programvare. I den *andre* fasen blir det elektroniske dokumentet innsamlet og sikret som et mulig bevis. Dokumentet kan bli samlet inn ved for eksempel speilkopiering av hardisk eller andre metoder for å sikre seg dokumentet på en slik måte at det beholder son autentisitet. I den *tredje* fasen blir det digitale dokumentet fremlagt som bevis. Her tar retten stilling til om dokumentet kan brukes som bevis eller om det må avskjæres(Larsen, 2007). Det blir tatt stilling til om beviset har relevans for saken, hvis ikke skal det avskjæres. I sivile saker bedømmes bevis ut fra partenes krav om beviset er relevant for saken eller ikke (Hov, 2007). Hvis man på dette stadiet kjenner til bevisets verdikjede kan man få en oversikt over bevisets historie og til en viss grad hvilke aktører som har vært delaktig i verdikjeden. Opplysninger som når dokumentet ble opprettet, når ble det sist lagret og har dokumentet blitt skrevet ut (Larsen, 2007). Den *fjerde* og siste delen i verdikjeden til et elektronisk bevis er om det blir avskåret eller antatt som bevis. Beviset kan bli avskåret dersom domstolen mener at beviset ikke har relevans for saken.

For å prøve ut noen av grunnprinsippene som er presentert i dette kapittelet om dataetterforskning og samtidig gjøre en undersøkelse av ulike dokumenters autentisitet og resistens mot endring, vil jeg i neste kapittel utføre testing på elektroniske dokumenter.

7. TESTING AV ELEKTRONISKE DOKUMENTER

For å finne ut i hvilken grad de elektroniske dokumentene klarer å beholde sin autentisitet ved forskjellige former for behandling har jeg gjennomført testing av elektroniske dokumenter. Det ble gjort testing i form av fire ulike tester på to forskjellige typer dokumenttyper: et MS Word 2007-dokument og et OpenOffice -dokument. I tillegg utførte jeg en manipulasjon av metadata i et MS Word 2003 dokument.

Videre følger det en metodebeskrivelse og en redegjørelse for resultater. Etter at resultater og tolkninger er presentert, vil jeg komme inn på hvilke praktiske implikasjoner som kan trekkes på grunnlag av resultatene i håndteringen av elektroniske bevis. Jeg vil også berøre dette temaet i oppgavens drøftingsdel.

7.1 Testbeskrivelse

Det ble i alt utført tester på tre forskjellige formater. Det var MS Word 2007, MS Word 2003 og Open Office dokumenter. På MS Word 2007 og OpenOffice ble det testet fire forskjellige lagrings- og kopieringsmåter. Det i tillegg utført en manipuleringstest i MS Word 2003. Årsaken til at manipuleringen ble gjort i MS Word 2003 var at det bare var i denne versjonen analyseverktøyet fikk opp all metadatainformasjon som lå i Word. I MS Word 2007 og Open Office var det bare fil navnet som kom opp i OLE metadata. I file system metadata kom informasjonen som vi bruker i testingen og analysen av MS Word 2007 og Open Office dokumentene.

Målet med testene er å undersøke hvorvidt metadataene og hashverdiene kan være med på å sikre integriteten til elektroniske dokumenter ved forskjellige lagrings- og kopieringsmåter. Poenget med denne testen var ikke en grundig analyse av alle metadata og hashverdier men heller å sjekke hvorvidt disse dataene forble statiske, eller om de endret seg. Dette for å teste (P1) og de relevante delspørsmål til denne problemstillingen.

Problemet er reelt i forhold til at et elektronisk dokument kan gå gjennom mange ledd i verdikjeden før det blir lagt fram som et bevis i en rettssak. I denne prosessen kan dokumentet bli håndtert av både mennesker og datasystemer. Derfor ønsker jeg å se på om håndtering av dokumenter på forskjellig vis uten noen form for retningslinjer kan være med på å redusere dokumentets integritet, og i hvilken grad metadata og hashverdier kan brukes til å vurdere dette. I tillegg har jeg utført en manipulering av metadata i Word 2003. Dette for å se om det blir noen endringer i hashverdiene når dokumentet manipuleres. Dersom dette er tilfelle vil det si at hvis noen for eksempel endrer forfatternavn i metadataene vil dette påvirke hashverdiene slik at dokumentet ikke beholder sin autentisitet. For at man skal kunne bruke hashverdien som indikator på kvalitet og integritet på et dokument er man selvfølgelig avhengig av at man først har ferdigstilt dokumentet og lagt til en hashverdi manuelt. Man kan ikke gjøre endringer i et dokument hvis man vil beholde dokumentets gyldighet, slik den er definert ved hashverdien. Det er også en forutsetning å notere seg hashverdien på et gitt dokument som senere skal evalueres. Dette fordi man trenger å sammenligne eventuelt nye verdier med originale verdier.

Først vil jeg beskrive de fire testene som ble gjort på hvert av to ulike dokumentformat. Før testingen kunne begynne ble originaldokumentet lagret. Her ble metadata og hashverdiene som de andre lagringsmåtene skulle testes opp mot generert og lagret. Selve testingen omhandlet lagrings- og kopieringsmåter. De samme testene ble utført i begge de to tekstbehandlingsprogrammene. Disse testene var som følger:

1: Lagring av dokumentet på en usb minnebrikke.
2: Dokumentet blir kopiert fra harddisk til usb minnebrikke.
3: Dokumentet lagres et annet sted på selve harddisken.
4:”Drag and drop” for å flytte dokumentet over på ekstern disk.

7.1.1 Analyseverktøy

Pinpoint Metaviewer er et gratis analyseverktøy som tillater brukere å raskt se på metadata i filsystemer, OLE metadata og hashverdier for MS Office-filer. Dette er et verktøy basert på

høyreklikk- og send funksjon. Med dette verktøyet kan man se på metadata og hashverdier i Windows. Med det samme man får ut informasjon i Metaviewer, kan man fritt kopiere alle meta- og hashverdier, eller velge ønsket verdi som man kan lime inn i et hvert tekstbehandlingsprogram.

Årsaken til at jeg valgte å anvende dette verktøyet i min testing av elektroniske dokumenter var at programmet var fritt tilgjengelig, gratis, og at det ga mulighet til å hente inn informasjon om både metadata og hashverdier, som jeg fokuserer på i denne oppgaven. Jeg skal videre gå gjennom testingen som ble foretatt i de to tekstbehandlingsprogrammene som ble brukt. Deretter presenteres fremgangsmåten for manipulasjon av metadata i et MS Word 2003 dokument.

7.1.2 Testing av MS Word 2007 dokument og OpenOffice- dokument

Testingen i Word 2007-dokumentet og OpenOffice- dokumentet ble gjennomført på tilsvarende måte; ved bruk av samme fire testmetoder. Nedenfor følger en beskrivelse av fremgangsmåten som ble fulgt når disse to dokumenttypene ble testet.

A- Opprettelse og lagring av originaldokumentet

Det ble først opprettet et dokument. Dette dokumentet representerte *originaldokumentet* og fungerte som en referanse på om originaliteten ble beholdt ved fire forskjellige lagrings- og kopieringsmåter

Etter at originaldokumentet var opprettet ble det lagt inn tekst i dokumentet. Dokumentet ble lagret i Word 2007 som: Test 1 Word2007.docx og i OpenOffice som: test2openoffice.odt.

Dokumentet ble deretter åpnet i Metaviewer, et analyseverktøy. Informasjon som kom opp i Metafeltet var: navn på dokument, dokumentets plassering på harddisken, tidspunktet dokumentet ble opprettet, sist modifisert og sist åpnet. I tillegg ble hash- verdiene MD5, SHA-1 og SHA-256 generert. Metadataene og hashverdiene ble kopiert og lagret i testmatrisen. Disse

verdiene ble videre brukt som referanseverdier i forhold til validering av originalitet til de forkjellige testdokumentene.

Først ble originaldokumentet åpnet. Deretter gikk jeg inn på ”Lagre som” og lagret dokumentet på en USB minnepinne. Navnet på originaldokumentet lot jeg stå uendret. Jeg brukte deretter Metaviewer for å hente metadataene og hashingverdiene, deretter ble disse verdiene lagret i en testmatrise.

B- Test 2: kopiering av originaldokument over på en USB minnepinne

Originaldokumentet, som ligger på harddisken, ble kopiert uten at jeg gikk inn og åpnet dokumentet først. Deretter ble dokumentet limt inn på en ekstern USB minnepinne. Jeg lagret testverdiene i en testmatrise.

C- Test 3: lagring av originaldokumentet et annet sted på lokal harddisk

Dette ble gjennomført ved å åpne dokumentet. Jeg gikk inn på ”lagre som”, og lagret dokumentet et annet sted på den lokale harddisken. Deretter åpnet jeg dokumentet med Metaviewer og lagret testverdiene i en testmatrise.

D- Test 4: ”Drag and drop”

Test 4 ble gjennomført ved å åpne mappen filen lå i, og deretter ble filen dratt over på den eksterne harddisken ved bruk av ”drag and drop” , som man kan bruke som kopieringsmetode i Windows XP dersom man ønsker å flytte dokumenter over til en ekstern enhet. Deretter ble Metaviewer brukt til å åpne dokumentet, og testverdiene ble lagret i en testmatrise.

7.1.3 Manipulering av metadata i MS Word 2003.

I denne testen ble det utført en manipulering av metadata for så å se om hashverdiene endret seg når dokumentet ble endret. Videre i oppgaven refererer jeg til denne testen som ”test 5”. Før selve testingen opprettet jeg et nytt originaldokument. Dokumentet ble lagret i MS Word

2003 format. Deretter ble dokumentet åpnet i Metaviewer og verdiene ble lagret i en testmatrise. Dette gjorde jeg for å ha et sammenligningsgrunnlag ved manipulasjonen, eller testingen, som skulle foretas. Målet var å se om hashverdiene endret seg ved manipulering av metadata.

E- Test 5: Manipulering av metadata i MS Word 2003

I neste fase ble originaldokumentet åpnet. Manipuleringen ble gjort ved at forfatternavn ble endret fra Robert Didriksen til Erik Eriksen. Jeg la i tillegg til teksten ”Manipulert dokument” i tittelfeltet. Deretter la jeg til teksten ”test ” i emnefeltet. Vider e la jeg til teksten ”Computer forensics” i nøkkelordfeltet. Dette ble så lagret. Dokumentet ble så avsluttet. Til slutt ble dokumentet åpnet i Metaviewer og verdiene ble til slutt kopiert inn i testmatrisen.

7.2 Resultater

I denne delen presenterer jeg resultatene fra testingen. Jeg vil legge frem resultatene i den samme rekkefølgen som de er beskrevet over. Etter at resultatene er presentert vil det følge en egen tolkningsdel med oppsummering og delkonklusjon av testingen.

7.2.1 MS Word 2007- testresultater

A- Opprettelse av originaldokument

OLE metadata:
File Name: Test 1 Word2007.docx
FILE metadata:
File Path: C:\Documents and Settings\user9\My Documents\Test 1 Word2007.docx
Created Date (FS): 28.03.2008 11:03:08
Last Modified (FS): 28.03.2008 11:03:08
Last Accessed (FS): 28.03.2008 11:03:08
File Size: 11719
MD5 Hash: C12C03AE4CBE9E55F7E9BE566D3FA33F
SHA-1 Hash: FFBBED3F0EA3CB78455F51795DC1CEC840D8D09A
SHA-256 Hash: B66D33B50F431D681E4D15756764DA0E14BA1BF0D2CDF698E8BFB078E07ED950

Den metadatainformasjonen som Word 2007 genererte var: filepath, dato for opprettelse av dokumentet, tid for siste modifisering og dato og klokkeslett for siste gang det ble åpnet. Det ble generert tre typer hash- verdier: MD5, SHA-1 og SHA -256. Disse verdiene ble brukt som referanseverdier i den videre testingen

B- TEST 1: Lagring av originaldokument på en USB minnepinne

OLE metadata
File Name: Test 1 Word2007.docx
File metadata
File Path: F:\Test 1 Word2007.docx
Created Date (FS): 28.03.2008 11:07:08
Last Modified (FS): 28.03.2008 11:07:10
Last Accessed (FS): 28.03.2008
File Size: 11726
MD5 Hash: D871D27A29EE4BE479716A0FB3BCBD0D
SHA-1 Hash: A4BE8247D08DCA84C871C6FF158CDDABBEE3298A
SHA-256 Hash: 3C3E9C9279467D39D86D4A7F59D4367A55A7D44383475FECA40A1634C4BE5793

- I denne testen endret Filepath seg fra det originale dokumentet til å referere til den eksterne enheten dvs: File Path: F:\Test 1 Word2007.docx.
- Dokumentet endret klokkeslett i "Created Date" -feltet. Det originale klokkeslettet var 11.03.08 og klokkeslettet i dokumentet lagret på den eksterne disken ble endret til kl 11.07.08. Dette indikerer at tidspunktet for det nye klokkeslettet ble generert i det øyeblikket dokumentet ble lagret på minnepinnen.
- Modifiseringstidspunktet ble også endret fra 11.03.08 til 11.07.10.
- Når det gjelder hashverdiene, ble også disse endret fra verdiene i originaldokumentet.

C- Test 2: kopiering av originaldokument over på en USB minnepinne

OLE metadata:
File Name: Test 1 Word2007.docx.vem
FILE metadata:
File Path: F:\Test 1 Word2007.docx.vem
Created Date (FS): 28.03.2008 11:36:25
Last Modified (FS): 28.03.2008 11:36:26
Last Accessed (FS): 28.03.2008
File Size: 10231
MD5 Hash: C12C03AE4CBE9E55F7E9BE566D3FA33F
SHA-1 Hash: FFBBED3F0EA3CB78455F51795DC1CEC840D8D09A
SHA-256 Hash: B66D33B50F431D681E4D15756764DA0E14BA1BF0D2CDF698E8BFB078E07ED950

- Filpath ble endret til FilePath: F:\Test 1 Word2007.docx.vem, en verdi som henviser til den eksterne lagringsenheten.
- Tid angitt i ”Created date”-feltet ble endret. Klokkeslettet på originaldokumentet var 11.03.08 Det nye klokkeslettet var 11.36.26. Dette markerer det tidspunktet dokumentet ble kopiert over til den eksterne enheten.
- Modifiseringstidspunktet ble også endret fra 11.03.08 til 11.36.26.
- Hashverdiene forble de samme som i originaldokumentet.

D- TEST 3: Lagring av originaldokumentet et annet sted på lokal harddisk

OLE metadata
File Name: Test 1 Word2007.docx
FILE metadata
File Path: C:\Documents and Settings\user9\Desktop\Test 1 Word2007.docx
Created Date (FS): 28.03.2008 11:47:57
Last Modified (FS): 28.03.2008 11:47:57
Last Accessed (FS): 28.03.2008 11:47:57
File Size: 11729
MD5 Hash: 5909F53F004CC5EC78EA050AA559519F
SHA-1 Hash: 645A3E5EC0D2F4C756A14E35E1D57DDAF38071A2
SHA-256 Hash: 215A912899858EC4FDD7901427786C86BB98F428D37CEDBB8159300496D8B006

- File path ble endret til: C:\Documents and Settings\user9\Desktop\Test 1 Word2007.docx.
- ”Created date” er endret fra 11.03.08 til 11.47.57. Man kan se at klokkeslettet viser tidspunkt for lagring av dokumentet,
- Verdiene i ”Last modified” ble endret
- Verdiene i ”Last accessed” ble endret
- Også hashverdiene endret seg i denne testen.

E- TEST 4: ”Drag and drop”

FILE metadata
File Name: Test 1 Word2007.docx
OLE metadata
File Path: F:\Test 1 Word2007.docx

Created Date (FS): 28.03.2008 11:03:08

Last Modified (FS): 28.03.2008 12:18:25

Last Accessed (FS): 28.03.2008 12:18:25
File Size: 15726
MD5 Hash: C12C03AE4CBE9E55F7E9BE566D3FA33F
SHA-1 Hash: FFBBED3F0EA3CB78455F51795DC1CEC840D8D09A
SHA-256 Hash: B66D33B50F431D681E4D15756764DA0E14BA1BF0D2CDF698E8BFB078E07ED950

- I denne testen endret filbanen seg når jeg dro dokumentet over på ekstern harddisk til: File Path: F:\Test 1 Word2007.docx.
- Her forandret ikke metadataverdiene for opprettelse av dokumentet seg.
- ”Created date” forble det samme som i originaldokumentet, det vil si 11.03.08.
- Klokkeslett for ”last modified ” og ”last accessed” endret seg begge til verdien 12.18.25,

dette var også tidspunktet der jeg gjorde drag and drop- handlingen.

7.2.2 OpenOffice - testresultat

A- Opprettelse og lagring av originaldokument

OLE metadata

File Name: test2openoffice.odt

FILE system Metadata

File Path: C:\Documents and Settings\user9\My Documents\test2openoffice.odt

Created Date (FS): 28.03.2008 14:33:56

Last Modified (FS): 28.03.2008 14:33:57

Last Accessed (FS): 28.03.2008 14:33:57

File Size: 7165

MD5 Hash: A0DC28D04DBC673B1B7A2E7F62C26A50

SHA-1 Hash: 5777615CC43AED40A4F1ACC7032C8EEE069CC30C

SHA-256 Hash: 43DF7B97869A21C6C415E0EA949DBE3AC9D8606BB44054E9062D4B1A80A6B84F

Den metainformasjonen som OpenOffice genererte, var: Filepath, dato og klokkeslett for opprettelse av dokumentet, dato og klokkeslett for sist modifisering, og dato og klokkeslett for siste gang det ble åpnet. Det ble generert tre typer hash- verdier MD5, SHA-1 og SHA -256. Disse verdiene ble brukt som referanseverdier i den videre testingen

B- TEST 1: Lagring av originaldokument på en USB minnepinne

OLE metadata

File Name: test2openoffice.odt

FILE system metadata

File Path: F:\test2openoffice.odt

Created Date (FS): 28.03.2008 14:58:38

Last Modified (FS): 28.03.2008 14:58:42

Last Accessed (FS): 28.03.2008

File Size: 7165

MD5 Hash: CA5D4A800FE8C5B6DE40B9D59CDA15CD

SHA-1 Hash: 0B3EAA8E7C15287941341F6720F6610DA411BD33

SHA-256 Hash: BC0D236293D8E94988E6A13B82F58147BD1B867A6B952ABEE1E100E14B4BAF78

- File path endret seg til: File Path: F:\test2openoffice.odt.
- Dokumentet endret i tillegg klokkeslett i ”Created Date” feltet. Det originale klokkeslettet var 14.33.56 og klokkeslettet i dokumentet lagret på den eksterne disken ble endret til kl 14.58.38.
- Modifiseringstidspunktet ble også endret fra 14.33.57 til 14.58.42
- Når det gjelder hashverdiene, ble disse endret fra verdiene på originaldokumentet.

C- TEST 2: Kopiering av originaldokument til en USB minnepinne

OLE metadata

File Name: test2openoffice.odt

FILE system metadata

File Path: F:\test2openoffice.odt

Created Date (FS): 28.03.2008 15:07:28

Last Modified (FS): 28.03.2008 14:55:28

Last Accessed (FS): 28.03.2008

File Size: 7165

MD5 Hash: A0DC28D04DBC673B1B7A2E7F62C26A50

SHA-1 Hash: 5777615CC43AED40A4F1ACC7032C8EEE069CC30C

SHA-256 Hash: 43DF7B97869A21C6C415E0EA949DBE3AC9D8606BB44054E9062D4B1A80A6B84F

- File Path: F:\test2openoffice.odt ble endret, henviser til den eksterne lagringsenheten en.
- Klokkeslettet i ”Created date” ble endret. Klokkeslettet på originaldokumentet var 14.33.56. Det nye klokkeslettet var 15.07.28. Dette markerer det tidspunktet dokumentet ble kopiert inn på den eksterne enheten.
- ”Last modified” tidspunktet ble også endret. I det originale dokumentet er modifiseringstidspunkt kl 14.33.57 og i det dokumentet som ble kopiert over på ekstern harddisk viser modifiseringstidspunktet kl 14.55.28.
- Hashverdiene forble de samme som i originaldokumentet.

D- TEST 3: Lagring et annet sted på den lokale harddisken

OLE metadata

File Name: test2openoffice.odt

FILE system metadata

File Path: C:\Documents and Settings\user9\Desktop\test2openoffice.odt

Created Date (FS): 28.03.2008 15:08:41

Last Modified (FS): 28.03.2008 15:08:42

Last Accessed (FS): 28.03.2008 15:08:42

File Size: 7165

MD5 Hash: 19935F6A82E53A6FD5C0C236CA786B66

SHA-1 Hash: 432B262DDC2DBA51D0FA09157108BC251A0C8C26

SHA-256 Hash: 45C7F9F20B2EE4C2D7264F5CC4AB8F1BD48A5A414C6693EC41E54B9ED58E113E

- File Path: (C:\Documents and Settings\user9\Desktop\test2openoffice.odt)endret seg til området på harddisken der dokumentet ble lagret.
- Klokkeslett på ”Created date” ble endret fra 14.33.56 til 15.08.41.
- Det skjedde endringer i klokkeslett på ”Last modified”
- Det skjedde endringer i klokkeslett på ”Last accessed.
- Hashverdiene endret seg

E- TEST 4: ”Drag and Drop”

OLE metadata

File Name: test2openoffice.odt

FILE system metadata

File Path: F:\test2openoffice.odt

Created Date (FS): 28.03.2008 14:33:56

Last Modified (FS): 28.03.2008 15:10:20

Last Accessed (FS): 28.03.2008 15:10:20

File Size: 7162

MD5 Hash: A0DC28D04DBC673B1B7A2E7F62C26A50

SHA-1 Hash: 5777615CC43AED40A4F1ACC7032C8EEE069CC30C

SHA-256 Hash: 43DF7B97869A21C6C415E0EA949DBE3AC9D8606BB44054E9062D4B1A80A6B84F

- File Path: F:\test2openoffice.odt
- Den var altså den samme som i originaldokument.
- Created Date endret heller ikke sitt opprinnelige klokkeslett, som var 14.33.56.
- Last modifified endret seg til 15.10.20
- Hashverdiene forble de samme som i originaldokumentet

7.2.3 Manipulering av MS Word 2003 dokument- testresultater

A- Opprettelse av originaldokument

OLE metadata:

File Name: Test2 Meta manipulering.doc

Title:

Author: Robert Didriksen

Comments:

App Name: Microsoft Office Word

Version: 12.0

Date Created (OLE): 26.02.2008 15:03:00

Date Last Printed:

Date Last Saved: 26.02.2008 15:58:00

Total Edit Time: 1

Template: Normal.dotm

Shared: False

Subject:

Category:

Company: Safran Software Solutions

Last Saved By: Robert Didriksen

Word Count: 976

Page Count: 2

Paragraph Count: 39

Line Count: 103

Character Count: 5509

Character Count (with spaces): 6446

Byte Count: 44032

FILE metadata

File Path: C:\Documents and Settings\user9\My Documents\Testing av metadata og hashing verdier\Word 2003 doc\Test2 Meta manipulering.doc

Created Date (FS): 26.02.2008 14:32:39

Last Modified (FS): 26.02.2008 15:58:30

Last Accessed (FS): 26.02.2008 15:58:30

MD5: 9716FE44F957319C17A5EE821D075F06

SHA-1: 89262CC8292094733B9A4C4A4C5527A1AFDB8738

SHA-256: 3C2276E2FEFC85DA84455B667CA5A1D957B5BA0A3783F090113774701C4313C0

F- TEST 5: Manipulering av metadata

OLE Metadata:

File Name: Test2 Meta manipulering.doc

Title: Manipulert dokument

Author: Erik Eriksen

Comments:

App Name: Microsoft Office Word

Version: 12.0

Date Created (OLE): 26.02.2008 15:03:00

Date Last Printed:

Date Last Saved: 26.02.2008 16:09:00

Total Edit Time: 2

Template: Normal.dotm

Shared: False

Subject: test

Category:

Company: Safran Software Solutions

Keywords: computer forensics

Last Saved By: Robert Didriksen

Word Count: 1029

Page Count: 2

Paragraph Count: 12

Line Count: 45

Character Count: 5456

Character Count (with spaces): 6473

Byte Count: 44032

FILE Metadata:

File Path: C:\Documents and Settings\user9\My Documents\Testing av metadata og hashing verdier\Word 2003 doc\Test2 Meta manipulering.doc

Created Date (FS): 26.02.2008 14:32:39

Last Modified (FS): 26.02.2008 16:09:39

Last Accessed (FS): 27.02.2008 12:59:38

MD5: 4C8A37351642E543DA11FD7B3FBD8C0A

SHA-1: BD542F02AA63951B6E11468A9FFA4C8E3A159327

SHA-256: FFAE0E55A4A261AA977E352F6F329FA65DE6B1F8FE8AF891FE206F6187BAD1D5

Ved manipulering av metadata i et Word 2003- dokument skjedde det følgende:

- Hashverdiene endret seg.

7.3 Tolkning

I denne delen vil jeg kort tolke alle testresultatene kort hver for seg. Etterpå følger en oppsummering av testresultatene, samt foreløpig konklusjon.

7.3.1 MS Word 2007

Test 1, lagring av originaldokument på USB minnepinne, viste at den nye lagringen av originaldokumentet på en ekstern disk førte til at det originale dokumentet mistet sin opprinnelige form når det gjaldt både metadata og hashverdier. Man kan derfor med sikkerhet konkludere med at den nye lagringen på ekstern USB førte til at dokumentet fikk redusert sin integritet.

Test 2, kopiering av originaldokument over på en USB minnepinne, viste et bedre resultat. Oppsummert vil man ut fra denne testen kunne konkludere med at ingen endringer i hashverdiene gjorde at dokumentet ikke fikk redusert sin integritet ved sammenligning med verdiene fra originaldokumentet.

Test 3, lagring av originaldokumentet et annet sted på lokal harddisk, viste at
å lagre et Word 2007 originaldokument et annet sted på harddisken uten å endre filnavnet fører til endringer i klokkeslett for oppretting, modifisering og ”last access”. Testen førte dessuten til at hashverdiene også ble endret. Resultatet viser at dokumentet fikk redusert sin integritet som følge av lagring av testoperasjonen.

Test 4, ”Drag and drop”, viste ikke like stor svekkelse i integriteten som Test 3. Selv om enkelte parametre i metadataene endret seg, forble hashverdiene uendret. Derfor vil man kunne fastslå

at selv om metadata slik som ”Last modified” og ”Last accessed” har endret seg har ingen ting i selve dokumentet blitt endret og man kan si at dokumentet ikke har fått redusert sin integritet som følge av lagring på ekstern harddisk ved bruk av funksjonen drag and drop.

7.3.2 Open Office

Test 1, Lagring av originaldokument på en USB minnepinne, viste at metadatainformasjon om klokkeslett og modifisering ble endret. Resultatet indikerer at tidspunktet for de nye klokkeslettene ble generert i det øyeblikket dokumentet ble lagret på minnepinnen. Hashverdiene ble også påvirket, noe som viser at den nye lagringen av originaldokumentet på en ekstern USB- enhet gjør at dokumentet har mistet sin opprinnelige form; både når det gjelder metadata og hash verdier. Oppsummert kan man si at lagring på nytt på ekstern disk fører til at dokumentet svekker sin integritet, på samme måte som ved tilsvarende testing i et MS Word 2007- dokumentet.

Test 2, kopiering av originaldokument til en USB minnepinne, viste slik som ved samme test i MS Word 2007 et lovende resultat. Ingen endringer i hash- verdiene gjør at dokumentet ikke har mistet integritet, selv om noen endringer i metadata oppstod.

Test 3, lagring et annet sted på den lokale harddisken, førte til at klokkeslettet ble endret til å vise tidspunkt for lagring, modifisering og åpning av dokumentet. Dette betyr at å lagre et originaldokument fra OpenOffice et annet sted på harddisken uten å endre filnavnet fører til endringer i ”created date”, ”last modified” og ”Last accessed. Også hash verdiene endret seg i denne testen, og dette resultatet innebærer at dokumentet tydelig fikk redusert sin integritet som følge av testoperasjonen. Resultatet sammenfaller med tilsvarende test i Word 2007.

Test 4, ”Drag and Drop”, viste slik som under testing i Word 2007 et lovende resultat.
Ut fra testverdiene klarte dokumentet å beholde sin integritet, da det ikke ble endringer i hashverdiene. Metadataverdiene endret seg også her.

7.3.3 MS Word 2003

Test 5, manipulering av metadata inne i et Word 2003- dokument, førte til at hashverdiene ble endret. Dette resultatet er en god indikasjon på at når metadata manipuleres, vil hashverdiene bli forandret. Dermed svekkes integriteten til dokumentet betydelig. Dersom man finner ut at et dokument (for eksempel et elektronisk dokumentbevis) har fått endret hashverdiene sine, er dette en god indikator på at noe har skjedd i forhold til det originale dokumentet.

7.4 Oppsummering og foreløpig konklusjon

Testingen viser at metadataene endret seg på alle testene. Derimot endret bare hashverdiene seg når dokumentet ble lagret på nytt ett annet sted enn der originalen lå, og når det ble lagret på USB minnepinne. Det var ingen endringer i hashverdiene når dokumentet ble kopiert eller overført ved bruk av ”dra og slipp”. Derimot endret en eller flere parametre i metadataene seg hver gang.

Ut fra testene gjennomført i Word 2007 og OpenOffice kom jeg, som vist over, frem til de samme resultatene. Metadata og hashverdiene skulle være en indikasjon på i hvilken grad dokumentene beholder sin integritet ved forskjellige måter å overføre og lagre dokumentene på, og det viste seg at metadatainformasjon ble endret hver eneste gang jeg lagret og overførte et dokument; selv om innholdet i dokumentet forble det samme.

Antakelsen var at dersom verdiene endret seg ved testoperasjonen, ville dokumentets originalitet forfalle. Dermed ville også ektheten svekkes.

Hovedkonklusjonen på testingen blir at hashverdiene ser ut til å være en bedre indikator enn metadata på et dokuments integritet og autentisitet.

Denne konklusjonen baserer seg på kunnskapen om hva en hashverdi representerer, altså et slags unikt, digitalt ”fingeravtrykk”. Hashverdiens betydning ble grundig gjennomgått i kapittelet om autentisitet. Metadata ble også beskrevet her. Grunnen til at metadata kan være

en dårligere indikator på autentisitet enn hashverdier, er at de lettere enn hashverdier ser ut til å forandre seg. Slik vil det være langt større risiko for at man forstyrrer eller ødelegger de verdiene man senere kan få bruk for i vurderingen av kvalitet på dokumentbevis. Følgelig vil det trolig være mer nyttig å ta utgangspunkt i hashverdier enn i metadataverdier når man skal evaluere kvalitet på et elektronisk dokumentbevis.

Resultatene fra testingen jeg har foretatt beskrives avslutningsvis i dette kapittelet ved hjelp av oversiktstabellene (tabell 1-2), som er presentert under. Slik det fremgår fra tabell 1 og 2 var resultatene fra testing i Word 2007 og OpenOffice helt sammenfallende.

Testnr	1 Lagre original dokument på USB minnepinne	2 Kopiere original dokument på en USB minnepinne	3 lagre original dokument et annet sted på harddisken	4 ”Drag and Drop” original dokument til en ekstern disk
Forandring i metadata	JA	JA	JA	JA
Forandring i Hashverdier	JA	NEI	JA	NEI
Behold integritet	NEI	JA	NEI	JA

Tabell 1. Oppsummering av Testing i MS Word 2007

Testnr	1 Lagre original dokument på USB minnepinne	2 Kopiere original dokument på en USB minnepinne	3 lagre original dokument et annet sted på harddisken	4 ”Drag and Drop” original dokument til en ekstern disk
Forandring i metadata	JA	JA	JA	JA
Forandring i Hashverdier	JA	NEI	JA	NEI
Behold integritet	NEI	JA	NEI	Ja

Tabell 2. Oppsummering av Testing i Open Office

7.5 Mulige feilkilder

Dette var en relativt enkel test. Det eneste jeg var ute etter var å sjekke om det ble endring i hashverdier og metadata som følge av testoperasjonen. Jeg gikk ikke inn og tolket alle enkeltverdiene i form av *hvilke typer* eventuelle endringer som hadde skjedd. Det er klart at jeg derfor har unnlatt å tolke en hel del data som ellers kunne vært interessante å se på. Likevel ble det vurdert at testingen og tolkningen som ble utført var tilstrekkelig for denne oppgavens hensikt.

7 DRØFTING OG FORSLAG TIL SJEKKLISTE

Denne oppgaven omfatter et bredt spekter av tema, som har til felles at de handler om ulike sider av elektroniske dokumentbevis.

Problemstillingen i oppgaven var todelt. Først ville jeg studere hvordan man på best mulig måte kan sikre autentisiteten til elektroniske dokumentbevis (P1). Deretter ville deg studere hvorvidt man kan gjøre noe spesifikt for å ivareta personvernhensyn i møte med elektroniske dokumentbevis (P2).

Jeg har forsøkt å besvare (P1) ved å foreta en grundig redegjørelse for begreper, teori, praksis og gjeldende lover og regelverk som er knyttet til elektroniske dokumentbevis. I tillegg reiste jeg innledningsvis to delspørsmål som omhandlet hvorvidt metadata og hashverdier kan brukes i autentifisering. For å prøve å besvare disse gjennomførte jeg noen enkle tester for å sjekke autentisiteten til et utvalg av elektroniske dokumenter etter hvert som disse ble utsatt for ulike lagrings- og kopieringsmåter.

Jeg ville også svare på (P2) ved å ta for meg problemstillinger som henger sammen med personvern. Jeg gjorde dette ved å foreta en gjennomgang av personvernteori, i tillegg til sider ved personopplysningsloven som angår innhenting av elektroniske bevis.

Jeg har allerede foretatt en hel del drøftning der dette har falt seg naturlig. Jeg vil likevel vie dette kapittelet til diskusjon av noen sentrale tema. Avslutningsvis i drøftingsdelen følger et forslag til sjekkliste for best mulig innhenting, sikring og lagring av elektroniske dokumentbevis. Her er både tekniske og juridiske hensyn inkludert. Denne sjekklisten bygger på det jeg i oppgaven har kommet frem til som de viktigste punktene for best mulig håndtering av elektroniske dokumentbevis.

8.1 Personvernmessige forhold

Personvernet har blitt viet mye plass i denne oppgaven, årsakene til dette er at personvernet er nært knyttet til innsamling og bruk av elektroniske bevis og offentlig myndighet og private bedrifters bruk av personopplysninger. Flere mennesker har gjennom offentlige eller private instanser mulighet til å innhente og lagre personopplysninger om enkeltindividet. På grunn av dette er det utvilsomt viktig å stadig etablere og oppdatere rutiner for hvordan informasjonen skal behandles.

Det såkalte integritetsperspektivet på personvern deler menneskers liv inn i "sfærer" med forskjellig grad av intimitet og sensitivitet. Med sfæreteorien har man tenkt seg en form for magisk kuppel eller sirkel, eller et sosialt gjerde rundt hjem og familie, hvor man selv bestemmer hvem som skal komme inn. Denne tanken om at man beskytter seg fra ytre påvirkning i en "privat sfære" er kanskje ikke så reel lenger, i form av at IKT har skapt en mer flytende grense mellom privatliv og kommunikasjon med "verden utenfor". Det kan være i form av chatting, dokumentutveksling, korrespondanse på e-post, utveksling av bilder og mulighet til å legge ut informasjon på internett slik at mange flere kan få tilgang til for eksempel dine private feriebilder eller en privat blogg. Folk er i mange sammenhenger ukritiske i bruk av IKT og skjønner kanskje ikke konsekvensene av å legge ut et manipulert bilde av en venn, eller endre verdiene i et viktig dokument. Årsaken til dette kan være manglende kompetanse på både personvern og bruk av datamaskiner.

Med den raske utviklingen innen IKT kan man si at grensene gradvis har blitt visket ut mellom hva som er privat informasjon og hva som er tilgjengelig for offentligheten. IKT med på å sette integritetsspørsmålene i et nytt lys. De tradisjonelle spørsmålene vedrørende dette temaet eksisterer i nær sammenheng med de nye integritetsspørsmålene som IKT genererer. Et eksempel på tradisjonell krenkelse av geografisk integritet, er den såkalte "kikkeren" som spionerer på mennesker i sin private eller intime sfære. Dersom denne "kikkeren" i tillegg

publiserer andres private bilder på nettet, er det et eksempel på en annen, ”nyere” form for krenkelse. (Schartum & Bygrave, 2004). Når man sammenligner ”nyere” og ”tradisjonelle” former for integritetskrenkelse, kan man si at informasjonsteknologi oftest er med på å forverre og forstørre omfanget av krenkelsen. Blant annet innebærer ny teknologi at privat informasjon raskt og effektivt kan spres til et stort antall tilskuere.

Dette betyr imidlertid ikke at det er riktig at en hver informasjon man får tak i kan brukes fritt. Som vist i kapittelet om personvern er det til tross for et stadig mer uoversiktlig informasjonssamfunn visse lover og retningslinjer man må følge når man behandler personopplysninger. At personopplysningsloven ble utviklet og vedtatt slik den er i dag har nok medført en bedre rettssikkerhet for enkeltmennesket i møte med den økende kompleksiteten i informasjonssamfunnet. Likevel er det mange spørsmål som står ubesvart på dette området, og mange har pekt på at lovene enda er for lite tilpasset (Thorvaldsen, 2006). Personopplysningene baserer seg for eksempel på at den informasjonen som faktisk blir lagret om oss er absolutt og korrekt, og dette kan skape situasjoner der det kan bli vanskelig å vite hvordan man juridisk sett skal forholde seg dersom det sås tvil om ektheten til et bevis. I slike tilfeller vil det reise seg behov for en gjennomgang av den elektroniske informasjonens autentisitet. Jeg nevnte i kapittel 6 skrev jeg om dataetterforskning, og dette er en gren som sannsynligvis vil få stadig mer å si i vanskelige avveininger knyttet til elektroniske bevis.

Mens integritetsperspektivet ser på de grensene man har for den ”private sfære”, ser beslutningsperspektivet på om det blir tatt korrekt avgjørelse om oss med utgangspunkt i personopplysningsloven når elektronisk informasjon hentes inn (Engebretsen, 2002). Personopplysninger om enkeltindividet har, som vi har sett i kapittel 5, ofte grunnlag i beslutninger som blir tatt av andre, det kan være alt fra bankers behandling av lånesøknader til ligningskontorets bruk opplysninger om selvangivelsen (Schartum & Bygrave, 2004). Det har blitt stadig enklere for offentlige instanser å få tak i personopplysninger, og viktige beslutninger om enkeltpersoner kan i dag bli styrt av for eksempel bankfunksjonæren som gjennom noen få tastetrykk skaffer seg informasjon om den aktuelle kundens økonomi.

Til slutt har vi maktperspektivet. Dette perspektivet ser på maktrelasjonen mellom offentlig myndighet og den enkelte. Den utstrakte bruken av IKT er med på å skape uklare personvernmessige forhold til innsyn i personlige data. Jeg har for eksempel drøftet dette i lys av e-post og private elektroniske dokumenter som ligger på arbeidsgiverens server. Innsynreglene er til tider vanskelig å skjønne, og dette har ført til at Datatilsynet har mottatt en rekke henvendelser med spørsmål knyttet til hvor grensen mellom lovlig og ulovlig innsyn går (Høringsnotat, 2007). Lov om innsyn er et viktig område i diskusjonen om innsamling av ulovlig informasjon. I mange tilfeller dukker det opp uenigheter mellom arbeidstaker og arbeidsgiver på spørsmålet knyttet til forholdet til om innholdet i e-posten er virksomhetsrelevant eller ikke., slik at arbeidsgiver må ha en saklig begrunnelse for innsyn. Hva som er privat e-post eller virksomhetsrelatert er ofte situasjonsavhengig, derfor ligger utfordringer i å ha klare retningslinjer for dette. Her anbefaler Datatilsynet at bedriftene utarbeider egne instrukser som også omfatter regler for innsyn i e-post. I denne enkeltsaken kan man argumentere for at lesing av arbeidstakers e-post er i grenseland for å krenke personvernmessige hensyn. Man kan på den andre siden si at datamaskinen og e-posten tilhører arbeidsplassen, og at den dermed er arbeidsgivers eiendom. Slike saker kommer til stadighet opp i media, noe som generelt sett tyder på at det kreves klare rutiner og regler knyttet til innsyn slik at det blir en balanse i styrkeforholdet mellom arbeidsgiver og arbeidstaker. Dette kan ha betydning i en eventuell arbeidstvist der arbeidsgiver har tilgang på alle elektronisk informasjon om arbeidstaker som ligger inne på arbeidsgivers servere mens arbeidstaker ikke har tilgang på slik informasjon og vil kunne stå uten mulighet til å kunne legge frem relevante elektroniske bevis.

Jeg har nå drøftet personvernhensyn i lys av de tre perspektivene på personvern som ble forklart i kapittel 5. Jeg vil videre drøfte sentrale tema knyttet til (P1), nemlig autentisitet og datakvalitet.

8.2 Autentisitet og datakvalitet

Autentisitet er et av kjernepunktene i oppgaven, og det er en kvalitet som man tar for gitt i alle dokumenter. Helt inntil den blir utfordret. Det er da vi skjønner at fordi, eller til tross for, oppbevaring gjennom lagring er den avgjørende karakter ved det elektroniske dokumentet dens intellektuelle og dens psykiske integritet, lett kan bli endret eller kompromittert slik at man kan dra tvil om ekteheten til dokumentet. Et av de største problemene knyttet til autentisiteten til elektroniske dokumenter er, som vi har sett i oppgaven, når det blir overført gjennom ” rom” og ”tid”. Det kan være når det blir sendt mellom to personer som for eksempel e-post, samtidig kan systemer eller applikasjoner være med å svekke autentisiteten til dokumentet.Det er essensielt at vi vet hva vi må gjøre for å sikre ekteheten til et dokument. Et pålitelig dokument er et dokument som påberoper seg å være ekte, ikke forfalsket eller forandret eller forsøkt ødelagt. (Interpares, 2002)

Kvalitet blir ofte definert på en slik måte at det kombinerer både den subjektive og objektive dimensjonen av betegnelsen. Erik Jersin (gjengitt i Bygrave, 1996) definerer kvaliteten på et produkts kapasitet ved å se på brukernes behov, ønske, krav og forventninger. Kvalitet kan være problematisk å konseptualisere. Dette begrepet er langt på vei knyttet til brukerens egen bedømmelse. International Organisation for Standarization (OSI) følger de samme linjene i sin definisjon. ISO definerer kvalitet som totaliteten av særtrekkene og kvaliteten på et produkt eller tjeneste som hviler på ens evne til å tilfredsstille fastlagte eller indirekte behov. ISO har i sin definisjon blitt kritisert for å være snever men summerer opp en forestilling som er vag og vanskelig å forstå. I Sverige har flere offentlige rapporter definert informasjonskvalitet med betegnelser som brukbarhet av informasjonen for et gitt problem og en gitt bruker. Vi har hatt lignende definisjoner om data og informasjonskvalitet i Norge, enten eksplisitt eller implisitt. (Bygrave, 1996).

Til tross for iherdig jobbing på feltet er det ikke enda utformet en samlende og fullgod definisjon av verken autentisitet eller kvalitet. Dette er en teoretisk tilkortkommenhet som medfører praktiske utfordringer når man skal sikre for eksempel et dokuments ekthet.

Det å sjekke om et elektronisk dokument har bevart autentisiteten er, som vi gjennom denne oppgaven har sett mange eksempler på, en kompleks og krevende prosess. Skal man kunne si med sikkerhet at et dokument er ekte kreves det at man har tilgang til originalen. Ofte har originalen blitt kopiert utallige ganger, og det er praktisk talt umulig å vite hva som er det "ekte" dokumentet. For å kunne sikre ekthet har jeg i oppgaven vist at hashverdier er gode indikatorer dersom man sammenligner en originalverdi med en gitt hashverdi. En stor svakhet med teknologien slik den er i dag er at vi trenger kjennskap til den originale hashverdien før dokumentets autentisitet kan testes igjen på et senere tidspunkt. Spørsmålet blir da om man for sikkerhets skyld må begynne å registrere hashverdier på alle viktige dokumenter. Dette vil igjen kreve opplæring av de som skal foreta denne operasjonen, eller at det blir utført som en automatisert prosess i systemet når dokumenter er ferdigstilte. Det vil si at dokumentet ikke kan endres uten at hashverdien endres, og at ektheten dermed svekkes.

Samfunnet er i dag i en endringsprosess, og det meste av informasjonsflyten mellom private bedrifter, offentlige institusjoner og privatpersoner foregår nå ved bruk av elektroniske kommunikasjonskanaler. Dette er et sentralt argument for at det stadig stilles høyere kvalitetskrav til lagring og bearbeiding av denne type informasjon. Hvis informasjonen skal ha noen grad av nytteverdi i som elektronisk bevis er det viktig at den har god nok kvalitet (Gulbrandsen, 1997). Hva er så kvalitet? Dette ble drøftet inngående i kapittel 3. Det er lansert flere definisjoner og modeller for å konseptualisere kvalitet, deriblant Bygraves (1996) modell. Denne er detaljert og omfattende, og den innlemmer også kvalitetsindikatorer som er brukt av andre forskere på området. Derfor vil jeg bruke Bygraves modell som et av utgangspunktene for sjekklisten jeg presenterer senere.

8.4 Juridiske utfordringer knyttet til elektroniske dokumentbevis

I løpet av gjennomgangen som til nå er gjort, har det kommet frem flere ganger at lovverket har sine klare mangler på feltet som berører digitale bevis. De digitale bevisene blir i dag ført på lik linje som vanlige analoge bevis (papirer, etc.). Med tanke på at elektroniske bevis har spesielle kvaliteter som ikke vises på en papirutskrift er disse bevisene særlig utsatt for manipulasjon når de legges frem som utskrifter. Et alternativ det er mulig å tenke seg i fremtidens rettssystem er at digitale bevis legges frem i de medier de har sin opprinnelse fra, men at sakkyndige har ansvar for å foreta en autentifisering før beviset er godkjent i bruk. Det er flere forhold som gjør at dette enda synes som en utopi, viktigst er kanskje den mye nevnte mangelen på både retningslinjer for autentifisering og tydelige lover for hvordan man skal forholde seg til elektroniske bevis.

I retten er det dokumentets innhold som er av betydning, ikke selve innhentingen. Men når man skal bruke elektroniske bevis kan kunnskap om innhentingsprosessen være avgjørende for bevisets autentisitet. Dersom man bare ser på selve innholdet til et elektronisk dokumentbevis, får man ikke vite hvordan man gikk frem for å innhente det, og ikke heller om personopplysningsloven ble fulgt. Man kan argumentere med at dersom det kommer frem at beviset er uekte eller har kommet frem på ulovlig vis, kan retten avskjære beviset. På den andre siden er det vanskelig å tenke seg hvor ofte slike forhold vil bli oppdaget dersom man ikke har retningslinjer som alle må følge for å autentifisere bevis. I fremtiden burde det derfor utarbeides slike retningslinjer.

Det er mange juridiske utfordringer om man ønsker å utforme en prosess for å sikre integriteten eller ekteheten til digitale bevis. En juridisk løsning på slike utfordringer kan være endringer i prosesslovgivningen. Prosesslovgivningen deles normalt inn i to disipliner – sivilprosess og straffeprosess, og er regler om hvordan straffesaker og sivile saker behandles. Det er sentrale forskjeller mellom straffeprosessen og sivilprosessen. I sivile saker har partene fri rådighet over saken og kan føre de bevisene de selv ønsker. I straffesaker har påtalemyndighetene bevisbyrden og må føre bevis for tiltaltes skyld. Beviskravene er også ulike ved at enhver tvil

skal komme tiltalte til gode i straffesaker, mens sannsynlighetsovervekt er hovedregelen i sivile saker. Straffeprosessloven behandler også den delen av prosessen som finner sted før domstolsbehandlingen det vil si regler om pågripelse, beslag, avgjørelse av tiltalespørsmålet (Hennum, 2007).

Et eksempel på prosedyreendring er å forberede rettprosedyren på en slik måte at det gjør det enklere for en dommer og meddommere å bestemme ekteheten av et elektronisk bevis. Det retter seg også spørsmål til om advokater kan anvende en definert prosedyre for å validere ekteheten til et elektronisk bevis som er sentrale og problematiske for en sak. (Thorvaldsen, 2006). Da det er vanskelig for teknologer å skaffe seg oversikt over alle forhold som har med jussen å gjøre (og omvendt), er det svært viktig at man jobber for å få til et aktivt tverrfaglig miljø slik at man kan sikre at fagligheten beholdes etter hvert som utviklingen av nye lover og regelverk skjer.

8.5 Forslag til sjekkliste for håndtering av elektroniske dokumentbevis (nb probl.stilling)

Med basis i det som har blitt gjennomgått i oppgaven skal jeg her presentere forslag til sjekkliste for håndtering av elektroniske dokumentbevis. Selv om det per i dag ikke eksisterer noen rutiner for hvordan man skal legge frem elektroniske bevis i retten vil denne sjekklisten kunne fungere som bidrag i det videre arbeidet i komponeringen av standardiserte rutiner for dette en gang i fremtiden. Praktisk forklart er poenget med sjekklisten er at man for eksempel skal kunne få inn et bevis per e-post eller andre former, og deretter vite mer om hvordan beviset skal håndteres ved følge sjekkpunktene. Målet vil naturligvis være at et bevis gjennom hele forvaringskjeden skal holde akkurat den formen det hadde i sin originale tilstand. Det er da viktig å kartlegge hva man har gjort i innsamlingen. Som vist over er det mange potensielle fallgruver man kan gå i under innsamlingen, som vil redusere eller ødelegge autentisiteten til beviset.

Tanken bak sjekklisten er også at man bedre og lettere skal kunne gjøre hensiktsmessige og fornuftige vurdering opp mot personvernmessige forhold, kvalitetskontroll, behandling av bevis i forvaringskjeden, i tillegg til å kunne legge frem det elektroniske dokumentbevisets verdikjede så langt bak det lar seg gjøre.

Det er viktig å understreke at denne sjekklisten er utformet med tanke på bevishåndtering i fasen før beviset kommer inn i forvaringskjeden. Etter at beviset kommer inn her, vil det være naturlig å følge de sjekkpunkter og metoder som er forklart i kapittel 6.

- Innhentingen må ikke være i strid med personvernet og personopplysningsloven
- Ikke åpne originaldokumentet
- Lage hashverdier til originaldokumentet og noter ned
- Kopiere originaldokumentet over på ekstern
- Sikre det elektroniske beviset autentisitet ved å generere hashverdier og sjekke det opp mot hashverdiene på originaldokumentet. Er disse de samme er kopien gyldig.
- Noter tidspunktet for innsamlingen
- Hvem samlet inn?
- Hvordan og hvor ble det elektroniske dokumentbeviset lagret?
- Hvilken beskyttelse hadde det elektroniske dokumentbeviset?

8 AVSLUTNING OG KONKLUSJON

Det er vanskelig å tenke seg et fullgodt svar på hvordan man bør håndtere elektroniske bevis, både på grunn av det gjeldende lovverket og den raske utviklingen på IKT-området. Imidlertid er det viktig å være oppmerksom på alle utfordringer som dette feltet er beheftet med, samt drive kontinuerlig arbeid for å tilpasse rutinene for sikring, lagring og validering av bevis.

Til slutt vil jeg konkludere (P1) og (P2) hver for seg.

(P1): Oppsummert kan man si at det ikke ser ut å eksistere noen måter som sikrer en hundre prosent autentifisering. Det foreligger heller ikke klart definerte rutiner for sikring av autentifisering. Likevel har det vist seg mulig å gjøre mange operasjoner som vil sikre autentisitet i et gitt bevis. Testingen i kapittel 7 så ut til å gi holdepunkt for at man bør fortrekke hashverdier over metadata når man skal undersøke et dokuments ekthet. Manipuleringstesten ga holdepunkt for at hashverdier er en god indikator på hvorvidt det har skjedd endringer i metadata. Det bør nevnes som en begrensning at man er nødt til å kjenne hashverdien fra originaldokumentet før en eventuell autentifisering kan skje. Det ser uansett ut for at enkelte metoder er bedre enn andre, og at det er mulig å komme frem til slike konklusjoner bare på grunnlag av noen få enkle tester. Fremover er det svært viktig at forskningen på dette feltet etterstreber tydeligere retningslinjer for prosedyrer på autentifisering.

(P2): Konklusjonen på (P2) er at man i dag står overfor mange utfordringer i forhold til personvern som følge av en lovgivning som enda ikke er tilpasset elektroniske bevis. Det mest spesifikke man kan gjøre for å ivareta personvernhensyn må på overordnet nivå bli å utarbeide et oppdatert lovverk. I den enkelte sak er det viktig å følge det gjeldende lovverket når man innhenter personopplysninger.

Grunnet oppgavens omfang ble det ikke mulig å gjøre alle testene som kunne vært ønskelig, som for eksempel teste dokumenter med digital signatur og i hvilken grad de endrer seg ved forskjellige behandlingsmetoder. Det er mange ubesvarte spørsmål innefor feltet elektroniske bevis, og slike spørsmål er viet mye oppmerksomhet i løpet av oppgaven. Hovedutfordringen fremover i dette enda nye og langt på vei upløyde feltet ligger i at lovverket må tilpasses bedre, og at det må etableres klare og gode rutiner for innsamling, sikring og annen bruk av elektroniske dokumentbevis.

LITTERATUR

2008., J. I. (17.06.2001). *Gangen i en straffsak*. Retrieved 14.04, 2008, from http://www.jus.no/index.db2?id=2314

Administrasjonsdepartementet, f. o. (2007). FORSLAG TIL REGLER OM ARBEIDSGIVERS TILGANG TIL
ANSATTES E-POST MV. – ENDRING AV
PERSONOPPLYSNINGSLOVEN § 3 OG § 46, NYTT KAPITTEL I
PERSONOPPLYSNINGSFORSKRIFTEN OG NY BESTEMMELSE I
ARBEIDSMILJØLOVEN. In f. o. Administrasjonsdepartementet (Ed.).

Aftenposten. (2005, 28.11.2005). *Kristensen Solås suspendert*. Retrieved 06.05, 2007, from http://www.aftenposten.no/nyheter/iriks/article1166506.ece

Australia, N. A. o. (2004). *Digital Recordkeeping*
Guidelines for Creating, Managing
and Preserving Digital Records
Exposure Draft.

authentic. (2008). *Meriam Webster*.

Bing, J. (1991). Personvern I faresonen.

Bing, J. (1998). *Landskap med tegn*: Pax Forlag

Boland, T., & Fisher, G. (2000). SELECTION OF HASHING ALGORITHMS: The National Software Reference Library.

Borchgrevink, M. (2006). Arbeidstaker som misbruker Internett eller e-post – bedre føre var enn etter snar (pp. 8).

Brattsberg, H. F. (1994). *Om juss, papir og elektronisk informasjon*. Retrieved 16.06, 2007, from http://www.jus.uio.no/iri/forskning/lib/rapporter/om_papir/om_papir.html

BSI. (2001). Informasjonsteknologi Administrasjon av informasjonssikkerhet. . In BSI (Ed.).

Bygrave, L. A. (1996). Ensuring Right Information on the Right Person(s)
Legal Control of the Quality of personal Information (pp. 23).

Caloyannides, M. A. (2004). *Privacy Protection and Computer Forensics*

Carrier, B. (2003). Open Source Digital Forensics Tools

The Legal Argument1 (pp. 11).

CLAES GRÄNSTRÖM, TORBJORN HORNFELDT, GARY PETERSON, MARIANA, M. P. R., UDO SCHÄFER, & ZWICKER, J. (2002). *AUTHENTICITY OF ELECTRONIC RECORDS*: INTERNATIONAL COUNCIL ON ARCHIVES

COMMITTEE ON ARCHIVAL LEGAL MATTERS.

CNSS. (2006). NATIONAL INFORMATION ASSURANCE (IA)

GLOSSARY: Committee on National Security Systems.

Coll, L., & Schartum, D. W. (2004). Rettslige spørsmål knyttet til innsamling og bruk av digitale bevis.

Cybex. (2008). *The new reality*. Retrieved 14.02., 2008, from http://www.cybex.es/en/pruebas_realidad.htm

Dommerud, T. (2007, 2007-02-22). *Et skrøpelig system*. Retrieved 10.04.2007, from http://www.dagensmedisin.no/nyheter/2007/02/22/et-skrpelig-system/index.xml

domstoler, N. (2008). *Sivil rettssak*. Retrieved 13.04, 2008, from http://gammel.domstol.no/Domstolene/index.asp?menuid=0&topExpand=1000102&subExpand=&strUrl=//internet/showObject.asp?i=1383959

Engebretsen, L. M. (2002). *"Private sfære på internett? En diskusjon av tilgangen til anonym bruk av Internett".* Universitetet i Oslo Oslo.

Figg, W., & Zhou, Z. (2007). A computer forensics minor curriculum proposal *J. Comput. Small Coll.* (Consortium for Computing Sciences in Colleges), 32-38

Føyen, A. (2006). *Bevis og dokumentasjon i en elektronisk tidsalder*. Retrieved 14.03.2007, 2007, from http://www.foyen.no/templates/Artikkel____1466.aspx

Glick, K., & Sloma, R. (2002). *Findings on the Preservation of Authentic Electronic Records*: US-InterPARES Project.

Gulbrandsen, A. D. (1997). Prosjektet "Kvalitetsstandarder og sertifisering i dataforedling" Oslo: USIT.

Hennum, R. (2007). Straffrettsprosess -utvalgte emner.

Hov, J. (2007). *Rettegang 1*.

IKT Strategi for justissektoren (2004). In J. o. Politidepartementet (Ed.).

Informasjonsteknologi

Adminstrasjon av informasjonssikkerhet (2001). In I. I. 17799:2000 (Ed.) (pp. 65).

Insa, F. (2006). *The Admissibility of Electronic Evidence in Court (A.E.E.C.)*: Cybex.

Jansen, A., & Schartum, D. W. (2005). *Informasjonsikkerhet*

Rettslige krav til sikker bruk av IKT: Fagbokforlaget.

Johansen, M. W., Kaspersen, K.-B., & Skullerud, Å. M. B. (2001). *Personopplysningsloven*

Kommentarutgave: Universitetsforlaget.

Juridisk ordliste. (2008). In Domstol (Ed.): Domstol.

Kerr, K. (2006). *The Institutionalisation of Data Quality in the New Zealand Health Sector.*

University of Auckland.

Larsen, A. E. (2007). *Kan metadata sikre validiteten til digitale dokumentbevis.* Universitet i Oslo

Oslo.

Lind, T. (2001). *SIKRING AV KVALITET PÅ*

PERSONOPPLYSNINGER VED

BEHANDLING AV OFFENTLIG

TJENESTEPENSJON. Universitetet i Oslo, Oslo.

Losey, R. C. (2007). HASH: THE NEW BATES STAMP (pp. 44): Journal of Technology Law & Policy

1.

Martin J Eppler, M. H. U. G. (2004). Information Quality: Organizational, Technological, and legal

perspective

Mason, S. (2007). *Electronic Evidence*

Disclosure, Discovery & Admissibility.

Mason, S., & Barrister. (2006). Proof of the authenticity of a document in electronic format

introduced as evidence

Mathisen, L. H. (2005). Offentlige krav til governance og

compliance (pp. 31). Oslo

Melkas, H. (2004). *Towards holistic management of*

information within service networks:

Safety telephone services for

ageing people. Helsinki University of Techno.

Mocas, S. (2004). Building theoretical underpinnings for digital forensics research, *Digital investigation* (Vol. 1, pp. 8): Elsevier

Monsen, E. (2007). Bevistilgang til elektronisk lagret material (1 ed., pp. 194-234): Tidsskrift for Forretningsjus.

Mæland, K. (2008, 11.02.2008). *Slik forfalsket han kontrakten*. Retrieved 26.03, 2008, from http://www.nettavisen.no/innenriks/article1594888.ece

NISO. (2004). *Understandig Metadata*.

Noark-5 Norsk arkivsystem, 296 (2007).

NOU:32. (2001). Rett på sak

Lov om tvisteløsning (tvisteloven). In J.-o. p. d. 2001. & I. Statens forvaltningstjeneste (Eds.).

Nybøe, T. (2007). Tiltalebeslutning. In STATSADVOKATENE, I & OSLO (Eds.).

Nysæter, O. (2006). Computer Forensics

Elektronisk bevissikring (pp. 37). Bergen.

Panzer, G. I. I. *Advokat Georg I.I. Panzer i Hus Panzer & Co har grundig vurdert eNotarius\' tjenester knyttet opp mot aktuell lovgivning og rettpraksis*. Retrieved 30.02, 2007

Riise, K. (2006). *Databevis radbrekkes i retten.* Retrieved 12.02, 2007, from http://www.dagensit.no/minit/article921630.ece?WT.svl=article_readmore

Sangchul, S., & Joseph, J. (2007). New techniques for ensuring the long term integrity of digital archives, *Proceedings of the 8th annual international conference on Digital government research: bridging disciplines \& domains*. Philadelphia, Pennsylvania: Digital Government Research Center.

Scannapieco, M. (2004). *DaQuinCIS : Exchanging and Improving*

Data Quality in Cooperative Information

Systems. Universitµa degli Studi di Roma \La Sapienza", Rome.

Schartum, D. W., & Bygrave, L. A. (2004). *Personvern i informasjonssamfunnet en innføring i vern av personopplysninger*: Fagbokforlaget.

Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Trans. Inf. Syst. Secur., 2*(2), 159-176.

SHA hash functions. (2008). Retrieved 08.03.2008, 2008, from http://en.wikipedia.org/wiki/SHA-1

Skauge, A., G, e. A., Mette Bredengen, Pål Gundersen, Arne Dag Hestnes, Jostein Håøy, et al. (1997). *Et bedre personvern - forslag til lov om behandling av personopplysninger*.

Slone, J. P. (2006). *INFORMATION QUALITY STRATEGY: AN EMPIRICAL INVESTIGATION OF THE RELATIONSHIP BETWEEN INFORMATION QUALITY IMPROVEMENTS AND ORGANIZATIONAL OUTCOMES.* Capella University.

Stallings, W. (2006). *Cryptography and Network Security* (Vol. Fourth edition).

Thorvaldsen, K. (2006, 11.01.2006). *E-post - et tvilsomt bevis*, from http://www.dagbladet.no/kultur/2006/01/11/454423.html

Thorvaldsen, K. (2006). *Prosjekt Uten penn og blekk*, NOU 274 (2001).

Warren, H., George, H., Sarah, M., Mark, M., & John, R. (2004). High-tech forensics. *Commun. ACM, 47*(7), 48-52.

Willasen, S. Y., & Stig Frode Mjølsnes. (2005). Digital forensics research, *Teletronikk* (Vol. 1): Teletronikk.

Willassen, S. Y., & Stig Frode Mjølsnes. (2005). Digital forensics research, *Teletronikk* (Vol. 1): Teletronikk.

Williams, J. (2006). Computer Forensics: A practical Guide to its use in Corporate Litigation KPMG.

Xu, H. (2003). *Critical Success Factors for Accounting Information*

Systems Data Quality

UNIVERSITY OF SOUTHERN QUEENSLAND.

Zetterstrom, H. (2002). Deleting Sensitive Information

Why hitting delete isn’t enough. In S. institute (Ed.).