Elektronisk dokumentfalsk

Kandidatnr: 567
Veileder: Stein Schjølberg

Til sammen 29.694 ord

Dato 01.06.04

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Tema for denne oppgaven er straffelovens § 182 jf. § 179 om dokumentfalsk anvendt på elektroniske dokumenter. Med elektronisk dokument mener jeg elektroniske data som oppfyller vilkårene i lovens definisjon av dokument i § 179. Papirutskrifter av data faller utenfor oppgaven. Både dokumentbegrepet og de nærmere vilkårene for elektronisk dokumentfalsk vil bli behandlet.

Utveksling av data i forbindelse med elektronisk samhandling reiser en rekke nye problemstillinger som utfordrer den tradisjonelle forestillingen om hva et dokument er. Noen problemstillinger er knyttet til dokumentets form. Hvilke typer av data kan være dokument? Hvordan skal dokumentet nærmere avgrenses? Andre problemstillinger knytter seg til dokumentets innhold og bevisverdi. Hvordan skal en betrakte data som er premiss for en automastisk databehandling? Kan et dataprogram produsere et dokument i strafferettslig forstand?

Når dokumentbegrepet er klarlagt reiser det seg spørsmål om tidspunktet for fullbyrdet forbrytelse. Når har forfalskning og ettergjøring funnet sted? Og når er et elektronisk dokument benyttet?

Flere av vilkårene for dokumentfalsk passer dårlig på elektroniske dokumenter. Jeg vil derfor avslutningsvis gi en vurdering av dagens dokumentfalskregler.

1.2 Temaets aktualitet

En analyse av reglene om dokumentfalsk anvendt på elektroniske dokumenter er spesielt aktuell av tre grunner. For det første på grunn av en de facto overgang til elektronisk dokumenthåndtering. Dette kan illustreres ved aktuelle lovgivningstiltak som legger til rette for denne overgangen. For det annet vil arbeidet med informasjonssikkerhet, herunder elektroniske signaturer, gi elektroniske meddelelser en slik tillit at den strafferettslige beskyttelse får øket berettigelse. For det tredje gjør

dagens elektroniske infrastruktur for pengetransaksjoner at dokumentfalskreglene til en viss grad tar over for tradisjonell pengefalsk.

1.2.1 Elektronisk kommunikasjon i lovgivningen

Kommunikasjon som tidligere skjedde skriftlig eller ved overføring av analoge signaler skjer i økende grad elektronisk over Internett og andre digitale nettverk.[1] Gjennom et utstrakt lovarbeid legger myndighetene til rette for elektronisk kommunikasjon. Ekomloven har til formål å sikre brukere i Norge gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester.[2] Overgangen til elektronisk kommunikasjon fører til sammensmelting av sektorer som tidligere var atskilt. Konvergensutvalget[3] drøfter behovet for felles lovregulering av medie- og kommunikasjonssektorene.

Lovgivningen har også til formål å skape aksept for bruk av elektroniske dokumenter i rettslivet. Regjeringens eRegelprosjekt[4] kulminerte i en rekke lovendringer for å legge til rette for elektronisk kommunikasjon.[5] Videre er det lagt til rette for elektronisk kommunikasjon med domstolene i sivile tvister.[6] Ehandelsloven tar sikte på å ivareta den frie bevegelighet av informasjonssamfunnstjenester innenfor EØS-området jf. § 1 første ledd.[7] Ordet informasjonssamfunnstjenester skal forstås vidt og omfatter alle kommersielle tjenester som tilbys over nett, herunder elektronisk avtaleinngåelse og nettbanktjenester.[8]

Den offentlige forvaltning har som målsetning å være tilgjenglig for publikums-henvendelser hele døgnet, såkalt døgnåpen forvalting. For å oppnå dette søker man å etablere løsninger for elektronisk saksbehandling, elektronisk tjenesteyting og

---

[1] For eksempel er mobilnettet, kabel-tv-nettet, ISDN, bredbånd alle digitale nett. All kommunikasjon på disse nettene forutsetter en datamaskin i hver ende.

[2] Lov av 04.07.03 nr 83 § 1-1.

[3] NOU 1999:26 *Konvergens.*

[4] Se Ot.prp.nr. 108 (2000-2001) kapittel 2.1.

[5] Lov av 21.12.01 nr 117.

[6] Lov av 25.04.03 nr 24.

[7] Lov 23.05.03 nr 35. Loven inkorporerer EUs Ehandelsdirektiv (2000/34/EF) i norsk rett.

[8] Ot.prp. nr. 31 (2002-2003) Om *lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester(ehandelsloven).* Kapittel 9.

elektroniske administrative rutiner. [9] Dokumentbegrepet i forvaltningslovgivningen er utvidet til å gjelde elektroniske dokumenter.[10] Elektronisk kommunikasjon med og i forvaltningen er nærmere regulert i forskrift.[11]

Som en oppsummering kan en si at lovgiver på en rekke områder arbeider med å legge til rette for elektronisk kommunikasjon der man tidligere brukte papirdokumenter. Såfremt formålet med lovendringene nås, vil de føre til at man i stor grad går over til å bruke elektroniske dokumenter til erstatning for tradisjonelle papirdokumenter.

1.2.2 Informasjonssikkerhet

Begrepet informasjonssikkerhet brukes som en samlebetegnelse på en rekke kjennetegn ved sikker informasjon. Tradisjonell tekst i papirformat har visse egenskaper som gjør at det er enklere å oppdage om det er gjort endringer, om underskriften er ekte, og om konvolutten papiret ligger i har vært åpnet av andre. Disse tre egenskapene vil jeg i denne sammenheng kalle henholdsvis autentisitet, integritet og konfidensialitet.[12]

Dokumentfalskreglene får øket betydning i den elektroniske verden i lys av utvikling og utbredelse av metoder for informasjonssikkerhet. Kryptografi kan brukes til å ivareta disse tre egenskapene ved sikker informasjon. Reglene om dokumentfalsk bygger på en forutsetning om at dokumenter har en viktig funksjon som bevismiddel på grunn av den alminnelige tillit til dokumentets ekthet.[13] Et dokument er ekte når dets integritet og autentisitet er i behold.[14] Med teknologi som ivaretar disse hensynene vil den alminnelige tillit til elektroniske dokumenter kunne bli den samme som til tradisjonelle dokumenter.

I e-signaturloven finnes regler om krav til krypteringsteknologier som samlet kalles elektronisk signatur.[15] Det finnes flere varianter av elektronisk signatur, for eksempel

---

[9] NOU 2001:10 *Uten penn og blekk.* Kapittel 2.1.

[10] Forvaltningsloven § 2 (1) bokstav f, offentlighetsloven § 3 (1) og arkivloven § 2 bokstav b ble endret ved Lov av 15.12.00 nr 98.

[11] Forskrift om elektronisk kommunikasjon med og i forvaltningen av 28.06.02 nr 656.

[12] For eksempel NOU 2001:10 side 17, annen spalte.

[13] Se om hensynene nedenfor.

[14] Se nedenfor om falskbegrepet i punkt 4.

[15] Lov 15.06.01 nr 81.

såkalt biometrisk signatur[16] og digital signatur[17]. I lovens § 3 nr 2 kreves av en "avansert elektronisk signatur" blant annet at den ivaretar både integriteten og autentisiteten til data.[18] Digitale signaturer er en teknologi som i dag tilfredsstiller kravene til avansert elektronisk signatur.[19] En viktig konsekvens av at et elektronisk dokument blir signert med en digital signatur er at signaturinnehaveren ikke senere kan nekte for å ha skrevet dokumentet. Dette kalles prinsippet om ikke-benekting og understreker den grad av tillit man kan ha til digitalt signert informasjon.

1.2.3 Særlig om elektroniske betalingstjenester

I NOU 2002:4 peker Straffelovkommisjonen på at giro- og kortbaserte betalingstransaksjoner i dag er vanligere enn bruk av tradisjonelle sedler og mynter.[20] Betaling av giroer og overføringer mellom konti skjer i økende grad elektronisk. Som en følge av utviklingen har reglene om pengefalsk i straffeloven kapittel 17 blitt mindre anvendelige enn før. Angrep på elektroniske bank- og betalingstjenester vil etter Straffelovkommisjonens syn i stedet rammes av dokumentfalskreglene, eventuelt i konkurrens med databedrageri. Man kan derfor si at dokumentfalskreglene også som en følge av dette har fått større aktualitet enn før.

1.3 Om data og datasystemer

Elektronisk dokumentfalsk innebærer at gjerningsmannen benytter falske data som om de var ekte. Den straffbare handlingen vil alltid involvere tre elementer; data som forfalskes, ett eller flere datasystemer som data er knyttet til, samt samhandling i en eller annen relasjon. Den virkelighet som beskrives er preget av avansert teknologi. Det er derfor viktig å bruke et oversiktlig begrepsapparat.[21] Jeg vil i det følgende gjøre rede for hva jeg mener med data og datasystem. Hva jeg mener med samhandling kommer jeg tilbake til i punkt 1.4.

---

[16] For eksempel ved at man signerer med penn på en trykkfølsom plate. Dette er vanlig i en del banker i Norge.

[17] Digital signatur innebærer at en bruker krypteringsteknikk for å identifisere utsteder.

[18] Lov om elektronisk signatur av 15.06.01 nr 81.

[19] Se NOU 2001:10 side 27 flg. om offentlig nøkkel-kryptering (PKI).

[20] NOU 2002:4 side 375.

1.3.1 Data

Slik ordet data brukes i dagligtalen kan det ha en rekke ulike betydninger. Ofte brukes ordet som en betegnelse på all informasjon som er elektronisk lagret. For eksempel kan en slektsforsker si at han har et stamtre tilbake til 1600-tallet ”på data”. I mange universitetsfag betegner data studieobjektet. Fra ex.phil vil man huske at hypotetisk deduktiv metode går ut på å utlede hypoteser og prøve disse mot ”data”.

I NOU 1985:31 side 31 definerte Straffelovrådet ordet data slik det brukes i straffeloven § 145 (2) meget vidt. For det første la man til grunn at data kunne ”lagres og overføres ved hjelp av tekniske midler.” Denne siden av definisjonen fremgår også av ordlyden i 145 (2). For det andre sier Straffelovrådet at data omfatter ”all slags informasjon, f.eks. om personlige, tekniske eller økonomiske forhold, og dessuten dataprogrammer.” I Ot.prp.nr. 35 (1986-87) uttaler departementet på side 20 at data omfattet ”informasjon som er lagret eller overføres ved hjelp av EDB eller andre tekniske midler.”

Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi [22] (heretter datakrimkonvensjonen) definerer i artikkel 1 bokstav b begrepet ”computer data”. Bestemmelsen lyder:

> b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;*

Definisjonen bygger på ISO-definisjonen av data[23]. Begrepet ”computer data” brukes for å understreke at alle data som behandles elektronisk eller i annen direkte prosesserbar form omfattes. ISO-definisjonen ligger også til grunn for den norske forståelsen av begrepet ”data”. I norsk rett forstår man data som en elektronisk representasjon av informasjon. Datakrimutvalget legger til grunn at data omfatter all informasjon som er egnet til elektronisk behandling.[24] I det følgende vil jeg legge denne forståelse til grunn.

---

[21] Bryde Andersen (2001). I kapittel 2 omtales denne problematikken som ”beskrivelsesproblemet”.

[22] Convention on Cybercrime, Budapest 23.11.2001. CETS no. 185.

[23] Se avsnitt 25 i den forklarende rapporten til konvensjonen.

[24] NOU 2003:27 side 10.

Konvensjonen legger til grunn at ”any representation” av informasjon kan være elektroniske data. Data kan følgelig være tekst, video, lyd og ethvert annet format som er i stand til å representere informasjon.[25]

1.3.2 Datasystem

Elektroniske dokumenter vil som regel være knyttet til et lagringsmedium i en datamaskin. Datakrimkonvensjonen bruker begrepet ”computer system” som betegnelse på datamaskin og programvare som kan behandle data automatisk. Konvensjonens artikkel 1 bokstav a lyder:

> a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

Begrepet “device” er teknologinøytralt.[26] Det vanlige vil være en personlig datamaskin slik vi kjenner den fra hverdagen, men moderne datautstyr kan anta mange former. I sammenheng med dokumentfalsk er for eksempel mobiltelefoner, minibanker, kortlesere ved dørene til bygninger og betalingsterminaler i butikker aktuelle.

Flere datasystemer kan være koblet sammen i nettverk.[27] Det elektroniske kommunikasjonsnettet kan være jordbasert eller basert på radiosignaler, uten at dette har betydning for om en innretning er et datasystem. Dette samsvarer med den forståelse som ble lagt til grunn i Ot.prp.nr. 58 (2002-2003) og som har kommet til uttrykk i ekomloven § 1-5 nr 1.

1.4 Former for elektronisk samhandling

Elektronisk dokumentfalsk forutsetter dernest en form for elektronisk samhandling. Med elektronisk samhandling mener jeg utveksling av data ved hjelp av datasystemer og elektroniske kommunikasjonsmidler. Kommunikasjon skjer typisk over et nettverk,

---

[25] Rt. 1994 s. 1610 og Rt. 1995 s. 35 la Høyesterett til grunn at fjernsynsprogrammer ikke var data. Dette ble kritisert av Knut Selmer (Selmer 1995). Selmer mente at data var all informasjon i elektronisk form. Følgelig kunne elektroniske fjernsynssignaler overført gjennom kabel betraktes om en type data. Dette stemmer godt med dagens forståelse.

[26] NOU 2003:27 side 10.

[27] Avsnitt 24 i den forklarende rapporten.

men kan også skje ved utveksling av flyttbare lagringsmedier som for eksempel diskett, cd-rom og harddisk. Man kan også tale om kommunikasjon mellom brukere av samme datasystem som har tilgang til hverandres data.

Man kan for oversiktens skyld snakke om tre typer elektronisk samhandling etter hvem som deltar i kommunikasjonen.[28] Straffbar benyttelse av falskt elektronisk dokument kan skje i forbindelse med alle de tre formene for samhandling.

1.4.1 Kommunikasjon mellom mennesker

For det første kan flere personer utveksle meldinger seg imellom. Typisk vil dette omfatte e-post, SMS eller annen utveksling av datafiler. Informasjonen i slike filer vil kunne gjøres forståelig for mennesker såfremt man har den rette programvaren. Samhandling mellom mennesker gjennom datasystemer svarer til samhandling ved utveksling av tradisjonelle meddelelser og dokumenter.

Det er ikke nødvendig at kommunikasjon skjer ved transport av data. Data kan også utveksles for eksempel ved at to mennesker har adgang til samme lagringsmedium og dataene som er lagret der.

1.4.2 Kommunikasjon mellom et menneske og et datasystem

For det andre kan kommunikasjon skje mellom en person og et datasystem. Ofte vil det være snakk om ulike web-teknologier, for eksempel nettbutikk eller nettbank. I slike tilfeller kan man si at data fra menneske til datamaskin har til hensikt å ”påvirke resultatet av en automatisk databehandling”.[29] En melding fra datasystemet til mennesket kan ha flere formål, for eksempel gi kvittering for en automatisk transaksjon.[30]

Datateknologi har gjort det mulig å rasjonalisere mange arbeidsoppgaver ved å sette en datamaskin til å gjøre jobben. Datasystemer utgjør i mange tilfeller grensesnittet mellom en tilbyder av ulike tjenester, og brukeren. Felles for alle disse systemene er at de tar imot en bestilling, et innskudd eller en betaling fra en bruker uten at tilbyderen

---

[28] Ot.prp.nr. 108 (2000-2001) kapittel 2.2.

[29] Jf. straffeloven § 270 nr 2. Slike data blir ofte kalt ”input”.

[30] Kalles ofte ”output”.

involveres i det hele tatt. Jeg kommer tilbake til hvordan slike systemer kan ses under synsvinkelen indirekte samhandling mellom brukeren av systemet og tilbyderen som driver tjenesten.

I ehandelsloven kalles slike systemer for informasjonssamfunnstjenester og omfatter da ulike kommersielle tjenester i forbindelse med handel og bankforhold. Når forvaltningen automatiserer saksbehandlingen og åpner for døgnåpne, nettbaserte tjenester vil man finne tilsvarende ubetjente offentlige tjenester.

Kommunikasjon mellom et menneske og en datamaskin trenger ikke å skje over avstand. Når man for eksempel autentiserer seg ved å taste pin-kode på mobiltelefonen, skjer kommunikasjon direkte og lokalt. Andre eksempler er bruk av pin-kode i minibank og bruk av kode for å komme inn døren til en bygning.

I det følgende vil jeg med "bruker" forstå den som benytter et datasystem.[31] Den som selv driver eller eier et datasystem som er tilgjengelig for en eller flere brukere omtaler jeg som "tilbyder".[32]

1.4.3 Kommunikasjon mellom datasystemer

For det tredje kan strukturert informasjon utveksles mellom datasystemer uten direkte innblanding av et menneske. Typisk skjer slik kommunikasjon ved bruk av ulike web-teknologier eller såkalt EDI-teknologi.[33]

Et eksempel på denne typen informasjonsutveksling er når datamaskiner automatisk identifiserer seg overfor hverandre, for eksempel utveksler IP-adresser, informasjon om programvare som kjøres og lignende. Slike data vil ofte ha et innhold som virker kryptisk for en menneskelig leser, men som kan tolkes av et dataprogram.

I denne oppgaven vil jeg først og fremst bruke eksempler fra de to førstenevnte formene for samhandling, nemlig i relasjonen mennesker imellom, og relasjonen mellom menneske og datasystem. Det sentrale er å få frem at både menneske og datasystem kan være både avsender og mottaker av elektroniske dokumenter. Benyttelse av falskt dokument kan derfor tenkes i alle de tre formene for samhandling.

---

[31] Tilsvarende i ekomloven (lov av 04.07.03 nr 83) § 1-5 nr 12.

[32] Tilsvarende i ekomloven § 1-5 nr 14.

1.5 Hensyn bak dokumentfalskreglene

Dokumentfalskreglene beskytter flere ulike hensyn. Det kan diskuteres om straff er en rasjonell måte å ivareta disse hensynene. Det kriminologiske spørsmål om straffens begrunnelser drøfter jeg ikke nærmere her.[34] Jeg nøyer meg med å forutsette at straff har en preventiv effekt.[35]

1.5.1 Vern av den alminnelige tillit til dokumenters ekthet

Det viktigste hensynet bak reglene om dokumentfalsk er å beskytte den alminnelige tilliten til dokumenters ekthet. Dokumentet er et viktig bevismiddel i det daglige samkvem og det er sentralt at mennesker kan ha tillit til informasjonen de er bærere av. For eksempel må cedenten kunne innrette seg i tillit til at et gjeldsbrev er ekte. I Straffelovkommisjonens utredning av 1896, heretter SKM 1896, omtales dokumentfalsk som en forbrytelse mot fides publica, den offentlige tillit.[36] Dokumentfalskreglene beskytter med andre ord først og fremst hensynet til allmennheten, og ikke hensynet til den som blir lurt i det konkrete tilfellet. Goos formulerte dette slik at dokumentfalskreglene er en forbrytelse mot ”den sosiale handlefrihet” i motsetning til ”den private handlefrihet”.[37]

Det kan hevdes at utveksling av usikrede data ikke fortjener den samme tillit som tradisjonelle dokumenter, og derfor ikke bør ha det samme strafferettslige vern. Mot dette kan innvendes at de fleste har liten kunnskap om den usikkerhet datakommunikasjon er beheftet med. Følgelig har mange, om enn ubegrunnet, tillit til datas integritet og autentisitet. Så lenge det finnes en alminnelig tillit til data kan det hevdes at de fortjener et visst vern selv om de er usikre. Et slikt synspunkt rimer imidlertid dårlig med bestemmelsen om datainnbrudd i § 145 (2). Der er det nettopp et vilkår for det strafferettslige vernet at data er gitt en ”beskyttelse”. Uten noen beskyttelse betraktes data som mindre verneverdige.[38] De lege ferenda kunne man

---

[33] Electronic Data Interchange.

[34] Hauge (1996). Dessuten NOU 2002:4 kapittel 4.2.

[35] Andenæs (1997) kapittel 7.

[36] SKM 1896 side 172.

[37] Waaben (1994) side 231.

[38] NOU 1985:31 side 31 første spalte.

derfor tenke seg at det ble stilt krav om kvalifisert elektronisk signatur for at data skulle være ”dokument” i lovens forstand.[39]

1.5.2 Vern mot uberettiget ervervelse av annens vitnesbyrd

I tillegg til å beskytte den alminnelige tillit til dokumenters ekthet, så fremgår det av forarbeidene at man ønsket å ramme det å tiltvinge seg en annens vitnesbyrd gjennom falsk.

Hensynet fremgår av SKM 1896 side 173 hvor det uttales at:

> (…) det er et særlig farligt Middel, som benyttes, naar man ved at efterskrive andres Navn paa en Vis, om end alene middelbart, erhverver disses Vidnesbyrd, og at dette derfor ogsaa kan fortjene at belægges med en eftertrykkelig Straf.

Uttalelsen har sammenheng med at man i 1902 innførte et vern for dokumenter som ikke objektivt fremstår som bevisbestemte. Slike dokumenter nyter ikke den samme grad av tillit i dagliglivet av den grunn at de normalt ikke brukes som bevis.

Også dokumenter som ikke fremstår som bevisbestemte kan imidlertid benyttes som bevis. Til forskjell fra reelle bevismidler er dokumentet bevis i kraft av å være bærer av et utsagn fra en person. Ved å benytte et slikt dokument som bevis i rettsforhold påberoper man seg derfor i virkeligheten utstederens vitnesbyrd. Det var misbruk av slikt vitnesbyrd man ønsket å ramme ved å gi denne dokumenttypen et strafferettslig vern.

1.5.3 Samfunnsøkonomiske hensyn

Et dokument er et samfunnsøkonomisk rimelig alternativ til annen bevissikring.[40] I dagliglivet er dokumentet den enkleste og rimeligste måten å sikre seg bevis for transaksjoner og andre mellomværender. Alternativet til dokumentbeviset ville være en langt mer kostnadskrevende bevisførsel om selv de enkleste rettsforhold.

---

[39] Brydensholtutvalget i Danmark avviste et slikt krav. Dette ville også være i utakt med e-signaturloven § 6, 2.pkt. som åpner for rettsvirkninger av signatur som ikke er kvalifisert.

[40] Slik Andenæs/Bratholm (1996) side 285 og Datakriminalitet (1995) side 202.

For eksempel hvis man bestiller kinobilletter på Internett kan man få tilsendt kvittering på e-post eller sms. [41] En slik kvittering vil være et dokument, og er et samfunnsøkonomisk rimelig bevis på at en har betalt for billetten. Alternativet kunne være at en måtte tilkalle noen som kunne bevitne kjøpet, eller man kunne ta opp bestillingen på video. Dette ville være uhyre lite praktisk; bevisførselen i skranken på Saga kino ville bli unødig kostbar.

1.6 Interesser som beskyttes

Hvilke interesser et straffebud beskytter har betydning ved avgrensningen av det straffbare forhold[42]. I det følgende vil jeg gjøre rede for beskyttelsesinteressen, men det faller utenfor oppgaven å redegjøre nærmere for det straffeprosessuelle identitetsspørsmål.

Der straffebud må anses for å beskytte flere interesser samtidig er det avgjørende hvilken interesse bestemmelsen primært beskytter.[43] Dokumentfalskreglene beskytter primært den offentlige interessen i å kunne innrette seg i tillit til dokumenter.[44] Som nevnt så forarbeidene dokumentfalsk først og fremst som et angrep på den alminnelige tillit. Påtalen er gjort ubetinget offentlig etter den alminnelige regel i straffeloven § 77.

Interesselæren kan kritiseres fordi det er en flytende overgang mellom de offentlige interesser og de private individers interesser, som samfunnet utgjøres av.[45] Det kan hevdes at tanken om beskyttelse av den alminnelige tillit er unaturlig fordi de aller fleste tilfeller av elektronisk dokumentfalsk skjer overfor én bestemt mottaker i forbindelse med for eksempel databedrageri.[46] I straffeloven av 1842 ble dokumentfalsk betraktet som et angrep på private interesser. Loven betraktet den som ble ført bak lyset ved bruk av falskt dokument som fornærmet. Videre var det et vilkår for påtale at det forelå begjæring fra fornærmede.

---

[41] For eksempel http://www.filmweb.no/

[42] For eksempel straffeprosessloven § 38.

[43] Rt. 1980 s. 360 (Nittedal). Vegtrafikkloven § 3 beskyttet først og fremst offentlige interesser, mens straffeloven § 239 beskyttet private interesser.

[44] Andenæs/Bratholm (1996) side 285.

[45] Hov II (1999) side 309 flg.

[46] For eksempel Rt. 1991 s. 532.

Dokumentfalsk kan imidlertid også ha til hensikt å forlede en ubestemt krets. For eksempel gjelder dette rettighetsdokumenter[47] som tinglyses i et rettighetsregister, og arbeidsattester beregnet på en rekke potensielle arbeidsgivere. De lege lata er det neppe noen tvil om at det er offentlige interesser som i første rekke krenkes.

1.7 Oppgavens avgrensning

I denne oppgaven vil jeg først og fremst drøfte dokumentbegrepet i straffeloven § 179 og analysere dokumentfalskregelen i § 182. Både de objektive og subjektive vilkår vil behandles. I tillegg vil jeg avgrense det straffbare forsøk nedad mot straffri forberedelse jf. straffeloven § 49. Den straffbare falskhandlingen i § 185 (2) behandles sammen med falskbegrepet i punkt 4. § 183 om straffskjerpelse ved konkurrens og § 184 om merker behandles ikke.

Parallelt med drøftelsen av vilkårene for dokumentfalsk vil jeg behandle vilkårene for benyttelse av falsk uttalelse, straffeloven § 371. En uttalelse er mer uformell enn et dokument, og det stilles ikke noe krav om at den har bevisverdi. Prinsipielt retter den seg mot misbruk av andres identitet på samme måte som dokumentfalskregelen. To grunner tilsier at bestemmelsen bør være med i en fremstilling om elektronisk dokumentfalsk. For det første er det en nær tilknytning mellom dokumenter av betydning som bevis i et aktualisert rettsforhold, og uttalelser uten bevismessig betydning. Jeg behandler dette i punkt 3.3.4 nedenfor. For det annet aktualiseres § 371 ved fremveksten av Internett som gjør det enkelt å misbruke andres identitet i ulike ikke-rettslige sammenhenger. Dette gjør det naturlig å fastlegge dens virkeområde der uttalelsen foreligger elektronisk.

For å belyse benyttelseshandlingen drøfter jeg § 185 (1) som likestiller forfalskning av offentlig protokoll med benyttelse av falskt dokument.

[47] I Rt. 1983 s. 451 var det tale om tinglysing av falsk erklæring om rett til vei og garasjeplass.

2 Rettskildesituasjonen

2.1 Forarbeider

Forarbeidene til straffeloven av 1902[48] er gamle. Etter hvert som rettspraksis kommer til reduseres forarbeidenes relative vekt. På området for elektronisk dokumentfalsk er det lite rettspraksis. Derfor har Straffelovkommisjonens utredning fra 1896 fortsatt en viss betydning ved tolkningen. Litteraturen bygger i stor grad på forarbeidene. Dessuten inneholder utredningen prinsipielle betraktninger som er nyttige også i dag.

Selv om lovbestemmelsene om dokumentfalsk ikke har vært endret formelt siden 1902 har loven vært omtalt i flere utredninger som har drøftet behovet for ny lovgivning. Man må sondre mellom utredninger som ligger til grunn for en beslutning fra lovgiver og utredninger som foreløpig ikke har ledet til lovgivning.

Straffelovrådet utredet i NOU 1985:31 behovet for å endre enkelte straffebestemmelser i lys av den teknologiske utviklingen. Ved tolkningen av § 182 jf. § 179 fant Straffelovrådet at elektroniske data var beskyttet som ”dokument” i straffelovens forstand. Tolkningen fikk tilslutning av Justisdepartementet i Ot.prp.nr. 35 (1986-87) og ble lagt til grunn av Justiskomiteen i Inst.O.nr. 65 (1986-87). Følgelig ble reglene om dokumentfalsk ikke anbefalt endret. Selv om utredningen og proposisjonen ikke ledet til et positivt lovvedtak ble den lagt til grunn for beslutningen om å ikke endre dokumentfalskreglene. Det er derfor rimelig å tillegge fremstillingene vekt som forarbeider til et vedtak om ikke å endre loven. Om man ser utredningen, odelstingsproposisjonen og innstillingen under synsvinkelen forarbeider eller etterarbeider[49] er i denne sammenheng uten praktisk betydning.

2.2 Juridisk litteratur

I tillegg til alminnelig litteratur på området har dokumentfalskreglene vært drøftet i enkelte utredninger. I NOU 2003:27 drøfter Datakrimutvalget spørsmålet om norsk rett er i samsvar med Europarådets datakrimkonvensjon. I denne forbindelse gis en kortfattet fremstilling av gjeldende rett. Utredningen er per dags dato ute på høring.

---

[48] Mest utfyllende er Straffelovkommisjonens utredning 1896 (SKM 1896). I denne oppgaven lar jeg de øvrige forarbeidene ligge.

[49] Helgesen, Jan E. Rettskildelære. 4.utg. Oslo 1997. Side 94 flg.

Datakrimutvalgets vurderinger er følgelig ikke lagt til grunn av lovgiver og har derfor vekt som annen juridisk litteratur.

I NOU 2002:4 foreslår Straffelovkommisjonen visse endringer i reglene om dokumentfalsk. I denne sammenheng gis også uttrykk for kommisjonens tolkning av gjeldende regler. Utredningen er forarbeider til en fremtidig straffelov, men på lik linje med Datakrimutvalgets vurdering er den ikke lagt til grunn av lovgiver enda. Også denne utredningen må derfor ha relevans og vekt som juridisk litteratur.

2.3 Rettspraksis

Elektronisk dokumentfalsk har bare vært behandlet av Høyesterett en gang, i dommen inntatt i Rt. 1991 s. 532. Dommen står sentralt ved tolkningen av dokumentfalskreglene anvendt på elektroniske dokumenter. Jeg vil derfor av hensyn til den videre fremstilling gjøre kort rede for saksforholdet i dommen her.

To ansatte ved Bankenes betalingssentral, heretter BBS, gikk inn i bankens utbetalingssystem og fikk tilgang til den datafilen som inneholdt kontonumre som det skulle utbetales penger til. De ansatte endret deretter listen slik at den inneholdt kontonumre til konti de selv hadde opprettet i et titalls banker. Hensikten var følgelig å påvirke dataanlegget til å foreta utbetalingene direkte til deres konti i stedet for de opprinnelige. Det skjedde imidlertid en feil da programmet skulle kjøres og utbetalingene ble derfor aldri foretatt. De to ble dømt for forsøk på databedrageri og fullbyrdet dokumentfalsk.

For øvrig finnes en rekke Høyesterettsavgjørelser vedrørende tolkningen av dokumentfalskreglene. Selv om de ikke direkte sier noe om elektroniske dokumenter er flere av dem uttrykk for rettsoppfatninger og tolkninger som kan være støtteargumenter ved tolkningen.

2.4 Folkerettslige kilder

Straffelovgivning mot datakriminalitet søkes harmonisert gjennom internasjonalt samarbeid av flere grunner. For det første er det langt enklere enn før å begå straffbare handlinger i ett land som får virkninger i et annet land. Konsekvensen av dette er at

straffbare handlinger kan pådømmes i flere land.[50] Det er da nødvendig med folkerettslige regler om litispendens og rettskraftens objektive grenser.

For det annet er det nødvendig med samarbeid mellom myndighetene i flere land for å gjennomføre en effektiv etterforskning av straffbare forhold og sikre utlevering av forbrytere. Slikt samarbeid forutsetter ofte at de samarbeidende landene har tilsvarende straffelovgivning. Dette kalles prinsippet om "dual criminality". Det fremgår som et vilkår for tvangsmidler i forbindelse med utlevering i utleveringsloven §§ 15, 20 og 24.[51]

Prinsippet om dual criminality er knesatt i Europarådets konvensjon om felles bistand i straffesaker[52] artikkel 5 nr 1 bokstav a-c. Prinsippet er også forutsatt i datakrimkonvensjonen artikkel 25 nr 5 og 29 nr 3 og 4.

Med hensyn til de materielle reglene om dokumentfalsk er det særlig datakrimkonvensjonen som er aktuell av folkerettslige kilder.

2.4.1 Datakrimkonvensjonen

Europarådets datakrimkonvensjon trer i kraft 1. juli i år etter ratifikasjon fra fem stater. Norge har signert, men ikke ratifisert konvensjonen. Konvensjonen oppstiller minstekrav til signaturstatenes straffe- og straffeprosesslovgivning. I januar 2002 ble Datakrimutvalget nedsatt for å klarlegge om norsk rett var i samsvar med konvensjonen. I NOU 2003:27 konkluderer utvalget med at de norske reglene om dokumentfalsk er i samsvar med konvensjonen.

Datakrimkonvensjonens artikkel 7 omhandler elektronisk dokumentfalsk.

Bestemmelsen lyder:

Article 7 – Computer-related forgery

---

[50] For Norges vedkommende følger dette av straffeloven § 12 annet ledd.

[51] Lov om utlevering av lovbrytere m.v. 13.06.75 nr 39.

[52] European Convention on Mutual Assistance in Criminal Matters. ETS 030. Med tilleggsprotokoller ETS 099 og ETS 182.

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Ved siden av artikkel 7 har også artikkel 4 om dataskadeverk og artikkel 6 om spredning av tilgangsdata en viss betydning for fremstillingen.

2.5 Andre lands rett

Dokumentfalskreglene i Danmark er svært like de norske. Både de finske og svenske reglene er derimot ganske ulike reglene i Norge og Danmark. Når rettsanvendere bruker utenlandsk rett i argumentasjonen, er det dels som illustrasjonsmateriale og dels som argumenter for at spørsmålene bør løses likedan hos oss.[53] I denne oppgaven vil jeg i noen grad trekke paralleller til dansk og svensk rett i forbindelse med lovtolkningen.

I forbindelse med den samlede vurderingen i punkt 9 vil jeg med utgangspunkt i dansk og finsk rett skissere mulige endringer av de norske reglene. Brukt på denne måten i vurderingen tjener utenlandsk rett som et forbilde som kan etterlignes.[54]

3 Elektronisk dokument

3.1 Dokumentets form

3.1.1 Innledning

Straffelovens § 179 inneholder en legaldefinisjon av begrepet ”dokument”. Det er en juridisk tolkningsoppgave å bestemme hvor langt det rekker. Straffeloven § 179 lyder:

---

[53] Eckhoff/Helgesen (1997) side 279.

[54] Eckhoff/Helgesen (1997) side 279.

> Ved Dokument forstaaes i denne Lov enhver Gjenstand, som i Skrift eller paa anden Maade indeholder et Tilkjendegivende, der enten er af Betydning som Bevis for en Ret, en Forpligtelse eller en Befrielse fra en saadan eller fremtræder som bestemt til at tjene som Bevis.

Definisjonen har etter sin ordlyd virkning for hele loven, jf "i denne lov". Ordet dokument brukes en rekke steder i straffeloven.[55] Bestemmelsen har derimot ikke direkte anvendelse ved tolkning av tilsvarende uttykk i andre lover. Her kan den i høyden tjene som tolkningsmoment. Straffelovens definisjon er snever fordi det strafferettslige vernet bare tilgodeses dokumenter som har en særskilt betydning som bevisbærer. Til sammenlikning har man en videre definisjon av ordet dokument i forvaltningsprosessen fordi begrepet der er knyttet til parters og andres rett til dokumentinnsyn.

3.1.2 Gjenstandsbegrepet

Straffeloven § 179 oppstiller to kumulative formkrav som må være oppfylt for at data skal anses som "dokument". For det første er et dokument i straffelovens forstand en "Gjenstand". For det annet må dokumentet "i Skrift eller på anden Maade" være uttrykk for en menneskelig tanke. Tolkningen av gjenstandsbegrepet har vært noe omstridt, men må anses klargjort av Høyesterett på 90-tallet.

En "gjenstand" er etter en naturlig forståelse av ordlyden noe håndgripelig. Dette samsvarer med en tradisjonell forestilling om dokumentet som et papirark med påtegning.

Selv om dokumentfalsk i første rekke har hatt til gjenstand papirdokumenter, setter ordlyden ingen grenser for hvilke legemlige gjenstander som tilfredsstiller lovens krav. For eksempel vil en tømmerstokk eller en sau merket med eierens merke, oppfylle lovens krav om "gjenstand".[56] I rettspraksis finnes dessuten en rekke dommer som angår benyttelse av falskt bilskilt eller båtregistreringsmerke.[57] Å snakke om "dokument" i disse tilfellene er etter en naturlig forståelse anstrengt, men det er ingen

---

[55] se note 1 til straffeloven § 179.

[56] Andenæs/Bratholm (1996) side 300.

[57] For eksempel Rt. 1977 s. 242 (bil) og Rt. 1982 s. 142 (båt).

tvil om at de alle omfattes. Noen uttømmende liste over alle mulige gjenstander er ikke mulig å oppstille. Straffelovkommisjonen avviste i NOU 2002:4 at det foreligger noe behov for å innta en legaldefinisjon i straffeloven.[58]

3.1.2.1 Kan data i seg selv være gjenstand?

Spørsmålet i det følgende er om data som sådan omfattes av begrepet ”gjenstand”. Etter ordlyden er en slik tolkning lite naturlig. Data eksisterer bare som elektroniske impulser og er følgelig ikke noe håndfast. Straffeloven § 6 utvider begrepet ”løsøregjenstand” i forhold til en alminnelig språklig forståelse av ordet.[59] Bestemmelsen lyder:

> Under Udtrykket Løsøregjenstand indbefattes i denne Lov ogsaa enhver til Frembringelse af Lys, Varme eller Bevægelse fremstillet eller opbevaret Kraft.

Etter ordlyden skal elektrisk strøm anses for å være ”løsøregjenstand” i lovens forstand. Ordet ”gjenstand” favner videre enn ”løsøregjenstand” slik at definisjonen i § 6 også vil gjelde ved tolkningen av begrepet gjenstand.[60]

En naturlig forståelse av ordet ”Kraft” tilsier at det er elektrisitet som energikilde til å drive elektriske apparater som menes. I rettspraksis har en betraktet ulovlig tilegnelse av elektrisk strøm som tyveri.[61]

Telefonsignaler og tv-signaler kjennetegnes ved at elektrisk strøm brukes til å overføre signaler, men det er ikke kraftforbruket som er det sentrale.[62] Data eksisterer likeledes bare som strømimpulser. Etter en naturlig tolkning av ordet ”Kraft” faller disse i utgangspunktet utenfor.

Straffelovens forarbeider åpner for å betrakte elektriske signaler som ”løsøregjenstand”. Av Forh.O. (1901-02) s. 433-435 fremgår at justiskomiteens formann mente at bestemmelsen også rammet uberettiget bruk av telefon. Videre fremholdt han at

---

[58] NOU 2002:4 side 209.

[59] Kommentert i Rt. 1997 s. 1760. Mindretallet mente penger i elektronisk form måtte anses som en ”løsøregjenstand” i relasjon til straffeloven § 255 første alternativ (underslag). Den vide tolkningen i § 6 ble ansett som et argument i denne retning.

[60] Andenæs (1996) side 7.

[61] Se Rt. 1932 s. 1155.

[62] NOU 1985:31 side 9 annen spalte.

bestemmelsen kunne anvendes på mulige nye naturkrefter, som kan tenkes å bli oppdaget. I Indst.O. I (1901-02) ble det videre lagt til grunn at ordlyden ”til til Frembringelse af Lys, Varme eller Bevægelse fremstillet eller opbevaret Kraft” mente å avgrense mot kraft som eksisterer fritt i naturen. Det var ikke meningen å begrense anvendelsesområdet med hensyn til typen energi.

Høyesterett har i flere dommer avvist at uberettiget bruk av telefonnettet er tyveri. I stedet har retten lagt til grunn at forholdet skal bedømmes som ulovlig bruk, § 261 eller § 393, avhengig av verdien på tellerskrittene. Det kan spørres om Høyesterett i disse dommene har utelukket at elektroniske impulser kan være ”Kraft” i lovens forstand. Problemstillingen foranlediger en nærmere gjennomgang av dommenes premisser.

I Rt. 1989 s. 980 var forholdet at en person hadde koblet seg til en telefonboks ved et sykehus. Ved hjelp av en kabel fikk han dermed tilgang til telefonnettet for sykehusets regning. Spørsmålet for Høyesterett var om forholdet skulle behandles som grovt tyveri av tellerskritt eller som ulovlig bruk av televerkets anlegg. Tyverisubsumsjonen forutsatte i så fall at tellerskrittene ble betraktet som ”løsøregjenstand” etter straffeloven § 6. Retten kom til at det riktige måtte være å straffe for ulovlig bruk. Begrunnelsen i dommen er svært kort. Dette skyldes at tiltalte og aktor var enige om at det var riktig å omsubsummere i denne saken. Førstvoterende uttalte at:

> §261 rammer etter sin ordlyd den urettmessige bruk av televerkets installasjoner som her foreligger, og bestemmelsens forarbeider gir støtte for å gi den anvendelse på forhold av denne art.

Det er noe uklart om førstvoterende med henvisningen til ”televerkets installasjoner” sikter til selve myntapparatet, eller om det er telefonsignalene som menes. I teorien er det hevdet at dommen av denne grunn neppe kan sies å avgjøre endelig om telefonsignaler i telenettet kan anses som ”løsøregjenstand” etter § 6.[63]

Dommen inntatt i Rt. 1992 s. 790 omhandler det forhold at en ansatt i Televerket koblet et såkalt telefonprøvenummer fra sin arbeidsplass til sin private bopel. Med dette koblingsarrangementet hadde han ringt gratis hjemmefra tilsvarende minst 10.000

[63] Bratholm/Matningsdal I (1995) s. 17-20. Slik også NOU 1992:23 side 68.

tellerskritt. Også i denne saken var spørsmålet for Høyesterett om tiltalte skulle dømmes for tyveri av tellerskritt eller for ulovlig bruk.

Høyesterett kom også i denne dommen til at det riktige var å dømme for ulovlig bruk. Førstvoterende, som de øvrige dommere sluttet seg til, la vesentlig vekt på at ordlyden i tyveribestemmelsen ”borttar […] en gjenstand” passet dårligere på sakens faktum enn bestemmelsen om ulovlig bruk som rammer den som ”rettsstridig bruker […] en løsøregjenstand”. Til støtte for dette anfører retten synspunktene fra NOU 1985:31 der det sies at

> For ordens skyld nevnes at innsyn i data medfører forbruk av strøm i den datamaskin hvor opplysningene er lagret. Etter straffeloven § 6 anses elektrisk kraft som løsøregjenstand. Innsyn i data kan da i prinsippet straffes som tyveri/ underslag av strøm, men dette virker svært kunstig.

Det Høyesterett uttrykkelig sier er med andre ord at det er mer naturlig å se telefonnettet som ”løsøregjenstand” (§ 261) enn å anse tellerskritt som ”gjenstand” (§ 257). Dommen kan derfor neppe sies å utelukke at strømimpulser kan være ”gjenstand” i andre sammenhenger.

Straffelovrådet la som til grunn at data i seg selv ikke kunne være gjenstand under henvisning til at strømforbruket ikke var det sentrale.[64] Denne tolkningen fikk tilslutning av departementet.[65]

I NOU 1992:23 og NOU 2002:4 foreslår Straffelovkommisjonen å videreføre en bestemmelse om at gjenstandsbegrepet omfatter elektrisk ”energi”. Det fremgår av NOU 1992:23 på side 68 at man med energi også skal forstå energi i telefonledninger og lyd- og billedenergi i kabel-TV-anlegg. På side 67 presiseres imidlertid at data ikke omfattes. Denne sondringen virker urimelig i lys av den pågående sammensmeltingen av elektroniske medier.[66]

Som drøftelsene ovenfor viser er ordlyden i § 6 uklar. De to dommene fra Høyesterett tar ikke uttrykkelig stilling til om elektroniske signaler kan være løsøregjenstand i den

---

[64] NOU 1985:31 side 9.

[65] Ot.prp.nr 35 (1986-87) side 14.

[66] NOU 1999:26 Konvergens.

betydningen § 6 bruker ordet. Eldre forarbeider synes å åpne for at elektroniske impulser kan være gjenstand, men nyere forarbeider har formentlig større vekt ved avgjørelsen. Det er et reelt behov for å betrakte data som gjenstand i relasjon til dokumentbegrepet. Jeg kommer tilbake til dette nedenfor i punkt 3.1.2.4.

Etter dette blir konklusjonen at data neppe er gjenstand etter gjeldende rett.

3.1.2.2 Et lagringsmedium er en gjenstand

Straffelovrådet la til grunn at et lagringsmedium åpenbart er gjenstand, og at elektroniske data som er lagret på et medium følgelig vil oppfylle kravet.[67] Straffelovrådet drøftet gjenstandsbegrepet i relasjon til § 291 om skadeverk. Den samme analysen ble lagt til grunn ved fremstillingen av reglene om dokumentfalsk.

Resonnementet fra Straffelovrådet tar utgangspunkt i relasjonen mellom programvare, herunder data, og maskinvare, som til sammen utgjør et datasystem.[68] Maskinvaren, herunder datasystemets lagringsmedier, er åpenbart "gjenstand" i § 291. Synspunktet er at dersom elektroniske data uberettiget blir endret eller slettet, så kan skadeverkbestemmelsen benyttes dersom handlingen "ødelegger, skader, gjør ubrukelig eller forspiller" lagringsmediet for eieren. Selv om ordlyden i § 291 isolert sett talte for at skaden måtte være av fysisk art, lagringsmediet blir jo ikke påført fysisk skade, kunne dette ikke være avgjørende. Uten programvare eller data er lagringsmediets nytteverdi redusert slik at § 291 kan benyttes. Straffelovrådet bygger på resonnementet i Rt. 1930 s. 1005 (Damlukedommen).

Saksforholdet var der i korte trekk at den tiltalte hadde stengt en luke i et damanlegg og derved stanset vanntilførselen til turbinene, med den konsekvens at anlegget ikke leverte strøm i tolv timer. Spørsmålet var om man kunne bruke skadeverkbestemmelsen all den tid luken bare var lukket, men ikke skadet. Høyesterett kom til at forholdet var straffbart skadeverk. Begrunnelsen var at man måtte se damluken i relasjon til dammen for øvrig. Damanlegget, som strømprodusent, ble gjort ubrukelig ved at luken stengte. Fra dommen siteres:

---

[67] NOU 1985:31 side 10.

[68] Se punkt 1.3.2 ovenfor.

> « Gjenstand » i lovens forstand er in casu ikke damluken isolert sett, men selve det anlegg hvorav luken var en enkelt bestanddel. Det kan efter min opfatning ikke stille sig tvilsomt, at den der ved at manøvrere en luke i et damanlegg i utide og derved gjør inngrep i damanleggets tilsiktede nytteeffekt gjør sig skyldig i et forhold som beskrevet i §291.

Straffelovrådets resonnement bygger på at data står i samme relasjon til datamaskinens lagringsmedium som damluken i relasjon til damanlegget. Data og lagringsmedium ses på som en enhet som fungerer sammen og ikke hver for seg. Endres data får dette følgelig konsekvenser for mediet de er lagret på. I forlengelsen av dette resonnementet er lagringsmediet som data er lagret på den ”gjenstand” som § 179 taler om. Data som er lagret på et lagringsmedium kan følgelig være dokument dersom de øvrige vilkår er oppfylt.

Utredningens konklusjon har siden fått tilslutning i teorien.[69] I dommen i Rt. 1991 s. 532 la retten til grunn at elektroniske data var dokument i straffelovens forstand under henvisning til Straffelovrådets utredning.

3.1.2.3 Midlertidig og permanent lager

Straffelovrådet skiller mellom to vesensforskjellige måter å lagre elektroniske data på.[70] For det første kan data lagres permanent på et magnetlager, for eksempel på en harddisk eller diskett, eller på et optisk lager, for eksempel på en cd- eller dvd-plate. Permanent lagring innebærer at elektroniske data etterlater fysiske spor på lagringsmediet som ikke forsvinner når strømmen slås av. Hvis en datafil er lagret på et magnet- eller optisk lager har filen etter dette en slik tilknytning til en gjenstand at den kan utgjøre et ”dokument”.

For det annet kan elektroniske data være lagret midlertidig i RAM.[71] RAM er et minne der datamaskinen oppbevarer programmer og data som er i bruk eller under bearbeidelse av maskinens øvrige komponenter. Til forskjell fra data lagret permanent, er data i RAM representert ved elektroniske impulser. Hvis strømmen slås av, forsvinner alle data som befinner seg i RAM. Også data som er under bearbeidelse skal

---

[69] Andenæs/Bratholm (1996) side 300, Bratholm/Matningsdal II (1995) side 396.

[70] NOU 1985:31 side 10.

[71] Random Access Memory.

etter utredningen anses for å ha en slik tilknytning til en "gjenstand" at en kan tale om et dokument.

Straffelovrådet tok derimot ikke stilling til om elektroniske data som ikke befinner seg på et datasystem, men som er under overføring mellom datamaskiner, oppfylte gjenstandsvilkåret. Data kan overføres på en rekke måter, i jordbasert kabel eller trådløst.[72] Når data overføres trådløst har de utvilsomt ikke lenger tilknytning til en fysisk gjenstand. Heller ikke ved overføring over en fysisk kabel mente Straffelovrådet at tilknytningen til gjenstand er tilstrekkelig.

3.1.2.4 Oppsummering og vurdering

Som en oppsummerende konklusjon kan man si at Straffelovrådet banet vei for å avgrense gjenstandsbegrepet ved å spørre om data har tilstrekkelig tilknytning til en fysisk gjenstand. Denne forståelsen må i dag betraktes som gjeldende rett.

Etter at Straffelovrådet innførte kriteriet om tilstrekkelig tilknytning til en fysisk gjenstand, herunder avgrensing av gjenstandsbegrepet mot data under overføring, har bruken av datamaskiner økt sterkt. Økende bruk av elektronisk kommunikasjon over nettverk, samt distribuerte lagringsformer, gir grunn til å vurdere hensiktsmessigheten av rettstilstanden fra NOU 1985:31.

3.1.2.4.1 Data under overføring

I dag vil elektroniske dokumenter til stadighet være under overføring mellom datasystemer i nettverk. Ved å betrakte lagringsmediet som gjenstand i § 179 vil man få den merkelige situasjonen at et dokument opphører å være et dokument under forsendelse, men igjen blir dokument når det kommer frem.

Med spesiallaget programvare er det mulig å slette eller på annen måte ødelegge data mens de er under overføring mellom to datamaskiner. Dette vil etter det etablerte syn ikke innebære straffbart skadeverk fordi ingen fysisk gjenstand skades i handlingen. På tilsvarende måte kan en tenke seg at elektroniske data med dokumentinnhold endres underveis. Avgjørende for bedømmelsen blir da om data på tidspunktet for forfalskningen har tilstrekkelig tilknytning til en gjenstand.

---

[72] Se punkt 1.3.2.

Et nettverk består av en rekke routere som leder datatrafikken på rett vei.[73] Slike routere er i virkeligheten også datamaskiner med lagringsmedier.[74] Det kan spørres om data har tilstrekkelig tilknytning til gjenstand et tusendels sekund mens de passerer gjennom routeren. Problemstillingen illustrerer hvilke praktiske problemer det innebærer å opprettholde en regel om at data må ha tilknytning til en gjenstand for å være dokument.

3.1.2.4.2 Distribuerte former for lagring av data

Distribuerte lagringssystemer gjør det mulig for brukere av datanettverk å lagre data på ulike lagringsmedier rundt om på nettverket. Brukeren vet ikke alltid hvor data fysisk er lagret. Dataene blir tilgjengelige for brukeren med noen tastetrykk, men rent fysisk er det likegyldig om data befinner seg i Nederland eller i USA. Et eksempel på distribuert bruk av datamaskiner er Internettbaserte e-posttjenere[75]. Brukere logger seg på slike fra hele verden, helt uavhengig av hvilken datamaskin de benytter. E-post lagres på operatørenes lagringsmedier ett eller annet sted i verden. Brukeren har som oftest ingen anelse om hvor de geografisk er plassert. I lys av at data overføres og lagres tilfeldig rundt i verden uten at det er av betydning hvor de rent faktisk befinner seg, kan det hevdes at det er søkt å holde fast på et krav om at elektroniske dokumenter må ha ”tilstrekkelig tilknytning” til en gjenstand. Gjenstanden vil i tilfelle være et lagringsmedium et tilfeldig sted i verden.

3.1.3 Data er ”paa anden Maade” bærer av menneskelige tanker

Data i seg selv består av såkalt binærkode som er uforståelig for mennesker dersom de ikke gis en visuell eller audiovisuell form. Det er likevel sikker rett at data oppfyller kravet om å fremgå ”i Skrift eller paa anden Maade”. Dette ble lagt til grunn av Straffelovrådet som i NOU 1985:31 på side 11 uttalte at:

> Det neste vilkår er at tilkjennegivendet fremtrer i ”Skrift eller paa anden Maade”. Det sistnevnte alternativ vil omfatte datalagret informasjon.

---

[73] En router er en datamaskin på et nettverk som leder data i pakker mellom kommuniserende datasystemer.

[74] Ehandelsloven § 17 omtaler dette som ”mellomlagring” jfr ehandelsdirektivet 2000/31/EF art 13.

[75] Noen av de mest kjente er Hotmail og Yahoo.

Denne forståelsen av loven ble formentlig også lagt til grunn av Høyesterett i Rt. 1991 s. 532 selv om vilkåret ikke eksplisitt drøftes.

Det har i forhold til formkravene ingen betydning hvilken visuell eller audiovisuell form data presenteres overfor brukeren. Det avgjørende er at dataene inneholder et tilkjennegivende, se punkt 3.2 nedenfor. For fotografier vil dette sjelden være tilfellet, se punkt 3.2.6.8.

3.1.4 Særlig om skriftkravet i straffeloven § 371

Straffeloven § 371 rammer benyttelse av ”skriftlig eller trykt” falsk uttalelse. Noe krav til gjenstandstilknytning oppstilles ikke. Det kan spørres om bestemmelsen rammer uttalelser som fremkommer elektronisk. Ordlyden taler mot å tolke skriftkravet slik at det omfatter data. Det er ikke naturlig å omtale elektroniske data som verken skriftlig eller trykt. NOU 1985:31 drøfter ikke skriftlighetskravet i § 371 og spørsmålet har ikke vært oppe i rettspraksis. Heller ikke teorien har befattet seg med spørsmålet.

Straffelovrådet sluttet at kriteriet ”i Skrift” i § 179 ikke omfatter elektronisk lagret informasjon, men at ”paa anden Maade” gjør det.[76] Dette er et moment som taler mot at ”skriftlig” omfatter elektroniske data. Kriteriet ”Trykt” er ikke brukt i § 179 og heller ikke omtalt i verken NOU 1985:31 eller NOU 2003:27.

Dokumentdefinisjonen inneholder alternativet ”paa anden Maade” først og fremst fordi en rekke merker og symboler kan ha bevismessig betydning uten at de omfattes av skriftkravet. En uttalelse er derimot noe annet enn et bevisende utsagn. Bevisende merker er derfor lite aktuelt her. Det er naturlig å anta at dette er årsaken til at § 371 ikke inneholder alternativet ”paa anden Maade”.

Sammenheng i regelverket taler for at elektroniske data omfattes av skriftkravet. Forskjellen mellom dokumenter i § 179 og uttalelser i § 371 er at sistnevnte ikke har betydning som bevis. Det var neppe lovgivers mening å skille mellom de to bestemmelsene etter hvilken teknologi meddelelsen formidles gjennom.

Det kan trekkes en parallell til straffeloven § 10 som definerer ”trykt Skrift”. Det sentrale med kriteriet trykt skrift er at det trykte materialet mangfoldiggjøres, jf

[76] NOU 1985:31 side 11.

ordlyden ”mangfoldiggjøres ved Trykken”. Det er usikkert om bestemmelsen rammer elektroniske data. Bratholm/Matningsdal hevder spørsmålet er høyst tvilsomt.[77] Jon Bing har i en utredning hevdet at elektroniske data kan være ”trykt Skrift”.[78]

Det kan være grunn til å nevne at den danske straffeloven § 171 stk 2, før lovendringen av 19.05.04, definerte dokument som en ”skriftlig” tilkjennegivelse. Kravet til skriftlighet ble lenge sett som et hinder for at elektroniske data kunne være dokumenter i straffelovens forstand. En dom i Østre landsret fra 2001 kom likevel til at en e-post var et skriftlig tilkjennegivende.[79] Som en følge av dommen, som ikke ble anket til Høyesterett, var rettstilstanden i Danmark lenge uavklart.[80]

I forbindelse med fremveksten av Internett og kommunikasjon gjennom ”pratekanaler” og ”nyhetsgrupper” er det i dag et klart behov for å ramme falsk av elektroniske uttalelser på linje med skriftlige. Behovet understrekes også ved den utstrakte bruken av SMS på mobiltelefoner.

Under en viss tvil kommer jeg til at kravet til uttalelse i § 371 også omfatter data.

I motsetning til begrepet ”paa anden Maade” kan man neppe tolke ”skriftlig” slik at det omfatter alle former for data. Multimediefremstillinger med bruk av lyd, illustrasjoner og video er neppe ”skriftlig”. Det er rimelig å begrense bestemmelsen til elektroniske data som fremkommer i tekst.

3.2 Dokumentets innhold. Tilkjennegivende.

Ovenfor konkluderte jeg med at formkravene ikke er til hinder for at elektroniske data kan være dokumenter. Likevel er ikke alle elektroniske data dokumenter. Det er først og fremst ved sitt innhold at dokumentet skiller seg fra andre meddelelser.

To vilkår må være oppfylt for at elektroniske data innholdsmessig skal kvalifisere som dokument. For det første må data inneholde et tilkjennegivende. For det annet stilles det krav om at tilkjennegivendet må ha en særlig bevisverdi. Beviskriteriet behandler jeg nedenfor i punkt 3.3.

---

[77] Bratholm/Matningsdal I (1995) side 26.

[78] Bing (1992).

[79] Østre Landsrets dom 26.09.01, saksnummer 5. Omtalt i Lov&Data nr 68 2001.

[80] Brydensholtutvalget side 105-106.

3.2.1 Avgrensning mot reelle bevismidler

En gjenstand må inneholde et ”Tilkjendegivende” for å være et dokument. Ordet tilkjennegivende betyr etter alminnelig forståelse at noen gir uttrykk for noe de mener, en tanke de har. Data er en bærer av informasjon, men ikke all informasjon er tilkjennegivender. Man kan si at et tilkjennegivende er informasjon om hva en person har tenkt.

Fra ordlyden og uttalelsen i forarbeidene trekker Andenæs/Bratholm den slutning at et tilkjennegivende er et ”uttrykk for en menneskelig tanke”.[81] Bratholm/Matningsdal formulerer kravet slik at dokumentet på en eller annen måte ”formidler et menneskelig budskap”.[82] Waaben forklarer det tilsvarende danske ”tilkjendegivelse” som et menings- eller forestillingsinnhold som noen har villet gi språklig uttrykk.[83]

Kriminalloven av 1842 oppstilte ikke noe krav om at et dokument var et tilkjennegivende. Den definerte dokument som enhver gjenstand som fremstår som bestemt til å tjene som bevis. Av SKM 1896 fremgår at man ved å tilføye ordet tilkjennegivende ikke mente å endre rettstilstanden. På side 172 i note 2 står at

> (…) ingen Gjenstand [kan] ”fremtræde som bestemt” til at bevise uden at indeholde et Tilkjendegivende, og denne Begrænsning siger sig derfor selv, saalenge man fastholder at den bevisende Bestemmelse skal fremgaa af Gjenstanden selv.

Utdraget peker på at kriteriet ”Tilkjendegivende” er en unødvendig presisering for dokumenter som man ut fra innholdet kan slutte er bestemt til å bevise noe.[84] Kriteriet innebærer imidlertid en nødvendig avgrensning mellom reelle bevismidler og dokumenter av betydning som bevis i rettsforhold.[85] Et reelt bevismiddel kan være av betydning som bevis, men er ikke et dokument fordi det mangler et tilkjennegivende. I

[81] Andenæs/Bratholm (1996) side 299.

[82] Bratholm/Matningsdal II (1995) side 397.

[83] Waaben (1994) side 233.

[84] Se punkt 3.3.5 nedenfor.

[85] Se punkt 3.3.4 nedenfor.

denne sammenheng er det grunn til å peke på at datasystemet og dets lagringsmedier er reelle bevismidler.[86]

3.2.2 Et tilkjennegivende er forståelig for mennesker

Tradisjonelle dokumenter har til formål å formidle et tilkjennegivende til en menneskelig mottaker. Dokumentets bevisverdi har også tradisjonelt vært knyttet til dets evne til å overbevise et menneske om faktiske omstendigheter. Derfor har man lagt til grunn i forarbeider og teori[87] at elektroniske data må kunne gjøres forståelige for mennesker for å inneholde et tilkjennegivende.

Straffelovrådet la en slik tolkning til grunn i NOU 1985:31 s. 11. De reiste problemstillingen om elektroniske data i det hele tatt hadde evne til å være tilkjennegivender i lovens forstand, om data kunne sies å være uttrykk for en menneskelig tanke. Rådet mente at dette var tilfellet og uttalte:

> Riktignok kan man innvende at det som er lagret bare foreligger i maskinlesbar form, og i denne form er data uforståelige. Dette kan imidlertid ikke være avgjørende *så lenge de maskinlesbare data kan overføres til en form som kan forstås av mennesker*, og de i denne form gir uttrykk for en menneskelig tanke. (min uthevning)

Det sentrale ved dette utdraget er at man så det slik at data ikke inneholder et tilkjennegivende med mindre de kan overføres til en form som er forståelig for mennesker.

I datakrimkonvensjonen artikkel 7 er det uttrykkelig sagt at data har vern mot falsk ”regardless whether or not the data is directly readable or intelligible.” Ordet ”directly” antyder at data må kunne gjøres forståelig for et menneske. Denne tolkningen har også støtte i den forklarende rapporten avsnitt 83 hvor det heter at vernet gjelder ”data which is the equivalent of a public or private document, which has legal effects”. Tradisjonell

[86] Datakriminalitet (1995) side 204.

[87] Andenæs/Bratholm (1996) side 300.

lære er at et dokument ikke kan ha rettslig betydning annet enn som bevis overfor et menneske.[88]

Det er akseptert i teorien at et tilkjennegivende kan komme til uttrykk i kode eller språk som bare et lite antall mennesker forstår.[89] Datateknologi er utviklet av mennesker. Datamaskinens evne til å prosessere data er begrenset av instruksjoner den har fått av et menneske. I prinsippet kan derfor alle data forstås av mennesker som er spesielt datakyndige. Kravet om at data må kunne gjøres forståelig for et menneske innebærer derfor neppe noen begrensning med hensyn til hvilke typer data som kan være bærer av et tilkjennegivende.

3.2.3 Et tilkjennegivende kan inngå som premiss i en automatisk databehandling

I forrige avsnitt konkluderte jeg med at alle data i prinsippet kan inneholde tilkjennegivender, fordi data prinsipielt alltid er forståelige for mennesker.

Det kan videre spørres om tilkjennegivendet må benyttes overfor et menneske. Et slikt vilkår følger ikke av ordlyden. Uttalelsen fra NOU 1985:31 som referert i forrige avsnitt gir imidlertid grunn til å reise problemstillingen.

I dagens samfunn skjer ikke bare mye kommunikasjon digitalt. Innføring av datateknologi innebærer på mange områder en rasjonalisering av oppgaver som tidligere ble gjort av mennesker. Dataprogrammer deltar i rettslig relevante prosesser på vegne av tjenesteytere. For eksempel styres betalingsformidlingstjenester av datamaskiner. I dag kan en flytte penger mellom konti uten at noe menneske i banken direkte er involvert i prosessen. Man kan kjøpe bøker, kino- eller flybilletter på Internett. Avtaleinngåelse og betaling skjer for da som regel på en webside av en bruker. Tjenesteyteren har ofte ingen direkte befatning med selve transaksjonen. Er det et tilkjennegivende når en mater data inn i et datasystem som en premiss for automatisk databehandling?

Kriteriet tilkjennegivende må ses i lys av bestemmelsen om databedrageri, straffeloven § 270 nr 2. Tradisjonelt har en pådømt dokumentfalsk i konkurrens med bedrageri der

[88] Se om bevisrekvisitten punkt 3.3.

[89] Andenæs/Bratholm (1996) side 300.

forledelsen har skjedd ved hjelp av et falskt dokument. Bestemmelsen om databedrageri tar konsekvensen av at manipulasjon av data kan lede til tap. Manipulasjonen gjelder data som ikke er beregnet for å leses av et menneske. Det sentrale er at de tolkes og behandles av et datasystem. Det er imidlertid ikke noe vilkår i § 270 nr 2 at de data som manipuleres er dokumenter.

Høyesterett har berørt problemstillingen i dommen i Rt. 1991 s. 532 (BBS-dommen), referert ovenfor. Her la Høyesterett til grunn at en liste over de kontonumrene som skulle ha utbetalt penger fra Bankenes betalingssentral var et tilkjennegivende. Listen over kontonumre ble brukt av dataprogrammet under overføringen av penger mellom konti. Høyesterett la uten videre drøftelse til grunn at listen var et tilkjennegivende.

Datakrimkonvensjonen artikkel 7 beskytter elektroniske data som kan bli ”considered or acted upon for legal purposes”. Ordene ”considered or acted upon” taler isolert sett for at tilkjennegivendet må brukes direkte overfor et menneske. I den forklarende rapporten avsnitt 81 pekes imidlertid spesielt på den rollen elektroniske data spiller i forbindelse med databedrageri. Således sies at ”Computer-related forgery involves unauthorized creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data (…)”. Det er naturlig å slutte fra dette at data som skal legges til grunn i en rettslig relevant automatisk prosess kan være dokument i konvensjonens forstand.

Konklusjonen blir at det ikke gjelder noe krav om at et tilkjennegivende skal være ment å brukes overfor et menneske.

3.2.4 Data som produseres av et dataprogram

En annen problemstilling er om data som fremstilles av et dataprogram kan innebære et tilkjennegivende. Slike data er for eksempel en logg som viser bevegelser på, og bruk av, et datasystem. Andre eksempler er kvitteringer som utstedes elektronisk ved kjøp av varer eller ved levering av selvangivelsen på Internett.

Verken Straffelovrådet eller Datakrimutvalget har berørt spørsmålet. Det finnes heller ingen rettspraksis på området. Når rettskildesituasjonen gir sparsomt med holdepunkter

blir man overlatt til en vurdering av hva som er naturlig i lys av ordlyden, teori og de reelle hensyn som gjør seg gjeldende.[90]

Programmererens tanker setter absolutte grenser for hva datamaskinen kan produsere av data. Gjennom de instruksjoner som gis til datasystemet gjennom programvaren rasjonaliseres bare oppgaver som tjenesteyter kunne gjort selv. Data produsert av et dataprogram er indirekte uttrykk for menneskelige tanker. I teorien har det av denne grunn vært hevdet at data produsert av et datasystem kan være tilkjennegivende.[91]

I prinsippet kunne programmereren selv for eksempel observert bevegelser på maskinen og logget disse manuelt. Ordningen med automatisk logging fremstår dermed bare som en praktisk måte å føre en logg. Måten loggen presenteres på, samt selve avgrensningen av hva slags informasjon som skal logges, er utslag av programmererens vurderinger. En automatisk ført logg er etter dette et tilkjennegivende.

Det samme synspunktet kan anlegges med hensyn til såkalte metadata. Metadata er elektroniske data knyttet til andre elektroniske data. Som logger kan metadata tjene ulike formål. Dels kan de være av betydning for programmer i operativsystemet til bruk ved lagring og sortering av filer. Dels kan de være av interesse for brukeren ettersom de gir nyttig informasjon om de filene hun har lagret på datamaskinen. Datakriminalitet (1995) konkluderer med at metadata er tilkjennegivender.[92]

Også kvitteringer som utstedes automatisk i forbindelse med transaksjoner på Internett blir etter dette å betrakte som tilkjennegivender. De genereres automatisk, men følger instruksjoner gitt av tilbyderen bak tjenesten. Et eksempel på en slik kvittering er den man får fra skatteetaten etter å ha levert selvangivelsen på Internett.

3.2.5 Tolkning og helhetsvurdering

Data skriver seg direkte eller indirekte fra et menneske og vil derfor som regel være uttrykk for en eller annen tanke. I de fleste tilfeller vil det ikke være tvilsomt at data inneholder et tilkjennegivende. Når noen i sammenhengende setninger skriver en

---

[90] Eckhoff/Helgesen (1997). På side 357 flg. defineres reelle hensyn som vurderinger av resultatets godhet.

[91] Datakriminalitet (1995) side 203.

[92] Datakriminalitet (1995) side 206. Her brukes ordet ”hjelpefiler”, men meningen er den samme.

redegjørelse, eller i et regneark lager en tabell over utgifter og inntekter i bedriften, er det uten videre klart at det er tale om menneskelige tanker. Det samme vil være tilfellet for en web-side med informasjon eller et utfylt bestillingsskjema for en nettbutikk.

Tvilsomme tilfeller oppstår hvis noen produserer data som isolert ikke gir mening. Det kan for eksempel være at noen mater inn i en datamaskin sin underskrift ved hjelp av trykkfølsom penn. Et annet eksempel er at noen skriver inn et passord eller pin-kode. Kan man tale om tilkjennegivender i slike tilfeller?

Utgangspunktet om at et tilkjennegivende er uttrykk for en menneskelig tanke må modifiseres noe i lys av rettspraksis. Det er for eksempel lagt til grunn av Høyesterett at enkeltstående ord på et ark[93] ikke oppfyller kravet om tilkjennegivende, selv om det åpenbart ligger en tanke bak. Det er følgelig et krav at ordene fremgår i en sammenheng der de gir mening.

I rettspraksis har en lagt til grunn at det må foretas en konkret helhetsvurdering i det enkelte tilfellet.[94] Sentralt i vurderingen blir hvilken sammenheng data forekommer. De samme dataene kan være et tilkjennegivende i en sammenheng, i en annen ikke. Nedenfor vil jeg til illustrasjon drøfte kriteriet tilkjennegivende i forhold til data benyttet under samhandling i ulike konstellasjoner, se punkt 1.4 ovenfor.

Et eksempel kan illustrere helhetsvurderingen. I Rt. 1940 s. 40 var saksforholdet at en mann hadde stjålet nummerskiltene fra en annen bil, endret numrene på skiltet, og satt skiltene på sin egen bil. Høyesterett la til grunn at mannen ved sine handlinger hadde forfalsket et dokument. Nummerskiltet, når det er påsatt en motorvogn, er et tilkjennegivende om at eieren kan bruke på veien. De tegnene som utgjør nummeret på et bilskilt ville ikke vært et tilkjennegivende dersom de simpelthen var skrevet inn i et tekstbehandlingsprogram i en datamaskin. Nummerkombinasjonen skrevet på en stålplate påført en bil, formidler derimot menneskelige tanker.[95]

---

[93] Rt. 1922 s. 542. I dette tilfellet var et fotografi påført dato. Datoen var åpenbart uttrykk for en menneskelig tanke etter en alminnelig forståelse. Likevel var det ikke tale om et tilkjennegivende.

[94] For eksempel Rt. 1922 s. 542.

[95] Dommen har dannet grunnlag for fast praksis, se for eksempel Rt. 1982 s. 142 og Rt. 1978 s. 410.

En elektronisk signatur skrevet inn i et tekstbehandlingsprogram, kan neppe sies å inneholde et tilkjennegivende.[96] Det faller unaturlig å si at et navnetrekk formidler noe menneskelig budskap. Derimot antar Andenæs/Bratholm at en signatur på et maleri vil inneholde et tilkjennegivende om hvilken kunstner som står bak aktstykket.[97] Det samme gjelder formodentlig en elektronisk signatur påført et elektronisk kunstverk.

3.2.5.1 Autentiseringsdata

Med autentiseringsdata mener jeg i det følgende data som autentiserer en bruker i møte med et datasystem. Eksempler kan være passord, pin-koder og data i magnetstripen på et bankkort. Det er følgelig tale om tilkjennegivender som inngår i samhandling mellom menneske og datasystem.

Systematisk kan man skille mellom to grupper av autentiseringsdata. Den ene gruppen består av data som er å betrakte som originale identifikasjonsdata, for eksempel magnetstripen i et bankkort, eller et nøkkelkort med magnetstripe som gir tilgang til en bygning. Den andre gruppen er data som skrives inn av en bruker for å autentisere seg fra gang til gang. Passord, pin-koder og andre koder er typiske eksempler på den siste gruppen. Denne sondringen har betydning for hvem som må anses som utsteder og ved tolkningen av falskbegrepet.

En hovedgruppe blant de tradisjonelle dokumenter er identifikasjonsbevis av ulike slag. For eksempel er førerkort[98], pass[99], representantkort[100] og kredittkort[101] betraktet som tilkjennegivender. Hva tilkjennegivendet går ut på beror på en tolkning av teksten på

---

[96] Brottsbalken kommentar (2000) side 73. Eksemplet gjelder håndskrevet signatur på et papirark i relasjon til svensk straffelov § 14:1. I den svenske bestemmelsen innfortolkes et krav om at et dokument fremstiller et ”föreställningsinnehåll” som tilsvarer et krav om tilkjennegivende. Som nevnt i innledningen kan en elektronisk signatur jf. e-signaturloven ha samme rettsvirkninger som en tradisjonell signatur.

[97] Motsatt i Danmark. Der kreves separat tilkjennegivende og utstederangivelse. Se om utstederangivelse nedenfor i punkt 5.1.2.

[98] For eksempel Rt. 1964 s. 1341.

[99] For eksempel Rt.1974 s. 382.

[100] Rt. 1966 s. 1388. Et representantkort var et legitimasjonsbevis for inspektører ved en mineralvannfabrikk.

[101] For eksempel Oslo tingretts dom TOSLO-2003-06126.

kortet sett i lys av den arten dokument det er tale om. Teksten alene gir ikke nødvendigvis uttrykk for noe tilkjennegivende. På et førerkort står det ikke annet enn personalia til innehaveren. Man må se førerkortet i relasjon til de regler som gjelder ferdsel med motorkjøretøy for å få et bilde av hvilket tilkjennegivende dokumentet inneholder. Man kan si at et førerkort er bærer av et tilkjennegivende om at innehaveren er berettiget til å føre bil av en viss størrelse på norske veier.

Magnetstripen på et bankkort eller annet elektronisk identifikasjonsbevis kan sies å være dataverdenens parallell til tradisjonelle identitetsbevis. Såfremt magnetstripen inneholder autentiseringsdata må de på samme måte som identitetsbevis for øvrig anses for å inneholde et tilkjennegivende om at innehaveren av kortet gis visse privilegier i forhold til et datasystem. Datas utforming og innhold kan variere etter hva kortet skal brukes til, uten at dette får betydning for vurderingen av kriteriet tilkjennegivende.

Passord og andre koder er det mer naturlig å sammenlikne med en tradisjonell signatur. Passord er neppe et tilkjennegivende hvis det skrives inn som tekst ved hjelp av et tekstbehandlingsprogram. Et passord er i seg selv, på samme måte som en håndskrevet signatur, ikke isolert uttrykk for noen menneskelig tanke. Annerledes stiller det seg hvis et datasystem spør om et passord, og passordet skrives inn for å identifisere en bruker overfor datamaskinen. Da utgjør passordet et tilkjennegivende om at den som skriver det er en berettiget bruker av datasystemet.

3.2.5.2 Hjelpedokumenter

Med hjelpedokumenter mener jeg i det følgende data som skal inngå som en premiss i en automatisk databehandling. Også her er det tale om tilkjennegivender som inngår i samhandling mellom menneske og datasystem.

Høyesterett la i Rt. 1991 s. 532 til grunn at en hjelpefil som var premiss i en databehandling var et dokument. Filens innhold besto simpelthen av en liste med kontonumre som et dataprogram skulle forestå utbetaling av penger til. Isolert fra sammenhengen hvor listen fremkom ville den neppe vært betraktet som et uttrykk for menneskelige tanker. Tolket i lys av hvilken funksjon den hadde ved pengeoverføringer måtte den likevel tolkes som et tilkjennegivende om at penger skulle overføres til kontiene på listen.

Datasystemer som er beskyttet med en eller annen form for passord eller kode har ofte lagret en fil som inneholder passord for alle autoriserte brukere.[102] Når brukeren skriver inn et passord for å autentisere seg overfor datasystemet kontrollerer programvaren om passordet stemmer med det som er lagret i passordfilen. I denne sammenheng er en slik passordfil å betrakte som et hjelpedokument. Listen med passord er et tilkjennegivende om hvilke brukere som har adgang til maskinen.

3.2.5.3 Dataprogrammer

Dataprogrammer skiller seg fra øvrige datafiler ved at de først og fremst inneholder instrukser til en datamaskin om å utføre visse prosesser. Det kan spørres om man skal betrakte et program som en del av datamaskinen, og derfor som reelt bevismiddel, eller om det er et tilkjennegivende. I teorien har det vært anført at det er mest nærliggende å betrakte programmer som tilkjennegivender.[103]

Dataprogrammer kan ha betydning som tilkjennegivender i to relasjoner. For det første kan dataprogrammet være et tilkjennegivende i samhandling mellom mennesker.

Programmereren skriver inn programkode som tekst. I denne formen er dataprogrammet klart et uttrykk for tankene til programmereren og følgelig et tilkjennegivende.[104] Programkoden gjøres om til maskinkode i en såkalt kompileringsprosess. Et kjørbart dataprogram kan igjen gjøres om til kildekode ved dekompilering.

Et dataprogram inneholder vanligvis, foruten instruksjoner til maskinen, data som presenteres overfor brukeren under kjøringen av programmet. Slike data er klart tilkjennegivender dersom de formidler meningsfull informasjon. For eksempel presenterer ofte programvareprodusenten brukeren med informasjon om hvem som utviklet programmet. Slike data er et tilkjennegivende og kan også ha den nødvendige bevisverdi.

---

[102] Imidlertid ikke alltid. PKI-kryptering kan brukes også som autentiseringskode. I disse tilfellene benyttes brukerens offentlige nøkkel til å autentisere brukeren. Se NOU 2001:10 side 30. Den offentlige nøkkelen vil da være tilgjengelig for datasystemet, men ikke nødvendigvis lagret der. Offentlige nøkler vil vanligvis være offentlige, dvs tilgjengelig i en offentlig database.

[103] Datakriminalitet (1995) side 204.

[104] L.c.

Derimot har en i teorien sett det slik at varemerker ikke er vernet som tilkjennegivender etter dokumentfalskreglene. Er et varemerke uberettiget brukt i et dataprogram kommer i stedet varemerkeloven § 37 til anvendelse.[105] Varemerket ville ellers blitt betraktet som et tilkjennegivende om hvem som stod bak produktet.

I tråd med det jeg ovenfor har anført om data som er premiss for et dataprogram kan en antakelig slutte at også et kompilert, kjørbart dataprogram er et tilkjennegivende. Tilkjennegivendet inngår da i samhandling mellom menneske og datasystem. Et slikt synspunkt har som nevnt støtte i teorien og har antakelig de beste grunner for seg. Problemstillingen er imidlertid lite praktisk av den grunn at rene maskininstruksjoner sjelden vil ha den nødvendige bevisverdi.

3.2.5.4 Informasjonssamfunnstjenester m.v.

I dag kan skattebetalere levere selvangivelsen elektronisk enten gjennom Internett eller gjennom SMS til skatteetaten. Leveringen skjer ved at en sender fødselsdato og pin-kode til en datamaskin. Det er ikke meningen at noe menneske skal lese den informasjonen brukeren sender. I den andre enden blir dataene verifisert av et dataprogram. Videre blir det automatisk registrert i en database at man har levert.

På samme måte som for autentiseringsdata må det avgjørende være at pin-kode og fødselsdato ses i sammenheng med formålet og omstendighetene for øvrig. De dataene som oversendes kan isolert være uforståelig for en leser. Utfra sammenhengen må dataene likevel sies å inneholde et tilkjennegivende om at avsenderen innestår for at opplysningene i selvangivelsen er korrekt.

Tilsvarende synspunkt må anlegges der det er tale om for eksempel å gjøre en bestilling i en nettbutikk eller overføre penger via nettbank. Bestillingen og den elektroniske blankett for pengeoverføring er tilkjennegivender som inngår i en automatisk prosess.

3.2.5.5 Logger, metadata og kvitteringer

Som drøftet ovenfor kan data produsert av et datasystem være uttrykk for menneskelige tanker. Dataprogrammer, herunder operativsystemer, oppretter ofte logger for å dokumentere bruk av program- og maskinvare. Slike data er ment å gi tjenesteyter eller

[105] Andenæs/Bratholm (1996) side 305.

bruker informasjon. Slike meningsbærende data har et innhold som ut fra sammenhengen må anses som tilkjennegivender. Det samme vil være tilfellet med automatisk utstedte kvitteringer ved for eksempel betalingstransaksjoner og netthandel.

3.2.5.6 Særlig om fotografier

Tradisjonelle fotografier er i rettspraksis ansett som reelle bevismidler fordi de ikke formidler noens tanker, men gjengir virkeligheten slik den fortonet seg i et brøkdels sekund da bildet ble tatt.[106] Dette stiller fotografiet i en særstilling i forhold til dokumentdefinisjonen. I motsetning til et fotografi kan både lyd og levende bilder formidle et tilkjennegivende i form av for eksempel en samtale eller monolog.

3.2.5.6.1 Attestasjon eller tilsvarende

Dersom fotografiet har blitt attestert av fotografen kan det inneholde et tilkjennegivende om at slik eller slik fotonet en situasjon seg.[107]

Et grensetilfelle ble behandlet av Høyesterett i Rt. 1922 s. 542. Et fotografi var stemplet med dato og det fremsto som om stemplet stammet fra fotografen. Spørsmålet var om fotografiet påført dato var et tilkjennegivende eller om det var tale om et reelt bevismiddel. Retten kom under dissens til at det ikke var nok til å gjøre et fotografi til et tilkjennegivende at det var påført dato. Mindretallet mente derimot at påføringen av dato måtte være nok. Mindretallet la til grunn at:

> (…) dateringen maatte gi enhver det umiddelbare indtryk, at datoen for det første var paaført den fotografiske film samtidig med eksponeringen og ialdfald før fremkaldelsen, og at dateringen tillike var skikket til at gi enhver iagttager det indtryk, at datoen var paaført av vedkommende fotograf for at konstatere netop det faktum, at omhandlede fotografi var tat den dag.

Utdraget illustrerer at det skal foretas en konkret vurdering der det avgjørende er om noen menneskelig tanke blir formidlet. Var datoen ikke påført et fotografi, men et blankt papirark, ville datoen i seg selv ikke inneholde et tilkjennegivende. Andenæs antar at utfallet ville vært annerledes dersom bildet var påført en klar attestasjon. Da

---

[106] Rt. 1922 s. 542.

[107] Slik Andenæs/Bratholm (1996) side 299.

ville fotografiet med attestasjonen være et tilkjennegivende om at slik eller slik forløp situasjonen.

3.2.5.6.2 Manipulering

For elektroniske fotografier kan det spørres om manipulering av bildet i seg selv gjør fotografiet til et tilkjennegivende. I Datakriminalitet (1995) hevdes at et elektronisk lagret fotografi ikke kan utgjøre et reelt bevismiddel, men alltid vil være et tilkjennegivende sammen med programvaren. I hvert fall, hevdes det, må dette gjelde hvis det foretas endringer i bildet ved hjelp av dertil egnet programvare. Synspunktet er antakelig at det er et menneske som har programmert datamaskinen til å kunne vise bildet på skjermen.

Et dokument står en først overfor dersom det objektivt fremgår av gjenstanden at den er uttrykk for en menneskelig tanke. Et manipulert elektronisk fotografi vil derfor inneholde et tilkjennegivende dersom det fremgår klart av bildet at det er manipulert. Derimot er det lite naturlig å tale om et tilkjennegivende dersom en står overfor en godt skjult forfalskning. Da må det riktige formodentlig være at det digitale bildet anses som et reelt bevismiddel som kan underkastes granskning på vanlig måte.[108]

3.2.6 Særlig om kriteriet ”Udtalelse” i § 371

Også i ordet uttalelse ligger etter alminnelig forståelse at tanker er gitt et språklig uttrykk. Det er således neppe noen grunn til å forstå ordet ”Udtalelse” i § 371 annerledes enn ordet tilkjennegivende i § 179. Hensynet bak § 371 er generelt å ramme den som utgir seg for å være en annen i skrift. Forskjellen på dette og dokumentfalsk er bevisrekvisitten som kjennetegner dokumentet. Uttalelsen kan for eksempel være en meningsytring i en samtalegruppe eller diskusjonsforum på Internett.

3.2.7 Et tilkjennegivende må identifisere utstederen

Kravet om at et dokument må inneholde et ”Tilkjendegivende” innebærer også at leseren skal kunne slutte seg til hvem som er utsteder gjennom en tolkning av utsagnet.

---

[108] I sivilprosessen er det uavklart om elektroniske data er å betrakte som dokumentbevis eller om de er reelle bevismidler. Se Hov I (1999) side 224.

Dette følger ikke av ordlyden i dokumentdefinisjonen, men er sikker rett.[109] I Danmark følger kravet om utstederbetegnelse direkte av ordlyden.[110]

Kravet har sammenheng med beviskriteriene. Et tilkjennegivende som er anonymt kan ikke ha en slik bevisverdi som kreves i § 179. Det dokumentet skal bevise er nettopp hva en bestemt person har tenkt om et eller annet bevistema.

Falskbegrepet i § 182 hviler dessuten på en forutsetning om at det fremgår av dokumentets innhold hvem som er utsteder. Man kan ikke snakke om krenkelse av datas autentisitet dersom det ikke er mulig å slutte seg til utstederens identitet ved å lese informasjonen.

Til utstederbetegnelse har rettspraksis stilt små krav. For eksempel er som nevnt bilskilter ansett for å være dokumenter[111]. Utstederen fremkommer ikke direkte av bilskiltet i seg selv, men må ses i lys av at en særskilt registreringsmyndighet etter vegtrafikkloven § 15 har kompetanse til å utstede slike. Følgelig betraktes registreringsmyndigheten som utsteder av bilskilt.

3.2.7.1 Det kreves ikke elektronisk signatur

At dokumentet må identifisere utstederen omfatter ikke et krav om underskrift. Dette følger av straffeloven § 184 der det er forutsatt at ulike typer merker kan være dokumenter selv om de åpenbart ikke er utstyrt med signatur. Eksempler på merker er frimerker og togbilletter.

Det samme ble uttrykkelig slått fast i Rt. 1937 s. 541. Av lagmannsrettens rettsbelæring, som Høyesterett sluttet seg til, fremgår at det avgjørende er om man etter en tolkning av tilkjennegivendet kan slutte seg til hvem som er utsteder.

På samme måte som for tradisjonelle dokumenter kan det ikke kreves at elektroniske tilkjennegivender er signert. Ovenfor har jeg kort gjort rede for hva som menes med elektronisk signatur[112]. Slik signatur kreves ikke for at et utsagn skal kvalifisere til tilkjennegivende.

---

[109] Se Andenæs/Bratholm (1996) side 303. Bratholm/Matningsdal II (1995) side 399.

[110] Dansk straffelov § 171 stk. 2.

[111] Rt. 1940 s. 40 og Rt. 1963 s. 1343.

[112] Se punkt 1.2.2.

En annen sak er at en signatur ofte vil føre til at en betrakter et tilkjennegivende som bestemt til å tjene som bevis. Dette berøres nedenfor i punkt 3.3.5.1.

3.2.7.2 Tradisjonelt bevisende dokumenter

For dokumenter som skal leses av et menneske må det fremgå enten direkte eller av sammenhengen hvem som har utstedt dokumentet. Som regel vil det være en enkel sak å fastslå om tilkjennegivendet oppfyller kravet. Her vil vurderingen falle ut som ved tradisjonelle dokumenter.

Et særlig forhold bør påpekes. Elektroniske tilkjennegivender vil svært ofte automatisk få tilknyttet informasjon om hvem utstederen er. Dette er ganske åpenbart ved for eksempel SMS og e-post. Mottakeren av en SMS vil uavhengig normalt legge til grunn at avsenderen er identisk med innehaveren av telefonnummeret. Likeledes er det naturlig at mottakeren av en e-post legger til grunn at innholdet skriver seg fra innehaveren av den kontoen som er angitt i avsenderfeltet. I slike tilfeller er det vel naturlig å se avsenderinformasjonen som en del av tilkjennegivendet, selv om den for så vidt ikke fremgår av teksten. Kravet til utstederbetegnelse må derfor anses for oppfylt.

Ofte lagrer operativsystemet eller annen programvare informasjon, metadata, sammen med for eksempel et tekstbehandlingsdokument. Denne informasjonen er produsert av datasystemet, se punkt 3.2.5 ovenfor. Hvis metadata inneholder informasjon om hvem som er utsteder, kan det spørres om slike data oppfyller kravet til utstederbetegnelse. I så fall må man anse dataene som en del av tilkjennegivendet. Dette er neppe like klart som for e-post og SMS. Det riktige er formodentlig å foreta en konkret vurdering. Antakelig må det kreves at metadata er rimelig tilgjengelig for en alminnelig bruker.

3.2.7.3 Hjelpedokumenter

I Rt. 1991 s. 532 la Høyesterett til grunn at en liste over kontonumre var et dokument, men drøftet ikke kravet om tilkjennegivende uttrykkelig. Det fremgikk ikke direkte av innholdet i listen hvem som var utsteder. Listen var imidlertid opprettet av ansatte ved Bankenes betalingssentral og befant seg på deres lukkede datasystem. I lys av sammenhengen var det derfor ikke tvilsomt at listen fremsto som utstedt av en autorisert ansatt ved sentralen.

3.2.7.4 Autentiseringsdata

For tilkjennegivender som går ut på å autentisere en person kan man spørre om hvem som egentlig er utsteder. Er det den som har tilgodesett brukeren med adgang til systemet eller er brukeren som trekker nøkkelkort i leseren eller skriver inn et passord?

Antakelig må det riktige være å sondre mellom autoriseringstegn som er utformet en gang for alle av en autoriseringsinstans, og passord, signaturer og andre adgangskoder som brukeren må skrive inn egenhendig fra gang til gang. Blant tradisjonelle dokumenter er førerkort åpenbart utstedt av offentlig myndighet og bilskilter av biltilsynet. Likeledes vil det være naturlig å se det slik at autoriseringsdata i magnetstripen på et betalingskort er utstedt av banken, elektroniske adgangskort til bygninger er utstedt av den som eier bygningen. På samme måte er et sertifikat som lastes ned til datamaskinen og brukes for innlogging på nettbank, utstedt av banken.

Passord og andre identifikasjonskoder er det som nevnt mer naturlig å sammenlikne med tradisjonelle signaturer. Slike autentiseringsdata må anses for å være utstedt av innehaveren av dataene i det enkelte tilfellet. Den som har gitt brukeren adgang til et datasystem eller programvare har kanskje i første omgang gitt brukeren passordet. Når brukeren har fått koden er det likevel opp til henne å skrive det inn fra gang til gang, og det synes naturlig å se det slik at brukeren er utsteder i slike tilfeller.

Begge typer autentiseringsdata har det til felles at tilkjennegivendet etter sin natur alltid også inneholder utstederbetegnelsen.

3.2.7.5 Logger, metadata og kvitteringer

Logger, metadata og automatisk utstedte kvitteringer betraktes som tilkjennegivender som er produsert av et datasystem, se ovenfor. I slike tilfeller må det riktige være å anse tilbyderen av tjenesten som utsteder. Dette følger naturlig i forlengelsen av at tilkjennegivendet indirekte er skrevet av henne. Der det er snakk om logger på et personlig datasystem må eieren av systemet anses som utsteder ettersom hun kan bestemme om logging skal skje.

3.2.7.6 Modifikasjon ved anonyme stemmetegn

Kravet om at utstederens identitet må fremgå av tilkjennegivendet er modifisert noe i rettspraksis. I Rt. 1935 s. 573 var situasjonen at en funksjonær ved et offentlig valg

endret innholdet på 23 stemmesedler. Høyesterett la uten videre drøftelse til grunn at stemmesedlene var dokumenter selv om de ikke inneholdt identiteten til utsteder. Det er et vesentlig trekk ved en stemmeseddel at den er anonym. Likevel kunne den ses på som et tilkjennegivende om hva en eller annen stemmeberettiget stemte. Den samme løsningen må legges til grunn dersom dagens valgordning endres slik at stemmer kan avgis på Internett. En annen sak er at de stemmeberettigede må autentiseres før de avgir stemmen. I dag skjer dette ved å fremvise legitimasjon for en vakt. I fremtiden kan autentisering skje for eksempel ved bruk av elektronisk signatur eller andre autentiseringsdata.

3.2.7.7 En uttalelse må hithøre fra en bestemt person, § 371

I § 371 har lovgiver presisert kravet om utstederbetegnelse direkte i ordlyden. Dette fremgår av kriteriet ” Udtalelse, der fremtræder som umiddelbart hidhørende fra en bestemt Person”. Bakgrunnen for tillegget er å presisere at underskrift ikke er nødvendig, men at ”enhver Maade, hvorpaa Forfatteren i Overensstemmelse med almindelig Skik og Brug kan tilkjendegives, ogsaa her vil tillægges betydning.”[113] Det er ingen holdepunkter i forarbeidene for at lovgiver tilsiktet noen realitetsforskjell mellom uttalelser og tilkjennegivender i forhold til kravet om utstederbetegnelse.

3.2.8 Logisk avgrensning av dokumentet

Ordlyden i § 179 taler isolert sett for at dokumentet er en benevnelse på den gjenstanden som inneholder tilkjennegivendet. Dette samsvarer med alminnelig oppfatning av tradisjonelle papirdokumenter. Straffelovrådet la til grunn at ordet dokument er en benevnelse på lagringsmediet, skjønt dette kan skyldes en unøyaktighet i fremstillingen.[114]

Høyesterett har lagt til grunn at et dokument avgrenses til det tilkjennegivendet som gir dokumentet dets bevisverdi. I Rt. 1977 s. 457 var forholdet at banken hadde utstedt interimskvitteringer til A som bevis for at han hadde kjøpt, men ikke fått utlevert ihendehaverobligasjoner. Interimskvitteringene var utvilsomt dokumenter. Ved overlevering av obligasjonene kvitterte A på interimskvitteringene med falsk signatur.

---

[113] SKM 1896 side 280.

[114] NOU 1985:31 side 12.

Den falske signaturen innebar et nytt tilkjennegivende og måtte betraktes som et separat dokument.

En datafil eller et lagringsmedium kan inneholde flere tilkjennegivender. For eksempel inneholder en database en rekke innførsler. Hvert tilkjennegivende skal da betraktes som dokument i lovens forstand.

Å avgrense elektroniske dokumenter til det enkelte tilkjennegivendet har gode grunner for seg. Tanken om at dokumentets avgrensning må gjøres logisk ut fra dets innhold er lagt til grunn i forvaltningsprosessen. Forvaltningsloven § 2 (1) bokstav f definerer således et dokument som en "logisk avgrenset informasjonsmengde".[115] Hensikten med avgrensning av dokumentet ut fra dets innhold er der begrunnet med at private ikke skal ha innsyn i hele dataregisteret der informasjon er lagret, men bare i de aktuelle data i saken.[116] Også den svenske Datastraffrättsutredningen peker på at man i forhold til elektroniske dokumenter må avgrense dokumentet logisk.[117]

Andenæs/Bratholm viser også til at det ikke nødvendigvis alltid er i samsvar med en naturlig forståelse å bruke ordet dokument om gjenstanden.[118] For eksempel er det åpenbart ikke naturlig å kalle en sau for dokument, selv om det brennmerket den er påført er et tilkjennegivende bestemt til bevis. På samme måte er det unaturlig å bruke ordet dokument om lagringsmediet som sådant. Et lagringsmedium har kapasitet til å inneholde et nærmest ubegrenset antall tilkjennegivender. Det er selve samlingen med tegn, eller data, som det er naturlig å kalle dokument.[119]

Den nærmere avgrensning av tilkjennegivendet må bero på en tolkning i hvert enkelt tilfelle. Rt. 1977 s. 457 viser at det ved avgrensningen mellom flere tilkjennegivender skal legges vekt på om det enkelte tilkjennegivendet er bevis for samme eller et annet faktum enn de øvrige.

---

[115] Tilsvarende offentlighetsloven § 3 2.pkt og arkivloven § 2 bokstav a.

[116] Ot.prp.nr.56 (1999-2000) kapittel 4.6.

[117] SOU 1992:110 side 252-253.

[118] Andenæs/Bratholm (1996) side 300.

[119] L.c.

3.3 Dokumentets innhold. Bevisrekvisitten.

Om bevisrekvisitten sier § 179 at et dokument ”enten er af Betydning som Bevis for en Ret, en Forpligtelse eller en Befrielse fra en saadan eller fremtræder som bestemt til at tjene som Bevis”.

Et dokument kan ha bevisverdi både i kraft av sitt innhold og i egenskap av reelt bevismiddel. Det er dokumentets bevisverdi i kraft av å inneholde et tilkjennegivende som er tema i dette punktet. Dokumentets fremste karakteristikum er dets evne til å være bevis i kraft av å inneholde menneskelige tanker om et faktum utenfor seg selv.[120] Dokumentets særlige bevisverdi er knyttet til utstederens identitet. Avslutningsvis vil jeg kort redegjøre for noen særlige spørsmål knyttet til granskning av elektroniske dokumenter i egenskap av reelle bevismidler.

3.3.1 Hva er bevis?

En nærmere analyse av bevisbegrepet hører hjemme i rettsfilosofien. Jeg nøyer meg derfor med å gjøre rede for enkelte utgangspunkter. Ordet bevis er ikke definert i straffeloven og er heller ikke berørt i SKM 1896. Det er naturlig å se hen til bevisbegrepet i domstolsprosessen. I tvistemålsloven § 300 nr 2 omtales bevis som omstendigheter saksøkeren støtter sitt krav på. Man skiller mellom saksforholdet og de bevis man bruker til å underbygge faktum. Dette fremgår for eksempel av tvistemålsloven § 86 hvor det heter at det er opp til partene å gjøre rede for ”de faktiske forhold og bevis” som er av betydning. Etter dette kan man si at bevis er omstendigheter som belyser et faktum. Et dokuments innhold kan være en bevisende omstendighet.

Formålet med dokumentfalskreglene er ikke først og fremst å beskytte bevisførselen for domstolene. Dette hensynet ivaretas delvis av straffeloven § 132 om bevisforspillelse og kapittel 15 om falsk forklaring. Disse bestemmelsene beskytter mot krenkelser av rettspleien og offentlig myndighet, mens dokumentfalskreglene beskytter den alminnelige tillit til dokumenter. Det er ikke bare rettsforhold[121] som kan være dokumentets bevistema, men alle situasjoner der det kan komme på tale å bevise noe.

---

[120] Kjerschow (1930) side 472.

[121] Tvistemålsloven § 54. Bare rettsforhold kan være gjenstand for sivil tvist.

En skiller mellom to hovedgrupper av bevisende tilkjennegivender. Den ene gruppen er de bevisbestemte dokumenter. Den andre gruppen er de dokumenter som er av betydning som bevis i et rettsforhold. De to kategoriene overlapper idet et bevisbestemt dokument godt også kan være av betydning som bevis i rettsforhold. Jeg drøfter de to gruppene nedenfor i punktene 3.3.4 og 3.3.5.

3.3.2 Data kan være bevis

Innledningsvis kan det spørres om et tilkjennegivende i elektronisk form i det hele tatt kan være bevis. Et særlig kjennetegn ved elektroniske data er at de er bærere av såkalt mediekompatibel informasjon.[122] Mediekompatibel informasjon kan defineres som informasjon som er løst knyttet til et medium, og lett kan overføres til andre medier. Data kan kopieres mellom lagringsmedier uten at kvaliteten forringes. Ofte er det praktisk umulig å avgjøre om innholdet er endret eller i det hele tatt skriver seg fra den som fremstår som utsteder. I dansk teori har det vært hevdet at disse egenskapene fratar den digitale meddelelse dens evne til å tjene som bevis for en rettighet.[123] I Sverige har en hovrättsdomstol kommet til at en tekstfil ikke var urkund av samme grunner.[124]

Data som ikke tilfredsstiller kravene til informasjonssikkerhet[125] har visse likhetstrekk med tradisjonelle ubekreftede avskrifter. Usikre data og ubekreftede avskrifter har det til felles at informasjonens integritet og autentisitet er tilnærmet umulig å verifisere.[126] I juridisk teori er det lagt til grunn at ubekreftede avskrifter ikke er dokumenter.[127] De er bare tilkjennegivender om at det foreligger et dokument med det angitte innhold. Imidlertid er det den forskjell at mens avskrifter åpent gir uttrykk for å være avskrifter, så utgir usikre data seg for å skrive seg fra en bestemt utsteder. For data som oppfyller

---

[122] Bryde Andersen (2001) punkt 2.2.b.

[123] op.cit. punkt 17.3.a. Dette synet deles imidlertid ikke av Brydensholtutvalget eller Justitsministeriet. Det danske lovarbeidet til den nye dokumentfalskbestemmelsen er kommentert nedenfor i punkt 9.

[124] Svea hovrätts dom 31.05.02 saksnummer B 5358-01. Omtalt i Lov&Data nr. 73 2003.

[125] Se punkt 1.2.2.

[126] Data inneholder som oftest metadata som i gir informasjon om tidspunkt for opprettelsen, angivelse av hvilken bruker som opprettet det m.v. Slike metadata er imidlertid sjelden praktisk tilgjengelig. Også metadata kan dessuten forfalskes.

[127] Andenæs/Bratholm (1996) side 304.

kravene til informasjonssikkerhet kan det uansett ikke være grunnlag for de innvendinger som har vært anført i teorien.

I norsk rett har en sett det slik at data kan ha bevismessig betydning. I NOU 1985:31 side 29 og Ot.prp.nr. 35 (1986-87) side 14 la man til grunn at data kunne være ”bevis”. Både Straffelovrådet og Justisdepartementet nøyde seg med å konstatere at det ”undertiden kan være vanskelig” å avgjøre om bevisvilkåret er oppfylt, men at dette ikke er spesielt for elektroniske dokumenter. Fra forarbeidene kan det derfor sluttes at data i norsk rett kan ha en slik bevisverdi at de er dokumenter. Likeledes la førstvoterende i Rt. 1991 s. 532 uten videre til grunn at listen over kontonumre fremsto som bevisbestemt, og følgelig hadde bevisverdi.

Også datakrimkonvensjonen forutsetter at data kan være av betydning som bevis i rettsforhold. I konvensjonens artikkel 7 angis kravet til bevismessig betydning noe annerledes enn i straffeloven, men det stilles ikke spørsmålstegn ved datas evne til å inneholde bevis. Etter konvensjonen må falskhandlingen skje “with the intent that it be considered or acted upon for legal purposes as if it were authentic”. I den forklarende rapporten avsnitt 81 uttales at “[m]anipulations of (…) data with evidentiary value may have the same serious consequences as traditional acts of forgery”.

Det er etter dette ikke tvilsomt at tilkjennegivende i elektronisk form kan være bevis.

3.3.3 Data som påvirker en automatisk databehandling

Foruten å ha til hensikt å påvirke et menneske på tradisjonelt vis, kan elektroniske tilkjennegivender være utformet med tanke på å instruere datamaskinens programvare. I slike tilfeller inngår de data som utgjør dokumentet i en automatisk databehandling. Det kan spørres om man kan tale om ”bevis” i slike tilfeller. Tradisjonelt har man med bevis ment omstendigheter som belyser et faktum for den menneskelige bevissthet.

NOU 1985:31[128] tar som nevnt ovenfor utgangspunkt i at et tilkjennegivende må ha en form som kan forstås av mennesker. Straffelovrådet hevder at først når data fremtrer ”i vanlig lesbar form” kan tilkjennegivendet tjene som bevis. Uttalelsen taler for å tolke beviskravet snevert til bare å gjelde tilkjennegivender som kan virke motiverende for et menneske.

Databehandlingen er bare en rasjonalisering av oppgaver et menneske kunne ha gjort. Det er derfor ikke unaturlig å omtale elektroniske data som ”bevis” såfremt de legges til grunn i en automatisk databehandling. Det må imidlertid, som for tradisjonelle dokumenter, kreves at dataene har en utstederbetegnelse og at det er i kraft av utstederbetegnelsen at dataene påvirker datasystemet.

Til støtte for dette synet er BBS-dommen i Rt. 1991 s. 542. De data som var gjenstand for ettergjøring hadde ingen annen betydning som bevis enn overfor dataprogrammet som skulle forestå utbetalingen. Uten at beviskravet ble direkte drøftet ble de tiltalte dømt for fullbyrdet dokumentfalsk. Høyesterett uttalte at byrettens dom var noe snau når det gjelder de faktiske forhold som ligger til grunn for bedømmelsen av om beviskravene er oppfylt. Imidlertid fant ikke retten holdepunkter for at byretten hadde bygget på uriktig forståelse av § 179. Dommen er derfor neppe noen sikker avgjørelse av spørsmålet. Den er imidlertid et moment for et data som mates inn i et dataprogram kan være bestemt til å tjene som bevis ved å påvirke resultatet av en automatisk prosess.

Sammenhengen med § 270 nr 2 om databedrageri gjør det naturlig å bruke ordet bevis også om data som bare er forståelige for en datamaskin. Det tradisjonelle dokumentfalsk blir ansett for å være nært beslektet med bedrageriet. Svært ofte fremkalles en villfarelse ved at fornærmede innretter seg i tillit til et falskt dokument. Da man ga bestemmelsen om databedrageri i 1987 tok man konsekvensen av at et dataprogram er uten bevissthet, og derfor ikke kan havne i villfarelse. I stedet rammet man den som ved ”endring i data” påvirker resultatet av en automatisk databehandling og påfører et tap. Fordi det i slike tilfeller er tale om data som er ment å inngå i en automatisk databehandling vil de ofte ikke være forståelige for en menneskelig leser. Straffelovrådet holdt det åpent om forholdet kan rammes som dokumentfalsk, NOU 1985:31 side 33.

I NOU 2002:4 side 375 legger Straffelovkommisjonen uten nærmere drøftelse til grunn at manipulasjoner av data i forbindelse med databedrageri etter dagens rettstilstand kan være dokumentfalsk.

Etter dette blir konklusjonen at et tilkjennegivende i elektronisk form som mates inn i et dataprogram kan oppfylle beviskriteriet.

---

[128] NOU 1985:31 side 11.

3.3.4 Dokumenter som har betydning som bevis i et rettsforhold

Den første av de to hovedgrupper bevisende tilkjennegivender er de som er ” af Betydning som Bevis for en Ret, en Forpligtelse eller en Befrielse fra en saadan”. Denne gruppen av dokumenter benevnes gjerne leilighetsdokumenter fordi deres status som dokument oppstår og bortfaller sammen med aktualiteten av tvister hvor de tjener som bevis. Avgjørende er om de er av betydning som bevis i et konkret rettsforhold.

Tradisjonelt har det vært vanlig å betrakte de bevisbestemte dokumenter som de eneste som bør ha det særskilte vernet som dokumentfalskreglene oppstiller. Dette var ordningen etter kriminalloven slik den så ut etter revidering i 1889.[129] Forarbeidenes omtale av beviskriteriet understreker at det er de bevisbestemte dokumentene som først og fremst oppfyller hensynet til vern av den alminnelige tillit. [130] Slik loven er utformet vil den største kategorien dokumenter likevel være dokumenter av betydning som bevis.

3.3.4.1 Rettsforhold

Det er et vilkår at tilkjennegivendet er av betydning som bevis for ”en Ret, en Forpligtelse eller en Befrielse fra en saadan”. I teorien har det vært hevdet at kriteriet faller sammen med begrepet ”retsforhold eller en rettighet” i tvistemålsloven § 54.[131] Andre har formulert dette som et krav om at dokumentet må ha et rettslig relevant innhold. [132] Realiteten er antakelig den samme. Følgelig omfattes alle rettsspørsmål som kan fremmes til behandling i tvistemål, herunder spørsmål om rett, plikt og kompetanse.[133]

Det er noe uklart hvorvidt kriteriet ”en Ret en Forpligtelse eller en Befrielse fra en Saadan” også omfatter spørsmål om straffansvar. Problemstillingen kommer på spissen der et dokument av ellers likegyldig innhold kan ha betydning for tiltaltes alibi i en straffesak. Er det for eksempel straffbart å ettergjøre en privat SMS-melding for å sikre seg alibi for tidspunktet for en voldtekt?

---

[129] SKM 1896 side 172.

[130] SKM 1896 side 172-173.

[131] Nærstad (1936) side 71, Kjerschow (1930) side 471. Andenæs/Bratholm (1996) side 302.

[132] Bratholm/Matningsdal II (1995) side 398.

[133] Hov III (2000) side 88-112.

Ordene rett, forpliktelse og befrielse passer i utgangspunktet dårlig på straffansvar. Man kan kanskje si at straff er en ”Forpligtelse”, men tolkningen ligger vel ikke akkurat i ordets kjerne.

SKM 1896 uttaler Straffelovkommisjonen at dokumenter kan tenkes å ”bevise et alibi eller et andet Faktum af Betydning i et Retsforhold.”[134] Ordet alibi betyr etter alminnelig forståelse bevis for at en var på et annet sted enn åstedet da en forbrytelse ble begått.[135] Forarbeidene gir derfor holdepunkter for at straffansvar omfattes.

Hensynet til konsekvens og sammenheng i rettssystemet tilsier at straffbare forhold omfattes. Tiltalte er etter straffeloven § 167 (3) fritatt for straffansvar for falsk forklaring. Tiltalte kan heller ikke straffes for bevisforspillelse, § 132 (2). Bestemmelsene innebærer imidlertid ikke straffritak for benyttelse av falske dokumenter eller andre fabrikkerte bevis i en straffesak.[136] Det kan videre anføres at vernet mot benyttelse av falskt dokument bør være like sterkt i straffeprosessen som sivilprosessen.

Konklusjonen blir at også straff omfattes av kriteriet ”en Ret, en Forpligtelse eller en Befrielse fra en Saadan”.

3.3.4.2 Av betydning som bevis

Det oppstilles ikke krav om at et dokument er tilstrekkelig bevis alene, det er nok at det er ”af Betydning”. Et bevisbestemt dokument kan også være av betydning som bevis i rettsforhold. Dette gjelder for eksempel de dispositive dokumenter. Når et slikt dokument brukes som leilighetsdokument er det ikke nødvendig at dokumentet brukes som bevis for det faktum som det fremstår som bevis for.[137]

Det er ikke nødvendig at dokumentet faktisk får bevismessig betydning.[138] Det kan for eksempel hende at andre bevis i saken gjør dokumentbeviset overflødig. Dokumentet

---

[134] SKM 1896 side 173.

[135] Se bokmålsordboka, http://www.dokpro.uio.no/ordboksoek.html.

[136] Rt. 1949 s. 142 og Rt. 1993 s. 927. I sistnevnte dom var saksforholdet at tiltalte i en sak om brudd på merverdiavgiftsloven. For å skjule forbrytelsen forfalsket de fakturaer.

[137] Kjerschow (1930) side 471.

[138] Op.cit. side 472.

kan likevel være av betydning som bevis i lovens forstand. Et tilkjennegivende må anses for å være av betydning som bevis selv om forfalskningen er så dårlig utført at ingen lar seg lure.[139] Avgjørende er om innholdet er av betydning som bevis dersom det blir trodd.

I sivilprosessen begrenses bevisførselen til bevis "som er av betydning for avgjørelsen", tvistemålsloven § 86 første ledd. Bevis som "ikke kommer saken ved" kan retten nekte ført etter § 189 nr 1.[140] Videre kan nektes ført bevis som "aapenbart ikke har nogen beviskraft". Benyttelse av falskt dokument kan skje ved fremleggelse i retten. Det gir da best sammenheng dersom en tolker kriteriet "af Betydning som Bevis" slik at det utelukker bevis som etter prosesslovgivningen ikke har bevismessig betydning.

3.3.4.3 Det avgjørende tidspunkt

På tidspunktet for den straffbare handlingen må tilkjennegivendet fylle alle vilkårene for å være dokument, herunder bevisvilkåret. Den straffbare handlingen kan enten være benyttelse etter § 182 eller forfalskning etter § 185 (2).

§ 179 oppstiller som vilkår at dokumentet "er" av betydning som bevis. Når et tilkjennegivende ikke er bevis i et konkret rettsforhold har det vern etter § 371 som uttalelse. Spørsmålet i dette avsnittet er når et tilkjennegivende "er" av betydning som bevis i rettsforhold.

Problemstillingen har ikke kommet på spissen i rettspraksis og er heller ikke behandlet i juridisk teori. Som et utgangspunkt for å bedømme et rettsforholds aktualitet er det naturlig å se hen til tvistemålsloven § 54.

Etter tvistemålsloven § 54 kan en for domstolene få avgjort tvister om et rettsforhold eller en rettighet "er til eller ikke er til". Presensformen peker på at det i hovedsak er rettsspørsmål av betydning for saksøkeren i dag som omfattes.[141] Dette kan uttrykkes

---

[139] Andenæs/Bratholm (1996) side 302-303. Bratholm/Matningsdal II (1995) side 398. Dette er ikke helt upraktisk for elektroniske dokumenter. For eksempel er en e-post forsøkt tilbakedatert, men gjerningsmannen har glemt å endre metadata som inneholder informasjon om det reelle forsendelsestidspunktet.

[140] Også reglene om edisjonsplikt hviler på en forutsetning om at dokumentene som provoseres fremlagt har betydning for saken jf. tvistemålsloven § 253 jf § 250, se Rt. 1992 s. 962.

[141] Michelsen (1999) side 65 flg.

som at søksmålsinteressen må være aktuell.[142] Det vil føre for langt å gå inn på avgrensingen av begrepet rettslig interesse her. Jeg nøyer meg med å antyde at fortidige og fremtidige forhold som en hovedregel ikke omfattes. Det skal imidlertid foretas en helhetsvurdering der det legges betydelig vekt på partenes behov for en avklaring av rettsspørsmålet.[143] Behovet for å få avgjort et spørsmål som ligger frem i tid vil blant annet bero på hvor sannsynlig det er at spørsmålet blir aktualisert.[144]

I aktualitetsvurderingen er det også naturlig å legge vekt på gjerningsmannens rettsstridige hensikt, jf. straffeloven § 182.[145] Dersom noen for eksempel forfalsker en privat SMS for å gi skinn av at vedkommende hadde alibi på tidspunktet for en straffbar handling, bør dette tillegges vekt ved vurderingen av om tilkjennegivendet "er" av betydning som bevis. Dette gjelder antakelig uavhengig av om straffesaken enda er aktuell. Etter dette vil også forfalskning av e-postveksel mellom næringsdrivende i den hensikt å skaffe bevis i en fremtidig rettssak rammes.

Avgrensningen av aktualitetskravet i § 179 er usikker de lege lata. Antakelig skal det foretas en helhetsvurdering av rettsforholdets aktualitet der viktige momenter vil være sannsynligheten for en fremtidig tvist, samt gjerningsmannens rettsstridige hensikt.

Utveksling av e-post vedrørende tolkning av en fremtidig kontrakt er etter dette neppe et bevis for kontraktsmessige plikter etter at det blir klart at kontrakt ikke blir sluttet. Det kan imidlertid tenkes at en slik e-post kan være bevis i en tvist om kontrakt var inngått eller ikke. Hvis den ene parten forfalsker e-posten i hensikt å sikre bevis for en fremtidig tvist bør aktualitetskravet antakelig anses oppfylt.

Et annet eksempel er en privat e-post der en person forteller en venn om sine planer om å begå ran. Etter å ha sendt e-posten vil gjerningsmannen sikre seg mot at brevet senere brukes mot ham i en straffesak. Under et besøk hos vennen endrer han noen setninger i e-posten og lagrer endringen. Når hensikten er å sikre seg bevismessig i en fremtidig straffesak, må forholdet formodentlig anses som straffbar dokumentfalsk selv om

---

[142] Hov III (2000) side 118 flg.

[143] op.cit. side 128-131.

[144] L.c.

[145] Se Bratholm/Matningsdal II (1995) side 170 angående aktualitetskravet i § 132 om bevisforspillelse i anledning offentlig undersøkelse.

forbrytelsen ikke er begått enda. Derimot vil forfalskning som skjer etter at det straffbare forholdet er foreldet neppe være dokumentfalsk.[146] Da er det ikke lenger tale om noen aktuell tvist.

Dersom aktualitetskravet først er oppfylt, kan det spørres om straffansvaret bortfaller fordi det tilfeldigvis ikke blir noen tvist likevel. I teorien er det for § 132 antatt at det ikke fritar for straff dersom en offentlig undersøkelse tilfeldigvis ikke blir igangsatt.[147] Det samme må antas å gjelde for aktualitetskravet i § 179. Hvis objektet for falskhandlingen var et dokument på handlingstidspunktet blir handlingen neppe straffri fordi tilkjennegivendet senere taper sin dokumentstatus.

3.3.4.4 Dokumenter som direkte og objektivt er av betydning

Man kan systematisk skille mellom leilighetsdokumenter som på en objektiv og direkte måte identifiserer det rettsforhold det er bevis for, og dokumenter av ellers likegyldig innhold som tilfeldigvis får betydning som bevis. Sondringen ble lagt til grunn i SKM 1896 side 173 hvor man skilte mellom ”den mellem Fraværende om Retsforhold eller Retshandler førte Skriftvexel” og ”Breve af i sig selv ligegyldigt Indhold”.

Jeg behandler først tilkjennegivender som på en direkte, objektiv måte[148] fremstår som bevis for et rettsforhold. SKM 1896 s. 173 bruker som eksempel den brevveksling som skjer mellom kontraherende parter forut for selve kontraktsslutningen. Tilkjennegivender om en fremtidig kontrakts innhold og fortolkning kan ofte være avgjørende bevis dersom det skulle oppstå tvist på et senere tidspunkt. Tilsvarende kan en varebestilling objektivt og direkte være av betydning som bevis i rettsforhold.[149] Ikke bare i tvister for retten kan det være aktuelt å benytte slike dokumenter. De har et innhold som av aktører i rettslivet vil bli vektlagt som bevis også utenfor prosess.

Nærstad hevder at slike dokumenters bevisverdi skal bedømmes abstrakt, uten hensyn til aktualiteten av det rettsforhold som dokumentet er av betydning som bevis i.[150] I lys av det som ovenfor er sagt om aktualitetskravet kan dette neppe være riktig. Om et

---

[146] Tilsvarende Bratholm/Matningsdal II (1995) side 170 i kommentar til § 132.

[147] L.c.

[148] Nærstad (1936) side 68.

[149] Rt. 1930 s. 901 og Rt. 1949 s. 678.

[150] Nærstad (1936) side 68.

tilkjennegivende objektivt og direkte fremstår som bevis i et rettsforhold som for lengst er avsluttet, har det neppe lenger den nødvendige bevisverdi.

Det vil være tale om et dokument etter dette alternativet dersom forretningsdrivende A utformer et utkast til kontrakt i en tekstfil og sender med e-post til en motpart B. Et annet eksempel er bestilling av varer i en nettbutikk. Det skjemaet kunden fyller ut med personalia og kortinformasjon er et dokument av betydning som bevis i rettsforholdet mellom tjenesteyter og bruker. I begge tilfellene tjener data som bevis i rettsforhold.

3.3.4.5 Dokumenter av tilsynelatende trivielt innhold

Den annen hovedgruppe er tilkjennegivender som i seg selv har et likegyldig innhold, men som av ulike grunner tilfeldigvis er av betydning som bevis for et rettsforhold. Det særegne med tilkjennegivender i denne gruppen er at de ikke på objektiv måte kan identifiseres som bevis. Deres status som dokumenter beror på om de tilfeldigvis er av betydning som bevis i et konkret rettsspørsmål. Når de ikke har betydning som bevis i noe aktuelt rettsforhold nyter de et svakere vern som "Udtalelse" etter straffeloven § 371.

De rene leilighetsdokumentene vil sjelden ha bevismessig betydning utenfor domstolsprosess. Hensynet som begrunner deres beskyttelse er derfor ikke først og fremst hensynet til den alminnelige tillit til dokumenter, men vernet mot at noen uberettiget bruker ens skriftlige vitnesbyrd i en domstolsprosess. I domstolsprosess får slike dokumenter bevisverdi omtrent som andre indisiebevis.[151]

Det klassiske eksemplet er kjærlighetsbrevet som brukes i en senere skilsmissesak.[152] Et annet eksempel er et fotografi med attestasjon fra fotografen. Bildet er med attestasjonen et tilkjennegivende som kan få betydning som bevis for fotografens tanker i en konkret sak. Fotografiet gir ikke objektivt og direkte uttrykk for å være av betydning som bevis i et rettsforhold. Legges det frem som bevis i et rettsforhold vil det likevel være et dokument etter dette alternativet.

Et tredje eksempel er en SMS-melding som sendes fra A til B med bekreftelse på en avtale om å gå på kino. Dersom A blir tiltalt i en straffesak kan det hende

[151] Nærstad (1936) side 69.

[152] For eksempel Andenæs/Bratholm (1996) side 302.

påtalemyndigheten vil føre meldingen som bevis mot A. Meldingen er følgelig av betydning som bevis i et rettsforhold og dermed et dokument etter dette alternativet.

3.3.5 Bevisbestemte dokumenter

Den andre av de to hovedgrupper av bevisende tilkjennegivender er de som ”fremtreder som bestemt til at tjene som Bevis”.

3.3.5.1 Objektivt fremstå som bevisbestemt

At et dokument ”fremtræder” som bestemt til å tjene som bevis innebærer at tilkjennegivendet etter en objektiv vurdering må gi uttrykk for å være bevis for noe.[153] Det har følgelig ingen betydning om dokumentets utsteder tilsiktet å gi det bevisverdi.[154] Utstederen kan ha ønsket å gi dokumentet skinn av bevisbestemthet uten å lykkes. Omvendt kan utstederen tenkes å ha fremstilt et bevisbestemt dokument uten selv å være klar over det.

Det er et moment som taler for at et tilkjennegivende er bevisbestemt dersom det har signatur. Signaturers bevisverdi understrekes i tvistemålsloven § 262 der det heter at ”[e]t privat dokument, som er egenhændig underskrevet med navn, og hvis indhold ikke gir særlig grund til mistanke, avgir fuldt bevis for, at indholdet skriver sig fra den, som har underskrevet dokumentet”. Signatur er imidlertid ikke noe krav.

3.3.5.2 Bevisets tema

Hva et dokument må være bevis for sier bestemmelsen intet om. Det er ikke nødvendig at det er tale om et rettsforhold. Dette fremgår av sammenhengen med alternativet ”af Betydning som Bevis for en Ret, Forpligtelse eller Befrielse fra en saadan”. Det samme er uttrykkelig sagt i SKM 1896 s. 173.

Skal man legge til grunn en alminnelig forståelse av ordlyden kan bevistemaet være et hvilket som helst spørsmål som det hersker usikkerhet om. Dette gir en svært vid tolkning av bevisbegrepet. For eksempel kan det tenkes at bonden A lenge har kranglet med naboen B om hvem som har den fineste hesten. Hvis B sender til A en SMS der

---

[153] Andenæs/Bratholm (1996) side 301.

[154] l.c. Nærstad (1936) drøfter spørsmålet inngående på side 72-73.

han innrømmer at A har den fineste hesten er dette et tilkjennegivende som objektivt fremstår som bestemt til å tjene som bevis i den private uenigheten. Det kan spørres om en slik melding er et dokument, eller om man må tolke dokumentbegrepet innskrenkende slik at det utelukker tilkjennegivender som beviser et faktum av helt triviell betydning.

Andenæs/Bratholm nøyer seg med å bemerke at det er "uten betydning" hva dokumentet skal tjene som bevis for.[155] De trekker imidlertid frem dispositive utsagn og attester[156] som to viktige grupper bevisbestemte dokumenter. Bratholm/Matningsdal peker på at det er uten betydning hva som er bevistema, men at det "i praksis" som regel er tale om rettslige forhold av en eller annen art.[157] Nærstad peker på at foruten dispositive utsagn og attester vil en del offentlige dokumenter vil være bevisbestemte.[158]

§ 182 oppstiller et krav til rettsstridig hensikt i tillegg til forsett. Jeg gjør nærmere rede for kravet til rettsstridig hensikt i punkt 11.4 nedenfor. Her nøyer jeg meg med å oppsummere at gjerningsmannen må ha hatt til hensikt å nå et rettslig relevant resultat.[159] Sammenhengen med kravet om rettsstridig hensikt viser at dokumentet ikke har noen beskyttelse etter dokumentfalskreglene dersom dets innhold er av helt triviell karakter. Hensiktskravet gjelder også for selve falskhandlingen, § 185 (2) jf § 182.

Kravet til rettsstridig hensikt er imidlertid ikke knyttet til dokumentdefinisjonen, men til den straffbare handlingen. Betydningen av hensiktskravet for dokumentdefinisjonen ligger i at dokumentets strafferettslige vern er knyttet til den egenskapen ved dokumentet at det har et rettslig relevant innhold. Det blir en rent teoretisk øvelse å tale om dokumenter i relasjon til dokumentfalskreglene dersom gjerningsmannen på grunn av dokumentets trivielle innhold ikke kan ha rettsstridig hensikt. Jeg kommer tilbake til dette i punkt 6.

---

[155] Andenæs/Bratholm (1996) side 301.

[156] For eksempel Rt. 1953 s. 204 som gjaldt ettergjøring av attest fra arbeidsgiver.

[157] Bratholm/Matningsdal II (1995) side 398.

[158] Nærstad (1936) side 72.

[159] Andenæs/Bratholm (1996) side 292.

Det må anses som sikker rett at dokumentet må være bestemt til å tjene som bevis for et faktum som ligger utenfor dokumentet selv. Man kunne ellers si at ethvert dokument er bestemt til å tjene som bevis for sitt eget innhold.[160]

Konklusjonen blir at det ikke kan utledes noen avgrensing av gruppen med bevisbestemte dokumenter basert på bevisets tema. Derimot vil ikke dokumenter bestemt til å bevise et faktum av helt triviell betydning være beskyttet av § 182 jf. kravet til rettsstridig hensikt.

Jeg vil i det følgende skille mellom elektroniske data som skal presenteres for et menneske på linje med tradisjonelle dokumenter, og data som skal inngå i en prosess for automatisk databehandling.

3.3.5.3 Bevis som benyttes overfor et menneske

3.3.5.3.1 Dispositive utsagn og attester

Det som skal fremstå til å tjene som bevis er det tilkjennegivendet utstederen har avgitt. I teorien trekkes først og fremst frem to hovedtyper, nemlig dispositive utsagn og attester[161]. Hvis en utsteder har avgitt et dispositivt utsagn fremstår tilkjennegivendet som bevis for avtalerettslig rett eller plikt. Det er utsteders privatrettslige kompetanse til å binde seg selv eller andre som gir dokumentet dets særlige bevisverdi. Men ikke bare disposisjoner av privatrettslig art kan være bevisbestemt. Også skriftlige forvaltningsvedtak vil ha en bevisverdi som gir det dokumentstatus. Det er i disse tilfellene tale om offentligrettslig kompetanse gitt i medhold av lov eller delegasjon. Er det tale om en attest er det utsteders særlige troverdighet eller kunnskap som gir tilkjennegivendet bevisverdi.

For eksempel har næringsdrivende i stor grad i dag tatt i bruk e-post som kommunikasjonskanal i forbindelse med avtaleslutning. Slike e-poster vil på samme måte som tidligere tiders brevveksling være bevisbestemte dokumenter dersom de inneholder dispositive utsagn.

---

[160] Kjerschow (1930) side 472.

[161] Andenæs/Bratholm (1996) side 301, Datakriminalitet (1995) side 205.

En arbeidsattest i elektronisk form vil være et dokument etter dette alternativet, jf. Rt. 1953 s. 204. Dette er kanskje upraktisk for usikrede elektroniske data, men vil formentlig bli vanlig når elektronisk signatur brer om seg. En eksamensbesvarelse i elektronisk form vil også være et bevisbestemt dokument, Rt. 1998 s. 217.

3.3.5.3.2 Logger, metadata og kvitteringer

Logger over bevegelser på et datasystem er som nevnt ovenfor tilkjennegivender. Det samme gjelder såkalte metadata produsert av et dataprogram for å akkompagnere elektroniske data. Hensikten med loggen er nettopp å være bevis for hvilke bevegelser som har skjedd i datasystemet over et tidsrom. Følgelig er det naturlig å si at den er bevisbestemt. Det samme synspunktet kan anvendes på metadata som for eksempel kan bevise hvilken bruker som har opprettet en bestemt datafil. Kvitteringer som utstedes i forbindelse med en online transaksjon må anses bestemt til å bevise i rettsforholdet mellom brukeren og tjenesteyteren.

3.3.5.3.3 Bevis av betydning for bedømmelsen av en kontraktsytelse

Dokumentfalsk kan det være dersom noen for eksempel åpner en betalingstjeneste på Internett der hun gir seg ut for å være en høyt ansett og kompetent person. Man kan tenke seg at for eksempel en middelmådig jurist skriver en juridisk lærebok i it-rett og gjør den tilgjengelig på Internett mot betaling. For å lokke lesere kaller han seg ”Mads Bryde Andersen”, professor i juss ved Universitetet i Danmark. Selve bedrageriet rammes her av straffeloven § 270 nr 1. I tillegg har hun gjort seg skyldig i dokumentfalsk fordi navnet til en ansett fagperson er avgjørende for verdien av en lærebok. Konkurrensspørsmålet behandles nedenfor i punkt 9.

Med Internett har det blitt enklere enn tidligere å utgi seg for å være en annen også i kommunikasjon med tredjepersoner. Et eksempel kan illustrere dette. A sender ut e-post til kunder av et internettselskap og ber dem logge seg på en internettside og oppgi opplysninger om sine kredittkort. E-posten er forsynt med selskapets logo. En må her kunne si at e-posten er bestemt til å tjene som bevis. Det falske tilkjennegivendet med logo er bestemmende for at brukeren oppgir konfidensielle data. Brukeren tror i et slikt tilfelle at han kan stole på sin medkontrahent som han kanskje i lengre tid har hatt et kundeforhold til.

3.3.5.3.4 Bevis for hvem som har opphavsretten til et verk

I rettspraksis har det vært lagt til grunn at en signatur påført et maleri er et tilkjennegivende om hvem som står bak aktstykket, Rt. 1961 s. 611. Synspunktet er her at maleriet med signatur er et tilkjennegivende som fremstår som en attest for hvem som er utsteder. Dette har rettslig betydning fordi maleriets verdi er avhengig av hvem som har malt det.

Et liknende synspunkt kan nok gjøres gjeldende der en programvareprodusent presenterer for brukeren en attest om hvem som har utviklet programmet. En slik attest har opphavsrettslig betydning. Dersom noen endrer attesten med tanke på salg i eget navn, er dette falsk av et dokument bestemt til bevis for produsentens identitet.[162] Dette synspunktet svarer også til resonnementet i høyesterettsavgjørelser om piratkopiering av musikkassetter[163]. Ulovlig kopierte musikkassetter ble utstyrt med kopier av de originale etikettene. Etikettene tjente som bevis for hvem som hadde opphavsretten. Det var dokumentfalsk da de ble gitt skinn av å stamme fra andre enn gjerningsmannen.

Dommene er kritisert i teorien under henvisning til at åndsverkslovens bestemmelser skulle vært benyttet.[164]

I teorien nevnes også som et eksempel at noen skriver en nyhetsmelding og offentliggjør den i NTBs navn.[165] Meldingen er etter visstnok å betrakte som et dokument. Beviskriteriet er oppfylt fordi meldingen fremstår som bevis for at det er NTB som er utsteder. Her beveger man seg formodentlig i grenseland til de uttalelser som ikke har bevismessig betydning, jf. straffeloven § 371. Det er antatt i teorien at leserinnlegg i en avis omfattes av sistnevnte bestemmelse.[166]

3.3.5.4 Data som mates inn i et dataprogram

Data som mates inn i et datasystem vil normalt fremstå som bevisbestemte fordi deres form er skreddersydd til å påvirke en automatisk prosess.

---

[162] Se Datakriminalitet (1995) side 206.

[163] Rt. 1978 s. 1115, Rt. 1979 s. 1363 og Rt. 1987 s. 49.

[164] Andenæs/Bratholm (1996) side 305.

[165] Datakriminalitet (1995) side 205.

[166] Bratholm/Matningsdal III (1998) side 178.

Autentiseringsdata vil etter denne forståelsen som regel måtte anses som bevisbestemte. Således vil passord, pin-koder og data i magnetstripen i et bankkort omfattes. Produktnøkler er koder som følger med programvare når man kjøper en lisens. Produktnøkkelen ligger vedlagt programvaren på et papirark eller i manualen og må skrives inn når man installerer programmet. Koden er ment å hindre at ulovlige kopier av programmet kan benyttes. Slike nøkler er tilkjennegivender på samme måte som andre autentiseringsdata. De er bestemt til å tjene som bevis for at brukeren har en betalt lisens av programvaren.

Et annet eksempel på slike bevisbestemte elektroniske data er de data som sendes Skattedirektoratet når man leverer selvangivelsen over Internett eller SMS.[167] Slike data er tilkjennegivender og også bestemt til å tjene som bevis på at avsenderen har oppfylt plikten til å levere selvangivelse. Det samme vil være tilfellet når man fyller ut et skjema for pengeoverføring gjennom nettbank. Dette web-skjemaet er et dokument som fremstår som bestemt til å tjene som bevis.

Ovenfor konkluderte jeg med at dataprogrammer i kjørbar form er tilkjennegivender. Det kan spørres om dataprogrammer kan sies å være bestemt til å tjene som bevis. Manipulasjon av programmer kan straffes om databedrageri, straffeloven § 270 nr 2. Det kan hevdes at dataprogrammer er bestemt til å tjene som bevis for hvordan et datasystem skal fungere. Her beveger man seg imidlertid utenfor det som med rimelighet kan kalles et ”dokument”. Programmet ligger til grunn for datasystemets operasjoner, men skiller seg vesentlig fra andre data som mates inn i datasystemet. Konklusjonen blir at kjørbare dataprogrammer neppe er bevisbestemte tilkjennegivender, og derfor heller ikke dokumenter.

3.3.5.5 Dokumentet som reelt bevismiddel. Gransking.

Et elektronisk dokument kan også være et reelt bevismiddel samtidig som det er dokumentbevis. For eksempel kan dokumentet selv være beheftet med spor etter forfalskningen. Dokumentet vil da kunne bli gjenstand for granskning i retten som ethvert reelt bevismiddel, tvistemålsloven kapittel 17. Michelsen[168] sier om gransking

[167] Short Messaging Service.

[168] Michelsen (1999) side 148.

av dokumenter at ”Man gransker et skriftstykke, ikke for å gjøre seg kjent med dets innhold, men dets utseende.”

Elektroniske dokumenter kan være gjenstand for granskning på to ulike måter.
For det første kan et lagringsmedium, som dokumentet er knyttet til, bli undersøkt som en fysisk gjenstand. Det er da et terminologisk spørsmål om en vil si at det er dokumentet som granskes.[169] Retten kan ved hjelp av sakkyndige undersøke mediets fysiske oppbygning og konstruksjon. For eksempel kan man ved hjelp av avansert teknologisk utstyr gjenfinne slettede data som fysiske spor i lagringsmediet. Slik analyse av de fysiske mediene gjøres av eksperter og foregår i laboratorier.[170]

For det annet kan elektroniske dokumenter granskes for å avgjøre om de er ekte. Dette kan skje ved å lete etter metadata, som sier noe om informasjonen i dokumentet. For eksempel kan de opplyse om når dokumentet ble opprettet, endret og kopiert og hvilken bruker som har produsert det. Hvis man ved granskingen finner metadata blir det et spørsmål for seg hvorvidt disse i det konkrete tilfellet er å betrakte som separate dokumenter.[171]

3.4 Oppsummering

Drøftelsen ovenfor viser at data kan være dokument enten de utstedes direkte av et menneske eller av et datasystem, og enten de er ment å leses av et menneske eller inngå i en automatisk databehandling. Kravene til dokumentets form, gjenstandsvilkåret og kravet til at tilkjennegivendet skal fremtre i skrift eller på annen måte, vil i prinsippet være oppfylt for alle elektroniske tilkjennegivender. Når det gjelder kravene til dokumentets innhold vil alle data som etter en helhetsvurdering inneholder menneskelige tanker omfattes. Det viktigste eksemplet på data som normalt ikke inneholder et tilkjennegivende er elektroniske fotografier.

Når det gjelder beviskravene må det som for tradisjonelle dokumenter foretas en konkret helhetsvurdering. Data som mates inn i et datasystem til bruk i en automatisk prosess, vil normalt være bevisbestemte fordi de har en form som programvaren er

---

[169] Se punkt 3.2.8.

[170] Mye omtalt i media er det norske firmaet IBAS (www.ibas.no).

[171] Se punkt 3.3.5.3.2.

instruert til å kjenne igjen. Autentiseringsdata og hjelpedokumenter vil følgelig være dokumenter. Det samme gjelder annen strukturert informasjon som for eksempel en bestilling av varer i en nettbutikk eller en elektronisk bankgiro i en nettbank.

4 Falskt elektronisk dokument

Straffeloven § 182 rammer benyttelse av et ”eftergjort eller forfalsket Dokument”. Som en samlebetegnelse på ettergjøring og forfalskning brukes ordet ”falsk” i kapitteloverskriften. Falskbegrepet er verken definert i loven eller i forarbeidene.[172] Begrepets innhold er fastlagt i rettspraksis og juridisk litteratur.

Falskt er et dokument etter tradisjonell forståelse når det helt eller delvis skriver seg fra en annen enn den som fremstår som utsteder. Dokumentets bevisegenskap henger sammen med at tilkjennegivendet skriver seg fra den personen som fremstår som utsteder. Loven skiller mellom ettergjøring og forfalskning. Skillet mellom de to formene for falsk er som regel uten rettslig betydning.[173] En systematisk gjennomgang av falskbegrepet fordrer likevel en redegjørelse av forskjellen mellom de to.

Datakrimkonvensjonen definerer i artikkel 7 falskhandlingen som ”input, alteration, deletion, or suppression of computer data, resulting in inauthentic data”. Konvensjonen benytter altså ordet ”inauthentic” som betegnelse på at et dokument er falskt. Dette samsvarer med læren om informasjonssikkerhet og beskyttelse av datas autentisitet, se punkt 1.2.2 ovenfor. I tillegg til å beskytte datas autentisitet verner dokumentfalskreglene datas integritet.[174]

---

[172] Straffelovkommisjonen foreslår å innta en definisjon av falskt dokument i fremtidig straffelov, NOU 2002:4 side 375-376.

[173] Skillet har betydning i forbindelse med §§ 184 (merker) og § 185 (1) om forfalskning av offentlig protokoll.

[174] I NOU 2003:27 side 22 fremholder Datakrimutvalget at det grunnleggende hensynet bak artikkel 7 er å verne om datas integritet. Ordvalget er noe uheldig ettersom konvensjonen artikkel 7 og den forklarende rapporten uttrykkelig sier at det primære er vernet av datas autentisitet, jf rapportens avsnitt 82.

Straffeloven kapittel 15 og 16 har regler om falsk forklaring og falsk anklage. I disse bestemmelsene brukes falskbegrepet om uriktige forklaringer og uriktige anklager. Et dokument av uriktig innhold er imidlertid ikke falskt. Derimot kan en erklæring av uriktig innhold etter omstendighetene rammes av § 372.

For eksempel er et elektronisk betalingskort med høy kredittgrense ikke falskt selv om en person har fått det av banken ved å lyve på seg høy inntekt, Rt. 1987 s. 650. Kortet inneholder et elektronisk dokument som er utstedt av rett instans og er følgelig ekte. At dokumentet er utstedt av banken på grunn av en villfarelse har ingen betydning for dets ekthet.

4.1 Ettergjort

Ettergjort er et elektronisk dokument etter alminnelig forståelse når det i sin helhet skriver seg fra en annen enn den som utad fremstår som utsteder.[175] Ettergjøring forutsetter ikke at det foreligger et ekte dokument av samme innhold. For eksempel skriver A en e-post som gir inntrykk av å stamme fra B. Dokumentet er ettergjort selv om B aldri har skrevet et brev av tilsvarende innhold. Datakrimkonvensjonen bruker ordet ”input” om det å lage et falskt dokument fra bunnen av.[176]

Som jeg har gjort rede for i punkt 3.2.8 må dokumentet avgrenses logisk ut fra dets innhold. I forlengelsen av dette er det naturlige å betrakte det som ettergjøring og ikke forfalskning dersom hele innholdet av en datafil er endret, selv om selve filen fortsatt eksisterer.

Med terminologi hentet fra læren om informasjonssikkerhet kan man si at vernet mot ettergjøring av dokumenter ivaretar hensynet til datas autentisitet. Et ettergjort dokument innebærer ikke endring i et ekte, derfor er det ikke naturlig å si at datas integritet krenkes ved ettergjøring.

4.1.1 Signaturliknende autentiseringsdata

Som nevnt ovenfor i punkt 3.2.5.1 kan autentiseringsdata være et tilkjennegivende. Det er lagt til grunn i rettspraksis at det er ettergjøring når noen underskriver en

[175] For eksempel Rt. 1998 s. 217.

[176] Jf. den forklarende rapporten avsnitt 83.

reseptblankett med legens underskrift.[177] Blanketten med påskrift for hvilke medisiner resepten gjelder, kombinert med legens underskrift, er alt som skal til for å opprette et dokument fra bunnen. På samme måte som tradisjonelle signaturer vil det være ettergjøring hvis en elektronisk blankett undertegnes med legens elektroniske signatur.[178]

Et eksempel på ettergjøring som skjer overfor et datasystem er bruk av falskt passord til autentisering. Dataene som utgjør passordet skriver seg i sin helhet fra en annen enn den som er berettiget til å benytte passordet. Tilsvarende må en kunne tale om ettergjøring av autentiseringsdata ved bruk av pin-kode i minibank eller pin-kode som supplement til et elektronisk nøkkelkortsystem.

4.1.2 Data i elektronisk identifikasjonsbevis

Ovenfor har jeg nevnt at en kopi av et dokument også er et dokument. En kopi av et tradisjonelt dokument er normalt like ekte som originalen. Det skriver seg i sin helhet fra den som fremstår som utsteder. Dette utgangspunktet må imidlertid modifiseres der det er tale om et dokument som bare er ekte hvis det er originalt. For eksempel vil en kopi av et ekte pass, førerkort eller tilsvarende identifikasjonsbevis ikke være ekte dersom noen har til hensikt å la det benytte som en original. Kopien må anses for en ettergjøring av et identifikasjonsbevis. Annerledes må det stille seg der kopien fremvises uten å legge skjul på at det er en kopi av et ekte dokument.

Et eksempel fra den elektroniske verden er den handlingen som går ut på å fremstille en kopi av et minibankkort ved å kopiere dataene på magnetstripen. Dataene er en perfekt kopi av et ekte dokument. Et slikt tilfelle må være å betrakte som ettergjøring av et ekte dokument. Data på det nye kortet skriver seg i sin helhet fra en annen enn banken som er utsteder. Et datasystem med kortleser vil gjenkjenne dataene på stripen og behandle dem som ekte.

---

[177] Se for eksempel Rt. 1958 s. 225 og Rt. 1960 s. 232.

[178] Dette er ikke upraktisk ettersom Rikstrygdeverket i dag jobber med en overgang til elektroniske resepter kombinert med elektronisk signatur.

4.2 Forfalsket

Forfalsket er et elektronisk dokument etter alminnelig lære når det bare delvis skriver seg fra en annen enn den som utad fremstår som utsteder.[179] Forfalskningen skjer ved at gjerningsmannen endrer innholdet i et eksisterende dokument. Endringen kan bestå i å slette eller legge til data i dokumentet.[180] Datakrimkonvensjonens artikkel 7 betegner forfalskning som ”alteration” og ”deletion”.[181]

Også forfalskning kan omformuleres med terminologi hentet fra læren om informasjonssikkerhet. En kan si at vernet mot forfalskning både ivaretar hensynet til informasjonens autentisitet og integritet. Autentisiteten krenkes ved at data ikke i sin helhet stammer fra den som har utstedt dokumentet i første omgang. Integriteten er krenket i og med endringen i data.

4.2.1 Endringen må være gjort i tilkjennegivendet

En særskilt problemstilling er om det er forfalskning dersom gjerningsmannen gjør endringer i andre faktiske omstendigheter, og dette gir dokumentets innhold ny mening. Praksis viser at det avgjørende er om endringen kan sies å være gjort i tilkjennegivendet eller ikke.

I rettspraksis har en betraktet det som dokumentfalsk der et bilskilt påmonteres en annen bil enn det opprinnelig er utstedt for.[182] Dette har sammenheng med at tilkjennegivendet ikke er bilskiltet isolert, men bilskiltet påsatt en bil.[183] Når skiltet settes på en annen bil endres tilkjennegivendets innhold. Å betrakte dette som forfalskning er dermed i tråd med den alminnelige forståelse av falskbegrepet.

Hvis det derimot gjøres endringer i andre faktiske omstendigheter enn dem som må ses som en del av tilkjennegivendet, har en i praksis ikke betraktet det som forfalskning. I Rt. 1930 s. 1301 var forholdet at en ansatt i Norges bank underslo penger fra en

---

[179] Andenæs/Bratholm (1996) side 286-287.

[180] For eksempel Rt. 1926 s. 291 hvor det uttales at ”Disse stempelmerker er blit brukt helt uforandret, der er ikke tat noget fra eller lagt noget til, og jeg kan da ikke finde, at der kan siges å foreligge nogen forfalskning av merkene.”

[181] Den forklarende rapporten avsnitt 83.

[182] Rt. 1948 s. 552.

[183] Se ovenfor punkt 3.2.6.

forseglet pakke med sedler. Han erstattet sedlene med papplater for å skjule underslaget. Omslagspapiret var å betrakte som et dokument. Det inneholdt en signert påtegning om pakkens innhold. Høyesterett kom til at forholdet ikke var dokumentfalsk. Etter alt å dømme bygget retten på at innholdet i pakkene ikke var en del av det tilkjennegivendet som fremgikk av omslagsarket.

Et eksempel er et dataprogram som er forsynt med informasjon om hvem som har laget programmet. Rubrikken med informasjon om opphavsrettshaveren er et dokument.[184] Følgelig ville det være dokumentfalsk om denne ble endret. Om en endring av programmet ville være dokumentfalsk kan være noe usikkert. Dette har vært hevdet i litteraturen.[185] Antakelig er det mest naturlig å dømme for krenkelse av opphavsretten i slike tilfeller, åndsverkloven § 54 jf. § 3.

4.2.2 Endringen må være relevant

Den klassiske forfalskning går ut på å fjerne eller legge til en null i et gjeldsbrev, eller å bedre karakterene i et vitnemål med tanke på jobbsøking. Det er antatt i teorien at ikke enhver endring i dokumentets innhold kvalifiserer til forfalskning. Forandringen må gjelde relativt vesentlige punkter. Ortografiske rettelser, eller endringer som bare har til formål å tydeliggjøre innholdet er derfor ikke å betrakte som forfalskning.[186] Derimot kan endringer av tids- og stedsangivelse innebære forfalskning.[187]

4.3 Særlig om §§ 180 og 181

Bestemmelsene i §§ 180 og 181 innebærer en viss utvidelse av falskbegrepet i forhold til det man ville legge til grunn uten dem.

§ 180 første alternativ har en særlig aktualitet for elektroniske dokumenter. Bestemmelsen rammer ”like med dokumentfalsk” den handling som består i å uberettiget anføre et tilkjennegivende der noen allerede har ”tegnet sitt” navn.

---

[184] Se punkt 3.3.5.3.4.

[185] Datakriminalitet (1995) side 206.

[186] Kjerschow (1930) side 487.

[187] L.c.

Som kjent sendes e-post normalt fra en brukers konto. I feltet for ”avsender” kommer navnet til innehaveren av kontoen opp idet man begynner å skrive e-posten. Såfremt e-posten gis et innhold som kvalifiserer til dokument vil det være tale om dokumentfalsk dersom noen annen enn kontoinnehaveren sender en e-post fra kontoen. Det er derimot neppe falsk hvis den virkelige forfatters navn fremgår av e-postens innhold.

Etter § 181 rammes det som dokumentfalsk dersom gjerningsmannen ved utstedelsen bruker et fiktivt navn, eller tillegger seg en bestemt stilling som har vesentlig betydning for dokumentets beviskraft, eller ved å bortta noen del av samme. Det antas i teorien at det første og siste alternativet ville være å betrakte som falsk også uten § 180.[188]

Bestemmelsen reiser neppe noen nye problemer i forbindelse med elektroniske dokumenter. Derimot er dette praktisk ved uformelle ”Udtalelser” etter § 371. I samtalegrupper og andre fora på Internett er det mulig å tillegge seg en fiktiv identitet. Forutsatt at dette omfattes av begrepet ”eftergjort”, vil det å uttale seg under fiktivt navn på Internett rammes av § 371.

4.4 Falskhandlingen, § 185 (2)

Selve forfalskningen eller ettergjøringen er i seg selv straffbar, jf. § 185 (2). Bestemmelsen rammer også det å anskaffe et falskt dokument. Forfalskning og ettergjøring av elektroniske dokumenter skjer ved at data endres eller skrives inn i et datasystem. Falskhandlingen er fullbyrdet så snart det foreligger et falskt dokument.

For eksempel er det fullbyrdet ettergjøring av et elektronisk dokument idet gjerningsmannen har skrevet et tilkjennegivende i en tekstfil og gitt det skinn av å stamme fra en annen. Det falske dokumentet trenger som nevnt ikke å lagres permanent. Fullbyrdet er falskhandlingen allerede mens dokumentet fortsatt er lagret i datasystemets RAM, se punkt 3.1.2.3.

På samme måte er et passord ettergjort allerede på det tidspunktet når gjerningsmannen skriver inn passordet, men ikke enda har trykket på den knappen som vil sende passordet til verifisering i datasystemet. Benyttelse skjer ved at passordet sendes til verifisering i datasystemet, se punkt 5.5.3 nedenfor.

---

[188] Andenæs/Bratholm (1996) side 289.

4.5 Forspillelse av dokumentbevis

I forbindelse med falskbegrepet er det naturlig å drøfte hva som skiller dokumentfalsk fra forspillelse av dokumentbevis, straffeloven § 187. Bestemmelsen rammer den som "fragaar sin Underskrift paa noget Dokument eller tilintetgjør, forstikker eller helt eller delvis ubrugbargjør et Dokument" som middel til en forbrytelse. Ordene "delvis ubrugbargjør" rammer etter alminnelig forståelse endringer i dokumentet som også kan bedømmes som forfalskning.

Datakrimkonvensjonen artikkel 4 om dataskadeverk rammer også forspillelse av dokumentbevis, jf. ordlyden "damaging, deletion, deterioration, alteration or suppression of computer data". Artikkel 7 er neppe anvendelig, da forspillelse av dokumentbevis ikke krenker datas autentisitet.

En problemstilling er om § 187 kan tenkes anvendt i stedet for § 185 (2) i forfalskningstilfellene. Spørsmålet kommer på spissen dersom gjerningsmannen i forbindelse med et datainnbrudd forsøker å skjule forbrytelsen ved å foreta endringer i datasystemets logg. En slik logg er et dokument, punkt 3.3.5.3.2 ovenfor.

Det foreligger så vidt vites ingen rettspraksis som drøfter spørsmålet. Sammenhengen mellom hovedregelen om dokumentfalsk i § 182 og spesialregelen i § 187 taler for å dømme for forfalskning der vilkårene er oppfylt. Motsatt ville forfalskning svært ofte rammes av § 187 fordi forfalskning i de fleste tilfeller medfører at det opprinnelige dokumentet ubrukbargjøres.

I Datakriminalitet (1995) hevdes at det riktige i er å dømme for forspillelse av dokumentbevis, og ikke dokumentfalsk, der en logg er endret.[189] Kjerschow (1930) mener at man må anse det som forfalskning etter § 185 (2) dersom dokumentets egenskap av bevismiddel opprettholdes, men som ubrukbargjørelse der dokumentets bevisende egenskap bortfaller.[190] Kjerschow sin løsning passer best med bestemmelsenes innbyrdes sammenheng. Hvilket av straffebudene som anvendes har imidlertid begrenset betydning da strafferammen er den samme.

---

[189] Datakriminalitet (1995) side 207 og 210.

[190] Kjerschow (1930) side 493. Antakelig er det dette Andenæs/Bratholm (1996) også mener jf. bemerkningen på side 297.

Straffeloven § 132 rammer forspillelse av bevis i hensikt å motarbeide en offentlig undersøkelse, for eksempel politietterforskning av et straffbart forhold. Etter ordlyden er det straffbart blant annet å "forvanske" gjenstander av betydning. I teorien er det lagt til grunn at gjenstand også omfatter dokumenter.[191] Dersom forvanskingen innebærer dokumentfalsk kommer imidlertid § 185 (2) i stedet til anvendelse.[192]

5 Benyttelse av falskt elektronisk dokument

5.1 Innledning og problemstilling

Fullbyrdet dokumentfalsk foreligger først når gjerningsmannen har benyttet det falske dokumentet.[193] Den fullbyrdede forbrytelse angir også forsøkets øvre grense.[194]

For fullbyrdet forbrytelse kreves etter straffeloven § 182 at gjerningsmannen "benytter" et falskt dokument. Dokumentet må benyttes "som ægte eller uforfalsket". Kravet til "retsstridig Hensigt" behandler jeg sammen med de øvrige subjektive vilkår i punkt punkt 6.

5.2 Hensyn bak vilkåret om benyttelse

Hovedformålet med dokumentfalskreglene er som nevnt ovenfor å ramme krenkelser av den alminnelige tillit til dokumenters ekthet. Det kan hevdes at det først og fremst er når det falske dokumentet gjøres tilgjengelig for andre at den alminnelige tillit krenkes. Særlig ved ettergjøring har et slikt synspunkt gode grunner for seg. Så lenge det elektroniske dokumentet er ettergjort, men fortsatt ubenyttet, er det ikke naturlig å si at den alminnelige tillit er krenket.

Ved forfalskning stiller dette seg annerledes. Da ødelegges det opprinnelige bevismidlet samtidig med at endringen gjøres. Det kan således hevdes at den alminnelige tillit til

---

[191] Bratholm/Matningsdal II (1995) side 170.

[192] Op.cit. side 173.

[193] Falskhandlingen i seg selv er imidlertid også straffbar som jeg har pekt på ovenfor.

[194] Forsøkets nedre grense er tema for punkt 5.8 nedenfor.

dokumentet som bevismiddel svekkes allerede ved falskhandlingen. En del andre land rammer primært falskhandlingen som fullbyrdet forbrytelse.[195] Slik er også regelen i datakrimkonvensjonen artikkel 7. Dette synet hviler på den betraktning at det allerede fra falskhandlingen oppstår en fare for at noen vil innrette seg i tillit til dokumentet.[196] Nærstad mener den alminnelige tillit til dokumenters ekthet med god grunn kan sies å svekkes allerede når det falske dokumentet foreligger.[197] Straffelovkommisjonen foreslår at man i den nye straffeloven primært rammer forfalskning og anskaffelse i stedet for benyttelsen.[198]

5.3 Benyttelse innebærer samhandling

Ordlyden "benytter" er vid og åpner for at enhver form for benyttelse omfattes. Sammenhengen med § 185 (2) viser at det som et utgangspunkt må kreves en handling utover det å forfalske dokumentet. En viss presisering ligger i kravet om at dokumentet skal benyttes som ekte eller uforfalsket. Kjernen i benyttelseshandlingen er at det falske dokumentet gjøres kjent for en person eller et datasystem som deretter kan innrette seg etter det som om det var ekte.[199]

5.4 Er § 182 et rent handlingsdelikt?

Av ordlyden fremstår benyttelse av falskt dokument som et rent handlingsdelikt, i motsetning til straffebud som krever en følge.[200] Hvis man først og fremst så dokument-falskreglene som et vern av private interesser hadde det vært naturlig å kreve en følge, nemlig at noen ble forledet ved den straffbare handlingen. Slik er det for eksempel for databedrageri som krever at handlingen fremkaller tap eller fare for tap. En konsekvens av denne forskjellen er at en godt kan ha fullbyrdet dokumentfalsk, men fortsatt være på forsøksstadiet i forhold til databedrageri.[201]

---

[195] For eksempel Sverige, jf. brottsbalken § 14:1.

[196] Den svenske loven bruker vilkåret "fara i bevishänseende".

[197] Nærstad (1936) side 120.

[198] NOU 2002:4 side 374 flg. Benyttelsen straffes bare hvis gjerningsmannen ikke kan straffes for forfalskning eller anskaffelse.

[199] Nærstad (1936) side 125.

[200] Andenæs (1997) side 102.

[201] Rt. 1991 s. 532.

For at den alminnelige tillit til dokumentet skal krenkes må imidlertid dokumentet også ha blitt gjort tilgjengelig for noen som kan forledes, se punkt 5.5. Det er derfor neppe riktig å si at dokumentfalskregelen er et rent handlingsdelikt. Snarere står den antakelig i en mellomstilling. Dette får betydning for adgangen til tilbaketreden der man antakelig må bedømme § 182 som et følgedelikt.

For eksempel er straffbar benyttelse ikke skjedd ved avsendelse av en ettergjort e-post. Hvis e-posten aldri kommer frem, for eksempel på grunn av teknisk svikt, betraktes det som forsøk på benyttelse, se punkt 5.8.2.

Et annet eksempel er at A forsøker å ta seg inn på datamaskinen til B ved hjelp av ettergjort brukernavn og passord. Det er ikke nok til fullbyrdet forbrytelse at passordet er skrevet inn. Det må også gjøres tilgjengelig for datasystemet for verifisering. Hvis passordet på grunn av teknisk feil ikke blir verifisert kan A bare straffes for forsøk.

5.4.1 Det er ikke nødvendig at noen har latt seg forlede

Det har ingen betydning for fullbyrdet forbrytelse om gjerningsmannen faktisk lykkes med å narre noen med det falske dokumentet.[202] Dette har forankring i ordlyden. Det samme følger av sikker rettspraksis.[203]

I Rt. 1977 s. 457[204] var forholdet at A kjøpte ihendehaverobligasjoner i fingert navn i en bank, for å lure unna penger fra beskatning. I forbindelse med innbetaling av kjøpesummen ble det utstedt interimskvitteringer som igjen skulle veksles inn i obligasjoner så snart banken skaffet disse. Da A skulle veksle inn obligasjonene måtte han overfor banken kvittere på at han hadde mottatt obligasjonene. Kvittering skjedde i det fingerte navnet.[205] Høyesterett uttalte som et obiter dictum at signering og overlevering av kvitteringen til banken var benyttelse av falskt dokument. Dette måtte gjelde selv om banken var klar over at signaturen var falsk. Det var skattemyndighetene som skulle føres bak lyset. Fullbyrdelsen skjedde allerede ved overlevering av den

[202] Slik Andenæs/Bratholm (1996) side 291 og Nærstad (1936) side 125.

[203] For eksempel Rt. 1969 s. 754.

[204] Som en kuriositet kan nevnes at det samme forholdet endte for Høyesterett igjen i Rt. 1978 s. 859.

[205] Straffeloven § 181 første alternativ.

signerte kvitteringen til banken. Kvitteringen ville tjene som bevis dersom skattemyndighetene igangsatte undersøkelser.

5.4.2 Det falske dokumentet behøver ikke ha kommet til noens kunnskap

Heller ikke er det avgjørende om gjerningsmannen ved benyttelseshandlingen bringer det falske dokumentet til noens kunnskap. Dette følger av sikker rettspraksis.

I Rt. 1919 s. 525 var forholdet at A i sitt arbeid som betjent i en privat forretning åpnet brev og underslo penger som var vedlagt brevene. For å dekke over underslaget ettergjorde han underskrifter i forretningens postkvitteringsbok. Underskriftene tjente som bevis for at postvesenet hadde mottatt forseglede konvolutter. Den handlingen som gikk ut på å returnere postkvitteringsboken med de falske signaturene i den overordnedes hylle ble betraktet som benyttelse av det falske dokumentet. Det hadde ingen betydning at det sjelden ble foretatt noen undersøkelser av boken, eller at ingen trolig ville innrette seg etter det som fremgikk av det falske dokumentet. Det avgjørende var at A ved sin handling realiserte dokumentets verdi som bevismiddel ved å gjøre det tilgjengelig for en eventuell kontroll. Dersom dokumentet ble undersøkt ville boken være det avgjørende bevismiddel.

Der et elektronisk dokument benyttes overfor et datasystem må data på en eller annen måte mates inn i datasystemet. Som eksempel kan nevnes at noen søker uberettiget tilgang til et piratkopiert dataprogram. For å kunne bruke programmet må gjerningsmannen skrive inn en produktnøkkel. Når han skriver inn en nøkkel han ikke er berettiget å bruke ettergjør han autoriseringskjennetegnet til en berettiget bruker og begår dokumentfalsk. Selve benyttelseshandlingen skjer her når gjerningsmannen setter i gang den automatiske prosessen som ender med at dataprogrammet gir ham tilgang.

5.5 Dokumentet må ha kommet frem til mottakeren

Et utgangspunkt er at det ikke er benyttelse dersom en person legger et forfalsket et dokument på et privat sted han råder over og noen tilfeldigvis finner det.[206] Dette må være tilfellet også om vedkommende person har et ubegrunnet håp om at noen vil finne det. I teorien er det lagt til grunn som et minstekrav at gjerningsmannen gir dokumentet

[206] Nærstad (1936) side 129.

en ”selvstendig tilværelse”.[207] Med selvstendig tilværelse menes her at dokumentet er gjort tilgjengelig for andre enn gjerningsmannen selv, og at han dertil er avskåret fra å hindre slik tilgjengelighet.

Selvstendig tilværelse må et elektronisk dokument sies å ha når det har kommet frem til mottakerens datasystem. For eksempel utformer gjerningsmannen et falskt elektronisk dokument ved hjelp av sin egen datamaskin. For å benytte det overfører han datafilen med e-post til mottakerens datamaskin. Dokumentet er da gjort tilgjenglig for mottakeren og avsenderen er avskåret fra å hindre at mottakeren leser det. Dette samsvarer med det som ble lagt til grunn i Rt. 1919 s. 525 hvor det var tilstrekkelig at kvitteringsboken ble satt på plass i den overordnedes hylle.

Så lenge et brev ikke har blitt utlevert til mottakeren har avsender råderett over det, jf. postloven § 9 (1). Høyesterett har lagt til grunn at benyttelse ikke skjer før utlevering til mottakeren, Rt. 1949 s. 678. Elektroniske meddelelser befordres på få sekunder. Når meldingen er sendt har avsenderen normalt heller ikke mulighet til å stanse den. Dette gjelder for eksempel e-post og SMS-meldinger. Dersom e-posten for eksempel på grunn av teknisk feil ikke kommer frem til mottakeren kan avsender bare dømmes for forsøk.[208]

Hvis et falskt dokument gjøres tilgjengelig på en Internettside eller for øvrig på et datasystem der gjerningsmannen vet at det er tilgjengelig for andre, må det antas at benyttelse er skjedd selv om datasystemet tilhører gjerningsmannen. Her er gjerningsmannen praktisk sett avskåret fra å hindre at andre skaffer seg kunnskap om dokumentets innhold. Hensynet til beskyttelse av den alminnelige tillit er dermed krenket.

5.5.1 Det må være relativt stor sannsynlighet for at noen vil bygge på dokumentet

I rettspraksis er det lagt til grunn at dokumentet må anbringes på en slik måte at noen, som kan tenkes å bygge på det, finner det eller får det fremlagt. I Rt. 1978 s. 337 var forholdet at en konto var opprettet i falskt navn for å hindre at skattemyndighetene fikk

[207] Nærstad (1936) side 128.

[208] Se punkt 5.8 nedenfor.

kunnskap om det innestående beløpet. Da kontoen ble oppgjort undertegnet innehaveren av kontoen med det fiktive navnet. Spørsmålet var om han hadde benyttet den falske kvitteringen overfor skattemyndighetene. Høyesterett kom til at det falske dokumentet var benyttet. Retten bygget på at skattevesenet ved en "eventuell kontroll" ville finne det falske dokumentet.

I dommen i Rt. 1977 s. 457 ble falske kvitteringer benyttet i forbindelse med en transaksjon i hensikt å skjule penger for skattemyndighetene, se punkt 5.4.1. Høyesterett trengte ikke ta stilling til om kravet til benyttelse var oppfylt. Som et obiter dictum uttalte førstvoterende på vegne av flertallet at "[m]uligheten for at den myndighet som eventuelt skal villedes, vil foreta en kontroll som fører til at dokumentet finnes eller blir fremlagt, vil være av betydning når man skal avgjøre om et tilfelle hører til den ene eller den annen gruppe."[209] Det må med andre ord være en viss sannsynlighet for at noen vil finne dokumentet.

Der et elektronisk dokument blir matet inn som premiss for en automatisk databehandling vil datasystemet normalt legge dokumentet automatisk til grunn. Det blir i disse tilfellene noe søkt å snakke om sannsynlighet. Synspunktet kan likevel ha gyldighet også her da det kan tenkes datasystemer som ikke med nødvendighet legger alle tilgjengelige data til grunn.

Etter dette kan det ikke fastslås en gang for alle hva som kreves av straffbar benyttelse. Det må foretas en konkret vurdering i hvert enkelt tilfelle der det avgjørende er hvor sannsynlig det er at den som skal forledes vil finne dokumentet.

5.5.2 Hvem benyttelse skjer overfor

At det falske dokumentet skal benyttes "som ægte eller uforfalsket" innebærer at dokumentet benyttes i den hensikt å føre noen bak lyset. Benyttelsesvilkåret må derfor vurderes i forhold til en person eller et datasystem som det er meningen å forelede.

Det følger av rettspraksis at det ikke er nødvendig at benyttelseshandlingen skjer direkte overfor den som skal forledes. Benyttelsen kan for eksempel skje ved at dokumentet formidles til en tredjeperson som vil levere dokumentet videre til den som skal forledes.

---

[209] Med "mulighet" mener førstvoterende etter alt å dømme det samme som "sannsynlighet".

I dommen inntatt i Rt. 1978 s. 337 var forholdet at A hadde opprettet en konto i fingert navn for å holde penger unna skattemyndighetene. Et spørsmål var om underskrift på en uttakskvittering innebar straffbar benyttelse av falskt dokument. Høyesterett kom til at dette var tilfellet. Banken var klar over at dokumentene var falske. Straffbar benyttelse skjedde derfor ikke i forhold til banken. Skattemyndighetene ville ved en eventuell kontroll bli forelagt de falske kvitteringene. Det var uten betydning at overlevering direkte skjedde til banken når skattemyndighetene indirekte ville bli kjent med dem. Saken er nesten parallell til Rt 1977 s. 457.

Det er ikke et vilkår at dokumentet benyttes overfor den som dokumentet vedrører. For eksempel ettergjør A et gjeldsbrev slik at det gir skinn av å være utstedt av B. Det normale vil være at dokumentet benyttes overfor skyldneren som bevis på en forpliktelse. Det er like fullt fullbyrdet benyttelse hvis A viser det falske dokumentet til C i håp om å få ekstra kreditt.

Benyttelse kan etter rettspraksis også skje ved fremleggelse i retten, Rt. 1922 s. 542, eller overfor tinglysningsmyndigheten, Rt. 1983 s. 451.

Jeg viser for øvrig til punkt 6 og begrepet rettsstridig hensikt, som utelukker straffbarhet der dokumentet benyttes i en sammenheng som ikke er rettslig relevant.

5.5.3 Falskhandlingen og benyttelsen kan smelte sammen

Falskhandlingen og benyttelsen kan ofte sies å smelte sammen til en og samme handling. For det første kan det være så nær sammenheng i tid at det er vanskelig å holde de to handlingene atskilt. [210] For det annet kan man si at de to handlingene smelter sammen der et ekte dokument som allerede er gitt en selvstendig tilværelse forfalskes.[211] Det vil ofte kreves lite til benyttelse av elektroniske dokumenter av disse grunnene. Vanligvis vil det rent teoretisk la seg gjøre å skille mellom falskhandlingen og bentyttelsen. For eksempel er det i og for seg to forskjellige handlinger å forfalske innholdet av data, og lagre data på en slik måte at det tilfredsstiller kravet til benyttelse.

[210] Andenæs/Bratholm (1996) side 290.

[211] Jf. hensynet bak spesialregelen i § 185 (1). Se punkt 5.5.3.3.

5.5.3.1 Samhandling mellom mennesker

I dommen i Rt. 1977 s. 457 så man det slik at ettergjøring av signatur smeltet sammen med benyttelsen på grunn av nærheten i tid. A kvitterte med falsk signatur ved mottakelse av ihendehaverobligasjoner som han kjøpte av en bank. Retten uttalte her at benyttelsen var fullbyrdet allerede ved signering av kvitteringen overfor banken.

Hvis det gjøres endringer i et dokument som allerede er gitt en selvstendig tilværelse, skjer benyttelsen samtidig med forfalskningen. For eksempel kan tenkes at to personer veksler på å bruke samme datasystem. B oppbevarer på sin harddisk en e-post fra A, der sistnevnte innrømmer å skylde B penger. Hvis A går inn og endrer innholdet i e-posten skjer benyttelsen idet B foretar endringene. Noe mer er ikke nødvendig å gjøre for at hun skal nå sin hensikt. B vil senere bygge på dokumentet. Det må bemerkes at det vanligvis kreves at endringene i data lagres ved en separat instruksjon til datasystemet. I slike tilfeller vil det å lagre endringene være benyttelseshandlingen.

5.5.3.2 Samhandling mellom menneske og datamaskin

Straffelovrådet la til grunn at man ikke kunne kreve noen separat benyttelseshandling når benyttelsen skjer overfor et datasystem som vil legge dokumentet til grunn for en automatisk databehandling.[212] Selve endringen av data er alt som skal til for at gjerningsmannen skal nå sitt mål. De endrede data blir automatisk lagt til grunn av maskinen.

I dommen inntatt i Rt. 1991 s. 532 (BBS-dommen) kom benyttelse av elektronisk dokument overfor et datasystem på spissen. Om saksforholdet viser jeg til punkt 2.4. Et spørsmål var om det forfalskede dokumentet kunne sies å være benyttet all den tid gjerningsmannen bare hadde gjort endringer i listen over konti. Gjerningspersonene hadde ikke foretatt seg noe utover dette. Høyesterett bygget på betraktningene i NOU 1985:31 og kom til at det falske dokumentet var benyttet. Høyesterett sluttet seg til underretten som uttalte:

> Retten finner at det er tilstrekkelig til å konstatere at det forfalskede [dokumentet] er benyttet, at det ble lagt inn i venteregisteret. At det først ville bli brukt under kjøringen neste dag, har ingen betydning. De endrede data ville

[212] NOU 1985:31 side 12.

automatisk bli brukt av maskinen. De tiltalte må etter dette også straffes for overtredelse av straffeloven § 183, idet retten finner at de har utvist forsett.

Datakrimutvalget sluttet seg under tvil til løsningen i Rt. 1991 s. 532 og Straffelovrådets konklusjon.[213] Etter dette må det anses som avklart at det ikke er nødvendig med noen særskilt benyttelseshandling når data mates inn som premiss for en automatisk databehandling. Også her må imidlertid antakelig gjøres den reservasjon at dokumentet vanligvis må lagres før endringene trer i kraft.

En konsekvens av denne tolkningen er for eksempel at falske autentiseringsdata er benyttet idet gjerningsmannen logger seg inn ved å angi passordet.[214]

5.5.3.3 Forfalskning av offentlig protokoll, § 185 (1)

Den regelen som kommer til uttrykk i NOU 1985:31 og Rt. 1991 s. 532 bygger på samme rettspolitiske betraktninger som spesialregelen om fremrykket fullbyrdelse ved forfalskning av offentlig protokoll i straffeloven § 185 (1). Det kreves etter ordlyden ingen benyttelseshandling.

En offentlig protokoll er etter alminnelig forståelse en samling av flere offentlige dokumenter.[215] Det har ingen betydning om protokollen er innbundet eller består av et løsbladsystem. Dette er lagt til grunn i rettspraksis for de militære rullers vedkommende.[216] De fleste offentlige registre føres i dag ved hjelp av datateknologi.[217] Når data kan være dokument i straffelovens forstand er det er antatt i teorien at ”protokoll” kan være en elektronisk database.[218] Viktige eksempler på offentlige protokoller i dag er det sentrale folkeregisteret[219], strafferegisteret[220], de offentlige

---

[213] NOU 2003:27 side 23.

[214] Benyttelse krever normalt at brukeren trykker enter eller tilsvarende.

[215] Slik også Bratholm/Matningsdal II (1995) side 416.

[216] Rt. 1956 s. 714. Retten tolket begrepet ”protokoll” i militær straffelov § 68. ”Offentlig protokoll” skal neppe forstås annerledes.

[217] Se for eksempel tinglysingsloven § 4 annet ledd.

[218] Bratholm/Matningsdal II (1995) side 417.

[219] Folkeregisterloven § 1.

[220] Strafferegistreringsloven § 1.

skattelistene[221], rettighetsregistrene grunnboken[222], løsøreregisteret[223], samt foretaksregisteret[224]. At protokollen skal være "offentlig" innebærer etter en alminnelig forståelse at den må være statlig, kommunal eller fylkeskommunal. Protokollen må dessuten være i bruk i den offentlige tjeneste. [225]

Det er bare forfalskning av offentlig protokoll som etter spesialregelen i § 185 (1) fører til fremrykket fullbyrdelse. Ettergjøring følger hovedregelen om krav til benyttelse i § 182. Ved forfalskning av protokollen er det vanskelig å tenke seg noen benyttelseshandling ved siden av. Gjerningsmannen har alt ved innførselen gjort alt som skal til for at noen kan la seg forlede. [226] Følgelig blir det ikke plass for noen benyttelseshandling. Ved ettergjøring kreves uansett benyttelse, nemlig at protokollen anbringes på en slik måte at noen kan komme til å bygge på at den er ekte. Hvis gjerningsmannen unntaksvis benytter den forfalskede protokollen kommer § 182 til anvendelse, jf. § 185 (3).

Sammenhengen mellom § 182 og § 185 (1) taler isolert sett imot å akseptere at benyttelse og forfalskning skjer i samme handling. Lovgiver fant etter alt å dømme å måtte gi spesialregelen i § 185 (1) fordi man ikke betraktet forfalskning alene som tilstrekkelig for benyttelse. Det har vært hevdet i litteraturen at det logiske er å kreve en eksplisitt benyttelseshandling for andre dokumenter enn offentlige protokoller.[227] Gjennomgangen av praksis viser imidlertid at et slikt syn ikke kan opprettholdes.

5.5.4 Dokumentet må benyttes som sådant

At dokumentet skal benyttes "som ægte eller uforfalsket" innebærer at det er dokumentets bevisende egenskaper som søkes realisert. Handlingen må utad bære preg av at det er et ekte dokument som benyttes.[228]

---

[221] Ligningsloven § 8-8.

[222] Tinglysingsloven § 4 første ledd nr 2.

[223] Tinglysingsloven § 34 første ledd.

[224] Foretaksregisterloven § 1-1 første ledd.

[225] Bratholm/Matningsdal II (1995) side 416.

[226] SKM 1896 side 175.

[227] Slik Nærstad (1936) side 132.

[228] Kjerschow (1930) side 480. Se motsatt punkt 7.1 om samtykke.

Motsatt er det ikke straffbar benyttelse av falskt dokument dersom dokumentet benyttes i en annen egenskap. For eksempel er det ikke benyttelse av falskt dokument dersom gjerningsmannen i anledning et DOS[229]-angrep mot en dataserver på Internett sender det falske dokumentet som "søppeldata" for å sette serverens tjenester ut av spill. Det er i dette tilfellet ikke dokumentets bevisende egenskaper som benyttes, men dokumentets egenskap som datamengde.

Et annet eksempel er at A, som er lærer på et gymnas, bruker et ettergjort dokument i forbindelse med undervisning i datafag. Det er ikke dokumentet som særskilt bevisbærer som benyttes, men dets egenskap av å være et eksempel til illustrasjon.[230] Det samme er tilfellet hvis dokumentet er rekvisitt i en teaterforestilling eller en multimediefremvisning.

Det er enighet i teorien om at det ikke har betydning for fullbyrdet forbrytelse om dokumentet er så lite overbevisende at det ikke blir tillagt noen troverdighet.[231] Hvis dokumentet er benyttet som ekte er det like fullt dokumentfalsk selv om ingen lar seg lure.

5.5.5 Det er ikke nødvendig at originaldokumentet benyttes

Det er ikke nødvendig at originaldokumentet benyttes. En kopi av et falskt dokument er også et falskt dokument.[232] Det tradisjonelle skillet mellom originaldokument og kopi har langt på vei blitt visket bort etter innføring av datateknologi. En kopi av et elektronisk dokument er normalt identisk med originalen. At kopiering i seg selv kan innebære ettergjøring er nevnt i punkt 4.1.2.

I saken inntatt i Rt. 1953 s. 204 var forholdet at A ettergjorde en attest fra en tidligere arbeidsgiver i forbindelse med at han søkte etter jobb. Han benyttet imidlertid ikke det originale falske dokumentet, men fikk laget en attestert avskrift ved et byrå. Avskriften ble så lagt frem for potensielle arbeidsgivere. Likevel ble A dømt for å ha benyttet falskt

[229] Denial of service.

[230] Her vil heller ikke kravet til rettsstridig hensikt være oppfylt.

[231] For eksempel Andenæs/Bratholm (1996) side 302.

[232] Rt. 1953 s. 204.

dokument. Det avgjørende var at den attesterte avskriften ”fullt ut [representerte] en benyttelse av originaldokumentets forfalskede innhold”. Dette var nok.

5.6 Særlig om utgivelse, § 371

Det følger av ordlyden i § 371 at benyttelse kan skje ved utgivelse, jf ”udgiver eller paa anden Maade benytter”. Bestemmelsen åpner for at fullbyrdelse kan skje ved flere typer handlinger enn dem som omfattes av begrepet ”benytter” i § 182. Det er ikke et krav at uttalelsen er rettet til en bestemt person.[233] For eksempel omfatter bestemmelsen det å få på trykk et falskt leserinnlegg i en avis.[234] Det er i dag langt enklere å gjøre uttalelsers innhold tilgjengelig for en større krets gjennom å legge dem ut på en web-side eller samtalegruppe på nettet.

5.7 Medvirkning

Straffeloven § 182 nevner uttrykkelig at medvirkning er straffbart. Problemstillingen er da om handlingen kan karakteriseres som en medvirkningshandling til den handlingen som straffebudet beskriver.[235] Medvirkning forutsetter av de subjektive vilkårene er oppfylt også for medvirkeren.[236]

Hvis A overlater til B et falskt elektronisk dokument kan han straffes for medvirkning til Bs senere benyttelse overfor C.[237] I dommen i Rt. 1968 s. 774 var saksforholdet at A ettergjorde en pantobligasjon i sin fars navn. Han overlot den deretter til B som var klar over at dokumentet var falskt. B benyttet siden dokumentet overfor banken til sikkerhet for en kredittytelse. Høyesterett kom til at A kunne straffes for medvirkning til As benyttelse overfor banken.

For elektroniske dokumenter som benyttes ved autentisering overfor et datasystem er problemstillingen særlig aktuell. Det er ikke uvanlig at lisensierte produktnøkler, passord og koder av andre slag gjøres tilgjengelig på websider eller samtalegrupper på

---

[233] Bratholm/Matningsdal III (1998) side 178.

[234] L.c.

[235] Slettan/Øie (1997) side 123.

[236] Op.cit. side 127.

[237] A kan imidlertid ikke straffes for benyttelse overfor B. Se punkt 7.1 om samtykke.

Internett. Et spørsmål blir derfor om den som deler slike autentiseringsdata kan straffes for medvirkning til benyttelsen av nøklene.

I forhold til de objektive vilkår for straff legger jeg til grunn at autentiseringsdata kan brukes til å fremstille et falskt dokument og viser til drøftelsen i punkt 4.1.1. Spørsmålet er om det å dele autentiseringsdata med andre er "medvirkning".

I dommen i Rt. 1994 s. 1610 var spørsmålet om omsetning av piratdekodere var medvirkning til beskyttelsesbrudd etter straffeloven § 145 (2). Høyesterett la til grunn som et obiter dictum at selgeren av en vare normalt ikke kan straffes for medvirkning til en forbrytelse som gjenstanden brukes til. Bare dersom produktet ikke har noen lovlig anvendelse kan selgeren straffes.[238]

Det er naturlig å se det på samme måte der et falskt passord gjøres tilgjengelig vederlagsfritt. Passordet har ingen lovlige bruksområder utenom å tjene som autentiseringsdata for den berettigede brukeren. Følgelig er handlingen objektivt en medvirkningshandling. De subjektive vilkårene vil regelmessig være oppfylt. Kravet er at den som gjør nøklene tilgjengelig regner det for sikkert eller overveiende sannsynlig at hovedmannen kommer til å begå dokumentfalsk.[239]

Tilsvarende må løsningen bli når det er tale om deling av andre former for autentiseringsdata. Eksempler er elektronisk signatur og data kopiert fra magnetstripen på et bankkort.

Datakrimkonvensjonen artikkel 6 nr 1 bokstav a punkt ii rammer den som gjør tilgjengelig "a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed". Datakrimutvalget foreslår at Norge reserverer seg mot bestemmelsen ved ratifisering av konvensjonen.[240]

---

[238] Tolkningen fremgår av herredsrettens domsgrunner.

[239] NOU 2003:27 side 19.

[240] NOU 2003:27 side 21.

5.8 Forsøk

5.8.1 Generelt

Ovenfor i avsnittene 5.1-5.5 har jeg gjort rede for hva som skal til for fullbyrdet dokumentfalsk. I dette avsnittet vil jeg skissere forsøkets grense nedad mot straffri forberedelse. Forsøk er gjort straffbart i straffeloven § 49.

> Strafbart Forsøg foreligger, naar en Forbrydelse ei er fuldbyrdet, men der er foretaget Handling, hvorved dens Udførelse tilsigtedes paabegyndt.

Det har flere rettsvirkninger at man statuerer forsøk. For det første utvides virkeområdet for den straffbare handlingen etter § 182. Konsekvensen av dette er at gjerningsmannen dømmes etter § 182 jf § 49, i stedet for den forberedende falsk- eller anskaffelseshandlingen. Konkurrensspørsmålet løses etter § 185 (3).

For det andre har gjerningsmannen ved forsøk sammenliknet med fullbyrdet handling anledning til å tre tilbake fra den straffbare virksomheten. I så fall er handlingen straffri, jf. straffeloven § 50.

5.8.2 Forsøk på benyttelse

Det må være foretatt en ”Handling”. Etter rettspraksis skal det foretas en konkret helhetsvurdering der både objektive og subjektive momenter har betydning.[241] Falskhandlingen er gjort straffbar i § 185 (2). Forfalskning og benyttelse kan ikke pådømmes i konkurrens, § 185 (3). Fra dette kan man slutte at forsøkstidspunktet ligger i tid etter falskhandlingen.

Når det falske dokumentet er gjort tilgjenglig for mottakeren er benyttelse fullbyrdet, se punkt 5.5. I rettspraksis har det vært lagt til grunn at forsøksstadiet ligger i tid mellom benyttelseshandlingen og tilgjengeliggjøringen.

Høyesterett har således lagt til grunn at forsøksgrensen er overskredet når gjerningsmannen har sendt et brev med posten. I Rt. 1949 s. 678 var saksforholdet at en person hadde sendt ettergjorte bestillinger på gummiartikler med posten. Noen av bestillingene ble sendt i retur av Postverket. Retten la til grunn at benyttelsen ikke var

[241] Rt. 1991 s. 95.

fullbyrdet for disse bestillingenes vedkommende og dømte for forsøk. På samme måte må en formodentlig bedømme det ved forsendelse av e-post hvis meldingen ikke når adressaten på grunn av teknisk svikt.

Når data benyttes overfor en datamaskin fullbyrdes forbrytelsen ved lagring eller ved å sende data til datasystemet for verifisering. Dersom brukeren følger vanlig prosedyre for å gjøre data tilgjengelig for systemet, men dette ikke lykkes på grunn av teknisk feil, kan det dømmes for forsøk. Det vil imidlertid ikke være rom for tilbaketreden.

Ved forsendelse av tradisjonelle dokumenter med posten har avsenderen rett til å råde over forsendelsen inntil brevet har nådd mottakeren. Dette følger av postloven § 9 (1).[242] Adgangen for straffri tilbaketreden må antakelig bedømmes etter straffeloven § 50 annet alternativ som i utgangspunktet retter seg mot følgedelikter. Dokumentfalskbestemmelsen står i en mellomstilling mellom handlings- og følgedelikter, se punkt 5.4 og 5.5. Gjerningsmannen kan da tre tilbake fra forsøk ved å kreve postsendingen holdt tilbake og derved hindre at dokumentet kommer frem til mottakeren.

Tilbaketreden kan også tenkes ved forsendelse av e-post, men muligheten blir mer subtil. Forsøksgrensen er overtrådt idet e-posten sendes og fullbyrdelsen skjer når den gjøres tilgjengelig for mottakeren. E-post befordres på brukerens kommando gjennom linje eller trådløst og kan normalt ikke stanses etter at de er avsendt. Forutsatt at det er mulig å stanse e-posten vil det også her kunne bli tale om tilbaketreden fra forsøk.

6 Forsett og rettsstridig hensikt

6.1 Forsett

Skyldkravet er forsett, straffeloven § 40. Gjerningsmannen må være klar over at han benytter et falskt dokument som ekte.

[242] Lov om formidling av landsdekkende postsendinger av 29.11.96 nr 73.

I forhold til elektronisk dokumentfalsk kan det, på grunn av den avanserte teknologien som er involvert, bli aktuelt med faktisk villfarelse, straffeloven § 42. Avgjørende er da om gjerningsmannen er i villfarelse om "[o]mstændigheder…der betinger Strafbarheden eller forhøier Strafskylden".

For eksempel kan det tenkes at datamaskinen automatisk sender e-post til gitte tidspunkt, og at gjerningsmannen har glemt at han instruerte datamaskinen til dette. Hvis han legger e-posten i utboksen vil den sendes automatisk. Han har for så vidt "benyttet" det falske dokumentet ved å instruere datamaskinen til å sende ut e-posten, men forsettet dekker i dette tilfellet ikke benyttelsen. Tilsvarende blir løsningen hvis A ettergjør et dokument og lagrer det på et lagringsmedium som B har tilgang til, uten at A vet at B har adgang. I dette tilfellet har A ikke forsett med hensyn til benyttelsen overfor B.

6.2 Særlig om "retsstridig Hensigt"

I tillegg til vanlig forsett kreves at gjerningsmannen har "retsstridig Hensigt". At hensikten må være rettsstridig innebærer ikke et krav om at hensikten er å oppnå noe i og for seg uberettiget. Det fremgår uttrykkelig av straffeloven § 182 (2) at man straffes for dokumentfalsk der hensikten er å bevise et berettiget eller beskytte seg mot et uberettiget krav. Sammenhengen mellom første og annet ledd tilsier at annet ledd er en mildere spesialregel der også kravet til rettsstridig hensikt gjelder.[243]

Kravet om rettsstridig hensikt må ses i lys av at det falske dokumentet skal benyttes som ekte eller uforfalsket. Som regel er det tilstrekkelig for dokumentfalsk at noen forleder en annen til å stole på et dokument som om det var ekte.

Det framgår av forarbeidene til § 182 at lovgiver med kravet til rettsstridig hensikt mente å utelukke straff der gjerningsmannen ved benyttelsen søker å bevise et faktum uten rettslig betydning.[244] I straffeloven av 1842 ble dette hensynet ivaretatt av kravet om påtalebegjæring fra fornærmede.[245] Andenæs/Bratholm formulerer kravet til rettsstridig hensikt som et vilkår om at gjerningsmannen må ha ønsket å oppnå et

[243] Slik også Andenæs/Bratholm (1996) side 292.

[244] SKM 1896 side 173.

[245] L.c.

rettslig relevant resultat.[246] Kjerschow tolker kriteriet som et krav om at dokumentet må brukes som bevismiddel for å forlede noen til en rettslig relevant handling eller unnlatelse, eller som bevis for en kjensgjerning som kan få rettslig betydning. [247] Bratholm/Matningsdal hevder kriteriet skal tjene til å utelukke fra det straffbare området tilfeller der det etter den alminnelige rettsfølelse ville være urimelig å straffe.[248]

Straffelovkommisjonen anser kravet om rettstridig hensikt som unødvendig ved siden av en ny alminnelig bestemmelse om innskrenkende tolkning, jf. forslagets § 3-7.249 Det heter i den foreslåtte bestemmelsen at "særegne omstendigheter" kan lede til straffrihet selv om handlingen objektivt dekkes av ordlyden. Den foreslåtte bestemmelsen svarer omtrent til den alminnelige ulovfestede rettsstridsreservasjon.250

Det sentrale synes etter dette å være at benyttelsen må skje i en sammenheng som gir dokumentet rettslig betydning. Kravet om at gjerningsmannen må benytte dokumentet som bevis for et forhold av rettslig betydning har to konsekvenser.

6.2.1 Dokumenter av betydning som bevis i rettsforhold

For det første innebærer kravet om rettsstridig hensikt at det ikke alltid er straffbart å benytte som ekte et falskt dokument med bevismessig betydning i rettsforhold.

Dokumenter som er av objektiv og direkte betydning i rettsforhold kan tenkes benyttet i en sammenheng der de ikke får betydning som bevis i noe rettsforhold. Et eksempel er studenten som henger opp falske kvitteringer for nedbetalt gjeld på juletreet for å glede sine foreldre. Handlingen innebærer benyttelse av et falskt dokument som om det var ekte. Kvitteringene er av betydning som bevis i rettsforhold. Likevel kan han ikke straffes fordi dokumentet ikke benyttes for å oppnå et rettslig relevant resultat.

Denne betydningen av begrepet rettsstridig hensikt har vært drøftet i rettspraksis. Et eksempel er Rt. 1900 s. 65. En kvinne fikk 20 kroner av sin mann for å sette dem i banken. Hun beholdt 10 kroner selv og satte inn de resterende 10. For å skjule dette

---

[246] Andenæs/Bratholm (1996) side 292.

[247] Kjerschow (1930) side 481.

[248] Bratholm/Matningsdal II (1995) side 409.

[249] NOU 2002:4 side 376.

[250] Op.cit. side 221-222.

overfor mannen forfalsket hun påtegningen i bankboken slik at den ga skinn av at hun hadde satt inn 20 kroner. Høyesterett kom til at det å levere bankboken til mannen var benyttelse av falskt dokument som ekte. bankboken Men ved denne konkrete bruken av dokumentet forelå ikke rettsstridig hensikt, fordi intet rettslig relevant resultat ble søkt oppnådd.[251]

6.2.2 Dokumenter bestemt til å tjene som bevis

For det andre innebærer kravet om rettsstridig hensikt en innsnevring av det strafferettslige vernet av bevisbestemte dokumenter. Bevisbestemte tilkjennegivender er i prinsippet dokumenter uansett hvilket faktum de er bevis for, se punkt 3.3.5.2. Det kan tenkes tilkjennegivender som er bevisbestemte, men som det uansett ikke vil være rettsstridig å benytte på grunn av dokumentets trivielle innhold.

Spørsmålet er ikke drøftet av Høyesterett. Et dokument som beviser et trivielt forhold uten rettslig relevans kan antakelig bare unntaksvis benyttes i rettsstridig hensikt. Målet for benyttelsen vil sjelden være å oppnå et rettslig relevant resultat.

Et annet eksempel er bonden som ettergjør en erklæring om at hans okse er finere enn naboens. Erklæringen er åpenbart bestemt til å tjene som bevis, men bevistemaet er av en slik art at tilkjennegivendet neppe vernes av dokumentfalskreglene. Derimot har erklæringen vern som uttalelse etter straffeloven § 371.

6.2.3 Rettsstridig påvirkning av datasystem

Det kan spørres om det kan sies å være ”retsstridig Hensigt” å søke å påvirke en automatisk databehandling ved å mate inn falske data. Det avgjørende er om påvirkning av den automatiske prosessen får rettslig relevante konsekvenser. Uberettiget tilgang til, og bruk av, et datasystem er straffbart etter §§ 145 (2) og 261. Adgangen i seg selv reiser derfor spørsmål av rettslig betydning. Antakelig er uberettiget tilgang et rettslig relevant formål. Rettslig relevant må forholdet også være når gjerningsmannen ved å mate inn data påvirker resultatet av en prosess som leder til tap for noen, jf. § 270 nr 2 om databedrageri.

---

[251] Dagens regler om formuesforholdet mellom ektefeller ville ledet til et annet resultat, jf. ekteskapsloven § 31 (1).

Det fritar ikke for straff at gjerningsmannen kunne oppnådd det samme med et gyldig dokument, Rt. 1966 s. 1375. Forholdet var her at gjerningsmannen hadde endret navnet i passet sitt til et annet navn som han for så vidt var berettiget til å bruke. Han kunne således fått utstedt nytt pass hos passmyndigheten. Det var likevel rettsstridig hensikt å endre i det opprinnelig utstedte identifikasjonspapiret. Tilsvarende er formodentlig kravet til rettsstridig hensikt oppfylt hvis A fremstiller en kopi av magnetstripen på sitt eget bankkort. Han kunne fått banken til å utstede et nytt kort. Ved selv å fremstille et nytt gjør han seg skyldig i ettergjøring av et elektronisk dokument og benyttelsen er straffbar.

7 Samtykke

Av straffrihetsgrunner kan særlig samtykke være aktuelt. Samtykke som straffrihetsgrunn er bare unntaksvis direkte lovregulert[252], og dette er ikke tilfellet for dokumentfalsk. Det beror i prinsippet på en tolkning av § 182 om samtykke kan gis straffriende virkning.[253] Man må sondre mellom samtykke i to relasjoner.

Dersom samtykket kommer fra den personen som dokumentet benyttes overfor, følger straffriheten direkte av § 182. Dokumentet skal benyttes som ekte eller uforfalsket. Dette vil ikke være tilfellet dersom mottakeren av dokumentet får vite av avsenderen at dokumentet er falskt.[254]

Dersom samtykket gis av den som fremstår som utsteder av dokumentet stiller saken seg annerledes. I innledningen konkluderte jeg med at dokumentfalskreglene primært beskytter offentlige interesser, men også ivaretar private interesser. En privatmann kan i alminnelighet ikke gi samtykke til krenkelse av offentlige interesser.[255] Der både

[252] For eksempel straffeloven § 235 for visse legemskrenkelser.

[253] Slettan/Øie (1997) side 153 flg.

[254] Andenæs/Bratholm (1996) side 293.

[255] Andenæs (1997) side 179-180. Eskeland side 249.

offentlige og private interesser krenkes beror straffriheten på en avveining mellom hvor akseptabel handlingen fremstår, og handlingens skadelige virkninger.[256]

I de tilfeller der den som fremstår som utsteder har samtykket er gjerningsinnholdet i § 182 oppfylt. Dokumentet er falskt, men benyttes som ekte. Samtykket innebærer imidlertid et avtalerettslig fullmaktsforhold og dette gjør handlingen mindre straffverdig enn annen benyttelse.[257] Det er etter alminnelig lære ikke nødvendig at fullmaktsforholdet fremgår av dokumentet for å binde fullmaktsgiver. Det vanlige vil likevel være at fullmektigen undertegner med påskrift ”på vegne av”, ”for” eller liknende.

Normalt vil det ikke få betydning for den dokumentet benyttes overfor om det er utstedt av den som fremstår som utsteder, eller dennes fullmektig. Imidlertid er det ikke nødvendigvis det samme for mottakeren om en underskrift er falsk eller ekte, selv om det foreligger et fullmaktsforhold. Som bevismiddel vil ikke dokumentet ha samme verdi. Fullmaktsgiveren kan for eksempel senere kan komme med innsigelser om at fullmektigen gikk utover fullmakten, eller benekte at hun i det hele tatt hadde fullmakt.

Høyesterett la i Rt. 1936 s. 459 under dissens til grunn at det ikke var straffbar dokumentfalsk hvis fullmektigen undertegnet med fullmaktsgivers navn uten å anføre fullmaktsforholdet. Det var i den konkrete saken tale om kvittering på en veksel mot utbetaling av et pengebeløp. Rettens begrunnelse var at det ville stride mot ”den alminnelige rettsfølelse” å straffe for å underskrive en annens navn med dennes samtykke.

Mindretallet i Høyesterett kom etter en konkret avveining til at handlingens skadelige virkning var mest tungtveiende. Mindretallet pekte på at kreditor ved å utbetale pengene mot den falske veksel utsatte seg for fare for tap. Derimot mente mindretallet at dette ville stille seg annerledes ved bestillinger, slik forholdet var i Rt. 1931 s. 603 og Rt. 1931 s. 605. Her er handlingens potensielt skadelige virkning mindre. Andenæs[258] og Andorsen[259] er kritiske til flertallets løsning.

---

[256] Eskeland (2000) side 250-251.

[257] Andenæs/Bratholm (1996) side 293.

[258] Andenæs (1997) side 179-180.

[259] Andorsen (1992).

I lys av Rt. 1936 s. 459 må konklusjonen bli at samtykke fra den som fremstår som utsteder fritar for straff. En konsekvens er at det ikke er straffbar dokumentfalsk dersom innehaveren av passord eller betalingskort lar en annen benytte det.

8 Konkurrensspørsmål

8.1 Innledning og problemstilling

I forbindelse med elektronisk dokumentfalsk reiser det seg enkelte spørsmål om ulikeartet idealkonkurrens som ikke er aktuelle for tradisjonelt dokumentfalsk. Konkurrens mellom falskhandlingen og benyttelsen er utelukket, jf. straffeloven § 185 (3). Når dokumentfalsk brukes som middel til å begå en forbrytelse som kan medføre fengsel i to år eller mer kommer § 183 til anvendelse i stedet for § 182. Jeg går ikke inn på tolkningen av denne bestemmelsen, men drøfter konkurrensspørsmålet isolert.

Etter straffeloven §§ 62 og 63 økes strafferammen i konkurrenstilfellene med inntil det halve i forhold til den høyeste strafferammen etter noe av enkeltstraffebudene. Avgrensningen av konkurrensspørsmålet er den samme etter de to bestemmelsene. Den rettslige problemstillingen er hva som ligger i begrepet ”flere Forbrydelser”.

Etter en rent språklig forståelse av ordet forbrytelser skulle man anta at det er en selvstendig forbrytelse for hvert straffebud gjerningsmannen overtrer. I fast og langvarig rettspraksis[260] er det lagt til grunn at det avgjørende for spørsmålet om ulikeartet idealkonkurrens er om straffebudene retter seg mot samme eller ulike sider ved den straffbare handlingen.[261] I teorien er dette også formulert som et spørsmål om det ene straffebudet kan tenkes overtrådt uten at det andre samtidig er overtrådt.[262] Dersom flere straffebud retter seg mot de samme sidene ved den straffbare handlingen

[260] For eksempel Rt. 1971 s. 882.

[261] Eskeland (2000) side 221-224 uttrykker dette som et spørsmål om straffebudene rammer samme eller ulike interesser. Interesselæren er vanligvis benyttet for å avgjøre det straffeprosessuelle identitetsspørmålet. Ut fra fremstillingen virker det som Eskeland mener spørsmålene skal løses utfra samme kriterium. Motsatt Andenæs (1997) side 337. Jeg vil her holde meg til Andenæs’ terminologi.

[262] Andenæs (1997) side 336.

skal bare ett av dem benyttes. Motsatt skal bare det ene benyttes hvis de retter seg mot samme side.

I dommen i Rt. 1935 s. 573 var saksforholdet at en valgbetjent foretok kumuleringer på innleverte stemmesedler. Dette innebar både valgfusk, straffeloven § 108, og benyttelse av falskt dokument. Spørsmålet var om de to bestemmelsene kunne anvendes i idealkonkurrens. Retten kom til at de kunne brukes i idealkonkurrens med den begrunnelse at § 182 inneholdt "strafferettslige kjennemerker" som ikke var omfattet av gjerningsbeskrivelsen i § 108. Disse kjennemerkene hadde videre "sin selvstendige betydning" ved siden av § 108.

Om to straffebud retter seg mot samme eller ulike sider av den straffbare handlingen må avgjøres ved en konkret tolkning av de aktuelle straffebudene. I det følgende vil jeg drøfte de mest aktuelle konkurrensspørsmålene i forbindelse med elektronisk dokumentfalsk. Jeg nøyer meg med å helt kort å skissere rettsgrunnlag og tolkning av de konkurrerende bestemmelsene. Hensikten er å kunne bedømme om de retter seg mot samme eller ulike sider ved handlingen.

8.2 Konkurrens med databedrageri

Rettslig grunnlag for databedrageri er straffeloven § 270 nr 2. Den straffbare handlingen er å påvirke resultatet av en automatisk databehandling som kan medføre tap, ved blant annet "endring i data". Spørsmålet er om endringen kan pådømmes i konkurrens med reglene om dokumentfalsk.

Høyesterett har i Rt. 1991 s. 532 tatt stilling til konkurrensspørsmålet. Om sakens faktum se punkt 2.4 ovenfor. Retten kom til at elektronisk dokumentfalsk og databedrageri kan pådømmes i konkurrens. Konkurrensspørsmålet er ikke direkte berørt. Antakelig bygger man her på samme løsning som er lagt til grunn for tradisjonelt bedrageri. Det har i en rekke dommer vært dømt for bedrageri og dokumentfalsk i konkurrens[263]. Løsningen må anses som sikker rett.[264]

[263] Se for eksempel Rt. 2002 s. 1385.

[264] Også NOU 2002:4 side 375.

8.3 Konkurrens med tyveri

Tyveri rammes av straffeloven § 257 og den straffbare handlingen retter seg mot den som ”borttar” en gjenstand som tilhører en annen. Uberettiget uttak i minibank ved overtrekk av konto har i rettspraksis vært bedømt som tyveri av pengene.[265] I NOU 1985:31 uttales at dette ”så meget mer” må være tilfellet når gjerningsmannen manipulerer kortet eller automaten.[266] Straffelovrådet antok også at benyttelse av falskt bankkort i så fall kan pådømmes i konkurrens med tyveriet. [267]

Problemstillingen har senere ikke vært behandlet av Høyesterett og er ikke drøftet i teorien. Dokumentfalsk og tyveri retter seg mot ulike sider ved den straffbare handlingen. Det kan dessuten hevdes å være et klart behov for å dømme for dokumentfalsk i disse tilfellene. Den alminnelige tillit til autentiseringsdata bør i seg selv vernes.

Konklusjonen blir at dokumentfalsk kan pådømmes i konkurrens med tyveri ved uttak fra minibank.

8.4 Konkurrens med datainnbrudd

Datainnbrudd er den handling som går ut på å skaffe seg uberettiget adgang til data eller programvare ved å ”bryte en beskyttelse”, straffeloven § 145 (2).

At misbruk av en annens brukernavn og passord kan innebære ulovlig beskyttelsesbrudd etter § 145 (2) følger av bestemmelsens forarbeider[268] og er lagt til grunn i rettspraksis[269]. Overtredelse av datainnbruddsbestemmelsen kan imidlertid skje på en rekke andre måter enn ved å ettergjøre en berettiget brukers passord, for eksempel ved å bruke en såkalt ”trojaner” til å åpne en ”bakdør” inn i systemet. Det er i utgangspunktet nærliggende å si at krenkelsen av passordets ekthet er en annen side av den straffbare handlingen enn det rene beskyttelsesbruddet. Hensynet til å sikre tilliten til passord er vesensforskjellig fra verdien av å sikre datasystemer mot beskyttelsesbrudd.

---

[265] Rt. 1982 s. 1816.

[266] NOU 1985:31 side 33 og Ot.prp.nr 35 (1986-87) side 26.

[267] NOU 1985:31 side 7.

[268] Ot.prp.nr 35 (1986-87) side 20.

[269] Se Rt. 1998 s. 1971 og Rt. 1995 s. 1872.

I rettspraksis har man i forbindelse med datainnbrudd ikke dømt for dokumentfalsk i konkurrens. Dette trenger imidlertid ikke være avgjørende. Det har i slike saker ikke blitt tatt ut tiltale for dokumentfalsk, og siden de to bestemmelsene beskytter ulike interesser har ikke domstolen foranledning til å ta opp spørsmålet, jf. straffeprosessloven § 38 (2).[270]

Et tungtveiende moment mot å pådømme i konkurrens mellom dokumentfalsk og datainnbrudd er at lovgiver har forutsatt at datainnbrudd alene rammes av § 145 (2) og ikke dokumentfalskbestemmelsene. Forarbeidene synes å bygge på den oppfatning at beskyttelsesbrudd i hovedsak skjer ved hjelp av uberettiget bruk av passord.[271] I et slikt lys er det unaturlig å dømme for falskhandlingen i konkurrens. Jeg antar at dette momentet blir avgjørende for konkurrensvurderingen.

Under tvil kommer jeg til at datainnbruddsbestemmelsen konsumerer dokumentfalskbestemmelsen.

8.5 Konkurrens med skadeverk

Straffbart skadeverk er regulert i straffeloven § 291. Bestemmelsen rammer den som ”rettsstridig skader, ødelegger, gjør ubrukelig eller forspiller en gjenstand”.[272] Problemstillingen er om det å ”skade” et elektronisk dokument retter seg mot en annen side enn forfalskningen. Det er endringen av data som både innebærer ”skade” og forfalskning. Det kan neppe tenkes forfalskning som ikke samtidig innebærer at originaldokumentet blir skadet. Utgangspunktet er derfor at bestemmelsene klart rammer samme side ved handlingen.

I NOU 2002:4 punkt 9.17.2 uttaler Straffelovkommisjonen at forfalskning kan pådømmes i konkurrens med skadeverk. Synspunktet er ubegrunnet og det er vanskelig å se gode grunner for det. Konklusjonen blir derfor at skadeverk og dokumentfalsk ikke kan pådømmes i idealkonkurrens.

---

[270] Bratholm/Matningsdal II (1995) side 214 nevner at datainnbruddsregelen primært beskytter private, men også offentlige interesser.

[271] NOU 1985:31 side 31.

[272] NOU 1985:31 side 10. Data er vernet dersom de er knyttet til et lagringsmedium.

9 Sammenfattende bemerkninger og vurdering

Hovedkonklusjonen i oppgaven er at reglene om dokumentfalsk også rammer forfalskning, ettergjøring, og benyttelse av falske, elektroniske dokumenter. Benyttelse av falske data kan tenkes i elektronisk samhandling mellom mennesker, mellom menneske og datamaskin, og datamaskiner imellom. Det er lite rettskildemateriale på området, og flere av konklusjonene er derfor usikre.

Spesielt er det behov for en avklaring av spørsmålet om konkurrens mellom dokumentfalsk og datainnbrudd. I nær sammenheng med dette Står spørsmålet om passord, pin-koder og andre signaturliknende autentiseringsdata har vern mot ettergjøring. I rettspraksis har dette aldri kommet på spissen. Her er det behov for avklaring fordi slike data tilsynelatende oppfyller alle kravene i dokumentdefinisjonen.

Dagens regler har en utforming som er påfallende lite tilpasset elektroniske dokumenter. Spesielt gjelder dette kravene til dokumentets form. Vilkåret om ”gjenstand” er en anakronisme i dagens virkelighet. Data under overføring har neppe tilstrekkelig tilknytning til gjenstand til å være dokument. Dette får den underlige konsekvensen at elektroniske dokumenter opphører å være dokumenter under overføring i nettverk. Brukere kan i dag lagre sine data på servere over hele verden. Dette fører til at data hyppig er under overføring, og brukeren vet ofte ikke hvor i verden dataene befinner seg. Det faller da unaturlig å operere med et krav om gjenstandstilknytning.

Straffelovrådet[273] så ikke dette som noe problem. Data under overføring var ikke et like utbredt fenomen som i dag. For alle praktiske formål var det data lagret i et frittstående datasystem som skulle beskyttes. Dokumentdefinisjonen ble derfor ikke foreslått endret.

Straffelovkommisjonen foreslår å gå bort fra begrepet gjenstand i den nye straffeloven.[274] Imidlertid synes det ikke som Straffelovkommisjonen vil fjerne kravet om tilknytning til et lagringsmedium. De nøyer seg med å vise til at man i forvaltningsretten har definert dokument som ”en logisk avgrenset informasjonsmengde som er lagret på et medium”. Videre viser Straffelovkommisjonen til at

[273] NOU 1985:31 side 10 og side 29.

[274] NOU 2002:4 side 375.

datakrimkonvensjonen rammer falsk av datalagret[275] informasjon og at den nye loven må være i samsvar med denne. Datakrimutvalget konkluderte med at norsk rett er i samsvar med konvensjonen.[276]

Som nevnt i punkt 2.6 ovenfor er det naturlig å se hen til de øvrige nordiske land ved en eventuell revidering av dokumentfalskbestemmelsene. De danske reglene om dokumentfalsk likner de norske mer enn de øvrige nordiske landenes regler. Den danske dokumentdefinisjonen inneholder kriteriet ”skriftlig” i stedet for et krav om gjenstandstilknytning.[277] Tradisjonelt tolket man bestemmelsen slik at den ikke rammer data, men etter en landsrettsdom[278] der en e-post ble betraktet som dokument fremsto rettstilstanden som uavklart.[279] Den 19. mai i år ble de danske reglene endret slik at ”eller elektronisk” ble føyd til som alternativ til det gamle skriftkravet.[280] Lovforslaget[281] bygger på utredningen ”IT-kriminalitet” gjort av det såkalte Brydensholtutvalget[282].

I Finland rammer straffeloven kapittel 33 falsk av en rekke ulike bevismidler, herunder ”upptagningar som lämpar sig för automatisk databehandling” jf. kapittel 33 § 6.[283] I Sverige har lovarbeidet kommet kortere enn i Danmark, men allerede i 1992 foreslo

---

[275] Datakrimkonvensjonen beskytter lagrede data og ikke data under overføring, jf. den forklarende rapporten punkt 81.

[276] NOU 2003:27 side 23.

[277] Dansk straffelov § 171 stk. 2.

[278] Østre landsrets dom 26.09.01 saksnummer 5.

[279] Lov&Data nr. 68 2001.

[280] Straffeloven med endringer finnes på Internett, http://www.retsinfo.dk/_GETDOCI_/ACCN/A20030081429-REGL

[281] Forslag til ændring af straffeloven, retspleieloven, markedsføringsloven og ophavsretsloven (IT-kriminalitet m.v.) av 05.11.03. Tilgjengelig på Internett http://147.29.40.90/DELFIN/HTML/20031/2L00055.htm.

[282] Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet. Betenkning nr 1417. Internett http://www.jm.dk/wimpdoc.asp?page=document&objno=64936.

[283] Tilgjengelig på Internett http://www.finlex.fi/

Datastraffrättsutredningen å knytte dokumentbegrepet til dets immaterielle innhold snarere enn til en gjenstand.[284]

Også i Norge bør man overveie å endre dokumentdefinisjonen slik at den tar hensyn til at data er immaterielle. Dokumentet finner sin naturlige avgrensning i tilkjennegivendet, se punkt 3.2.8 ovenfor. Det er derfor liten grunn til å beholde et krav om at data må manifestere seg fysisk. Den nye danske straffeloven § 171 stk. 2 og den finske strafflag kapittel 33 § 6, er eksempler på at man kan innarbeide et alternativ i dokumentdefinisjonen som rammer elektroniske data.[285]

[284] SOU 1992:110 ”Information och den nya InformationsTeknologin – straff- och processretsliga frågor m.m.” Se side 273-275.

[285] Forlaget til ny § 171 stk 2 lyder: Ved et dokument forstås en skriftlig eller elektronisk med betegnelse af udstederen forsynet tilkendegivelse, der fremtræder som bestemt til at tjene som bevis.

10 Litteraturliste

10.1 Litteratur

Andenæs (1997) Andenæs, Johs. *Alminnelig strafferett*. 4. utg. Oslo 1997.

Andenæs (1996) Andenæs, Johs. *Formuesforbrytelsene*. 6. utg. Oslo 1996.

Andenæs I og II (1994) Andenæs, Johs. *Norsk straffeprosess*. Bind I og II. 2. utg. Oslo 1994.

Andenæs/Bratholm (1996) Andenæs, Johs. *Spesiell strafferett*. Johs. Andenæs og Anders Bratholm. 3. utg. Oslo 1996.

Andorsen (1991) Andorsen, Kjell. Bokanmeldelse i Juristkontakt nr 6 1991 side 69.

Andorsen (1992) Andorsen, Kjell. Strafferettslig samtykke. TfR 1992 s. 387-396.

Bing (1992) Bing, Jon. *Straffelovens definisjon av "trykt skrift" anvendt på datamaskinbaserte informasjonssystemer.* Vedlegg til NOU 1992:23 Ny straffelov. Alminnelige bestemmelser.

Bjerke/Keiserud (1996) Bjerke, Hans Christian og Keiserud, Erik. *Straffeprosessloven med kommentarer.* Bind I og II. 2. utg. Oslo 1996.

Bratholm/Matningsdal I (1995) Anders Bratholm og Magnus Matningsdal. *Straffeloven med kommentarer*. *Første del. Almindelige bestemmelser*. Oslo 1995.

Bratholm/Matningsdal II (1995) Anders Bratholm og Magnus Matningsdal. *Straffeloven med kommentarer*. *Anden del. Forbrydelser*. Oslo 1995.

Bratholm/Matningsdal III (1998) Anders Bratholm og Magnus Matningsdal. *Straffeloven med kommentarer*. *Tredje del. Forseelser*. Oslo 1995.

Brottsbalken kommentar (2000) *Brottsbalken. En kommentar. Del II.* Lena Holmqvist … [et.al]. Stockholm 2000.

Bryde Andersen (2001) Bryde Andersen, Mads. ”IT-retten”. København 2001.
(http://www.it-retten.dk)

Brydensholtutvalget (2002) *It-kriminalitet*. Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet. (betenkning nr 1417)

Datakriminalitet (1995) *Datakriminalitet*. Sverre Lilleng … [et al.]. Oslo, 1995. (ØKOKRIMs skriftserie nr 9)

Eckhoff/Helgesen (1997) Torstein Eckhoff og Jan E. Helgesen. *Rettskildelære*. 4.utg. Oslo 1997.

Enorge (2003) *e-norge*. Nasjonal strategi for informasjonssikkerhet.

Forsvars-, Nærings- og handels-, Justis- og politidepartementets dokument fra juni 2003.

Eskeland (2000) Eskeland, Ståle. *Strafferett*. Oslo 2000.

Hauge (1996) Hauge, Ragnar. *Straffens begrunnelser*. Oslo 1996.

Hov (1998) Hov, Jo. Avtaleinngåelse og ugyldighet. Oslo 1998.

Hov I (1999) Hov, Jo. *Rettergang. Sivil- og straffeprosess*. Bind I. Oslo 1999.

Hov II (1999) Hov, Jo. *Rettergang. Straffeprosess*. Bind II. Oslo 1999.

Hov III (2000) Hov, Jo. *Rettergang. Sivilprosess*. Bind III. Oslo 2000.

Kjerschow (1930) Kjerschow, Straffeloven med kommentarer. Oslo 1930.

Kronqvist (2003) Kronqvist, Stefan. *Brott och digitala bevis. En handledning*. Stockholm 2003.

Michelsen (1999) Michelsen, Hans M. *Sivilprosess*. Oslo 1999.

NOU 1999:26 Konvergens

NOU 2001:10 Uten penn og blekk

NOU 2002:4 Ny straffelov

NOU 2003:27 Lovtiltak mot datakriminalitet. Datakrimutvalgets delsinnstilling I.

Nærstad (1936) Nærstad, Henry. Om dokumentfalsk efter norsk rett. Oslo 1936.

OECD (1997) OECD. Rådets anbefalinger vedrørende retningslinjer for kryptopolitikk. Vedtatt 27.03.97.

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

Pfleger (1997) Pfleeger, Charles P. *Security in computing*. 2. utg. Upper Saddle River, USA 1997.

RITS (1998) Rådet for IT-sikkerhet (RITS). Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse. NHD. Oslo 1998.

Røstad (1993) Røstad, Helge. *Innkast i straffefeltet*. Oslo 1993.

Schjølberg (1982) Schjølberg, Stein. *Datamaskinassistert kriminalitet*. Oslo 1982.
Publisert i Nordiske kriminalkrønike 1982 s 9-21.

Schjølberg (1983) Schjølberg, Stein. *Computers and penal legislation*. Oslo 1983.

Schjølberg (1983A) Schjølberg, Stein. *EDB og kriminalitet*. Lov og rett 1983 side 467-487.

Selmer (1995) Selmer, Knut. *Hva er data?* Lov og rett 1995 s. 149-150.

Slettan/Øie (1997) Slettan, Svein. *Forbrytelse og straff*. Svein Slettan og Toril Marie Øye. Oslo 1997.

Stallings (1999) Stallings, William. Cryptography and network security. 2. utg. Upper Saddle River, USA 1999.

Telekommunikasjonsrett (2001) *Innføring i telekommunikasjonsrett*. Jon Bing … [et al.]. Oslo 2001.

Waaben (1994) Waaben, Knud. *Strafferettens specielle del.* 4.utg. København 1994.

Westman (2003) Westman, Daniel. *Digitala urkunder?* Lov&Data nr. 73, mars 2003

10.2 Forarbeider

Ot.prp.nr. 12 1889

SKM 1896 Straffelovkommisjonens utredning av 1896.

Forh.O. (1901-02)

Indst.O. I (1901-02)

NOU 1985:31 Datakriminalitet.

Ot.prp.nr 35 (1986-87) Om endringer i straffeloven (datakriminalitet).

Inst.O.nr 65 (1986-87) Innstilling fra justiskomiteen om endringer i straffeloven (datakriminalitet).

10.3 Domsregister

Rt. 1900 s. 65

Rt. 1919 s. 525

Rt. 1922 s. 542

Rt. 1930 s. 1005

Rt. 1930 s. 1301

Rt. 1931 s. 603

Rt. 1931 s. 605

Rt. 1935 s. 573

Rt. 1936 s. 459

Rt. 1937 s. 541

Rt. 1940 s. 40

Rt. 1949 s. 678

Rt. 1953 s. 204

Rt. 1961 s. 611

Rt. 1966 s. 1375

Rt. 1968 s. 774

Rt. 1977 s. 457

Rt. 1978 s. 337

Rt. 1983 s. 451

Rt. 1987 s. 650

Rt. 1989 s. 980

Rt. 1991 s. 532 (Bankenes betalingssentral-dommen)

Rt. 1992 s. 790

Rt. 1994 s. 1610

Rt. 1995 s. 1872

Rt. 1998 s. 217

Østre Landsret, Danmark. Dom 26.09.01 saksnummer 5. Lov&Data nr. 68, desember 2001.

Svea hovrätt, Sverige. Dom 31.05.02 saksnummer B 5358-01. Lov&Data nr. 73 2003.

10.4 Konvensjoner

Convention on cybercrime. Budapest, 23.11.01.

http://conventions.coe.int/

Norsk tittel: Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi. Med den forklarende rapporten.