Automatisert inndragning

Inger Marie Sunde
Oslo, mars 2010

Forord

Atten år etter endt studietid var jeg svært spent på hvordan det ville bli å komme tilbake til universitetet. Det har vært en flott opplevelse. Jeg takker professor *Jon Bing* som inspirerte meg til å begynne som stipendiat, og IoR som etter hvert tok meg under sine vinger. Jeg takker for tilliten jeg er blitt vist gjennom finansieringen fra Justisdepartementet, Økokrim og UiO. Og jeg takker for hjelpen jeg fikk gjennom phd-programmet til "å akademisere tanken". Tiden ved juridisk fakultet har vært meget inspirerende og gitt meg gode kår for arbeidet.

Jeg står i gjeld til noen spesielle personer. Det er særlig min oppmuntrende, humørfylte og skarpe veileder professor *Ragnhild Helene Hennum*, og den støttende biveileder førsteamanuensis *Lee Bygrave*. Dr.ing. *Svein Willassen* har hjulpet meg med råd og kritikk til arbeidets tekniske sider, både om selve teknologien og de policyvalg som den byr på (det som i jussen kalles rettspolitiske hensyn). Uten denne støtten hadde jeg ikke fått det til. Og selvsagt: Eventuelle feil og alle meninger som arbeidet inneholder, står utelukkende for min egen regning. Selv om hjelpen har vært upåklagelig er det alltid mulig å misforstå, eller å utnytte et poeng på en annen måte en rådgiveren har forutsatt.

Videre takker jeg student *Benita Tjørn* for munter bistand til utarbeidelse av register, kildekontroll og korrekturlesning. Og takk til stipendiatkollega *Thomas Frøberg* som ga meg svært verdifulle råd, om enn på et sent tidspunkt i arbeidet. Jeg skulle spurt før.

Bibliotektjenesten har imponert meg. De elektroniske informasjonssystemene likeså. Problemet med å finne frem til publikasjonene lettes ved svært kyndig hjelp fra staben. Stor takk til dere! Administrasjon og ledelse ved institutt og fakultet har også på alle måter vært behjelpelige. Jeg anbefaler helhjertet et opphold ved "institusjonen".

Jeg takker også kolleger ved fakultetet, vi er flere som har strevet sammen. Jeg opplever at det har hersket en felles opplevelse av at når alt kommer til alt, er man svært alene om et stort prosjekt, hvor det skal treffes avgjørende valg med de største konsekvenser, både hva gjelder muligheten for å fullføre og det på en god måte. Miljøet har vært vennlig og støttende, noe jeg har ønsket å bidra til.

Til slutt går en varm hilsen til familien og mange gode venner, som har kommet med oppmuntrende tilrop og alltid virket forunderlig skråsikre på at dette nok kom til å gå bra. En ekstra stor takk går til mor og far, som til tross for skrantende helse har gjort hva de kan for å hjelpe, til min søster *Randi* med familie, og til mine humørfylte barn *Ingrid* og *Finn Bendik* som med en stor tro på mor aldri lot det være tvil om at prosjektet måtte fullføres!

Bekkestua 22. mars 2010
Inger Marie Sunde

Tilegnet Ingrid og Finn Bendik

Innholdsoversikt

I Innføring i emnet

1 Tema, formål, metode

1.1 Tema

Avhandlingen behandler inndragning av datafiler med rettsstridig innhold. Foranledningen til valg av tema er problemet med rettsstridig innhold på nettet, og jeg konsentrerer meg om inndragning av overgrepsbilder og skadelig dataprogram. Jeg skal undersøke om de bestemmelsene i straffeloven 2005 som hjemler inndragning av "ting", kan anvendes for å inndra datafiler og gjennomføre inndragningen i nettet ved bruk av filtrering. Med 'filtrering' mener jeg en teknisk løsning som "gjenkjenner" og blokkerer de inndratte filene slik at anskaffelse og tilgjengeliggjøring hindres. Filtreringen må utføres automatisk, så i nettet er det tale om *automatisert inndragning.*

Med 'overgrepsbilder' mener jeg innhold som rammes av legaldefinisjonen i strl. 2005 § 311 bokstav a, dvs. "fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn". Strl. 2005 § 311 første ledd lyder:

> "Med bot eller fengsel inntil 3 år straffes den som
> a) produserer fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn,
> b) utgir, tilbyr, selger, overlater til en annen, gjør tilgjengelig eller på annen måte søker å utbre fremstillinger som nevnt i bokstav a,
> c) anskaffer, innfører eller besitter fremstillinger som nevnt i bokstav a, eller forsettlig skaffer seg tilgang til slikt materiale,
> d) holder offentlig foredrag eller istandbringer offentlig forestilling eller utstilling av fremstillinger som nevnt i bokstav a." [1]

Jeg behandler bare visuelle fremstillinger, dvs. bilder (herunder film). Legaldefinisjonen omfatter også tekstlige ytringer, tegneserier og animasjoner, men jeg avgrenser til reelle overgrepsbilder som er det alvorligste problemet.[2]

---

[1] Den korresponderende bestemmelsen i strl. 1902 § 204 a lyder: "Den som
a) produserer, anskaffer, innfører, besitter, overlater til en annen eller mot vederlag eller planmessig gjør seg kjent med fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn,
b) befatter seg med fremstillinger av seksuelle overgrep mot barn eller fremstillinger som seksualiserer barn, på annen måte som nevnt i § 204 første ledd."

[2] Legaldefinisjonen for barnepornografi var frem til innføringen av strl. 1902 § 204a (endret ved lov nr. 29/2005), begrenset til visuelle fremstillinger. Det fremgikk av formuleringen "kjønnslige skildringer i rørlige og

Det er vanlig å betegne materialet som 'barnepornografi', men jeg velger istedet betegnelsen 'overgrepsbilder'. Legaldefinisjonen i bokstav a er todelt. 'Overgrepsbilde' er klart dekkende for den første delen som forutsetter at bildet viser et seksuelt overgrep (jf. "fremstilling av seksuelle overgrep mot barn"). Legaldefinisjonens siste del omfatter bilder hvor barnet er avbildet i en positur eller kontekst som gir seksuelle assosiasjoner (jf. "fremstilling som seksualiserer barn"). I den sammenheng får betegnelsen 'overgrepsbilder' frem at bildet er en krenkelse - et overgrep - overfor barnets personvern.[3] 'Overgrepsbilder' gir derfor en dekkende beskrivelse av problemets og materialets karakter.[4]

'Skadelig dataprogram' kan benyttes til å begå krenkelser mot data og datasystemer, for eksempel datainnbrudd, dataskadeverk, ulovlig avlytting og kopiering av datatrafikk. Da er programmet et middel til å begå en overtredelse av blant annet strl. 1902 § 145 annet ledd, § 291, § 145 a og § 262, smlg. de korresponderende bestemmelser om datakriminalitet i straffeloven 2005 kapittel 21 "Vern av informasjon og informasjonsutveksling" §§ 203-206.[5]

---

urørlige bilder hvor det gjøres bruk av barn", jf. strl. 1902 § 204 første ledd bokstav d. Departementet foreslo videreføring av definisjonen i forbindelse med at forbudet ble skilt ut fra den alminnelige pornografibestemmelsen til en egen bestemmelse i strl. § 204a, jf. Ot.prp. nr. 37 (2004-2005) s. 5 og 6. Justiskomiteen endret imidlertid legaldefinisjonen til "fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn", og uttalte at "fremstilling" var ment også å ramme tekst, se Innst. O. nr. 66 (2004-2005) s. 2-4. At tegnefilm kan være rettsstridig pornografi ble fastslått av Høyesterett i Rt. 1984 s. 1016, i en sak som gjaldt «Snowwhite and the seven lovers», "en tegnefilm av ca ti minutters varighet". Av nyere praksis kan det vises til LB-2008-18408 (Borgarting) som gjaldt besittelse av ca. 9000 overgrepsbilder lastet ned fra internett. Det fremgår at en del av det rettsstridige materialet besto av "tegneseriebilder og såkalte magna (sic), dvs. animasjoner". I sitatet er nok "magna" feilstaving for "manga", som er japanske tegneserier og animasjoner. Både datakrimkonvensjonen (185 ETS) art. 9.2.c og konvensjonen om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk (201 ETS) art. 20.2, lar begrepet barnepornografi omfatte visuelle fremstillinger med simulerte aktiviteter.

[3] I Justiskomiteen ble det fremholdt at også de såkalte poseringsbildene representerte krenkelser overfor barna, se Innst. O. nr. 66 (2004-2005) s. 2-4 hvor det blant annet står: "Selv i tilfeller der fremstillingen viser barn som ikke er utsatt for seksuelt misbruk på bildet, er selve poseringen og eksponeringen krenkende for den enkelte." (s. 3).

[4] Bruk av begrepet "barnepornografi" har vært kritisert for å tilsløre og dermed ha en viss legitimerende effekt for de overgrep som produksjon og bruk av materialet representerer. EUs "Safer Internet Program" er meget tydelig i sin anbefaling om å opphøre med bruken av ordet "barnepornografi", se www.circamp.eu. Her står følgende: "Circamp and other Law Enforcement agencies believe it is time to stop the use of the misleading term "Child Pornography" when describing images of sexual abuse of children, and use a term or title that gives a better understanding of the crime and more respect to the child victims … Law Enforcement should always try to describe the crime accurately and enforce this message to others working in this area as well as Media." Se mer om Circamp til slutt i kapittel 14.4. Justiskomiteen understreket også det uheldige i å bruke "barnepornografi", og omtalte selv materialet som "overgrepsbilder". Komiteen ønsket at "selve lovteksten bedre må få frem at man her taler om dokumentasjon på overgrep mot barn.", se Innst. O. nr. 66 (2004-2005) s. 2-4. Departementet gir uttrykk for et tilsvarende syn i Ot.prp. nr. 37 (2004-2005), s. 5 og 6, se særlig sitat fra *Redd Barnas* høringsuttalelse på s. 5. Se også *Sunde* (2006) kapittel 8.1.1 s. 218 og *Walden* (2007) s. 138.

[5] Dataskadeverk kan etter omstendighetene rammes både av strl. 2005 § 206 (fare for driftshindring), og § 351 annet ledd (skadeverk). Strl. 2005 § 351 er i utgangspunktet ikke dataspesifikk og er plassert i strl. 2005 kapittel 28 "Skadeverk og fremkalling av fare for allmennheten". Men lovgiver har tilføyd et annet ledd som gjelder krenkelser av "andres data".

Noen populære betegnelser på skadelig dataprogram er ”hackerverktøy”, ”datavirus”, ”orm”, ”trojaner”, ”exploits” og ”malware”.

Med straffeloven 2005 gjøres selve befatningen med skadelig dataprogram straffbar, forutsatt at det skjer ”med forsett om å begå en straffbar handling”. Dette følger av strl. 2005 § 201 bokstav b. Hele bestemmelsen lyder slik:

> ”Med bot eller fengsel inntil 1 år straffes den som med forsett om å begå en straffbar handling uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen
>
> a) passord eller andre opplysninger som kan gi tilgang til databasert informasjon eller datasystem, eller
>
> b) dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem. På samme måte straffes den som uten forsett om å begå en straffbar handling besitter et selvspredende dataprogram, og besittelsen skyldes uberettiget fremstilling eller anskaffelse av programmet.”[6]

Programmet som omfattes av strl. 2005 § 201 må være ”særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem”. Det kan for eksempel være slike handlinger som nevnt over.

Etter den objektive gjerningsbeskrivelsen er befatning med overgrepsbilder og skadelig dataprogram langt på vei likestilt, ved at det gjøres straffbart å *produsere, besitte, anskaffe og tilgjengeliggjøre* begge former for innhold. Likhetene i den strafferettslige regulering og det faktum at både overgrepsbilder og skadelig dataprogram representerer alvorlige og utbredte *innholdsproblemer* i elektroniske nettverk, er årsaken til at jeg har foretatt en felles behandling av inndragningsspørsmålene.

Hovedspørsmålet er å kartlegge om datafilene med det rettsstridige innholdet kan være selvstendige objekter for inndragning, slik at man kan tale om *datainndragning* i ren form.

[6] Strl. 2005 § 201 representerer en reservasjonsløs gjennomføring av datakrimkonvensjonen art. 6, se Ot. prp. nr. 22 (2008-2009) kapittel 1 s. 12. Etter straffeloven 1902 er konvensjonsforpliktelsen gjennomført med reservasjon mot skadelig dataprogram, jf. strl. 1902 § 145b, som bare rammer uberettiget tilgjengliggjøring av ” passord eller andre data som kan gi tilgang til et datasystem”. Det finnes noen andre bestemmelser som innenfor saklig avgrensede områder svarer til strl. 2005 § 201. Den ene er strl. 1902 § 262 første ledd som avløses av strl. 2005 § 203 første ledd (uberettiget tilgang til fjernsynssignaler mv). Den andre er åvl. § 53a annet ledd og § 53c, jf. § 54 (omgåelse av tekniske beskyttelsessystemer). Forholdet mellom bestemmelsene reiser noen harmoniseringsspørsmål som er kommentert, men ikke løst ved arbeidet med straffeloven 2005, se Ot.prp. nr 22 (2008-2009) kapittel 2.6 s. 25 flg. Se også NOU 2007: 2 s. 55; Ot.prp. nr. 46 (2004-2005) (endringer i åndsverkloven) kapittel 3.5.1.3.3 s. 112 flg., og *Sunde* (2005) s. 161 flg., og (2006) kapittel 5.6. s. 168 flg.

Jeg ser problemstillingen som et utslag av den store utviklingen med hensyn til tjenestetilbud, kapasitet og global utbredelse innen informasjons- og kommunikasjonsteknologien ("IKT"). De elektroniske omgivelsene formes og endres av mennesker, noe som i et strafferettslig perspektiv reiser muligheten for å anvende inndragning i det elektroniske nettet. Det betinger at datafilen er en "ting" som kan inndras, jf. strl. 2005 §§ 69 flg.

Temavalget skyldes at jeg begynte å fundere på om man kunne bruke såkalt "antivirusteknologi" mot overgrepsbilder. Når tanken først var tenkt, var veien kort til å vurdere muligheten for automatisert inndragning i nettet.

Jeg mener det er interessant både å drøfte overgrepsbilder og skadelig dataprogram. En årsak er den nevnte likheten i utformingen av straffebudene, jf. strl. 2005 §§ 201 og 311. I tillegg vet man at det finnes velprøvd teknologi mot skadelig dataprogram i nettet, som man kan tenke seg utnyttet for inndragning. Siden teknologien virker mot skadelig dataprogram virker den også mot overgrepsbilder. En datafil er en datafil og teknologien er blind for innholdet.[7] Siden innholdstypene er forskjellige, bidrar parallellbehandlingen til å behandle et ganske bredt sett med spørsmål i den strafferettslige tilnærmingen til inndragning av rettsstridige data.

Skjematisk fremstilt tenker jeg meg at inndragningen kan følge opplegget beskrevet nedenfor, og det er denne fremgangsmåten jeg har lagt til grunn gjennom hele avhandlingen:

Trinn 1: Det er tatt databeslag med overgrepsbilder eller skadelig dataprogram i en straffesak. I forbindelse med pådømmelsen av saken inndras de rettsstridige filene med hjemmel i reglene om inndragning av "ting". I tillegg treffes beslutning om inndragning av dublettene (kopiene) til de datafilene som er inndratt i straffesaken. Beslutningen om å inndra dublettene treffes uten at noen er gjort til saksøkt.

Trinn 2: De inndratte filene legges i en referansedatabase ("RDB"). Hver datafil er *unikt identifisert* med *sjekksum*.[8] Når datafilen er lagt i RDB er den "svartelistet".

[7] Jf. kapittel 2.3.4.
[8] Sjekksum er forklart i kapittel 3.3.3.

Trinn 3: Inndragning av datafiler med samme sjekksum som de "svartelistede" filene, fullbyrdes automatisk i nettet. Filene i nettet er *dubletter* i forhold til de "svartelistede" datafilene i RDB.

Fremgangsmåten utelukker automatisert inndragning av filer som ikke på forhånd er bedømt som rettsstridige og inndratt i en straffesak. Automatisert inndragning er *reaktiv filtrering* som rammer dubletter som sirkulerer på nettet. Tiltaket kan ikke rettes mot førstegangsspredning av innhold.[9] RDB, som er grunnlaget for den automatiserte inndragningen, bygges opp under judisiell kontroll. Fullbyrdingen av inndragningen i nettet retter seg dermed bare mot filer hvor innholdets rettsstrid er konstatert på betryggende måte.

Kort om rettsspørsmålene:

Inndragningen forutsetter at de rettsstridige filene er "ting" strafferettslig sett. Videre må dublettene kunne inndras uten at noen er gjort til saksøkt og uten at de først er tatt i beslag. Den automatiserte inndragningen i nettet, er basert på at filene som avdekkes er identiske med de som finnes i RDB, dvs. at de er dubletter. Det reiser spørsmål om grunnlaget for å gi den opprinnelige inndragningsbeslutningen i trinn 1, rettsvirkning for dublettene i nettet. Til sist oppstår det spørsmål om vernet om privatlivet og ytringsfriheten setter skranker for fullbyrdingen i nettet.

1.2 Nærmere om problemstillingen

Avhandlingen analyserer rettstilstanden *de lege lata.* Automatisert inndragning må imidlertid skje ved filtrering i nettet. Det gir foranledning til en kommentar til behandlingen av Datakrimutvalgets filtreringsforslag i datakrimutredningen fra 2007.[10] Et mindretall i utvalget foreslo å innføre filtrering av utenlandske nettsteder som drev virksomhet som er ulovlig i

[9] Førstegangsspredning kan her forstås å omfatte to tilfeller. Det ene er førstegangs tilgjengeliggjøring i nettet av data man har lagret på sin datamaskin. Det skaper dubletter i nettet. Det andre tilfellet er sanntidsoverføring, av bilder ved bruk av web-kamera. Det skaper ikke i seg selv en dublett fordi innholdet ikke som utgangspunktet er lagret. Selve konseptet "dublett" forutsetter en lagret kildefil som fungerer som kopieringsgrunnlag for dublettene.

[10] NOU 2007: 2. Filtreringsforslaget er beskrevet i kapittel 5.13 s. 120 flg.

Norge, og mente at en ny bestemmelse om dette burde "… være så lik reglene om inndragning som mulig...".[11]

Departementet forholdt seg til en sondring mellom filtrering "på nasjonalt nivå" og "på tilbydernivå", og sa at filtrering på nasjonalt nivå ikke under noen omstendighet var aktuelt i Norge. Med filtrering "på tilbydernivå" mente departementet

> "… at de enkelte internettleverandørene blir pålagt å filtrere bestemte internettsteder gjennom å blokkere tilgangen for norske brukere."[12]

Det var altså tale om eventuelt å innføre en lovpålagt plikt for tilbyderne til å blokkere tilgangen til bestemte nettsteder som er "svartelistet". I vurderingen av om tilbyderne bør pålegges en slik filtreringsplikt innledet departementet med å vise til at det "… er knyttet store utfordringer til den tekniske gjennomføringen av en slik ordning."[13] Det ble vist til risikoen for at filteret kan stanse legitim trafikk, noe som reiser spørsmål i forhold til ytringsfriheten. Hvordan denne risikoen eventuelt skulle håndteres ble ikke kommentert, men departementet antok at

> "… selv om legitim trafikk også kan stanses ved en avtalebasert filtreringsordning, er betenkelighetene ved en slik løsning vesentlig mindre enn ved lovpålagt filtrering."[14]

Departementet påpekte at behovet for filtrering er størst i forhold til "... nettsider som tilbyr seksualiserte skildringer av barn…", og at det var innført en frivillig filtreringsordning for å blokkere for slike nettsteder.[15] Det ble vist til den såkalte "Faremo-rapporten", som

[11] NOU 2007: 2 kapittel 5.13, sitat fra s. 123. Forslaget gikk ut på at filtreringsbestemmelse skulle inntas i strl. 2005 § 76b og lød som følger "Tjenesteyter kan pålegges å blokkerer tilgangen til bestemte steder på internett for sine brukere dersom innholdet ville kunne medføre straffansvar utover bøter i Norge. § 69 tredje ledd og § 76a gjelder tilsvarende. De øvrige regler om inndragning gjelder tilsvarende så langt de passer." (s. 124).
[12] Ot.prp. nr. 22 (2008-2009) kapittel 2.18 s. 70. Det er uklart hva som menes med filtrering "på nasjonalt nivå". Dersom myndighetene tar rollen som tilbyder av elektronisk kommunikasjonsnett og -tjenester, kan myndighetene selv direkte foreta filtrering. Av mange grunner er dette er neppe et aktuelt scenario. Dermed er situasjonen at filtrering må skje med assistanse fra tilbyder. Det gjelder enten sluttbrukeren ønsker beskyttelse inn til sin datamaskin (avtalebasert filtrering), om tilbyder filtrerer skadelig dataprogram og spam som ledd i tilbudet av en sikker tjeneste, eller om *myndighetene* har behov for filtrering som ledd i rettshåndhevelsen. Det har ikke betydning om filtreringen retter seg mot nettsteder i inn- eller utland, uansett må filtreringen skje med assistanse fra tilbyder. Jeg kommer tilbake til dette temaet i kapittel 13.1.
[13] Ot.prp. nr. 22 (2008-2009) s. 71.
[14] Ot.prp. nr. 22 (2008-2009) s. 71.
[15] Ot.prp. nr. 22 (2008-2009) s. 71.

> "… styrker departementet i synet på at en frivillig løsning er å foretrekke. En slik løsning er også best i samsvar med prinsippene for bruk av straff som ligger til grunn for straffeloven 2005."[16]

Den frivillige filtreringsordningen som departementet viser til, er det som kalles "Kripos-filteret". Filtreringen gjelder *nettsteder*, noe som skiller seg vesentlig fra filtrering av *datafiler* som er objektene for automatisert inndragning. Filtrering av datafiler er mer presist, og har mindre konsekvenser for ytringsfriheten enn filtrering av nettsteder.[17] Hvorfor en frivillig filtreringsordning skulle være mer forenlig med ytringsfriheten, enn pliktig filtrering utført som ledd i rettshåndhevelsen, ble ikke begrunnet i redegjørelsen nevnt over. Kripos-filteret har imidlertid det til felles med den filtrering som avhandlingen behandler, at det er tale om gjennomføring via tilbyderne ("på tilbydernivå"). Avhandlingens filtreringssystem forutsettes imidlertid å følge av en lovpålagt plikt, ikke en frivillig ordning.

I lys av at filtrering reiser komplekse spørsmål både av rettslig og faktisk art, må den behandlingen som ble utført av Datakrimutvalget og departementet anses å være nokså kortfattet. I Norge hvor ytringsfriheten holdes høyt, er det ikke overraskende at man er opptatt av betenkelighetene ved filtrering, som på den annen side må holdes opp imot tydelige politiske signaler om behovet for effektive tiltak, om nødvendig filtrering, for å bekjempe problemet med overgrepsbilder.

Avhandlingens drøftelser springer dermed ut av følgende problemstillinger:

En problemstilling er om data som selvstendig objekt kan være gjenstand for inndragning, hvilke rettslige betingelser som da gjelder, og hvilke rettsvirkninger som følger av inndragningen. Problemstillingen innebærer en avgrensning mot *den fysiske bæreren*, dvs. datanettet og lagringsenheter som harddisk, minnepinne og CD-ROM. Fysiske bærere er klart "ting", jf. vanlig strafferettslig begrepsbruk, og synes ikke å reise nye spørsmål om

[16] Ot.prp. nr. 22 (2008-2009) s. 71. "Faremo-rapporten" er en arbeidsgrupperapport avgitt av Faremo-utvalget 30. januar 2007 til Justisdepartementet, med tittel "Forebygging av internettrelaterte overgrep mot barn". Her omtales "norsk filterteknologi" (s. 3) og "en frivillig sperreordning" (Faremo-rapporten (2007) s. 17 pkt. 5.1.2). Sperreordningen er det såkalte "Kripos-filteret". Arbeidsgruppen skriver om filteret at: "Politiets rolle i prosjektet er av mange fremhevet som en viktig årsak til at filteret har oppnådd en høy grad av troverdighet, og internettleverandørene unngår påstander om sensur." (s. 22 pkt. 6.3.2).

[17] Dette behandler jeg som *presisjonsproblemet*, i en drøftelse av automatisert filtrering i forhold til EMK art. 8 og 10, se del VI og kapittel 14.

inndragning. Videre innebærer det en avgrensning mot det innholdet dataene bærer. Innholdet kan som sådan ikke inndras, men følger med dersom mediet (data) inndras.[18]

Konseptualiseringen av data som selvstendig objekt synes å representere en ny strafferettslig tilnærming, i den forstand at det trekkes rettslige konsekvenser av at data anses som "ting", nærmest på linje med fysiske objekter. Det finnes bare svært knappe beskrivelser av hva som menes med 'data' i strafferettslige lovforarbeider og teori, og det fremstår som noe uklart i hvilken grad man har vurdert data uavhengig av den fysiske bæreren og meningsinnholdet. Her tar avhandlingen sikte på å foreta en avklaring av gjeldende rett.

En annen problemstilling tar utgangspunkt i at IKT har iboende funksjonalitet for å lage identiske kopier av data.[19] Kopiering av datafiler over nett er ressursdeling hvor kildefilen beholdes intakt samtidig som den kan kopieres i et ubestemt antall identiske instanser. Delingen leder til at det blir *mer* identiske data, ikke mindre slik som ved deling av fysiske goder, noe som er et problem når datafilene har rettsstridig innhold.[20] Delingsevnen innebærer at data kan anses som et *ikke-rivaliserende* gode. Kopiene er *dubletter* sett i forhold til den opprinnelige filen (kildefilen) og i forhold til hverandre. Dublettene er *identiske* uavhengig av når og hvor de forekommer, og påvirkes ikke av generasjonstilhørighet, dvs. om de er kopier av hverandre eller av den opprinnelige filen.

Et hovedspørsmål er om inndragning av en rettsstridig datafil har rettsvirkning for alle dublettene, og hva grunnlaget i så fall er. Den automatiserte inndragningen forutsetter dette, fordi det ligger i selve automatiseringen at det ikke skal foretas en menneskelig vurdering av hver dublett. Jeg ser derfor automatisert inndragning som fullbyrding av en inndragningsbeslutning som omfatter dublettene. Et mulig grunnlag er å anse dublettene som eksemplarer med samme serienummer (dataidentitet) som kan inndras under ett. En annen mulighet er at den inndratte datafilen i straffesaken og dublettene i nettet anses å være deler av ett og samme fenomen, som inndras under ett.

[18] Innholdet kan være meningsinnhold beregnet på et menneske, eller innhold beregnet på en datamaskin, og da er det tale om et dataprogram. I det første tilfellet utløses kognitive prosesser, og i det andre tilfellet operasjoner på en datamaskin. Det er mediet (data) som kan inndras, ikke de kognitive eller automatiske prosessene. Dette er nærmere beskrevet i kapittel 2.
[19] Dette er forklart i kapittel 3.3.4.
[20] Det kan være et problem i annen sammenheng også, jf. problemet med pirateri av opphavsrettslig vernet materiale på internett. Delingen krenker rettighetshaverens økonomiske interesser, men innholdet (musikk, film og programvare) er selvsagt ikke rettsstridig.

Dublettene representerer et tilbakevendende tema gjennom avhandlingen, særlig i forhold til rettsregler om "produksjon" og "besittelse". *Blir* det mer dersom man fremstiller dubletter, og *har* man mer dersom man besitter flere like filer? Dette har betydning for fortolkningen av produksjons- og besittelsesalternativene i straffebudene og i inndragningsreglene. Temaet har også betydning for å identifisere et rettsgrunnlag for inndragning av dublettene i nettet.

På et nivå er avhandlingen en rettslig analyse av inndragningsreglene med tanke på å utøve rettshåndhevelse overfor alvorlige innholdsproblemer på nettet. På et annet nivå bidrar drøftelsene til å avklare viktige begreper for analyse av praktiske strafferettslige spørsmål i tilknytning til internett.

1.3 Avgrensning

Jeg avgrenser mot spørsmål om personlig straffansvar, som bare behandles i den utstrekning det har betydning for inndragningsspørsmålene. Jeg begrenser meg også til å behandle inndragning med hjemmel i straffeloven i relasjon til skadelig dataprogram og overgrepsbilder. Jeg kommer derfor ikke inn på et praktisk spørsmål som det omfattende pirateriet av opphavsrettslig vernet materiale på internett. Opphavsretten er et komplisert rettighetsregime med mange interessenter, og åndsverkloven har en egen inndragningshjemmel, jf. åvl. § 56. Det utelukker ikke bruk også av straffelovens inndragningsregler, men jeg har altså ikke gått inn på en analyse av forholdet mellom disse bestemmelsene.

1.4 Om metode og enkelte andre forhold

I avhandlingen har jeg brukt såkalt vanlig juridisk metode for å fastlegge gjeldende rett, og holdt meg til *Eckhoffs* rettskildelære.[21] Videre har jeg gjort noen valg som preger oppbygningen av drøftelsene. Det viktigste grepet har vært å anvende rettsinformatikkens innsikter som metodisk grunnlag for de strafferettslige drøftelsene. Det viser seg særlig i arbeidet med begrepsdannelsen. Det har også medført at jeg har tatt i bruk en analytisk modell som beskrevet i kapittel 2.1.

[21] *Eckhoff* (2001).

Jeg står i stor gjeld til det sterke nordiske fagmiljøet innen rettsinformatikken. Miljøet ved SERI (Senter for rettsinformatikk) ved det juridiske fakultetet i Oslo, har vært til stor inspirasjon, og likeså mye av produksjonen i dansk teori de senere år. Innen svensk teori har jeg særlig holdt meg til *Seipels* "Juridik och IT" (2004). For så vidt gjelder rent tekniske opplysninger, har jeg holdt meg til teknisk litteratur som er vanlig brukt innen etterforsking og analyse av elektroniske spor.

Siden temaet ligger i krysningsfeltet mellom rettsinformatikk, strafferett og teknologi, har jeg i større grad enn det som kanskje er vanlig ved avhandlingsarbeid, vært henvist til bruk av sekundærkilder. Det er jo ikke mulig å være ekspert på alle områder, og det er bare innenfor den egentlige strafferettslige behandlingen at jeg har gått nøye inn på norske primærkilder.

Jeg har også trukket inn noe utenlandsk teori, mest tysk og amerikansk, men ikke lagt opp til noen komparativ analyse, fordi jeg ikke kjenner til at inndragningsregler er anvendt som grunnlag for filtrering i nettet i rettssystemer som det kunne være naturlig å se hen til.

I det hele tatt har jeg ikke sett at filtrering av datafiler basert på "antivirusteknologi" har vært behandlet i arbeider om internettfiltrering. Jeg har lest to grundige arbeider om filtrering som behandler forskjellige metoder, fordeler og ulemper, samt hvordan de kan (mis)brukes for å demme opp for bestemte ytringer. Det er tale om studiene som er inntatt i antologien *Access Denied*, utgitt av *Open Net Initiative* i 2008.[22] *Open Net Initiative* er et samarbeidsprosjekt mellom universitetene i Toronto (Canada), Cambridge og Oxford (UK) og Harvard (USA).[23] Den andre studien er laget ved *Max Planck Insitute* (Freiburg, Tyskland) og heter "Sperrverfügungen im Internet".[24] Ingen av studiene behandler den filtreringstypen jeg legger til grunn at kan anvendes med tanke på inndragning i nettet.

Uansett har man i mange rettssystemer støtt på et vell av nokså likeartede spørsmål som følge av den raske utbredelsen av internett og den mobile kommunikasjonsteknologien. Diskusjoner om de samme problemer føres derfor i mange land og bidrar til at vi kan se på norsk rett med nytt blikk. I norsk tradisjon med utforming av generelle regler som skal tåle tidens tann, er vi åpne for at en eldre regel kan komme til anvendelse på et fenomen av nyere dato. I dette

[22] *Deibert* (2008).
[23] Prosjektet har et nettsted hvor formålet er beskrevet slik: "to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion." Se http://opennet.net.
[24] *Sieber* (2008).

ligger en rettslig dynamikk som åpner for inntak av argumenter fra utenlandske rettskilder, selv om de ikke er bindende for norsk rett. Rettskildemessig får de, som andre fornuftige argumenter som ikke har formell forankring i lovtekst, forarbeider eller rettspraksis, status som en type reelle hensyn.

Det har ikke budt på særskilte rettslige problemer at drøftelsene føres opp mot en lov som teknisk sett er ny, nemlig straffeloven 2005. Det mangler selvfølgelig rettspraksis med utgangspunkt i den nye loven, men likevel er ikke situasjonen direkte kildefattig. For det første har jeg selvsagt forarbeidene til den nye loven å holde meg til. To lovproposisjoner har jeg brukt mye: Det er Ot.prp. nr. 90 (2003-2004) som behandler inndragningsreglene, samt det strafferettslige gjenstandsbegrepet og forholdet til data. Den andre er Ot. prp. nr. 22 (2008-2009) som behandler straffebestemmelsene i lovens spesielle del, herunder reglene om datakriminalitet og om overgrepsbilder m.v..

For det andre viderefører straffeloven 2005 i hovedsak de ordninger som følger av straffeloven 1902 for så vidt gjelder inndragning, og representerer i så måte tradisjonen. Rettspraksis og andre rettskilder i tilknytning til straffeloven 1902 er således fremdeles relevante.

Teamet har reist det såkalte "beskrivelsesproblemet" som *Andersen* har fremhevet som særlig utfordrende for "IT-retten".[25] De rettslige drøftelsene er knyttet til forutsetninger om hva data er i rent faktisk forstand, og om egenskaper ved teknologien som kan brukes til å kontrollere dublettene ved filtrering. Jeg har løst beskrivelsesproblemet ved legge inn to "transportetapper" som vesentlig er viet faktiske beskrivelser, nemlig én om data som faktisk fenomen (kapittel 3) og én om presisjonsproblemet ved filtrering (kapittel 14). Ytterligere et kapittel av mer generell art, gjelder *teknologinøytralitet.* Jeg har hatt behov for å kartlegge hva hensynet går ut på og hvordan det gjør seg gjeldende i fortolkningen (kapittel 6.3-6.4)

Til slutt bør jeg antakelig si noe om min bakgrunn, som nødvendigvis har gitt meg en forforståelse som har influert på arbeidet. Jeg har vært førstestatsadvokat og leder av Politiets datakrimsenter ved ØKOKRIM, hvor jeg arbeidet mye med overgrepsbilder og såkalte "hacker saker". Dessuten har jeg vært medlem av Datakrimutvalget 1 som leverte utredningen

[25] *Andersen* (2005) s. 99 flg. Jeg kommer tilbake til beskrivelsesproblemet i kapittel 3.2.

NOU 2003: 27 *Lovtiltak mot datakriminalitet – delutredning I*, og sekretær for Datakrimutvalget 2, som leverte utredningen NOU 2007: 2 *Lovtiltak mot datakriminalitet – delutredning II*. Jeg har også aktorert eller hatt påtaleansvar for noen av sakene som er nevnt i avhandlingen. Det er bare Rt. 2002 s. 1187 (straffutmåling for besittelse av overgrepsbilder) som er verdt å nevne her, fordi det var den første høyesterettsavgjørelsen vedrørende overgrepsbilder fra internett, og Høyesterett understreket at dublettene som verserer på nettet representerer "en livsvarig krenkelse" av barnet på bildet. Etter mitt syn er det vesentlig for problemforståelsen og har konsekvenser for den rettslige tilnærmingen til dublettene. Til slutt kan jeg nevne at jeg har skrevet boken "Lov og rett i cyberspace", som kom ut i 2006. I bokens kapittel 4 drøftet jeg det strafferettslige gjenstandsbegrepet i forhold til data. Det er et tema som jeg har utviklet i avhandlingen.

1.5 Oversikt over avhandlingen

Avhandlingen består av syv deler I-VII som er lagt opp på følgende måte:

Del II (kapittel 2-4) er viet begrepsbruken, det teoretiske og faktiske grunnlaget, samt noen rettslige karakteristikker av *innholdet* i data, som er nødvendige for de senere drøftelsene. Her beskrives også analysemodellen som avhandlingen gjør bruk av.

Avhandlingen har separate drøftelser av inndragning av data som er tatt i beslag i forbindelse med en straffesak, og av automatisert inndragning i nettet (fullbyrdingen). Datainndragning i straffesaken behandles i del III (kapittel 5), mens den automatiserte inndragningen i nettet behandles i del VI (kapittel 12-16). I de mellomliggende delene avklares det normative grunnlaget for automatisert inndragning i nettet. Det ene hovedtemaet gjelder en strafferettslig konseptualisering av data som strafferettslig objekt, se del IV (kapittel 6-10). Det andre hovedtemaet gjelder rettslige inndragningsgrunnlag for dubletter, se del V (kapittel 11). I siste del VII foretas en oppsummering av avhandlingens viktigste funn.

II Grunnleggende begreper

2 Begrepene 'data' og 'databasert informasjon'

2.1 Introduksjon - modell

I denne delen behandles begrepene 'data' og 'databasert informasjon' (dvs. innholdet i data). Fremstillingen beskriver begrepenes teoretiske og faktiske grunnlag, og avklarer hva som er inndragningsobjektet. Begrepene anvendes i forbindelse med avhandlingens fortolkningsspørsmål, hvor det har gjennomgående betydning om en datafil er en "ting" i inndragningsreglenes forstand, og hvilke rettsvirkninger som i så fall følger av det.

Jeg anser det hensiktsmessig å plassere begrepene i *en modell* for å strukturere den elektroniske konteksten og dermed også den rettslige analysen. Man kan se for seg et trelags hierarki med infrastruktur nederst, data i midten og databasert informasjon øverst. Datakrimutvalget baserte seg på et slikt hierarki, med datasystem og elektronisk kommunikasjonsnett nederst (infrastruktur), data og dataprogram i midten (data), og databasert informasjon øverst.[26] Utvalgets forslag til legaldefinisjoner gjenspeilet hierarkiet.[27] Departementet fant at det ikke var ønskelig å ta inn slike legaldefinisjoner i straffeloven 2005, så forholdet mellom de tre nivåene i den elektroniske konteksten kommer ikke eksplisitt frem i lovens kapittel 21 "Vern av informasjon og informasjonsutveksling".[28] Det har imidlertid vist seg i annen sammenheng at en slik modell kan være nyttig for rettslig analyse. For eksempel benytter *Schartum* en modell som ligner Datakrimutvalgets i en analyse av e-forvaltning.[29] Selv finner jeg at modellen gir god støtte for tanken.

[26] NOU 2007: 2 s. 60 flg.
[27] NOU 2007: 2 s. 59. Lovforslaget § 1 bokstav a - e inneholdt fem legaldefinerte begreper. I forhold til avhandlingens modell forholder de seg slik: Modellens nivå for infrastruktur omfatter "datasystem" og " elektronisk kommunikasjonsnett", jf. § 1 bokstav a og e; nivået for data omfatter "data" og "dataprogram", jf. § 1 bokstav b og c; nivået for databasert informasjon omfatter "databasert informasjon", jf. § 1 d.
[28] Departementet uttaler i Ot.prp. nr 22 (2008-2009) på s. 21 at "det er vanskelig å utforme presise og dekkende definisjoner som samtidig er føyelige nok […] Departementet mener imidlertid at begrepene ikke bør «låses» i en legaldefinisjon, men i den grad det er nødvendig og mulig forklares i motivene og utvikles i takt med teknologien".
[29] *Schartum* (2007) s. 27. Det skilles mellom tre nivåer: teknisk (smlg. data), semantisk (smlg. innhold) og organisatorisk (smlg. infrastruktur). Et annet eksempel er den svenske utredningen SOU 1992: 110 "Information och den nya InformationsTeknologin – straff- och processrättliga frågor m.m", hvor det står at "Viktig är att hålla isär information och informationsbärare. Information är nogot immaterielt medan informationsbärare är fysiska föremål. Data är något däremellan. De ger en fysisk representation av information men de är inte påtagliga; de har som vi ofta återkommer till en kvasimateriell karaktär." (s. 156).

De tre nivåene bygger på hverandre. Infrastrukturen er en forutsetning for at man kan ha og utnytte elektroniske data, og data er en forutsetning for at det kan foreligge databasert informasjon. Man kan si at data er et maskinavhengig fenomen, mens innholdet er et dataavhengig fenomen.

Infrastrukturen har liten betydning for de rettsspørsmål som skal behandles, den danner bare en faktisk kontekst for automatisert inndragning. Etter modellen omfatter infrastrukturen alt fra CD-plater, minnepinner og datasystemer, til satelitter og undersjøiske kabler for dataoverføring. Infrastrukturens omfattende og sammensatte karakter kunne kanskje tilsagt at modellens nederste nivå var mer nyansert, men det har ikke fremstått som nødvendig ut fra avhandlingens formål.

I det følgende rettes fokus mot begrepene ’data’ og ’databasert informasjon’, jf. modellens midterste og øverste nivå.

2.2 ’Data’ og ’databasert informasjon’

Slik jeg benytter ’data’ i avhandlingen er det et teknologispesifikt begrep som er forbundet med bruk av IKT. ’Data’ betyr *et maskinlesbart signal*, og betegner signalstrømmen *som overføres* mellom datamaskiner i et nett, og som *lagres* på fysiske lagringsmedier som minnepinne, harddisk, CD- og DVD-plater, minnekort i digitalt kamera m.v.. Data i denne betydningen, er ment for automatisk behandling i et datasystem.

Nedover skal data skilles fra infrastruktur. Infrastruktur i form av datasystemer og -nett, er nødvendig for å lagre, behandle og overføre data. Data er altså et objekt som behandles ved hjelp av verktøy i infrastrukturen.

Når adressaten for dataene er et *menneske,* må data skilles fra sitt innhold, som er den databaserte informasjonen. I overgangen fra data til databasert informasjon må det skje en *presentasjon*, for eksempel i form av tekst eller bilder på dataskjermen, eller lyd i høyttaleren (jeg holder meg i det følgende til presentasjon via skjermen). Innholdet *slik det er presentert på skjermen,* dvs. de ufortolkede tegnene, kaller jeg *databasert informasjon i objektiv forstand.* Det er innhold som er beregnet på menneskets sensoriske ”mottaksapparat”, det man kan se og lese. Meningsinnholdet i det som er presentert er databasert informasjon *i subjektiv*

forstand. Dette er den fortolkede oppfatningen av den objektive informasjonen. Overgrepsbilder presentert på skjermen er databasert informasjon i objektiv forstand, og bildene slik de oppfattes av mennesker er databasert informasjon i subjektiv forstand. Databasert informasjon har mennesket som adressat og ligger på nivået over data i henhold til modellen.

Data kan også ha en *datamaskin* som adressat og innholdet i disse dataene kan iverksette prosesser på datamaskinen. Dataprogrammer har slik funksjonalitet. Også i dette tilfellet foregår en *presentasjon* for en adressat (datamaskinen), men prosessen foregår bare på det midterste nivået i modellen, og endrer ikke karakteren av å være data. Når dataene har datamaskinen som endelig adressat, er det ikke for avhandlingens formål nødvendig å skille mellom data og innholdet. Data som har maskinen som adressat kan for eksempel være brukt som middel til å begå datainnbrudd, eller de kan være under overføring i nettet som et "datavirus" med stor utbredelse.

Dataprogram er derfor som hovedregel et fenomen som hører hjemme på datanivået i modellen. Det gjelder et unntak her, nemlig når dataprogrammet er representert som kildekode. Da er det skrevet i et språk som kan leses av mennesker. Dette forklarer jeg nærmere i kapittel 4.4.2.

Data kan dermed karakteriseres som et "medium", dvs. et mellomledd, jf. den latinske opprinnelsen *medius.*[30] Mediet transporterer eller bærer innholdet, og kan med et annet ord kalles "informasjonsbærer", som er det uttrykket inndragningsreglene bruker, jf. strl. 2005 § 76 første ledd, hvor "informasjonsbærer" er legaldefinert som

> "… trykt skrift eller annet som formidler en skriftlig, visuell, auditiv eller elektronisk lagret informasjon."

Data er dermed et medium på linje med tinglige medier, som bøker, blader, CD- og DVD-plater. Hvorvidt data er en "informasjonsbærer" i rettslig forstand, er et tolkingsspørsmål, men det faktiske utgangspunktet er uansett at inndragning må rette seg mot et objekt.[31] Inndragning som har til formål å ramme en rettsstridig ytring, må praktisk sett rette seg mot

[30] Se *Aschehoug og Gyldendals Store Norske Leksikon* (1995), stikkord "medium", samt ordnett.no (besøkt 27.7.2009). *Berulfsen og Gundersen* (1986) definerer medium som et "middel til å lagre informasjon på".
[31] Det nevnte tolkingsspørsmålet er behandlet i kapittel 5.4.1.

mediet (informasjonsbæreren). Følgelig er det aktuelt å rette inndragningen mot data, og den rettslige adgangen til å gjøre det skal jeg behandle.

Innholdet derimot, kan ses som en prosess. Med det mener jeg at det potensielt virker på en adressat. Det innhold som er presentert rent objektivt, kan skape meningsinnhold rent subjektivt. Prosessen kan også forårsake operasjoner på en datamaskin. Innholdet kan følgelig ikke i seg selv være gjenstand for inndragning, man må rette inndragningen mot mediet.

2.3 Begrepenes teoretiske grunnlag

2.3.1 Utgangspunkt for begrepsdannelsen

Ved informasjonsrettslige problemer er det gjerne behov for å ta stilling til hvordan man skal benytte begrepene 'data' og 'informasjon', selv om det riktignok er slik at forfatteren ikke alltid finner grunn til å skille mellom dem.[32] For mitt formål er det imidlertid behov for en begrepsbruk som tydelig får frem at det er *data selvstendig sett* som er objekt for inngrepet, dvs. at data er den "ting" som kan inndras.[33] En annen sak er at inndragning av mediet nødvendigvis også rammer innholdet.

Eng fremholder at *hensiktsmessighet, operasjonaliserbarhet, og behov for en bestemt erkjennelse eller interesse* er viktige kriterier for et godt begrep.[34] Jeg mener at 'data' er *hensiktsmessig* for avhandlingens analyse av inndragningsspørsmål, fordi det klart

[32] *Walden* (2007) skriver i sin lærebok om datakriminalitet at forfatteren står fritt til å velge sine begreper. Han velger ikke å skille mellom data og informasjon, jf. at "[t]he term «information» is being used … to denote that which is being processed by computers and communicated via networks, ie it is the substance on which computers and networks operate. It is also used synonymously with «data», a term more familiarly connected with the world of computing and networks" (s. 2); "… the book uses data and information interchangeably" (s. 14). Jeg finner at en slik tilnærming kan være hensiktsmessig for å gi en oversikt over et rettsfelt, men blir for lite presist i forhold til rettslige tolkingsspørsmål. Da må man vite om spørsmålet gjelder data eller informasjon. Dette er et gjennomgående tema i avhandlingen.

[33] *Udsen* (2009) s. 38, konstaterer at på fagfelt som reiser såkalte "informasjonsrettslige spørsmål" – som automatisert inndragning må sies å gjøre – er det "sædvanligt, at juridiske afhandlinger af informationsretlig natur strukturerer informationsbegrebet med udgangspunkt i de juridiske spørgsmål, der skal behandles". *Bygrave* (2006) er en som har etterlyst en mer stringent begrepsbruk i forholdet mellom 'data' og 'informasjon' i juridisk teori. Han tar utgangspunkt i vernet om personopplysninger, og generaliserer poenget sitt slik: "most commentary in the field tends to employ the two terms as synonymous, interchangeable concepts without reflecting in detail over their logical content. This is remarkable given that this field is one of the few *directly* regulating "data" and "information". …Accordingly, one would expect in principle a relatively rigorous and in-depth treatment of such concepts. The failure of this treatment to materialise in precisely this field speaks volumes for the state of equivalent discourse in other legal areas", *Bygrave* (2006) s. 121.

[34] *Eng* (2007) om kriterier for utvikling av begreper s. 519 flg: s. 530 (operasjonaliserbarhet), s. 533 (hensiktsmessighet) og s. 534 flg. (erkjennelse, interesse).

identifiserer inndragningsobjektet. Og 'data' defineres til dels negativt ved å skille mot 'databasert informasjon', noe som blant annet har betydning ved fastleggelsen av straffetrusselens rekkevidde, jf. strl. 2005 §§ 201 og 311.[35] Begge begrepene er *operasjonaliserbare*, fordi det er enkelt å konstatere hvorvidt man har med data eller databasert informasjon å gjøre. Begrepene får altså på en tydelig måte frem om man forholder seg til et objekt (ting) eller en prosess slik jeg beskrev over. For det tredje forebygger begrepene glidning mellom objekt og prosess i den rettslige analysen, og bidrar derfor til *erkjennelse* av avhandlingens sentrale rettsspørsmål.

Begrepene har en teoretisk forankring i de såkalte ISO-definisjonene av data og informasjon, som er omtalt nedenfor. Disse definisjonene ligger i sin tur til grunn for definisjonen av "elektroniske data" i datakrimkonvensjonen, som er gjennomført i norsk rett. Også lov om elektronisk kommunikasjon (ekomloven) har basert seg på en korresponderende begrepsbruk. I det følgende redegjør jeg for begrepenes teoretiske grunnlag.

2.3.2 ISO-definisjonene av data og informasjon

Den internasjonale standardiseringsorganisasjonen (ISO) utformet i 1993 definisjoner av data og informasjon.

ISO-definisjonen av "data" lyder:

> «Data»: "a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means".[36]

ISO-definisjonen av "informasjon" lyder:

> «Information»: "the meaning assigned to data by means of conventions applied to that data".[37]

[35] Se kapittel 9.
[36] Vilkåret "formalised manner" viser en sammenheng med kybernetikken, hvor mønster ("pattern") er et kjennetegn på kommunikasjon. *Wiener* (1988), utkom første gang i 1950), se kapittel V s. 95 flg. "Organization as the message" og på s. 96 "A pattern is a message, and may be transmitted as a message".
[37] ISO 2382-1, Information Technology - Vocabulary - Part 1: Fundamental Terms. 1993.

Definisjonen av "informasjon" er avledet av datadefinisjonen, jf. "the meaning assigned to data". Rekkevidden av datadefinisjonen påvirker dermed rekkevidden av informasjonsdefinisjonen.

Avhandlingens databegrep bygger bare på *annet alternativ* av ISO-definisjonen av data, nemlig den delen som sier at data kan utnyttes av en maskin (dvs. en datamaskin), jf. "or by automatic means".[38] Ifølge dette alternativet er 'data' "facts, concepts or instructions" som er egnet for *automatisk behandling* ("processing… by automatic means"). En form for databehandling er visning av innholdet på dataskjermen, dvs. det jeg kaller 'presentasjon'. Da oppstår 'databasert innhold i objektiv forstand' altså et fortolkningsgrunnlag for mennesket, som skaffer seg 'databasert informasjon i subjektiv forstand' (smlg. informasjonsdefinisjonen "the meaning assigned to data").

Min definisjonsbruk gir grunnlag for å skille mellom menneske og maskin som adressat for kommunikasjonsstrømmen (dataene). Dersom mennesket er adressat oppstår "databasert informasjon". Dersom maskinen er adressat har vi bare med "data" å gjøre, fordi dataene ikke er umiddelbart tilgjengelige eller ment for mennesker.

For avhandlingens spørsmål har sondringen betydning på den måten at data kan utveksles mellom datamaskiner og påvirke dem, uten at innholdet eksponeres for mennesker. Man kan tenke seg at datafiler som overføres i signalstrømmen mellom datamaskinene, identifiseres, plukkes ut og inndras. Siden handlingen må gjøres med bruk av dataverktøy, er objektet for inndragningen data. I og med at det ikke foreligger noe element av eksponering for et menneske i den forbindelse, foreligger det ikke databasert informasjon.[39]

Ved *presentasjon* på skjerm tilrettelegges det for at mennesket kan gjøre seg kjent med innholdet i dataene, men de elektroniske signalene er og forblir data. Ved presentasjonen har

[38] Avhandlingens databegrep støttes derfor på følgende del av ISO-definisjonen: "A representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing … by automatic means".

[39] Ifølge *Walden* (2007) er det en slik situasjon, dvs. data i betydningen maskinlesbare signaler, som ligger til grunn for at europeisk persondatalovgivning har valgt å bruke begrepet "person*data*" (min uth.). På grunn av dataenes sårbarhet anses det å være utilstrekkelig om det rettslige vernet skulle inntre først etter at innholdet er blitt eksponert for omverdenen, dvs. blitt konvertert til informasjon, vernet må gjelde også de elektroniske signalene som sådan, dvs. *persondataene*. *Walden* skriver således at "…the threats to privacy arise from the accumulation of raw data before it is transformed into information that can be used in relation to an individual; therefore the law intervenes at this earlier stage". *Walden* (2007) s. 14, pkt. 2.12.

mennesket befatning med meningsinnholdet (databasert informasjon), og det kan etter omstendighetene være straffbart.[40] Men selv om lovbryteren har hatt kontakt med meningsinnholdet via dataskjermen, er det ikke sikkert at det er noen data å inndra, det kommer jo an på om vedkommende har lastet ned dataene.

ISO-definisjonene åpner for at 'data' og 'informasjon' kan brukes om prosesser som utelukkende foregår mellom datamaskiner, jf. "suitable for … processing … by automatic means" i datadefinisjonen. Informasjonsbegrepet avledes jo også av denne passusen, og betyr at datamaskinen "forstår" innholdet i dataene. Det har ikke noe med meningsinnholdet for mennesker å gjøre. Med tanke på denne avhandlingens spørsmål ser jeg bort fra "informasjon" i betydningen at datamaskinen formidler elektronisk kommunikasjon til en annen datamaskin, eller at datamaskinen er endepunktet for kommunikasjonen, for eksempel dersom den er mål for et datainnbrudd.

Først ved *presentasjon* blir data til informasjon som kan få mening for et menneske, ved å følge regler som normalt brukes for å utlede meningen (grammatikk, regneregler, språk osv). Den maskinelt utførte *presentasjonen* viser databasert informasjon i objektiv forstand, det fortolkede innholdet er databasert informasjon i subjektiv forstand.[41]

Jeg anvender således 'databasert informasjon i objektiv forstand' på samme måte som man ellers tradisjonelt bruker 'data'. Avgjørende er at kommunikasjonsprosessen er utenfor den fasen hvor dataene er adressert til datamaskinen, i presentasjonsfasen er de adressert til mennesket.

'Databasert informasjon i objektiv forstand' skal derfor forstås på tilsvarende vis som når data brukes om tegn eller faktiske opplysninger som må *tolkes* for å skape informasjon. I forhold til avhandlingens formål kan jeg imidlertid ikke bruke 'data' på nevnte måte, fordi jeg må skille mellom signaler som kun datamaskinen kan forstå og signaler som bare mennesker kan forstå. Når signaloverføring og presentasjon skjer elektronisk får ikke det ene begrepet 'data' frem skillet mellom situasjonene.

[40] Se kapittel 9.2.3. Tilgangsalternativet i strl. 2005 § 311 bokstav c etablerer straff for å ha sett på overgrepsbilder, uten vilkår om at dataene er lagret på harddisken..
[41] Fortolkning inntrer uvegerlig ved presentasjon. *Seipel* illustrerer dette med tegnkombinasjonene AJ og JA, hvor man i en gitt kontekst umiddelbart vil tolke det første som det siste og anta at det foreligger en stavefeil, se *Seipel* (2004) s. 30.

Dermed får jeg begreper på to nivåer ('data' og 'databasert informasjon') som begge er begrenset til en elektronisk kontekst, og et databegrep som utelukkende omfatter de maskinlesbare signalene. Dette er vesentlig smalere begrepsbruk enn etter ISO-definisjonene som ikke knyttet til noen spesifikk teknologi, men gjelder kommunikasjon generelt. Også skrift og tale er formalisert signalformidling som omfattes av definisjonen av data, jf. "suitable for … interpretation … by human beings". Signaloverføring mellom mennesker uten elektronisk kommunikasjon, for eksempel ved å sende brev eller føre en samtale, kan imidlertid ikke omfattes av avhandlingens databegrep, fordi rettsspørsmålene bare knytter seg til elektroniske data. Det er bare *det automatiserte alternativet* i ISO-definisjonen av data, som jeg siterte over, som er relevant som *objekt* for automatisert inndragning.

Avhandlingens databegrep er altså helt forskjellig fra en begrepsbruk som tar utgangspunkt i det latinske utspringet for data, *datum,* som betyr opplysning eller "noe som er gitt".[42] Data i en slik betydning kan for eksempel være statistiske meteorologiske opplysninger (såkalte "værdata") og andre fakta, som rapportering av nyheter. I Rt. 1994 s. 1610 (BetalTV) fortolket Høyesterett ordet "data" i strl. 1902 § 145 annet ledd. Bestemmelsen setter straff for uberettiget adgang til "data … som er lagret eller som overføres ved elektroniske … hjelpemidler." Spørsmålet var om "data" omfattet betalingsbelagte beskyttede fjernsynsprogrammer levert av TV1000, dvs. fjernsynssignaler som var beskyttet ved kryptering. Høyesterett delte seg 3-2 i spørsmålet, og flertallet kom til at så ikke var tilfelle. Førstvoterende, som representant for flertallet, uttalte at:

> "rent språklig ligger det nærmest å forstå uttrykket data slik at det omfatter faktiske opplysninger og informasjon."[43]

Fortolkningen baserte seg på en forståelse som kan utledes av databegrepets språklige opprinnelse *datum*, som gjenspeiles i ordet "facts" i ISO-definisjonen av data. I dansk teori brukes uttrykket "operasjonell informasjon" for å betegne det samme.[44] Motsatsen er "emosjonell informasjon" som har evne til å frembringe følelser hos adressaten, som for eksempel musikk og poesi.[45]

[42] *Bing* (1982) s. 66-69 ; *Seipel* (2004) s. 25; *Andersen* (2005) s. 108 sitat: "Data (af latin: "dare", at give).
[43] Rt. 1994 s. 1610 på s. 1612.
[44] *Andersen* (2003) s. 10; *Udsen* (2009) s. 39.
[45] *Andersen* (2003) s. 10; *Udsen* (2009) s. 34 og 39.

Dissenterende dommer *Schei* sluttet seg ikke til en konklusjon som bygget på sondringen mellom operasjonell og emosjonell informasjon. Han mente at innholdets karakter av underholdningsstoff ikke var til hinder for at de elektroniske signalene kunne anses som data, og uttalte at:

> "Innholdsmessig behøver det ikke være forskjell på det som hentes ut fra en database sammenholdt med det som sendes ut som fjernsyn, begge deler kan være ren underholdning." (s. 1615).

Denne begrunnelsen skiller mellom data og innholdet (den databaserte informasjonen). Innholdets karakter anses irrelevant for om det foreligger "data" i datainnbruddsbestemmelsens forstand. Jeg har lagt til grunn en korresponderende begrepsbruk i avhandlingen.

Ut fra min begrepsbruk er en elektronisk basert *opplysning* å anse som databasert informasjon, som adressaten blir kjent med ved presentasjon. Forut for presentasjon foreligger opplysningene som signaler som bare kan behandles maskinelt, dvs. data. Det samme gjelder emosjonell informasjon, som også er data før den er presentert. 'Data' må heller ikke forveksles med *tegn* som kan oppfattes av mennesker, for eksempel bokstaver på en skjerm. Etter ISO-definisjonen kan nemlig data brukes som betegnelse for ufortolkede tegn, jf. "representation of… concepts or instructions".

Som en oppsummering kan det konstateres at det definisjonsmessige forholdet mellom data og databasert informasjon går ved *presentasjonen for et menneske*. Det betyr at det hersker *et sekvensielt forhold* mellom data og databasert informasjon, hvor overgangen skjer ved den nevnte presentasjonen. Dermed er det treffende som *Bing* gjør, å karakterisere data som 'potensiell informasjon'.[46] Og avslutningsvis viser jeg til *Seipel,* som har konstatert at en begrepsbruk som er løsrevet fra de aktuelle tekniske redskaper, leder til at:

> "informationsrätten får en diffus och närmast obegränsad utsträckning – finns det egentligen något innom rättssystemet som inte på ett eller annat sätt har anknytning til information?".[47]

[46] *Bing* (1982) s. 67; *Bing* (2008) s. 22-23.
[47] *Seipel* (2004) s. 275. Smlg. *Sunde* (2006) s. 30-31, med kritikk av begrepet "informasjonssikkerhet" fordi det er for bredt til å være hensiktsmessig.

Seipel bekrefter her behovet for å gi 'data' en konkret avgrensning for å bli et velegnet begrep. I mitt tilfelle er avgrensningen foretatt for å drøfte inndragningsreglenes anvendelse på data som er tatt i beslag, og data som er lagret eller er under overføring i nettet.

2.3.3 Datakrimkonvensjonens begrepsbruk: Elektroniske data

Datakrimkonvensjonen art. 1 bokstav b inneholder en legaldefinisjon av data, som er basert på ISO-definisjonen. Definisjonen lyder som følger:

> "«elektroniske data»: enhver framstilling av fakta, informasjon eller begrep i en form som er egnet for behandling i et datasystem, herunder et program som kan få et datasystem til å utføre en funksjon."[48]

Det sentrale er at definisjonen er avgrenset til maskinlesbare signaler, noe som også omfatter dataprogram. Poenget er fremhevet i den forklarende rapporten til datakrimkonvensjonen som følger:

> "The definition of computer data builds upon the ISO-definition of data. This definition contains the terms «suitable for processing» [egnet for behandling]. *This means that data is put in such a form that it can be directly processed by the computer system. In order to make clear that data in this Convention has to be understood as data in electronic or other directly processable form, the notion «computer data» is introduced."*[49]

Det innebærer at et menneskelig individ ikke kan være direkte adressat for data. Dermed er det klart at konvensjonen skiller mellom data og databasert informasjon, selv om det siste ikke har fått en egen legaldefinisjon. *Spannbrucker* har gjort samme observasjon. I redegjørelsen for "Computerdaten" skriver han:

> "Damit werden «menschliche» Verarbeitungsvorgänge (z.B. Datenerfassung, -eingabe, usw.) ausgeschlossen. Für den «Aggregatzustand» der Daten bedeutet dies, dass sie nur in digitaler, binärer Codierung «Computerdaten» im Sinne der Konvention darstellen".[50]

Avhandlingens begrepsbruk er således i samsvar med datakrimkonvensjonens begrepsbruk.

---

[48] Konvensjonsteksten i engelsk originaltekst: "«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".
[49] Den forklarende rapporten til datakrimkonvensjonen punkt 25. Min utheving og tilføyelse i klamme.
[50] *Spannbrucker* (2004) s. 34.

2.3.4 Ekomlovens begrepsbruk: Elektronisk kommunikasjon

Også ekomlovens begrepsbruk har en viss interesse, blant annet har den slått inn i den straffeprosessuelle terminologi.[51] Ekomloven behandler data under overføring, og lovens uttrykk for dette er "elektronisk kommunikasjon" som er legaldefinert i ekomloven § 1-5 nr. 1. Definisjonen lyder:

> "elektronisk kommunikasjon: overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for signaltransport."

"Data" er nøkkelbegrepet, mens "lyd, tekst, bilder" er eksempler på hva innholdet kan være. Formuleringen "andre data" peker i retning av at ekomloven kun gjelder data, ikke innhold. Denne fortolkningen støttes av klare uttalelser i forarbeidene og må anses som sikker rett.[52] Definisjonen gir derfor uttrykk for et poeng som har betydning for automatisert inndragning, nemlig at teknologien er "blind" for innholdet. I et teknisk perspektiv er en datafil en datafil, og kan behandles uavhengig av hva slags innhold dataene bærer. Det blir omtrent som at man på et transportbånd kan håndtere pakker og bokser uavhengig av hva de inneholder.

Ekomlovens definisjon av "elektronisk kommunikasjon" korresponderer med datakrimkonvensjonens definisjon av "elektroniske data", dog med ett forbehold, den omfatter ikke data som er lagret, noe som fremgår av ordet "overføring". Men definisjonen omfatter overføring av elektroniske signaler også når *grunnlaget* for kommunikasjonen er data som er lagret, for eksempel en word-fil som overføres ved epost. Eposten lagres i begge ender og er elektronisk kommunikasjon under overføringen. Begrepet 'elektronisk kommunikasjon'er avgrenset til det tekniske nivået hvor data anses som et maskinlesbart signal.[53] Avhandlingens databegrep er i samsvar med dette, dog slik at det også omfatter data som er lagret.

[51] Se kapittel 6.3.2.2.
[52] Se Ot.prp. nr. 58 (2002-2003) på s. 86 i tilknytning til § 1-5 nr. 4 (elektronisk kommunikasjonstjeneste), som må ses i sammenheng med definisjonen av elektronisk kommunikasjon, jf. § 1-5 nr. 1. Se også s. 10, hvor det står at "innhold ikke skal reguleres av denne loven".
[53] For taletelefoni betyr det at overføringen omfattes, men idet signalene mottas av adressatens mottakerapparat og konverteres til lydbølger som går ut av høyttaleren, er de blitt databasert informasjon, som faller utenfor begrepet elektronisk kommunikasjon.

2.3.5 Oppsummering

I dette kapitlet er det redegjort for at avhandlingens sondring mellom 'data' og 'databasert informasjon' har forankring i ISO-definisjonene. Videre er det konstatert at legaldefinisjonene av "elektroniske data" og "elektronisk kommunikasjon" i datakrimkonvensjonen og ekomloven uttrykker tilsvarende databegrep som avhandlingens.

Avhandlingens begrepsbruk må følgelig anses som anerkjent begrepsbruk for elektroniske forhold. Det er en begrepsbruk som Norge er folkerettslig forpliktet til å gjennomføre i strafferettslig sammenheng, jf. tiltredelsen til datakrimkonvensjonen. Data som et elektronisk medium er følgelig et rettslig relevant objekt i forhold til strl. 2005 §§ 201 og 311, som gjennomfører datakrimkonvensjonen artikkel 6 og 9 i norsk rett.[54] Det betyr at man bør anse data som ting slik fysiske medier er ting, som det kan være straffbart å ha befatning med etter de nevnte bestemmelsene. Dermed bør det vurderes om denne tingen kan være gjenstand for inndragning.

For det tredje er det konstatert at datamaskinen kan behandle datafiler uavhengig av hva slags innhold de bærer. Det betyr at teknologien er "blind" for innholdet. Det å inndra datafiler i nettet ved å plukke ut og blokkere dem rent teknisk, kan derfor ikke sammenlignes med kommunikasjonskontroll hvor man skaffer seg tilgang til den databasert informasjonen (innholdet) i kommunikasjonen eller til metadata som trafikk- og lokaliseringsdata. Med det begrepsmessige grunnlaget som er lagt, ser man at data kan behandles som et selvstendig objekt uavhengig av om innholdet er adressert til et menneske eller en datamaskin. Det gir grunnlag for en viss "tingliggjøring" av data, som kan utnyttes ved automatisert inndragning.

3 Data som faktisk fenomen

3.1 Problemstilling

I dette kapitlet forholder jeg meg til "beskrivelsesproblemet", som gjelder det å gi en rettslig relevant faktabeskrivelse. Det rettslige problemet er om datafilen er "ting" i strafferettslig forstand. Ifølge strl. 2005 § 69 første ledd er det "ting" som kan inndras, og i bestemmelsens

[54] Det ligger mange folkerettslige forpliktelser bak forbudet mot overgrepsbilder. Se Ot.prp. nr. 37 (2004-2005) s. 4, og oppsummeringen i Ot.prp. nr. 22 (2008-2009) pkt. 7.20.3 s. 264.

annet ledd presiseres det at også ”elektronisk lagret informasjon” regnes som ”ting”.[55] Presiseringen løser imidlertid ikke alle spørsmål for rettsanvendelsen. Det er for eksempel et tankekors at loven opererer med et krav om at data, i motsetning til andre ting som inndras, må være ”lagret”. Vilkåret om lagring innebærer at data ses i sammenheng med det fysiske lagringsmediet, og gir grunn til å reise spørsmål om loven virkelig ser data som et selvstendig inndragningsobjekt.

Vi kjenner nå til databegrepets teoretiske forankring og gjennomføringsforpliktelsen i norsk rett. Men for å ta stilling til de strafferettslige tolkingsspørsmålene, er det behov for en fyldigere beskrivelse av data.

3.2 Beskrivelsesproblemet

Beskrivelsesproblemet består i dette tilfellet fortrinnsvis av *utvelgelsen av de opplysninger* som er nødvendige for å kunne ta stilling til om data er et selvstendig strafferettslig objekt. De data som avhandlingen behandler kan beskrives på forskjellig måte. Hver beskrivelse kan være *sann*, men alle beskrivelsene fremstår ikke som like *relevante*. Ved en gjennomgang av litteratur om emnet, kan det konstateres at forskjellige kilder gir forskjellige faktiske beskrivelser av data. Beskrivelsene er preget av formålet og av den tid de ble skrevet i. På dette feltet har utviklingen har gått raskt og forståelsen for hva data er, har nok økt betraktelig på kort tid.

Jeg har for eksempel funnet ut at data er beskrevet som *en tilstand*, dvs. som ”noe annet” enn et fysisk objekt. *Negroponte* som jeg kommer inn på nedenfor, gir en slik beskrivelse, som følgelig legger vekt på forskjeller mellom data og fysiske objekter. Beskrivelsen gir følgelig ikke gir noe godt grunnlag for å argumentere for at data og fysiske bærere skulle være rettslig likstilte i relasjon til begrepet ”ting”, men så hadde *Negroponte* heller ikke strafferettslige spørsmål for øye da han skrev ”Mit digitale liv”.[56] Han var opptatt av det økonomiske potensialet som lå i digitalisert informasjon og hvordan online overføring endret tradisjonelle forutsetninger for kreativitet og verdiskaping.[57]

[55] Strl. 2005 § 69 er i sin helhet sitert i kapittel 5.3.1.
[56] *Negroponte* (1997).
[57] Se mer om dette i kapittel 3.3.1 og 8.2.

Data er også beskrevet som *en serie av et-tall og nuller*. Straffelovrådet baserte seg på en slik beskrivelse i datakrimutredningen fra 1985, og konkluderte med at data ikke var "ting".[58] Konklusjonen er forståelig sett på bakgrunn av at databeskrivelsen var svært "tynn".

Data kan også beskrives som et objekt som lar seg *spesifisere, konkretisere og kontrollere.* Det er min tilnærming til data, og da er det mulig rent strafferettslig å konseptualisere data som "ting".

Andersen har gitt følgende anbefaling for løsning av beskrivelsesproblemet i "IT-retten":

> "Som en generel tommelfingerregel kan man sige, at den faktiske beskrivelse bør søge imod et kompleksitetsniveau, der gør det mulig at anlægge relevante retlige sondringer."[59]

Dermed oppstår spørsmålet om hva "ting" skal avgrenses mot og hvilke kriterier som gjelder for avgrensningen. Som nevnt avgrenser jeg mot den fysiske bæreren og den databaserte informasjonen. Det er altså de elektroniske signalene som skal beskrives. De strafferettslige kriteriene for "ting" må imidlertid identifiseres i forbindelse med tolkingsprosessen, noe som gjør det vanskelig å gi en dekkende beskrivelse av faktum på et tidlig stadium.[60] Situasjonen er velkjent; den gjelder vekslingen mellom juss og faktum hvor man kan ha behov for å gå frem og tilbake flere ganger, for å forvisse seg om at man har tilstrekkelig grunnlag for å ta stilling til rettsspørsmålet. De mulige ulemper til tross, har jeg valgt å gi en faktisk beskrivelse av data før den rettslige drøftelsen.

Formålet er å bevisstgjøre den strafferettslige betydningen av å ha en dekkende beskrivelse av data, samt å låse beskrivelsene til det databegrepet som avhandlingen faktisk anvender. Det er også så mye å si om data som faktisk fenomen, at det synes mest oversiktlig å foreta en samlet presentasjon relativt tidlig i fremstillingen.

En problemstilling som det er nyttig å ha med seg i den videre lesning, gjelder forholdet mellom data på den ene siden, og fysiske objekter, enkle fordringer og energi på den andre. De tre sistnevnte fenomenene regnes alle som "gjenstand" strafferettslig sett.[61] Fysiske

[58] NOU 1985: 31 s. 9. Se avhandlingen kapittel 7.6.3.
[59] *Andersen* (2005) på s. 101, i kapitlet "Beskrivelsesproblematikken".
[60] Kriteriene som ligger til grunn for de strafferettslige begrepene "gjenstand" og "ting" er behandlet i kapittel 7.
[61] Se mer om dette i kapittel 7, særlig oversikten i 7.2 og om enkle fordringer i kapittel 7.6.4.

objekter og enkle fordringer regnes også som ”ting”. Hvorvidt det foreligger rettslig relevante forskjeller mellom data og de andre fenomenene, i forhold til ”gjenstand” og ”ting”, må avgjøres ved fortolkningen. Enkelte spørsmål kan likevel antydes allerede nå, for eksempel: Hva er det ved fysiske objekter som gjør at de omfattes av begrepene? Neste spørsmål er om data har tilsvarende egenskaper, og om det i så fall har betydning for fortolkningen? Det samme spørsmålet kan stilles med hensyn til enkle fordringer. Hva er kriteriet som medfører at enkle fordringer anses som ”gjenstand”? Er dette kriteriet også oppfylt for data? Til slutt har vi energi, som er legaldefinert som ”gjenstand”, jf. strl. 2005 § 12. Hva er det som er *problematisk* med energi som nødvendiggjør legaldefinisjonen, og hva er det som *berettiger* at energi anses som ”gjenstand”? Finnes tilsvarende egenskaper ved data?

3.3 Faktisk beskrivelse av data

3.3.1 Atomer vs. bits

Teknologen *Negroponte* – sjef ved MIT medialab – ble på midten av 1990-tallet berømt for sitt budskap om hva som atskiller ”det digitale liv” fra det fysiske: Mens den fysiske verden består av atomer som minste enhet, består den digitale verden av *bits* som minste enhet. Dersom man kjøper en bok, leveres informasjon på papir som består av atomer. Det samme gjelder trykksverten. Dersom man kjøper en ebok, leveres informasjon ved at man skaffer seg rådighet over *bits* via nettverket. ”Bit”, forklarer *Negroponte* (dansk oversettelse):

> ”…har ingen farve, størrelse eller vægt, og den kan rejse med lysets hast. Det er den mindste atomare komponent i informationernes DNA-molekyler. Det er en tilstand: slået til eller slået fra, sand eller falsk, oppe eller nede, inde eller ude, sort eller hvid. Af praktiske grunde betragter vi en bit som værende enten 1 eller 0. Betydningen af 1 eller 0 er en sag for sig. I computerens barndom repræsenterede en bit-streng almindeligvis numerisk information.”[62]

Her kan man merke seg at det er *forskjellen* mellom fysiske objekter og data som fremheves. De grunnleggende komponentene – *atomer og bits* – er forskjellige. Denne forskjellen har preget *grunngodetenkningen* som har gjort seg gjeldende i forsøkene på å gi en strafferettslig relevant beskrivelse av data. Jeg tviler imidlertid på at det er en fruktbar rettslig tilnærming, fordi datafiler lar seg spesifisere og kontrollere. I henhold til disse rettslig relevante kriteriene *ligner* data mye på fysiske objekter. Ved strafferettslige fortolkningsspørsmål synes jeg det er

[62] *Negroponte* (1997) s. 22.

fornuftig å ta utgangspunkt i om data tilfredsstiller rettslig relevante kriterier, fremfor å vektlegge det som skiller data fra fysiske objekter i henhold til naturvitenskapelige kriterier. Dessuten har data dypest sett en fysisk manifestasjon i form av molekyler på harddisk, selv om det ikke er synbart for et menneske. Men det er jo ikke atomer heller. Jeg tror derfor ikke at vektlegging av data som "noe annet" enn fysiske objekter er et heldig strafferettslig utgangspunkt.

Den "tilstand" *Negroponte* fremhever, er en forutsetning for ikke-rivalisering, dvs. at deling gir mer data. Det er en *teknologiskapt* egenskap som etter mitt syn har betydning for automatisert inndragning av datafiler. Dubletter har én og samme dataidentitet og bør derfor kunne inndras under ett med henvisning til denne identiteten. Inndragning av én datafil i straffesaken kan således tenkes å få rettsvirkning for alle dublettene i nettet.[63]

For det annet beskriver sitatet av *Negroponte* hva *bits* er. *Bits* er binære elementer (binary digits), derav karakteristikken "slået til eller slået fra, sand eller falsk, oppe eller nede, inde eller ude, sort eller hvid.". Null eller en (0 eller 1) er det numeriske uttrykket for en *bit*. En bitstreng med åtte tegn er en *byte*. Bruken av tall gjør det mulig å uttrykke data skriftlig som et *bitmønster*. Dette kan gjøres på et stykke papir, slik den samme *Negroponte* har gjort i sin hilsen til Elaine: "som har holdt mit digitale liv ud i nøjagtig 11111 år."[64] Med dette mener han 11111 "bit-år", dvs. 31 kalenderår.[65]

Av dette forstår man at en beskrivelse av data som "en serie et-tall og nuller" er klart utilstrekkelig dersom rettsspørsmålet gjelder *elektroniske data*. Da må det presiseres at man mener "en serie et-tall og nuller" som uttrykker *et elektronisk innhold*. Straffelovrådets beskrivelse baserte seg på nevnte beskrivelse, men da var det klart at konteksten var elektronisk, så akkurat dette bød ikke på tvil. Men beskrivelsen ga bare et minimum av grunnlag for rettslig resonnement. Det var utvilsomt behov for nærmere opplysning om hva data er.

[63] Se kapittel 11.
[64] *Negroponte* (1997) innledningsvis på upaginert side.
[65] Om tellemetoden for bits, se *Negroponte* (1997) på s. 22. Se også *Kristensen* (1996) s. 30-31.

3.3.2 Opplysninger om data - konkretisering

Data kan beskrives ved hjelp av opplysninger som konkret knytter seg til en bestemt datamengde. Slike opplysninger kalles ”metadata” og finnes for eksempel i filsystemet.

Man kan for eksempel få frem opplysning om størrelsen på den enkelte fil og om den totale mengden data. Måleenheten er *bytes*. Mengden beskrives som kilo-, mega-, giga- eller terabytes, jf. forkortelsene Kb, Mb, Gb og Tb. Ved kvantifisering kan man blant annet kartlegge hvor mye lagringsplass som er forbrukt, og følgelig hvor mye ledig plass som finnes på en lagringsenhet. De lagrede data fyller opp lagringsplass, omtrent som bokser på et lager.

Filsystemet opplyser også om antallet filer som er lagret på et system. Videre gir det opplysning om tidspunkter, blant annet når en fil er opprettet og når den sist ble endret eller flyttet på systemet. Dessuten kan det angis hvorvidt innholdet er tekst, grafikk eller dataprogram, selv om slike opplysninger ikke alltid er helt pålitelige.[66] Dersom dataene er lagret, vil man kunne få opplysninger om hvilket system eller lagringsenhet de hører til. Dessuten kan det gis oversikt over hvilken andel av en datamengde som er brukergenerert (dvs. skapt eller anskaffet av brukeren selv). Det er gjerne denne som er mest interessant i strafferettslig sammenheng, siden standard systemfiler er velkjente og identiske overalt (de er dubletter).

Slike opplysninger gir en beskrivelse av spesifikke data, uten at innholdet er presentert. Også en slik konkretisering synes å kunne være relevant som kriterium for å beskrive et fenomen som skal henføres under begrepet ”ting”. For å gi en helt entydig og teknisk kontrollerbar beskrivelse av dataene, kan man bruke *sjekksum*. Sjekksum er i realiteten en spesiell type metadata som har stor betydning for avhandlingens rettslige resonnementer, se beskrivelsen i neste kapittel.

3.3.3 Data som et entydig identifiserbart objekt

Enhver datafil kan gis en unik identitet ved å beregne filens tekniske verdi med et hash program. Resultatet av regneoperasjonen er en tegnstreng som kalles ”sjekksum” (eller hash

[66] Opplysningene er som regel basert på tillegget i filnavnet, for eksempel .doc, .jpeg, . avi eller .exe. Disse tilleggene kan endres av brukeren, for eksempel for å skjule at man har mye bilder og film.

verdi).[67] Sjekksummen er et unikt uttrykk for datafilen og kan forsåvidt sammenlignes med en DNA-profil.[68] Som det fremgikk av forrige kapittel, er sjekksummen en opplysning om dataene, dvs. en type metadata.

Fremstilling av sjekksummen skjer ved at hash programmet foretar enveis kryptering av datafilen. Krypteringen leder ikke til forvanskning av filens innhold, den resulterer bare i et produkt, nemlig sjekksummen. Selve datafilen er intakt.[69] Sjekksummen er et *unikt uttrykk* for filens innhold, fordi hash algoritmen er kollisjonsfri. En annen datamengde kan ikke gi samme sjekksum, med mindre innholdet er *identisk*, altså en *dublett*.[70]

Sjekksum er et meget rigid kriterium for identitet. Bare en bit-forskjell mellom to filer gir forskjellig sjekksum. *Knetzger* har påpekt at hash har høyere sikkerhetsgrad enn DNA; den statistiske sannsynligheten for at to forskjellige datamengder gir samme sjekksum er *"mathematically infinitesimal"* (min uth.).[71] Selv om innholdet i to filer for det menneskelige øye ser likt ut, er de ikke dubletter dersom dataverdien ikke er den samme. Filene kan altså bære *lik informasjon*, uten å være dubletter. På grunn av kopieringsfunksjonen i nettverksteknologien, er imidlertid dubletter et vanlig fenomen, se neste kapittel.

Av dette følger det at to filer med lik dataidentitet (sjekksum) har identisk innhold, men man kan ikke slutte den andre veien, og konkludere med at to filer med forskjellig sjekksum har innhold som er forskjellig for adressaten. Mennesker tolker og vurderer, og vil ofte konkludere med at meldinger som er ulike etter strengt formelle kriterier, likevel har likt

[67] Sjekksum inngår som en viktig komponent i elektronisk signatur. *Riisnæs* kaller sjekksummen "et entydig «uttrekk» («fingeravtrykk») av meldingen", jf. *Riisnæs* (2007) s. 56.
[68] I DNA-utredningen, NOU 2005: 19, opplyses det på s. 17 at "en DNA-profil, består derfor av en tallrekke samt angivelse av kjønn. Dette er et resultatformat som er enkelt å håndtere mht. databaser. […] Det kalles en "match" når to profiler som sammenlignes, for eksempel en sporprofil og en identitetsprofil, er identiske." Som det fremgår gir DNA-profilen en opplysning om innholdet, nemlig om kjønn. En sjekksum derimot, er rent formell, det er kun en identitet for datamengden og sier intet om innholdet, for eksempel om det dreier seg om tekst, lyd eller bilde.
[69] Enveiskryptering gir et irreversibelt resultat, noe som betyr at man ikke kan "dekryptere" sjekksummen for å regne seg tilbake til filens innhold.
[70] Dette er forklart rapporten "MD5 Collisions – The Effect on Computer Forensics", *Access Data* (2006); se også *Casey* (2004) s. 635-636. Se også om hashfunksjonalitet i Wikipedia: http://en.wikipedia.org/wiki/Cryptographic_hash_function (21. oktober 2008). *Vacca* (2002) skriver på s. 610: "To be valid, hash functions must meet two primary requirements: The original text may not be determined from the hash function, and they must be collision free – meaning that two different messages cannot produce the same hash value."
[71] *Knetzger* (2008) s. 292. Nederst på s. 291 viser han til beregninger som underbygger påstanden om at sjekksum har større treffsikkerhet enn DNA. Men her er man inne på svært små sannsynlighetsgrader; som det er sagt i DNA-utredningen på side 19, er det "1 milliard ganger mer sannsynlig å få dette resultatet [en match] dersom sporet er avsatt av denne personen enn om det er avsatt av en tilfeldig ubeslektet person."

meningsinnhold.[72] Videre kan et dataprogram som er endret ha samme funksjonalitet som det opprinnelige, men de to programmene er ikke dubletter.

Forekomsten av dubletter er så utbredt at det har skapt viktige anvendelsesområder for hash teknologien. Teknologien går ut på å identifisere sjekksumdefinerte filer (masterfiler) for deretter å gjøre noe med dem. Tre vanlige formål er *datareduksjon, blokkering* og *verifikasjon.*

Datareduksjon tar sikte på å "vaske" en datamengde for overflødig materiale ved å utelukke irrelevante filer. Det letter etterforskingsbyrden ved store databeslag ettersom mengden potensielt relevant materiale reduseres. Normalt er etterforskingen rettet mot det brukergenererte materialet, som epost, notater og samlinger av bilder og musikk m.v. Dersom et hash program for eksempel inneholder sjekksummene til alle programfilene til Windows, kan programfilene "vaskes" fra beslaget før bevisanalysen.[73] Årsaken er at operativsystemet er identisk overalt hvor det er installert, så systemfilene er dubletter. "Vaskingen" letter dataanalysen fordi operativsystemet består av flere titusen filer (anslagsvis 30 000). Siden identifikasjon på grunnlag av sjekksum er umulig hvis filen er endret, kan hash programmet benyttes til å identifisere systemfiler som er *erstattet eller endret* av uvedkommende. Dersom systemfilen ikke fanges opp av hash programmet er originalfilen erstattet med en annen som det er relevant å undersøke, for eksempel med tanke på om det er en såkalt "trojaner" på systemet.[74]

Blokkering tar sikte på å hindre gjennomstrømming av bestemte filer. Hash teknologi brukes derfor i såkalte "antivirus filtre", for å hindre kjente instanser av skadelig dataprogram å infisere datasystemene. Ta for eksempel et selvspredende dataprogram som "Slammer":[75] Det isoleres og analyseres av datasikkerhetsforetaket, som klassifiserer det som skadelig, beregner

[72] Se kapittel 11.5.2 for eksempler
[73] *Casey* (2004) s. 229 lister opp fire punkter for hva en slik prosess innebærer: Å eliminere systemfiler; å rette undersøkelsen mot de antatt mest interessante brukergenererte data; å behandle overflødige filer (back up); å identifisere forskjeller (avvik) ved bruk av hash teknologi.
[74] I følge Datakrimutvalget er trojaner "et program som gir seg ut for å være et nyttig program, men som i tillegg til (eller i stedet for) nyttige funksjoner inneholder programkode som gir gjerningspersonen tilgang til datamaskinen.", jf. NOU 2007: 2 kapittel 3.4.1 på s. 24.
[75] Slammer er klassifisert som en "orm", dvs. et dataprogram som sprer seg selv via datanettverk. Et datavirus er også selvspredende, men spredningen skjer ved at viruset hekter seg på en annen spredningstjeneste, for eksempel epost. ILOVE YOU var et slikt virus, og skal ha infisert 45 millioner datamaskiner over hele verden. Slammer spredte seg selv til 75 000 maskiner på 10 minutter, se NOU 2007: 2 kapittel 3.4.8, s. 28-29.

sjekksummen, og lagrer virusfil og sjekksum i en referansedatabase.[76] Antivirusfilteret i nettet oppdateres med nye sjekksummer fra referansedatabasen så snart et nytt virus er klassifisert. Dersom en dublett av viruset treffer filteret, blir det identifisert av sjekksumkontrollen og blokkert, slik at det ikke kan strømme gjennom til adressatens datasystem. Som beskrevet i kapittel 1.1, er det slik teknologi jeg tenker brukt ved automatisert inndragning.[77]

Behovet for *verifikasjon* oppstår i mange sammenhenger.[78] Her skal det pekes på tre vanlige formål: Det ene er å skape sikkerhet for at en kopi er identisk med originalen. Dette formålet er viktig ved sikkerhetskopiering og databeslag. Innholdet på en server kopieres og tas for eksempel i beslag. Deretter beregnes sjekksummen til innholdet på serveren og sjekksummen til kopien. Identiske sjekksummer betyr at kopien er identisk med innholdet på serveren. På et senere tidspunkt kan man beregne sjekksummen av kopien på nytt, for å kontrollere om den er intakt, eller om det har skjedd endringer i mellomtiden. Sjekksumkontroll kan altså verifisere at beslaget er likt de originale data som opprinnelig ble kopiert.

Teknologien brukes også ved elektronisk signatur (offentlig nøkkel kryptering). Ved hjelp av sjekksum verifiseres det at meldingen som sendes fra A til B er intakt (integritetshensynet), og at den virkelig kommer fra A (autentisering og uavviselighet).

Et annet formål er å analysere databeslag. Siktelsen gjelder for eksempel datainnbrudd, og det er relevant å avdekke om siktede var i besittelse av skadelig dataprogram. På grunnlag av sjekksumkontroll, kan kjente tilfeller av skadelig dataprogram identifiseres og bekrefte mistanken. Men dersom sjekksumanalysen er negativ, kan det ikke sluttes at siktede ikke er i besittelse av skadelig dataprogram; det betyr bare at vedkommende ikke er i besittelse av et program som alt er sjekksumdefinert. Analysen må deretter rettes mot det brukergenererte materialet som ikke ble identifisert ved sjekksum.

[76] Å være først ute med å identifisere skadelig dataprogram gir anerkjennelse. For så vidt gjelder Slammer, sendte fire personer på samme dato med kort tids mellomrom, epost til forskjellige varslingstjenester om ormen, og det hersker uenighet om hvem som er berettiget til anerkjennelsen. http://en.wikipedia.org/wiki/SQL_slammer_(computer_worm) (besøkt 31.3.2009).
[77] Mer generelt inneholder filtreringsmetoder en deteksjonsfase og en aksjonsfase, hvor det gjøres noe med funnet (se kapittel 14.3). Sjekksumidentifikasjon er en deteksjonsform som skiller seg fra andre filtreringsmetoder ved å være særlig presis. Se mer om dette i kapittel 14 (presisisjonsproblemet).
[78] Verifikasjon kan også brukes som synonym med identifikasjon, når formålet er å avdekke hvorvidt filer med kjent sjekksum finnes i et beslag. I så fall er enhver bruk av sjekksumkontroll å anse som verifikasjon.

Fremgangsmåten kan også benyttes for overgrepsbilder.[79] Ved sjekksumanalyse kan det maskinelt avdekkes om siktede er i besittelse av kjente filer med overgrepsbilder, antallet og om beslaget inneholder dubletter. Sjekksumkontrollen viser for eksempel at besittelsen gjelder 3 950 bilder, hvorav filene A, B og C forekommer mellom 8 og 13 ganger.[80] Siden sakstypen ofte gjelder store mengder rettsstridig materiale, innebærer maskinell analyse uansett en betydelig effektivisering av etterforskingen.[81] Men siden stadig nytt materiale gjøres tilgjengelig i nettet, kan man ikke gå ut fra at programmet avdekker alle filene med rettsstridig innhold. De som er gjenkjent kan imidlertid utelukkes fra resten av analysen (datareduksjon), og den manuelle gjennomgangen kan rettes mot brukergenererte filer som foreløpig ikke har noen sjekksum. Etter at nye filer med rettsstridig innhold er identifisert, kan de gis en sjekksum og legges i politiets referansedatabase (RDB), jf. trinn 2 beskrevet i kapittel 1.1.

En tredje praktisk anvendelse av verifikasjonsfunksjonen gjelder fildeling. Fildelingsprogrammet genererer sjekksummer til det materialet som tilbys på tjenesten. På grunnlag av sjekksum identifiseres identiske filer hos forskjellige brukere. Dermed er filene søk- og delbare uavhengig av hvilken tittel brukeren har satt på filen. Man unngår problemer på grunn av feilstaving, uriktig filtillegg osv., og delingen effektiviseres.[82]

Som en oppsummering kan det fastslås at sjekksum er en teknisk verdi som gir en unik dataidentitet. Den sier ikke noe om innholdet. Sjekksumkontroll kan bare foregå maskinelt og innholdet eksponeres ikke i den forbindelse. Dubletter har lik sjekksum, dvs. samme dataidentitet. På grunnlag av sjekksum kan kjente dubletter identifiseres (gjenkjennes) maskinelt i nettet. Jeg reiser spørsmålet om inndragningsreglene de lege lata gir rettsgrunnlag for blokkering av de rettsstridige dublettene, dvs. automatisert inndragning.

[79] Faremo-rapporten (2007) anbefaler styrket nordisk samarbeid om å utvikle et "verktøy for å forenkle gjennomgangen av beslag" (s. 2. pkt. 1.1 og s. 23 pkt. 6.3.3). Oppbygning av referansedatabasen som gir grunnlaget for sjekksummene er tidkrevende arbeid, hvor samarbeidsfordelene er store. Det ligger imidlertid vel til rette for internasjonalt samarbeid om utveksling av sjekksummer, se kapittel 11.5.3.3.

[80] Eksemplet er hentet fra RG 2006 s. 595 (Agder). Forekomsten av dubletter i beslaget gir opphav til et beregningsproblem vedrørende antallet, dvs. om dublettene skal telles som én eller flere filer. Dette har jeg tatt opp i kapittel 11.5.2.

[81] Det illustreres av en tingsrettsdom som gjaldt 218 735 bilder og 59 filmklipp "beregnet av et dataprogram" (TBERG-2007-70663). Omfanget viser behovet for automatisert analyse av beslag. Av Kripos har jeg fått opplyst at man har redusert den ukjente delen av beslag både med 30 og 40 prosent, ved bruk av sjekksumanalyse. I en sak med 20 000 brukergenererte filer innebærer det reduksjon til 12 000 ukjente filer. Når de er analysert kan de legges i en referansedatabase og øke antallet kjente filer, for deretter å oppnå enda mer effektiv datareduksjon i neste sak.

[82] *Aquilina* (2008) s. 205, sier om identifikasjon av "malware" ved hjelp av sjekksum: "When a particular piece of malware already has been identified, hash analysis may identify other files with the same data but different names." Det samme gjelder datafiler som for eksempel inneholder overgrepsbilder eller musikk. Identifikasjonsverktøyet tar ikke hensyn til typen innhold.

3.3.4 Data, dubletter og gjentakelser

Data deles og spres ved kopiering. Kopiene er dubletter, dvs. datafiler med lik sjekksum. Kopiering skjer både som følge av bevisste handlinger hos brukerne, og på grunn av automatiske funksjoner i teknologien selv. Automatiserte funksjoner for kopiering er lagt inn i teknologi og tjenester for å lette tilgjengeliggjøring og sørge for at kommunikasjonen går mest mulig effektivt. Brukeren kan for eksempel skape dubletter av sitt eget materiale, selv om intensjonen bare er å skaffe seg kopier fra andre. Det er tilfelle ved moderne fildelingsteknologi, hvor deltakerne tvinges til å dele data med andre.

Nettverksteknologien leder altså til utbredelse av dubletter *som følge av teknologiens egen funksjonalitet og dynamikk*. Derfor er det treffende som den norske bloggeren og journalisten *Kalsnes* sier, at "Internett er den beste kopimaskinen mennesker noen gang har laget."[83]

Internett er sagt å ha gitt informasjonsmakten til brukerne. Dette aspektet av det nye *informasjonsparadigmet* har ifølge den amerikanske juristen *Benkler,* endret informasjonsmarkedet fra enveiskommunikasjon med brukerne som *konsumenter*, til et marked med brukerne som informasjons*produsenter*.[84] Det stimulerer meningsbrytningen i samfunnet, noe som er til gagn for alle. Karakteristikken "informasjonsprodusent" kan imidlertid forstås å bety at brukeren tilveiebringer *nytt stoff*. Men som sitatet av *Kalsnes* indikerer, slår ikke denne forutsetningen bestandig til. Det ville være å overse en stor dimensjon av nettbruken om man neglisjerte dublettene.

Med tanke på det rettsstridige innholdet som avhandlingen behandler, leder dublettene til at det rettsstridige innholdet stadig verserer, fordi det stadig kopieres og tilgjengeliggjøres på nytt. Dublettene kan anses som *verserende gjentakelser* av noe som tidligere er ytret eller

[83] *Kalsnes* (2009) "Krigen mot kidsa", artikkel i Morgenbladet 24. april 2009, på s. 9.
[84] *Benkler* (2000). Se for øvrig *Hannemyr* (2005) s. 99-100, som interessant forteller om hvordan Bertold Brecht i et essay på 1920-tallet kritiserte den nye oppfinnelsen *radioen* for bare å bli brukt til *distribusjon* og ikke til *kommunikasjon.* Dermed ble radioens politiske og pedagogiske potensial uforløst. I essayet beskrev Brecht en fremtidig radio hvor skillet mellom avsender og mottaker var opphevet ("Der Rundfunk als Kommunikationsapparat"). Senere i avhandlingen kommer jeg inn på et annet aspekt av informasjonsparadigmet, nemlig at elektronisk informasjon blir ansett som et produkt eller vare i seg selv (se kapittel 8.2).

tilgjengeliggjort.[85] Gjentakelsene leder til en stor opphopning og utbredelse av det rettsstridige materialet i nettet. På denne bakgrunn konkluderer den britiske kriminologen *Wall* med at det er behov for en ny tilnærming ved beskrivelsen av de straffbare handlingene, føringen av kriminalitetsstatistikken og oppfatningen om viktimiseringen. Han kaller problemet *"the globalized aggregate volume".*[86]

Dubletter som problem er også registrert her hjemme, uten at ordet "dublett" nødvendigvis er brukt. Personvernkommisjonen har blant annet behandlet risikable sider ved barns nettbruk, for eksempel at de legger ut seksualiserte bilder av seg selv på en tjeneste som deiligst.no, eller bilder fra helgens fest på Facebook.[87] Kommisjonen konstaterer at

> "Personopplysninger som legges ut på Internett *kan bli liggende lenge* og kan påvirke de sosiale relasjonene barnet søker å opprette i lang tid fremover." (min uth.).[88]

Det at bildene blir "liggende lenge" innebærer ikke at de nødvendigvis ligger på en og samme nettadresse over tid. Poenget er at bildet lastes ned og redistribueres på stadig nye nettadresser, så de kan bli liggende lenge på nettet selv om de er slettet fra den opprinnelige nettadressen.

Høyesterett har kalt effekten av dublettene "en livsvarig krenkelse" av barnet på bildet (Rt. 2002 s. 1187 på s. 1191). Uttalelsen står i følgende avsnitt hvor konsekvensene av dublettene er beskrevet:

> "I tillegg til den enorme spredning som oppnås ved å legge bilder ut på Internett, er det *i praksis ikke mulig å få slettet dem*. Barn som er blitt misbrukt gjennom produksjon av pornografi, vil således oppleve å kunne bli gjenkjent i årevis. Det dreier seg i slike tilfeller om *en livsvarig krenkelse*, som aktor ganske treffende uttrykte det. Man må regne med at risikoen for at andre kommer over bildene vil være en betydelig tilleggsbelastning senere i livet for den det gjelder." (s. 1192, min uth.).

[85] Jeg skrev "tilgjengeliggjort" fordi at som jeg forklarer i kapittel 4.4, kan ikke skadelig objektkode anses å være en ytring.
[86] *Wall* (2007) s. 19.
[87] NOU 2009: 1 s. 136.
[88] NOU 2009: 1 s. 128. Kommisjonen påpeker at "det å publisere bilder og opplysninger om seg selv og andre [er] blitt en naturlig del av måten å kommunisere på" for barn og ungdom, og at det "er ikke like lett å forstå hva det innebærer at informasjon om deg og vennene dine *blir lagret for lang tid* og at denne kan være av interesse for kommersielle aktører *og andre uvedkommende (for eksempel kriminelle aktører)*" (s. 135) (min uth.). Det er dublettene som forårsaker problemene med at bildene stadig kan dukke opp igjen.

Man kan se det slik at dublettene er utslag av ett og samme fenomen. Det er bærende tanke hos *Wall,* det samme fenomenet gjør seg gjeldende "overalt".[89] Jeg anvender denne tilnærmingen som grunnlag for å inndra dublettene under ett (se kapittel 11).

Kopieringsevnen har også betydning for spørsmålet om eiendomsretten til dublettene. Strafferettslige regler om inngrep overfor "ting" og vern av "gjenstand", forutsetter at objektet er undergitt eiendomsrett. Inngreps- og straffebestemmelsene speiler hverandre, så "ting" og "gjenstand" må antas å være nært beslektede begreper.[90] Dublettene er utslag av ikke-rivalisering, dvs. at deling medfører at det blir mer og ikke mindre av godet.[91] Dublettene er derfor forskjellige fra fysiske objekter hvor den enes utnyttelse går på bekostning av en annens (ekskluderbarhet). I kapittel 7.5 reiser jeg spørsmål om kopiering kan anses å berøre eiendomsretten til data. Det har betydning for om inndragning kan brukes overfor dublettene.

Dublettene har altså betydning for flere av avhandlingens rettsspørsmål, så det er behov for ytterligere konkretisering av hva som kan forårsake delingen og produksjonen av dubletter:

Brukeren kan ha som motiv å sørge for størst mulig spredning av innholdet. Da kan det være hensiktsmessig å bruke spesielt effektive tjenester som fildeling eller news. Vedkommende kan også sende ut et selvspredende program "(datavirus"), som har funksjonalitet for å skape dubletter av seg selv. Men selv om brukeren bare ønsker begrenset spredning - han sender for eksempel et overgrepsbilde med epost til en venn - har avsender gitt fra seg kontrollen over bildet, og kan ikke hindre at mottaker i neste omgang deler bildet på mer effektive tjenester. *Førstegangsspredning* er derfor en nærmest uopprettelig handling dersom det ikke settes inn omfattende og systematiske tiltak for å avbøte skaden

Men produksjon av dubletter kan også være et resultat av hvordan teknologien virker, uten at brukeren har hatt stor spredning som motiv for bruken av en tjeneste. Her er noen eksempler på hvordan dubletter skapes:

[89] *Wall* (2007), jf. "the globalized aggregate volume".
[90] Se problemstillingen beskrevet i kapittel 6.2, og drøftelsene i del IV.
[91] Ikke-rivalisering er egentlig definert ved at den enes nytelse av et gode ikke skjer til fortrengsel for en annens nytelse av det samme godet. Et slikt gode kalles gjerne fellesgode ("a public good"). *Gaustad* (2002) mener at pirateri av vernede verk leder til at verket endres fra et salgbart til et ikke salgbart fellesgode, og viser til ikke-rivaliseringens effekter. Se mer om dubletter som ikke-rivaliserende gode i kapittel 11.5.1.

- Når man sender et bilde i en melding til en newsgruppe, sørger "backbone nettet" (Usenet) for å spre meldingen til newsgrupper over hele verden. I løpet av et par minutter er et utall dubletter gjort tilgjengelig globalt. Kildefilen er intakt så avsender beholder kontrollen over sin dublett.[92]

- Når man sender en epost er det vanlig at kopien legges i mappen "sendt". Etter sending har både avsender og mottaker en identisk kopi av eposten, dvs. dubletter.

- Når man ser på en webside, lastes et eksemplar ned for mellomlagring i nettleseren (en såkalt "temp-fil", jf. Temporary Internet Files). Websiden er intakt og en dublett er lagret hos brukeren, som kan velge å lagre den permanent.

- Dersom man laster en fil opp til et nettsted, finnes en dublett på den lokale maskinen og på nettstedet. Den videre spredning av dubletter vil skje selv om brukeren logger av den lokale maskinen, fordi andre brukere laster ned meldingen fra nettstedet. Meldingen er uansett tilgjengelig dersom nettstedet er opprettet hos en nettvert. Filen kan også være programmert for automatisk viderespredning, dvs. et selvspredende dataprogram som for eksempel automatisk legger seg inn på datamaskinen til brukeren som oppsøker nettstedet.

- Fildelingsteknologien tvinger deltakerne til å dele data samtidig som de laster ned. Delingen starter idet filene gjøres tilgjengelig fra brukerens datamaskin, og dermed skapes en "sverm" av data som kopieres mellom alle deltakerne. Alle gjøres automatisk til bidragsytere.[93] Funksjonen bidrar til å jevne ut belastningen i nettet og

[92] *Sunde* (2006) redegjør for spredningsforbudet i strl. § 204a, og angir posting i news som et alternativ. Posting til news forklares der som: "en e-postliknende melding sendt til en newsgruppe. Siden meldingen blir tilgjengeliggjort globalt i løpet av få minutter, er dette en spredningshandling med vidtgående effekt.", s. 237. Se også *Sunde* (2006) s. 223-224 og s. 249-251 om fildelingstjenester. Av relevant rettspraksis, kan nevnes Rt. 2003 s. 1091. I lagmannsretten (LG-2002-322) antok man at den aktuelle postingen ikke kunne regnes som spredning, ettersom domfelte kun hadde sendt bildet til avsenderen (den newsgruppe han hadde hentet bildene fra). Høyesterett fant det "ikke tvilsomt" at det dreide seg om en reell spredningsfare (avsn. 16). Avgjørende var at materialet som lastes ned, også er tilgjengelig for andre som er tilknyttet tjenesten. Tilbakesending av materialet *øker tilgjengeligheten* fordi at etter postingen kan informasjonen nås på flere nettadresser i news.

[93] De blir også til lovbrytere, siden delingen er en straffbar overtredelse av eneretten til tilgjengeliggjøring av verket, jf. åvl. § 2, jf. § 54, med mindre noen av reglene som gjør delingen rettmessig kommer til anvendelse. Det kan tenkes at delingen bare skjer innen en privat krets, dvs. at den er satt opp mellom et begrenset antall kjente. Det var ikke tilfelle i den svenske "Pirate Bay"-saken (B 13301-06, første instans) hvor tilretteleggerne ble domfelt for medvirkning til overtredelse av eneretten til tilgjengeliggjøring m.v.. Åpen deling kan skje for verk som har falt i det fri, eller hvor det foreligger samtykke fra rettighetshaveren eller noen som representerer

effektiviserer kopieringen. Deltakelsen medfører at en stadig større mengde dubletter akkumuleres blant deltakerne på tjenesten.

De nevnte eksemplene tar utgangspunkt i individuell bruk. Større innholdsleverandører og tilbydere av overførings- og mellomlagringstjenester bidrar også til fremstilling av dubletter, blant annet ved "cache-" og "mirroring"-løsninger. Det er funksjoner som går ut på å lagre samme materiale mange steder i nettet, for å korte ned distansen til brukerne. Dermed effektiviseres trafikken. Et annet eksempel er "bufringssider" som benyttes i søketjenester ("søkemotor"). Selv om den opprinnelige websiden er fjernet, kan dubletten ligge "bufret" hos søketjenesten slik at materialet gjøres tilgjengelig lenger og flere kan utnytte det.

Alle aktivitetene genererer dubletter uten konsekvenser for kildefilen; den forblir intakt. Dersom noe materiale skal "forsvinne" må slettingsfunksjoner iverksettes, eller det må gis instruks om "ikke-lagring". Sistnevnte mulighet er ikke et reelt alternativ for mange tjenester. Sletting er imidlertid mulig, og det kan søkes etter rettsstridig materiale i nettet for å iverksette sletting. Dessuten kan elektronisk kommunikasjon blokkeres for å redusere spredningen, slik det gjøres mot datavirus, og slik spørsmålet dermed er for automatisert inndragning.

Sletting har sine begrensninger siden data kan rekonstrueres. Rekonstruksjon av data på et lagringsmedium er mulig inntil de er overskrevet av nye tegn.[94] Filer kan også tilsynelatende fjernes ved å sørge for at de ikke er søkbare. Filer er ordnet etter en "innholdsfortegnelse" og dersom "pekeren" er fjernet kan ikke filen leses på systemet på vanlig måte.[95] Dataene finnes imidlertid på lagringsmediet og kan avdekkes ved dataanalyse. Med god lagringskapasitet tar det lang tid før systemet har behov for å overskrive slettede data med nye tegn.[96]

rettighetshaveren. Se *Rognstad* (2008) særlig s. 532 flg., og (2009) s. 365 om samtykkespørsmålet på nettet (omtalt også her i avhandlingen i kapittel 7.5 om eiendomsrett til data).

[94] Slik tilfellet var i Rt. 2007 s. 422: "Av de 37 bildene var 28 slettet på beslagstidspunktet" (avsn. 8). Interessant i denne sammenheng er også RG 2004 s. 929 (Eidsivating), hvor tiltalte umiddelbart hadde slettet de aktuelle filene, og dermed "gjort materialet utilgjengelig for seg selv.", nederst i domspremissene. Tiltalte ble frifunnet da lovens krav til "besittelse" ikke kunne anses oppfylt (filene var såkalte "Temporary Internet Files")

[95] *Casey* (2004) s. 257: "To locate data on a volume, these file systems [FAT12, FAT16 og FAT32] use directories and a FAT. The root directory … is at a pre-specified location on the volume so that the operation system knows where to find it."

[96] Se *Vacca* (2002) s. 209 flg.

Dubletter skapes ikke bare ved nettverkstrafikk, men også ved aktiviteter som skjer lokalt. Med "lokalt" menes data som er i besittelsen til en fysisk eller juridisk person, på vedkommendes brukerområde, datamaskin, og løse lagringsmedier. Det at dubletter kan forekomme hos ett og samme individ kan ha flere årsaker, blant annet at

- Samme data er lastet ned flere ganger fra nettet;
- det kan være foretatt sikkerhetskopiering ("back up");
- filer er flyttet rundt mellom forskjellige områder på harddisk;[97]
- filer er flyttet fra en datamaskin / brukerområde til en annen;[98]
- dubletter finnes blant slettede filer;
- mer tilfeldige årsaker, for eksempel at mangel på system og oversikt leder til at samme fil lagres flere steder;
- midlertidig lagring som skjer automatisk av programmer på systemet, for eksempel i word, i printerprogrammet og i nettlesern).

Spredningen av dubletter på nettet har betydning for avhandlingen fordi det er overfor dublettene at automatisert inndragning kan la seg praktisere. Delingsevnen som skaper dublettene er etter mitt syn en egenskap som gir rettslig grunnlag for at inndragningen i straffesaken gis rettsvirkninger for dublettene i nettet, se kapittel 11.

3.3.5 Asymmetriske rettighetsforhold – Web 2.0

Tidligere var det vanlig at data var bundet til et bestemt lagringsmedium, hvor både data og fysisk bærer tilhørte samme person. Nettverksteknologien har radikalt endret situasjonen. Nå legges det opp til bruk av "hosting"-tjenester, hvor brukerens data lagres på servere i den såkalte "internettskyen" ("the cloud"). Utviklingen har fått betegnelsen "web 2.0", eller "cloud computing".[99]

[97] Rt. 2005 s. 1058: "Han har imidlertid i 10 års perioden ikke fjernet noe av det materialet han lastet ned, kun lagret det på et annet område på serveren i perioder." (avsn. 9).
[98] Rt. 2005 s. 919 "over en periode på tre måneder sommeren 2001 lastet [han] ned, lagret og videreformidlet barnepornografiske bilder og filmer. Etter nyttår lagret han materialet på sin datamaskin på arbeidsstedet" (avsn. 9).
[99] Uttrykket "web 2.0" ble lansert av *O'Reilly* (2005) og betegner ressursdeling med webben som plattform. Personvernkommisjonen bruker web 2.0 om de "sosiale nettsamfunn", som Facebook, Nettby og MySpace (NOU 2009: 1 s. 113), smlg. *Storsul* (2008) s. 9. Det som uansett er helt sentralt, er *ressursdelingen,* enten det er tale om tanker og ideer, rådata, maskinkapasitet eller forretningsforholdet mellom store og små aktører på nettet. Ressursdelingen er det fenomen som ligger under uttrykk som "the long tail", "den kollektive intelligensen", "the generative net" (*Zittrain* (2006b) og (2008a)) og "wikinomics" (*Tapscott* (2008)).

Tankegangen er at i en mobil tilværelse med høye krav til effektivitet, er det behov for å ha enkel tilgang til sine data uansett hvor man er. Dataene er sikrere og lettere tilgjenglig når de er lagret hos en nettvert enn når man har dem på sin lokale maskin. Brukeren trenger bare utstyr for å koble seg opp til serveren. I en rapport fra tidsskriftet *"The Economist"* i 2008 forklares det at

> "…data centres are becoming factories for computing services on an industrial scale; software is increasingly being delivered as an online service; and wireless networks connect more and more devices to such offerings."[100]

Dermed går utviklingen i retning av at *asymmetriske rettighetsforhold* blir vanlige, hvor den fysiske bæreren i infrastrukturen tilhører nettverten, mens dataene tilhører den individuelle bruker. Brukeren kan administrere og utnytte sine data ved bruk tjenester som tilbys fra "skyen" (eller "nettet"), uten å ha noe forhold til hvor dataene fysisk er lagret.

Utviklingstrekket gir støtte for å anse data som et fenomen som må holdes prinsipielt atskilt fra den fysiske bæreren. Interessene mellom rettighetshaverne kan til og med komme i konflikt, for eksempel dersom nettverten oppdager at brukerens data har et verdifullt innhold, og ønsker å skade eller tilegne seg dem.

Asymmetrien gir grunnlag for å reise spørsmål ved holdbarheten av å anse data og den fysiske bæreren som et integrert objekt strafferettslig sett. Doktrinen om det funksjonelle gjenstandsbegrepet er basert på et slikt syn, og det er mulig at formuleringen "elektronisk lagret informasjon" i inndragningsregelen i strl. 2005 § 69 annet ledd, må anses som utslag av det samme.[101] Asymmetrien leder også til at spørsmålet om muligheten for å ha eiendomsrett til data kommer på spissen. Det gir grunn til å se den fysiske bæreren og dataene som to forskjellige objekter strafferettslig sett. Konsekvensen i forhold til inndragning er at dataene kan inndras dersom de er lagret i "internettskyen", uten at det oppstår spørsmål om å foreta inndragning av nettvertens server. En tilsvarende situasjon oppstår i forholdet mellom arbeidsgiver og arbeidstaker, der arbeidstakeren har misbrukt datautstyret til å laste ned

[100] *The Economist* (2008) s. 2. Sitatet følges opp med at "Cloud applications … will be used by billions of devices of all kinds, many of them untethered, but will be connected to the "internet of things" (s. 2)
[101] Disse spørsmål er behandlet i del IV, særlig kapittel 7.6.3.

overgrepsbilder fra nettet. Også da kan det være praktisk at bare datafilene inndras. Ytterligere gir det mulighet for å inndra dublettene i nettet uavhengig av hvor de befinner seg.

Asymmetrien mellom det nederste og midterste nivået i modellen, føyer seg til en asymmetri som er mer velkjent, nemlig forholdet mellom data og databasert innhold på øverste nivå i modellen. Dette forholdet kommer for eksempel opp ved spørsmål om retten til eget bilde, jf. åvl. § 45 c. Fotografen eier bildet og følgelig dataene som representerer det, mens den avbildete person kan nekte samtykke til offentliggjøring. Den avbildete har en rettighet i innholdet, mens mediet tilhører fotografen. Eksemplet er egnet til å lede tanken over på rettigheter til barn som er avbildet på overgrepsbilder. De har en selvstendig rett til innholdet, en rett til respekt for sitt privatliv, jf. EMK art. 8, og må antas å ha en rett til å få brakt integritetskrenkelsen til opphør. Dette er et hensyn som inngår i inngrepsvurderingen med hensyn til automatisert inndragning i nettet.[102]

3.4 Oppsummering

I dette kapitlet har det fremgått at data kan konkretiseres og identifiseres, og at hash teknologi er et velprøvd verktøy for å gjøre dette. Videre har jeg beskrevet årsaken til det problem avhandlingen analyserer, nemlig produksjonen av dubletter med rettsstridig innhold. Dublettene er gjentakelser av innhold som tidligere har vært tilgjengeliggjort. Dublettene kan gjenkjennes (kontrolleres) i henhold til dataidentiteten (sjekksummen). Til slutt har jeg beskrevet den vanlig forekommende asymmetrien i rettighetsforholdene til den fysiske bæreren, dataene og innholdet i dataene. Det gir grunn til å inndra datafilene som selvstendige objekter.

I neste kapittel går jeg inn på forholdet mellom data som objekt og den databaserte informasjonen som ytring. Det har betydning for inngrepsvurderingene, både etter inndragningsreglene, og i forhold til EMK art. 10, ved vurderingen av automatisert inndragning i nettet.

[102] Se del kapittel 16.3.

4 Forholdet mellom ’data’ og ’ytring’

4.1 Problemstilling

I det foregående er det konstatert at en datafil kan gis en identitet og senere gjenkjennes ved bruk av hash teknologi. Det har også fremgått at for et datasystem som skal identifisere rettsstridige datafiler i henhold til dataidentiteten, er filenes innhold uten betydning. Rent teknisk kan data lagres, behandles, overføres og identifiseres uten hensyn til innholdets karakter.[103] Men i forhold til *de rettsregler* avhandlingen behandler har innholdet betydning. I første rekke er det viktig å avklare spørsmålet om datafilen representerer en *ytring*. Det har betydning for subsumsjonsvalget ved forebyggende inndragning, reglene for gjennomføring av inndragning, og betingelsene for filtrering i nettet (automatisert inndragning).[104] Dersom datafilen bærer meningsinnhold kan kommunikasjonen anses som en ytring, og da gjør vernet om ytringsfriheten seg gjeldende.

Men hvis dataene ikke bærer meningsinnhold, hvordan bør de da karakteriseres? Er datafilen i så fall bare en ting, kanskje et verktøy? Dette berører *tingliggjøringen* av data, hvor dataene kan ses som en ”boks” eller en ”bok” med innhold. I en mengde data kan bestemte filer plukkes ut og inndras, slik man kan plukke ut andre ting fra en mengde. På samme vis som bøker og spritflasker er ting, er data etter min mening en ting. Noen ganger bærer dataene meningsinnhold, andre ganger er de bare ting. Uavhengig av en mulig status som ytring, kan teknologien behandle datafilen som en ting, noe som er helt sentralt for anvendelsen av inndragningsreglene på data. Men det at data, selv om de bare er en ting*, kan ha forskjellig status* i forhold til et sentralt begrep som ytring, er iblant et rettslig relevant poeng.

Behandlingen av inndragningsreglene og forholdet til vernet om ytringer kommer jeg inn på flere steder i avhandlingen, men jeg har valgt å behandle det generelle forholdet mellom data og ytring allerede her. Alternativet er å foreta fastleggingen av begreper i forbindelse med

[103] Jeg utelukker ikke at det for eksempel er mer kapasitetskrevende å håndtere store mediefiler enn mindre tekstfiler, men slike tekniske omstendigheter har ikke betydning her.
[104] Ved forebyggende inndragning er spørsmålet om inndragningen skal skje med hjemmel i strl. 2005 § 70 første punktum (”ting”) eller tredje punktum (”informasjonsbærer” – som forutsetter at dataene bærer et meningsinnhold) (se kapittel 5.4). Ved alminnelig reaktiv inndragning av ”ting”, jf. strl. 2005 § 69, oppstilles særregler for gjennomføring av inndragningen når ”tingen” er ”informasjonsbærer”, jf. strl. 2005 § 76 (se kapittel 5.6). Inndragning ved filtrering i nettet må også forholde seg til vernet om ytringer. Direkte gjelder det dersom datafilen som filtreres bærer en ytring. I tillegg må det vurderes om inngrepet på grunn av sin generelle karakter innebærer et inngrep overfor andre lovlige ytringer på nettet, jf. doktrinen om ”chilling effect” (se kapittel 15).

drøftelsen av gjeldende rett, men det gir bedre flyt i drøftelsene å kunne basere seg på at forholdet mellom sentrale begreper allerede er avklart.

4.2 Begrepet 'ytring'

En ytring er meningsinnhold som formidles mellom mennesker.[105] Meningsinnholdet behøver ikke faktisk å ha blitt formidlet, men det må være av en slik art at det kan oppfattes av mennesker dersom det formidles.[106] En ytring må følgelig ha menneskelig avsender og adressat. Det utelukker ikke bruk av *formidlere* av teknisk art, for eksempel radio eller internett, men meningsinnholdet må komme fra og være beregnet for et menneske.[107]

For avhandlingens formål er det ikke behov for en fullstendig kartlegging av ytringsbegrepet. Det kan kort konstateres at sentrale bestemmelser til vern om ytringsfriheten taler om "Oplysninger, Ideer eller Budskab" (G § 100), "opplysninger og ideer" (EMK art. 10) og "opplysninger og tanker av alle slag" (SP art. 19). Ytringsbegrepet i de nevnte konvensjonene er innlemmet i norsk rett med forrang fremfor formell lov, jf. mrl. § 2, jf. § 3, men viker ved eventuell motstrid for Grunnlovens bestemmelser. Motstridsspørsmål er det ikke nødvendig å komme inn på her. Og i den grad det er behov for å trekke inn rettskilder knyttet til konvensjonene holder jeg meg til EMK med sin rikholdige rettspraksis.

De siterte formuleringene refererer seg til vilkåret om at en ytring må ha et meningsinnhold, noe som skal forstås langt videre enn tekst og tale. Ifølge *Eggen* omfattes

> "ikke bare språklige ytringer, men enhver ytring som gir uttrykk for et meningsinnhold. Eksempelvis omfattes malerier, fotografier, skulpturer og ytringer i form av fysiske bevegelser som gir uttrykk for en meningsytring."[108]

[105] *Andenæs/Fliflet* (2006) s. 385: "Med «ytring» menes formidling av informasjoner eller ideer, meninger."
[106] *Bing* (2008) s. 22-25. Ytringsfrihetskommisjonen gir uttrykk for det samme i sin gjennomgang av forskjellige kategorier som omfattes av ytringsbegrepet. Se NOU 1999: 27 kapittel 2.3.
[107] Begrensningen til mellommenneskelig kommunikasjon er reelt begrunnet i ytringens betydning for menneskets personlige utfoldelse (autonomibegrunnelsen), og for dets evne til å opptre som bidragsyter til et godt samfunn og styresett (demokrati- og sannhetsbegrunnelsene). Om disse hensynene, se *Eggen* (2002) kapittel 2 og *Barendt* (2007) kapittel I.2 s. 56 flg. Grunnhensynene bak ytringsfriheten ble ved innføringen av ny G § 100 inntatt i lovteksten, jf. annet ledd første punktum som lyder: "Ingen kan holdes retslig ansvarlig for at have meddelt eller modtaget Oplysninger, Ideer eller Budskab, medmindre det lader seg forsvare holdt op imod Ytringsfrihedens Begrundelse i Sandhedssøgen, Demokrati og Individets frie Meningsdannelse."
[108] *Eggen* (2002) s. 162 i relasjon til EMK art. 10. Smlg. *Bing* (2008)s. 22; *Van Dijk* (2006) s. 779 som skriver at art. 10 blant annet omfatter "photos, medical secrets, the search for historical truth, factual statements in

I datasammenheng må innholdet i data kunne *presenteres for et menneske* for å være meningsinnhold. Det er altså tale om presentasjon av skrift eller bilder på skjerm (databasert informasjon i objektiv forstand).[109] I straffeloven 2005 er slike ytringer kalt "budskap", jf. legaldefinisjonen av offentlig handling som består i fremsettelse av et budskap, i strl. 2005 § 10 annet ledd annet punktum, som lyder

> "Består handlingen i fremsettelse av et budskap, er den også offentlig når budskapet er fremsatt på en måte som gjør det egnet til å nå et større antall personer."

Legaldefinisjonen er utformet slik at den kan fange opp ytringer på internett, selv om forarbeidene understreker at bestemmelsen er medienøytral.[110] Det sies således at definisjonen også omfatter budskap "som er lagt ut på internett".[111] Og "budskap" omfatter ifølge forarbeidene

> "alle typer av budskap uansett innhold og formidlingsform: skriftlig, muntlig, billedlig, tegn, symboler mv.".[112]

Videre er det slik at en ytring er en handling, mens ikke alle handlinger er ytringer. Da ville det ikke vært behov for et særskilt vern om ytringsfriheten. *Ytringsfrihetskommisjonen* har således presisert at

> "… institusjonaliseringen av ytringsfriheten er basert på et klart skille mellom tale og handling som fører til materiell eller fysisk skade".[113]

Skadevoldende handlinger og vold mot person faller utenfor ytringsbegrepet.[114] Andre handlinger kan imidlertid omfattes, men da må de oppfylle noen vilkår: Det gjelder et krav

---

interviews, television commercials, and advertisements in newspapers"; se også *Harris* (2009) s. 444-445 og om forskjellige kategorier av ytringer på s. 455-465.
[109] Se kapittel 2.2.
[110] Ot.prp. nr. 90 (2003-2004) kapittel 12.2.2 s. 164.
[111] Ot.prp. nr. 90 (2003-2004) kapittel 12.2.2 s. 163. Den formulering som er inntatt for å gjøre legaldefinisjonen anvendelig for budskap på internett er "egnet til". En tilsvarende formulering ble i 2005 inntatt i strl. 1902 § 135 a for å ramme diskriminerende og hatefulle ytringer på nettet, uten at legaldefinisjonen i strl. 1902 § 7 ble endret tilsvarende (lovendring 3. juni 2005 nr. 33). Jeg har skrevet om dette i forbindelse med straffenormenes anvendelse på internett og internett som arena for strafferettslig rettshåndhevelse, se kapittel 11.2.1.
[112] Ot.prp. nr. 90 (2003-2004) kapittel 12.2.2 s. 164.
[113] NOU 1999: 27 kapittel 2.3.1 s. 26. Se også *Eggen* (2002) s. 680 flg.
[114] NOU 1999: 27 kapittel 2.3.1 s. 26 hvor det sies at "Voldshandlinger vil ikke ha noen beskyttelse som ytring."

om at handlingen utføres i den hensikt å kommunisere informasjon eller ideer til omverdenen. Denne hensikten må være objektivt synbar for omgivelsene. Det er ikke tilstrekkelig at den handlende sier at vedkommende ønsket å ytre seg ved handlingen, det må også fremstå slik for omgivelsene.[115] Hvis ikke kunne enhver handling anses beskyttet som ytring, bare fordi den handlende *sa* at den var ment slik.

Elektroniske skadeverk kan begås på nettet, for eksempel i form av overbelastningsangrep (såkalt "Denial of Service" eller "tjenestenekt").[116] Fordi det er en straffbar skadevoldende handling faller det allerede i utgangspunktet utenfor ytringsbegrepet. Men dersom man stilte seg velvilling og likevel vurderte om det kunne være en ytring, ville det ikke være tilstrekkelig at vedkommende som sto bak angrepet *sa* at det var en ytring (for eksempel en politisk mishagsytring som kom til uttrykk ved å lamme regjeringens nettbaserte opplysningstjeneste www.regjeringen.no). Det kreves at kommunikasjonshensikten virkelig forelå og var objektivt synbar. Særlig synbarhetsvilkåret er vanskelig å oppfylle på nettet. Ved et overbelastningsangrep sendes så mange elektroniske signaler til serveren som er målet for handlingen, at den overbelastes og lammes. Handlingen legger ikke igjen noen beskjed, den resulterer kun i funksjonssvikt. Det er intet ved handlingen isolert sett som viser at den er ment som en politisk ytring. Lovbryteren kan poste en begrunnelse for overbelastningsangrepet på en nettside eller en pratekanal, og begrunnelsen er i så fall en ytring. Men den medfører ikke at DOS-angrepet blir en ytring, fordi handlingen mangler en dimensjon som kan vise kommunikasjonshensikten.

Med disse utgangspunkter går jeg over til å behandle databaserte overgrepsbilder og skadelig dataprogram i forhold til ytringsbegrepet.

[115] *Eggen* (2002) s. 688. *Eggen* fremholder at det "skal meget lite til for at en «handling» skal anses som en «ytring»", men har ikke relatert uttalelsen til nettbaserte handlinger.

[116] Ringerike herredsretts dom av 13. desember 2001 (sak nr. 01-00552 M) (domfellelse) gjaldt skadeverk begått ved å lamme servere ved DOS-angrep. I strl. 2005 § 206 er det tatt inn en bestemmelse om fare for driftshindring som er direkte anvendelig på handlingen. Bestemmelsen lyder: "Med bot eller fengsel inntil 2 år straffes den som ved å overføre, skade, slette, forringe, endre, tilføye eller fjerne informasjon uberettiget volder fare for avbrudd eller vesentlig hindring av driften av et datasystem." Se motivene i Ot.prp. nr. 22 (2008-2009) kapittel 2.15.5.2 s. 63 og s. 405. Bestemmelsen kommer til anvendelse for angrep som er rettet direkte mot datasystemet eller indirekte "ved at båndbredden er oppbrukt. Det betyr at såkalte DOS-angrep vil omfattes av bestemmelsen." (s. 405).

4.3 Overgrepsbilder i elektronisk form

Fotografier av barn som utsettes for seksuelle overgrep og bilder av barn i seksuelt betonte poseringer, formidler faktiske hendelser og er således opplysninger, jf. "opplysninger og ideer" i EMK art. 10, jf. det som alt er sagt om dette. Bestemmelsen omfatter bilder. [117] Overgrepsbilder er ment for menneskelige adressater, innholdet er meningsinnhold og bildet oppfyller kriteriene for å være en ytring. Inndragning av datafiler med overgrepsbilder, må følgelig ta hensyn til de reglene som er beregnet på ytringer.

4.4 Skadelig dataprogram: Kildekode og objektkode

"Datamaskinprogram" nyter opphavsrettslig vern som *litterært* verk, jf. åvl. § 2 nr. 12.[118] Det impliserer likevel ikke at et dataprogram representerer meningsinnhold og er en ytring. Med 'dataprogram' menes strafferettslig sett dataprogrammet slik det konkret foreligger, ikke åndsverket. Det er altså dataprogram i form av objekt- eller kildekode som omfattes av "dataprogram" i strl. 2005 § 201 bokstav b. Det er dataprogram i konkret manifestasjon, som også omfattes av det strafferettslige begrepet "ting" (se kapittel 5.3.1).[119]

Kildekoden er en formalisert tekst som beskriver et dataprogram. Datakrimutvalget har beskrevet kildekode på denne måten:

> "Kildekode er en beskrivelse av virkemåten til et dataprogram, i en form som er lett forståelig for mennesker og som er eller kan oversettes til et kjørbart dataprogram. En slik beskrivelse er som en

[117] *Van Dijk* (2006) fastslår at den siterte formuleringen i konvensjonsbestemmelsen "offers a broad protection […] *inter alia,* photos…" (s. 779). Fiktive bilder, tegneserier og animasjoner med tilsvarende motiv representerer fantasier om det samme, og gir således uttrykk for "ideer". Jeg har som nevnt avgrenset avhandlingen mot å behandle slikt materiale (se kapittel 1.1).

[118] Ot.prp. nr. 33 (1989-1990) kapittel 5.1. Det fremgår at man vurderte å presisere at vernet fulgte av alternativet "litterære verk", siden det ikke fremsto som helt innlysende. Innledningen til åvl. § 1 omfatter tre hovedkategorier, litterære, vitenskapelige og kunstneriske verk, og alle eksemplene i bestemmelsens liste nr. 1-13, må kunne henføres til ett av disse alternativene. Departementet kom til at det ikke var behov for en særskilt presisering for datamaskinprogrammer når det ikke var gjort for de øvrige eksemplene. Se også *Wagle* (1997) kapittel 3.1.2 s. 72 som opplyser at "Lovgiver har ansett datamaskinprogrammer som en undergruppe av litterære verk." *Wagle* påpeker også at åndsverkloven bruker "datamaskinprogram" både om *verket* og om *eksemplarene.* I §§ 1 og 39g betyr det verket, og i § 12 annet ledd bokstav b, § 19 annet ledd og §§ 39h, 39i og 53c (tidligere § 54a) om eksemplarene (kapittel 3.1.3 s 72).

[119] I opphavsretten taler man om "eksemplar" når verket foreligger i konkret form, men "eksemplar" er ikke et strafferettslig begrep. I forhold til inndragningsreglene er det "ting" som er det relevante begrepet. I kapittel 11.3.4 har jeg gått inn på forholdet mellom begrepene "eksemplar" og "ting" i diskusjonen av mulige rettsgrunnlag for inndragning av dublettene.

> prosatekst som beskriver virkemåten til programmet. Teksten følger som enhver tekst grammatiske og syntaktiske regler, som i tilfelle kildekode er definert i programmeringsspråket som er benyttet." [120]

Kildekoden kan beskrive et skadelig dataprogram så vel som et annet program. Den kan leses av en kyndig person, og utgjør som det fremgår av sitatet, et meningsinnhold. Kildekoden kan derfor representere en ytring, men det forutsetter i tillegg at den presenteres for en menneskelig adressat.

For bruk på datamaskinen er det vanlig å konvertere kildekoden til objektkode.[121] *Objektkoden* er beregnet på datamaskinen, dvs. at den kan bare virke på en datamaskin.[122] Et menneske kan undersøke kodens innhold, omtrent som man kan undersøke hvordan en bil er bygd opp, men innholdet i koden er ikke ment som budskap til et menneske.[123] Objektkoden er derfor ikke en ytring og kan vel best anses som et verktøy som gir instruksjoner til datamaskinen om hvordan den skal oppføre seg (for eksempel slippe inn en ny ukjent bruker), og om hvilke operasjoner den skal utføre (for eksempel slette alle data på harddisken på begynnelsen av hver partallsuke).[124]

Med en referanse til rettsinformatikken synes karakteristikken "integrert informasjon" å være treffende for objektkoden. Integrert informasjon er hva som kan utledes av den form og funksjonalitet en gjenstand har. Det er vanlig å utelukke integrert informasjon fra informasjonsbegrepet generelt, og det faller også utenfor begrepet ytring. Selv om et dørhåndtak ved sin utforming gir informasjon om hvordan det skal brukes, er det ikke meningsinnhold som inngår i en ytring.[125] Det samme må gjelde objektkoden.[126]

---

[120] NOU 2007: 2 s. 104. Smlg *Wagle* (1997) s. 541 som skriver at "Kildeprogrammet er en ferdig versjon av datamaskinprogrammet skrevet i programmeringsspråk, og kildeprogrammet kan forstås av de som kjenner programmeringsspråket."

[121] Konverteringen kalles kompilering, se om dette hos *Wagle* (1997) s. 546.

[122] *Wagle* (1997) gir i kapittel 19 s. 533 flg, en faktisk beskrivelse av "Hva er et dataprogram?", hvor kilde- og objektkode beskrives og illustreres med eksempler. For å se et eksempel på skadelig kildekode kan man bruke denne linken sendt ut av datasikkerhetstjenesten Sophos (9.11.09). Kildekoden gjelder en "morsom orm" som rammer iPhone: http://www.sophos.com/blogs/gc/g/2009/11/08/iphone-worm-discovered (besøkt 16.11.09)

[123] Det finnes flere muligheter for å skaffe seg innsikt i hvordan programmet virker. Man kan analysere kildekoden, skaffe seg erfaring ved bruk av programmet, og foreta omvendt utvikling, dvs. en grundigere analyse av objektkoden, jf. åvl. §§ 39h og 39i. I et program (en såkalt " hex editor") kan det også fremskaffes skjermbilde med "nuller og ettall" i objektkoden, som gir den kyndige person opplysninger om filformatet m.v.

[124] Et slikt program kalles en "logisk bombe", se NOU 1985: 31 kapittel 4.3.1 s. 9; NOU 2007: 2 kapittel 4.6.2 s. 52. Se nærmere om "logisk bombe" i kapittel 7.6.3.

[125] Se *Udsen* (2009) s. 40, som holder integrert informasjon opp mot fleksibel informasjon. Fleksibel informasjon er ikke bundet til et medium, en tekst er således fleksibel informasjon, og kan være meningsinnhold i en ytring. Kildekoden er derfor et eksempel på fleksibel informasjon. Smlg. *Andersen* (2005) s 108-109. *Frost* (2002) s. 34 skriver at "*Integrerede* informationsydelser udgjøres … af de mer traditionelle fysiske formuesgoder."

Men for å komplisere bildet noe: Den tekniske utviklingen har gitt mulighet for å anvende kildekoden som et funksjonelt program på datamaskinen. *Meningsinnholdet i digitalisert form* kan altså utnyttes direkte av datamaskinen som et funksjonelt verktøy. Spørsmålet er hvordan man da skal karakterisere kildekoden, som ytring eller som verktøy (ting)? Karakteristikken synes å henge på vilkåret om at en ytring må ha menneskelig avsender og mottaker. En kildekode som anvendes direkte på en datamaskin, har datamaskinen som endelig adressat. Da er kildekoden et verktøy i likhet med objektkoden. Man kan for så vidt sammenligne med at en bok kan kastes inn gjennom et vindu for å gi den til en person som står og tar imot. Man har da besørget overføring av en ytring. Men en bok kan også kastes på et vindu, og har da samme funksjon som en stein. Hva slags adressat kildekoden har kan ikke et filter i nettet "se", og dermed oppstår et spørsmål om hvordan man skal forholde seg til regler som regulerer inngrep i ytringer.

I og med at teknologien ikke vet hva som i det enkelte tilfellet er formålet med tilgjengeliggjøringen av kildekoden, synes man å måtte basere seg på det alternativet som best sikrer hensynet til ytringsfriheten, nemlig at den anses som en ytring uansett. Derfor må eventuelle inngrep på nettet rettet mot kildekoden, uansett rettferdiggjøres i lys av de vilkår som følger av EMK art. 10.2.[127]

Ved innføring av forbudet mot befatning med skadelig dataprogram, ble forholdet til ytringsfriheten tatt opp av Datakrimutvalget.[128] Et mindretall påpekte at et forbud som rammet

---

Irgens-Jensen (2008) tar en spesiell posisjon innen nordisk teori, fordi han lar informasjonsbegrepet omfatte fysiske objekter som "… *biologisk materiale,* for eksempel en kultur mikroorganismer." (s. 19). Mikroorganismene representerer integrert informasjon. *Irgens-Jensen* skriver om bedriftshemmeligheter og opplyser at han gir informasjonsbegrepet videre betydning enn vanlig fordi det gir et hensiktsmessig utgangspunkt for å kartlegge hvilke fenomener som ligger innenfor reglenes beskyttelsessfære. Etter min mening er en annen mulig løsning å anse mikroorganismene som *hemmeligheter*, uten at de er "informasjon".

[126] *Klang* (2006) har i sin doktoravhandling om "Disruptive Technologies", påpekt at det finnes visse datavirus som etter hans mening, har gode virkninger ved at de fremmer demokratiske kjerneverdier. I kapitlet om ytringsfrihet ("Communications") presenterer han "five non-harmful and possibly beneficial uses of virus-like software" (s. 98). Han beskriver deretter dataprogram som er *verktøy* for effektiv distribusjon av ytringer, for eksempel et selvspredende program som også inneholder en melding som kommer opp på skjermen til den infiserte datamaskinen. Hans avhandling har en overskrift som indikerer at dataprogrammet kan være en ytring: "Virus as free expressions" (s.100), men intet her indikerer at *programmet som sådan* er en ytring. Han synes å legge til grunn samme oppfatning som jeg har av objektkoden, nemlig at den er et verktøy for å iverksette en funksjon på datamaskinen (som kan være å presentere en ytring), og er ikke en ytring i seg selv.

[127] Dette er spørsmål jeg kommer tilbake til i del VI.

[128] Straffelovkommisjonen tok ikke opp hensynet til ytringsfriheten, men kom inn på problemet med kriminalisering av forberedelseshandlinger, og frarådet på dette grunnlag gjennomføring av datakrimkonvensjonen art. 6 i norsk rett, se NOU 2002: 4 s. 318-319.

skadelig ”dataprogram”, måtte forstås ikke bare å ramme det skadelige verktøyet (objektkoden), men også kildekoden, og sa at man ønsket:

> ”å påpeke forslagets innvirkning på ytringsfriheten. Det er fare for at utkastet § 11 innebærer et utilbørlig inngrep i retten til å fremsette ytringer som inneholder beskrivelser av omgåelse av sperrer på datasystemer, i form av kildekode. Det er ikke straffbart å fremsette slike ytringer i dag. Mindretallet er bekymret for at § 11 utgjør en begrensning i ytringsfriheten.”[129]

Departementet var enig i at et straffebud ville representere et inngrep i ytringsfriheten, men mente at:

> ”Særlig kravet om at befatningen må være uberettiget, gjør at beskyttelsesverdig spredning av kildekoder ikke rammes. Det inngrep i friheten til å gjøre tilgjengelig kildekoder som bestemmelsen likevel representerer, lar seg etter departementets vurdering forsvare ut fra behovet for vern av data, datasystemer og databasert informasjon.”[130]

Forbudet mot skadelig dataprogram i strl. 2005 § 201 omfatter derfor både skadelig objektkode og kildekode, og inndragning av datafiler som bærer skadelig dataprogram kan måtte ta hensyn både til reglene om inndragning av ”ting”, og til regler som verner ytringer.

4.5 Oppsummering

I dette kapitlet er det konstatert at overgrepsbilder og (skadelig) kildekode er meningsinnhold som omfattes av begrepet ytring. Ved inndragning av datafiler med slikt innhold må det tas hensyn til vernet om ytringsfriheten. Videre har vi sett at (skadelig) objektkode ikke er meningsinnhold, og at en elektronisk kommunikasjon ikke blir en ytring bare fordi den hevdes å være ment som en ytring. Skadelig kildekode i digital form kan etter omstendighetene brukes direkte på datamaskinen (slik som objektkoden), og er da ikke en ytring rent objektivt. Siden teknologien ikke kjenner formålet med bruken, må det ved generelle inngrep uansett reises spørsmål ved om det oppstår noe problem i forhold til ytringsfriheten. Til slutt kan det konstateres at forholdet mellom ’data’ og ’ytring’ bryter med forholdet mellom ’data’ og ’informasjon’ etter ISO-definisjonene. Informasjonsdefinisjonen

[129] NOU 2007: 2 s. 104.
[130] Ot.prp. nr. 22 (2008-2009) s. 38.

inneholder ordet *”meaning”*, men gjelder ikke nødvendigvis en menneskelig adressat. Også objektkodens instrukser til datamaskinen er *”meaning”*, men kan altså ikke anses som ytring.

III Hjemmelsgrunnlaget for inndragning av data

5 Inndragning av data i beslag

5.1 Problemstilling

Spørsmålet er om datafiler kan inndras som selvstendige objekter uavhengig av den fysiske bæreren. For data som er lagret lokalt på datautstyret til lovbryteren, åpner det for å kunne foreta inndragning i tilfeller hvor det ville være en uforholdsmessig reaksjon å inndra det fysiske datautstyret. Videre kan inndragning foretas selv om dataene er lagret hos en nettvert. Sist, men ikke minst, danner inndragning av filene grunnlaget for automatisert inndragning i nettet. Inndragning i straffesaken kan på den måten skape en rettshåndhevende effekt i nettet.

Rent konkret kan datainndragning utføres ved at beslutningen spesifiserer hvilke datafiler som inndras. Deretter kan de kopieres over i RDB med tanke på automatisert inndragning. Overføring til RDB kan anses som "svartelisting" av datafilene.[131] I tillegg må de destrueres, dvs. slettes fra den fysiske bæreren dersom ikke også den er inndratt. For overgrepsbilder og skadelig dataprogram er det ikke tale om salg til fordel for statskassen eller til dekning av skadelidtes erstatningskrav, jf. strl. 2005 § 75. Det er bare destruksjon som er aktuelt.[132] Dersom også datautstyret ønskes inndratt, må det spesifiseres for seg i inndragningsbeslutningen.

Ordet "inndragning" brukes både om den rettslige beslutningen som kommer til uttrykk i dommen eller inndragningsforelegget, og fullbyrdingen, dvs. den praktiske handlingen som på varig vis setter siktede ut av rådigheten over inndragningsobjektet. Loven bruker primært 'inndragning' om den rettslige beslutningen som angir hva som kan inndras og hvem kravet

[131] Se *Staksrud* (2002) s. 72, om forskjellen på "svartelisting" og "hvitelisting" som kriterium for filtrering. "Svartelisting" betyr at objektet er forbudt, mens "hvitelisting" betyr at det er godkjent. Begge kriteriene forutsetter at "et menneske først vurderer hver fil eller nettsted og bestemmer hvorvidt det kan plasseres på listen over forbudte eller godtatte filer". Automatisert inndragning av datafiler er basert på forhåndsvurdering av filer som via inndragningsbeslutningen "svartelistes" og legges i RDB som "matching"-grunnlag overfor dublettene.

[132] I andre tilfeller er det behov for at inndratte data tilbakeføres til den berettigete. Det kan for eksempel være data med forretningshemmeligheter som er kommet på avveie. Et slikt tilfelle finnes i Rt. 2003 s. 825 (Kvearner.com), hvor en epost med et vedlegg som inneholdt en hemmelig oppkjøpsstrategi for et foretak, var feilsendt til en forvekselbar epostadresse (Kvearner.com v. Kvaerner.com). I dette tilfellet hadde avsenderen den opprinnelige kildefilen i behold, så interessen gikk i realiteten ut på å forvisse seg om at mottakeren slettet den feilsendte eposten. Etter et datainnbrudd hvor lovbryteren sletter kildefilen hos fornærmede etter å ha kopiert dataene, er det imidlertid behov for tilbakeføring. Inndragning kan besørge både sletting og tilbakeføring avhengig av hva som er hensiktsmessig i saken.

kan rettes mot, se strl. 2005 §§ 69, 70 og 76 første ledd (inndragningsobjektet), og §§ 71 flg. (hvem kravet kan rettes mot). Jeg bruker 'inndragning' i samsvar med dette. Loven gir få regler om hvordan fullbyrdelsen skal skje, men for inndragning av informasjonsbærer finnes det noen regler i strl. 2005 § 76 annet og tredje ledd. Disse bestemmelsene er aktuelle ved inndragning av datafiler. Siden det er tale om praktiske handlinger kaller jeg det gjerne 'gjennomføring' av inndragning. Også filtrering av dubletter i nettet anser jeg som et praktisk tiltak for å gjennomføre inndragning. Sagt med andre ord *fullbyrder* automatisert inndragning den tidligere avsagte inndragningsbeslutningen.

Jeg har identifisert to hovedproblemstillinger vedrørende inndragning av datafiler. Det ene problemet gjelder anvendelsen av reglene om gjenstandsinndragning på data som er tatt i beslag. Dette er data som er lagret, og som uten synderlige problemer synes å kunne henføres under inndragningsreglene, ikke minst fordi strl. 2005 § 69 annet ledd presiserer at som "ting" regnes også "elektronisk lagret informasjon". Men spørsmålet er altså om det gis hjemmel til å inndra datafilen som sådan, hvordan inndragningsbeslutningen i så fall bør utformes og inndragningen gjennomføres. Disse spørsmålene behandler jeg i dette kapittel 5.

Det andre hovedproblemet gjelder grunnlaget for inndragning av dublettene. Jeg tar utgangspunkt i at bruk av automatisert filtrering forutsetter at beslutningen om hva som skal inndras er truffet på forhånd.[133] Det er nærliggende å basere seg på inndragningen i straffesaken fordi dublettene i nettet er identiske med filene i beslaget. Spørsmål som oppstår er hvem inndragningen kan rettes mot, og hvilket rettsgrunnlag man eventuelt har for å inndra dublettene. Jeg behandler spørsmålet om hvem inndragningen kan rettes mot her i kapittel 5, fordi beslutningen bør treffes i saken som behandler inndragning av beslaget. Hvorvidt det finnes materielt rettsgrunnlag *de lege lata*, for å gi beslutningen i straffesaken rettsvirkning for dublettene i nettet er et eget tema. Det behandler jeg i del V, hvor jeg har identifisert to mulige grunnlag.[134]

[133] Se kapittel 11.2.2, hvor jeg drøfter valget mellom bruk av en automatisert vs. en manuell metode for rettshåndhevelse i nettet. Automatisert inndragning er dessuten en "lukket" metode, som skiller seg fra "åpen" automatiserte metoder, ved at det ikke skal utføres noen vurderinger etter gjennomføring av blokkeringen. Ved "åpne" metoder brukes automatiseringen for å skaffe en "fangst" av data som deretter skal vurderes. Se mer om metodene i kapittel 14.3.

[134] Det ene grunnlaget er at dataidentiteten gir en felles referanse til dublettene, på samme vis som ISBN gir en referanse til alle eksemplarene i en bokutgivelse (kapittel 11.4). Det andre grunnlaget er at dublettene anses som ett og samme fenomen, og kan behandles under ett fordi inndragningsbeslutningen integreres i teknologien i nettet (kapittel 11.5).

For å forstå oppbygningen av avhandlingen, bør det nevnes at jeg også har reist spørsmålet om hva datafilens karakter av å være "ting" innebærer. Dette er jo en betingelse for å kunne inndras etter reglene om gjenstandsinndragning. For dublettenes vedkommende kan det ikke tas som forutsetning at filene er "lagret", slik det står i strl. 2005 § 69 annet ledd, jf. sitatet over, fordi de ikke på forhånd er tatt i beslag. Jeg ser dette som et mulig problem for automatisert inndragning, fordi man kan spørre om det er adgang til *å gjennomføre* inndragningen overfor dubletter som er under overføring i nettet dersom det ikke er hjemmel til å beslutte det. Jeg har derfor kartlagt den strafferettslige konseptualiseringen av data som "ting", med tanke på om dublettene kan henføres direkte under strl. 2005 § 69, som ikke anvender vilkåret "lagret".

Kartleggingen er foretatt i del IV (kapittel 6-10) og jeg anlegger da et bredere perspektiv enn inndragningsreglene. De samlede drøftelsene i del II-IV (kapittel 2 -10), legger grunnlaget for vurderingen av automatisert inndragning i nettet, i del V flg.

5.2 Hjemmelsgrunnlaget

5.2.1 Oversikt over reglene om gjenstandsinndragning

Etter straffeloven 2005 er det sentrale regelsettet for gjenstandsinndragning §§ 69, 70 og 76. Inndragningsreglene i straffeloven 2005 viderefører rettstilstanden etter straffeloven 1902. Ifølge forarbeidene er det bare gjort mindre endringer i forhold til gjeldende rett.[135] En endring gjelder inndragning av "trykt skrift", hvor spesialregelen i strl. 1902 § 38 avløses av den teknologinøytrale bestemmelsen om inndragning av "informasjonsbærer", jf. strl. 2005 § 76.[136]

Strl. 2005 § 69 kommer til anvendelse for inndragning av "ting" i relasjon til en straffbar handling som er begått, jf. alternativene i bestemmelsens første ledd bokstav a-c, som bestemmer at tingen må ha vært fremstilt ved, vært gjenstand for eller vært brukt eller bestemt til bruk ved "en straffbar handling". Det er ikke et vilkår at handlingen er fullbyrdet, men

[135] Ot.prp. nr. 90 (2003-2004) kapittel 1.1 s. 31 opplyser at "[det er] foreslått regler om inndragning, som i det vesentlige viderefører gjeldende rett, men med enkelte materielle og språklige endringer." Smlg. kapittel 26.4. om Straffelovkommisjonens forslag om videreføring av rettstilstanden for gjenstandsinndragning etter straffeloven 1902 (s. 346), og departementets tilslutning til dette (s. 347).
[136] Dette gir et mulig inndragningsgrunnlag for dublettene, se kapittel 11.4.

forsøksgrensen må være passert.[137] Bestemmelsen gir også hjemmelsgrunnlaget for inndragning av bøker og andre medier, som loven altså kaller "informasjonsbærer", jf. legaldefinisjonen i strl. 2005 § 76 første ledd.

Strl. 2005 § 70 gjelder forebyggende inndragning, dvs. at gjenstanden inndras for å hindre at et straffbart forhold begås. Dette er et preventivt virkemiddel, ikke en strafferettslig reaksjon.[138] På samme vis som strl. 2005 § 69, gjelder strl. 2005 § 70 inndragning av "ting". Bestemmelsen har en spesialregel for inndragning av "informasjonsbærer", som er å anse som en spesiell type "ting".[139] Spesialregelen skyldes vernet om ytringsfriheten, som gjør at det oppstilles særlig strenge krav for inndragning av medier som bærer ytringer.

Når inndragningsobjektet er en "informasjonsbærer", suppleres strl. 2005 §§ 69 og 70 av strl. 2005 § 76 annet og tredje ledd. I annet ledd oppstilles krav om presis spesifisering i beslutningen av "hvilke deler av innholdet som begrunner inndragningen", og i tredje ledd gis det regler om gjennomføring av datainndragning.

Inndragningskravet behandles etter straffeprosessuelle regler, jf. strpl. § 2 nr. 2. Inndragning besluttes ved dom, og kravet skal varsles i tiltalebeslutningen, jf. strpl. § 252 siste ledd. Det er også adgang til å ilegge inndragning ved forelegg for å avgjøre saken "med bot eller inndragning, eller begge deler", jf. strpl. § 255, smlg. strl. 2005 § 66 som bestemmer at inndragning kan ilegges "alene eller sammen med straff eller andre strafferettslige reaksjoner." I visse tilfeller delegerer loven inndragningskompetansen til påtalemyndigheten. Påtalemyndigheten kan således beslutte inndragning av en "beslaglagt ting" dersom verken eieren, lovbryteren eller besitteren er kjent, jf. strpl. § 214 b.[140]

5.2.2 Noen utgangspunkter for fortolkning

Inndragning er en strafferettslig reaksjon og ikke formelt å anse som straff, jf. strl. 2005 § 30 bokstav e, jf. § 29.[141] Selv om inndragning formelt sett ikke er straff etter straffeloven,

[137] *Matningsdal* (1987) s. 153.
[138] Ot.prp. nr. 90 (2003-2004) kapittel 26.5 s. 348.
[139] Bestemmelsens første og annet punktum gjelder forebyggende inndragning av "ting", mens tredje punktum gjelder inndragning av "informasjonsbærer". Reglene er behandlet i kapittel 5.4.1.
[140] Se kapittel 5.8.
[141] Smlg. straffeloven 1902 som regner opp hva som er straff i § 15 (omfatter ikke inndragning), men mangler en bestemmelse som regner opp de strafferettslige reaksjonene, slik strl. 2005 § 30 gjør. Ifølge forarbeidene er strl.

omfattes inndragning av Grunnlovens straffebegrep, jf. G § 96 om at ingen må dømmes til straff uten at det er hjemmel i formell norsk lov.[142]

Bestemmelsene må imidlertid tolkes. Sentrale problemstillinger for datainndragning er betydningen av lovens begreper "ting", "elektronisk lagret informasjon" og "informasjonsbærer", som jeg skal drøfte. Med hensyn til fortolkningen er det alminnelig antatt at man på strafferettens område er avskåret fra bruk av analogisk fortolkning. Man må holde seg innenfor ordlyden, og kan etter omstendighetene "strekke" den litt, dvs. tolke den utvidende. En analogi derimot, innebærer at bestemmelsen brukes på et annet tilfelle enn det som følger av ordlyden, men hvor underliggende reelle grunner er så like at det synes rimelig, naturlig og nærmest tvingende, å henføre tilfellet under regelen. På strafferettens område er legalitetsprinsippet til hinder for analogisk fortolkning, fordi det er klart at tilfellet ligger utenfor ordlyden.[143] Da mangler det hjemmel. Dette gjelder dog med det forbehold at dersom analogien går i siktedes favør, representerer ikke hjemmelskravet noe hinder for fortolkningen. Som analysen kommer til er det aktuelt med analogisk fortolkning av strl. 2005 § 76 annet og tredje ledd ved inndragning av skadelig objektkode, som neppe kan anses som "informasjonsbærer".[144] Men siden analogien går i favør av den som må tåle inndragningen, er ikke legalitetsprinsippet til hinder for dette.[145]

Etter disse innledende betraktningene kan det tilføyes at avhandlingens tolkingsspørsmål i liten grad gjelder problemer med å henføre data under bestemmelsenes ordlyd. Det later ikke til å oppstå problemer verken med utvidende eller analogisk fortolkning. Problemene har vist seg å ligge på to andre plan: Det ene har jeg alt vært inne på, og gjelder søk etter *de kriterier som lovens begreper hviler på* for å kunne ta stilling til begrepenes og dermed reglenes

2005 § 30 tatt med "utelukkende av rettspedagogiske grunner for å gi en samlet oversikt over hjemler for reaksjoner som bare kan ilegges i en straffesak." Bestemmelsen innebærer i seg selv ingen realitetsendring i forhold til straffeloven 1902, se Ot.prp. nr. 90 (2003-2004) kapittel 30.1 på s. 433.

[142] Ot.prp. nr. 90 (2003-2004) kapittel 14 s. 194-195; *Andenæs/Matningsdal/Rieber-Mohn* (2004) s. 104: G § 96 "Ingen kan dømmes uden efter Lov" innebærer at "å statuere straffansvar og idømme en strafferettslig reaksjon" krever hjemmel i formell lov.

[143] Slik *Eckhoff* (2001) s. 124, som likevel åpner for å bruke 'analogi' om tilfeller som dekkes av ordlyden, men som ligger " noe fjernere" enn slike som omfattes av en utvidende fortolkning. (s. 125). *Jakobsen* (2008) forbeholder 'analogi' for handlinger som ligger utenfor *ordlyden*, men hvor man på bakgrunn av reelle hensyn, likevel kommer til at den omfattes av *regelen*. *Jacobsen* sier: "Ved analogisk tolking har ein derimot som utgangspunkt at den aktuelle handlinga ikkje er omfatta av ordlyden i det heile, noko som fører til at lovteksten ikkje kan fungere som primær rettsheimel for rettsregelen." (s. 300). Jeg slutter meg til *Jacobsens* beskrivelse av hva analogisk fortolkning går ut på.

[144] Se kapittel 5.4.1.

[145] Se kapittel 5.6.

rekkevidde *de lege lata*.[146] Problemet oppstår ved anvendelse av begrepet "ting" på data, og det gjelder hvorvidt "ting" forutsetter at dataene er bundet til et lagringsmedium eller om de er et objekt i seg selv. Jeg behandler rettsspørsmålet i del IV, og gir en fyldigere beskrivelse av rettskildesituasjonen og tolkingsproblemet i kapittel 6.3.1.

Det andre problemet gjelder *samspillet mellom regler,* som påvirkes av at teknologien har forårsaket et tredimensjonalt problem, nemlig de rettsstridige dublettene i beslaget og i nettet. Problemet er tilstede i identisk form uavhengig av tid, både i topartssituasjonen i straffesaken i nettet. "Identisk" skal forstås helt bokstavelig, og identiteten er et mulig grunnlag for å inndra dublettene under ett.

5.3 Strl. 2005 § 69 – inndragning av "ting"

5.3.1 Data – "elektronisk lagret informasjon"

Hjemmel for inndragning av "ting" som strafferettslig reaksjon, finnes i strl. 2005 § 69. Hele bestemmelsen lyder:

> "Ting som
> a) er frembrakt ved,
> b) har vært gjenstand for, eller
> c) har vært brukt eller bestemt til bruk ved
> en straffbar handling, kan inndras. Istedenfor tingen kan hele eller deler av tingens verdi inndras. § 67 første ledd tredje punktum og fjerde ledd gjelder tilsvarende.
> Som ting regnes også rettigheter, fordringer og elektronisk lagret informasjon.
> Ved avgjørelsen av om inndragning skal foretas, og hvilket omfang inndragningen skal ha, skal det særlig legges vekt på om inndragning er påkrevd av hensyn til effektiv håndheving av straffebudet, og om det er forholdsmessig. Når forholdsmessigheten vurderes, skal det blant annet legges vekt på andre reaksjoner som ilegges, og konsekvensene for den som inndragningen rettes mot."

Inndragningshjemmelen står i første, jf. annet ledd, mens tredje ledd gir anvisning på de vurderinger som skal foretas for å avgjøre "om inndragning skal foretas, og hvilket omfang inndragningen skal ha." Det skal både tas hensyn til en effektiv håndheving av straffebudet og til inngrepets forholdsmessighet. Vilkåret om at det må foreligge en straffbar handling innebærer som utgangspunkt at både de objektive og de subjektive vilkår for straff må være

[146] Se kapittel 3.2, fulgt opp i del IV, kapittel 6.3.1.

oppfylt. Men ved henvisningen til strl. § 67 tredje punktum i strl. 2005 § 69 første ledd siste punktum, gjøres det unntak for manglende tilregnelighet og subjektiv skyld. Det kan imidlertid oppstå spørsmål om unntaket gjelder ved inndragning forbundet med overtredelse av strl. 2005 § 201, som inneholder det subjektive overskuddet om å ha forsett om å begå en straffbar handling.[147]

I det følgende kartlegger jeg anvendelsen av strl. 2005 § 69 ved inndragning av skadelig dataprogram og overgrepsbilder som er tatt i beslag. Første spørsmål er hva som er hjemmelsgrunnlaget for inndragning av datafile. Strl. 2005 § 69 første ledd viderefører bestemmelsen om inndragning av ”ting” i strl. 1902 § 35, og er ikke ment å innebære noen endringer i forhold til denne. Det samme gjelder annet ledd som presiserer at som ”ting” regnes også ”rettigheter, fordringer og *elektronisk lagret informasjon*” (min uth.). Den korresponderende presiseringen i strl. 1902 § 35 første ledd annet punktum, nevner bare ”rettigheter og fordringer” (bestemmelsen er i sin helhet sitert i fotnoten her).[148] Men av forarbeidene til straffeloven 2005, fremgår det at strl. 1902 § 35 gir adgang til å inndra elektronisk lagret informasjon (jf. ”ting”), og at strl. 2005 § 69 annet ledd bare er en presisering av denne adgangen.[149] Også elektronisk lagret informasjon er altså ”ting”.

Slik uttrykket ”elektronisk lagret informasjon” er benyttet i lovteksten kan det åpenbart ikke bety ’databasert informasjon’, dvs. meningsinnhold, så her peker lovens formulering på det som avhandlingen betegner ’data’, som er plassert på midterste nivå i modellen i kapittel 2.1. Fortolkningen støttes av uttalelser i forarbeidene til bestemmelsen, hvor det står at

> ”Elektronisk lagret informasjon er informasjon som er egnet til elektronisk behandling, i dagligtalen ofte omtalt som «data».”[150]

[147] Se kapittel 1.1 om det subjektive overskuddet. Jeg kommer inn på vilkåret i kapittel 5.3, 5.4 og 5.7.
[148] Strl. 1902 § 35 lyder:
”Ting som er frambrakt ved eller har vært gjenstand for en straffbar handling, kan inndras såframt det finnes påkrevd av hensyn til formålet med den bestemmelse som setter straff for handlingen. Som ting regnes også rettigheter og fordringer. Regelen i § 34 første ledd tredje punktum gjelder tilsvarende.
Det samme gjelder ting som har vært brukt eller bestemt til å brukes ved en straffbar handling.
Istedenfor tingen kan inndras et beløp som svarer til dens verdi eller en del av verdien. Det kan bestemmes i dommen at tingen hefter til sikkerhet for inndragningsbeløp.
Istedenfor å inndra tingen kan retten treffe bestemmelse om tiltak for å forebygge at tingen blir brukt til nye lovovertredelser.”
[149] Ot.prp. nr. 90 (2003-2004) kapittel 26 s. 347 ”Departementet er enig med kommisjonen i at det trolig er adgang til slik inndragning i dag, men at det likevel kan være grunn til å avklare spørsmålet ved uttrykkelig å nevne elektronisk lagret informasjon i lovteksten.”; smlg. kapittel 30.1 s. 463.
[150] Ot.prp. nr. 90 (2003-2004) kapittel 30.1 s. 463.

Presiseringen av adgangen til å inndra data som "ting", er overflødig dersom den ikke gjelder dataene som selvstendig objekt, fordi den fysiske bæreren uten videre omfattes av begrepet "ting". Formålet med presiseringen i strl. 2005 § 69 annet ledd må følgelig være å gjøre det klart at data er et selvstendig inndragningsobjekt.[151] Det må sies å følge nokså klart av forarbeidene også, hvor det uttales at:

> "Et eksempel på data som det kan være aktuelt å inndra etter § 69, er virusprogrammer, som gjerne vil være brukt eller bestemt til å brukes ved en straffbar handling, jf. første ledd bokstav c. Slik informasjon vil normalt kunne inndras ved at dataene slettes."[152]

Det henger godt sammen med gjennomføringsreglene i strl. 2005 § 76 tredje ledd, hvor det fremgår at å "slette innhold som tilhører lovbryteren" er en måte å gjennomføre inndragningen på når dataene er lagret hos en tilbyder.[153] I web 2.0-situasjonen er rettighetene til dataene og til den fysiske bæreren på forskjellige hender, og da er det helt tydelig et behov for å inndra dataene separat. Det forutsetter at datafilene spesifiseres som selvstendige objekter i beslutningen, slik at man vet hva inndragningen omfatter.[154]

Siden denne delen av avhandlingen gjelder data som er tatt i beslag, er de "lagret", jf. strl. 2005 § 69 annet ledd. Vilkåret om lagring er derfor ikke noe tema her. Det reiser seg i forhold til dublettene i nettet.

Til tross for at straffeloven 1902 gir adgang til det, har jeg ikke kunnet finne avgjørelser som inndrar data. Praksis går ut på å inndra det fysiske utstyret, og da inndras datamaskinen (med

[151] Av dette ser vi at inndragningsbestemmelsen og bestemmelsen om skadeverk i strl. 2005 § 351 annet ledd bruker *forskjellige* begreper om det samme. Mens den førstnevnte bruker "elektronisk lagret informasjon", bruker den andre enkelt og greit "data".
[152] Ot.prp. nr. 90 (2003-2004) kapittel 30.1 s. 463. Smlg. eksemplene i Økokrims høringsuttalelse til inndragningsreglene, sitert i NOU 2004: 2 kapittel 8.13.4 s. 258. Eksemplene er: "Virusprogrammer", "analyseprogrammer", "programmer som ringer opp et stort antall telefonnummer og genererer spesiell informasjon, for eksempel finner frem til hvilke oppringte telefonnummer som besvarer med modem" og "dataprogrammer som kan produsere kredittkortnumre i store antall som fyller de vilkår og matematiske betingelser som benyttes av kredittkortprodusentene." RG 2007 s. 961 inneholder eksempler på dataprogrammer "for masseutsendelse av epost; så som 1st Mass Mailer, Mailboy 2004 og Bulk E-mailer" Programmene var brukt til masseutsendelse, noe som i utgangspunktet er forbudt, jf. mfl. § 2b, jf. § 17. Det var imidlertid ikke tatt ut tiltale for masseutsendelsen, fordi adressatene var utenlandske. Derimot ble det domfellelse for overtredelse av pol. § 48, jf. § 31 m.v., blant annet for manglende rapportering til Datatilsynet om behandling av personopplysninger.
[153] Bestemmelsen er sitert i kapittel 5.6.
[154] Hvis alt innhold på et brukerområde skal inndras, kan en henvisning til dette også være tilstrekkelig, men da mister man identifikasjonen av datafilene, noe som er uheldig dersom de bør "svartelistes", se kapittel 5.7.

det mener jeg kabinettet og sentralenheten, dvs. CPUen ("Central Processing Unit")), og annet fysisk utstyr, som tastatur, skjerm og lagringsmedier (såkalte periferienheter).

Det kan for eksempel vises til noen saker om befatning med overgrepsbilder:

> Rt. 2002 s. 1187: Her ble det inndratt "270 disketter, og ett stk. MacIntoch (sic) datamaskin med kabinett, harddisk, tastatur, skjerm og adapter". I Rt. 2005 s. 1058 ble det inndratt "- en - PC med grønn Tower inneholdende 3 - tre - harddisker."

For så vidt gjelder såkalt "datakriminalitet", er Rt. 2004 s. 1619 (Bakdør) illustrerende.[155]

> Saken gjaldt datainnbrudd og dataskadeverk over nett mot en rekke datasystemer i inn- og utland. Tingretten inndro datautstyret, beskrevet som "fire disketter, en PC uten deksel med en harddisk og to løse harddisker."

Dersom *datainndragning* hadde vært anvendt i de nevnte sakene, skulle inndragningsbeslutningen omfattet datafilene med overgrepsbilder og skadelig dataprogram som var tatt i beslag. I Rt. 2002 s. 1187 fremgår det at besittelsen gjaldt 7 000 overgrepsbilder og 191 videosnutter. En beslutning om datainndragning skulle følgelig gått ut på inndragning av 7 191 datafiler som hadde vært gjenstand for en straffbar handling, jf. strl. 1902 § 35 første ledd første punktum (smlg. strl. 2005 § 69 første ledd bokstav b).

I Rt. 2005 s. 1058 gjaldt besittelsen 30 000 overgrepsbilder og 2 000 videosnutter, og inndragningsbeslutningen kunne omfattet 32 000 datafiler, jf. hjemmelsgrunnlaget nevnt over.

I "Bakdørsaken" fremgår det av tingrettens dom at de domfelte hadde:

> "hatt og brukt forskjellige typer exploits, som har rettet seg mot ulike svakheter de har skannet etter."[156]

Med "exploits" mente tingretten skadelig dataprogram.[157] De domfelte hadde blant annet benyttet "exploits" med funksjon som "bakdør", dvs. dataprogram som skaper en ny og

[155] Tingrettens slutning er gjengitt i Høyesteretts dom. For Høyesterett var ikke inndragningsspørsmålet noe tema. Høyesterett prøvet lovanvendelsen med hensyn til straffelovens stedlige virkeområde, jf. strl. 1902 § 12, jf. § 145 annet ledd og § 393, og fortolkningen av strl. 1902 §§ 291, jf. 292, på uberettigete endringer i data, samt straffutmålingen.
[156] Stavanger tingretts dom 19. august 2003 (02-634 M og 02-635 M) s. 22.

uberettiget vei inn i datasystemet.[158] Dersom datainndragning hadde vært anvendt skulle de nevnte "exploits" vært inndratt, med spesifikasjon av filene. Hjemmelsgrunnlaget var i så fall strl. 1902 § 35 annet ledd, fordi de nevnte "exploits" enten var "brukt eller bestemt til å brukes" ved en straffbar handling (smlg. strl. 2005 § 69 første ledd bokstav c).[159]

Datainndragning retter seg altså mot datafiler som selvstendige "ting", og kan anvendes alene eller supplere inndragning av det fysiske datautstyret. I beslutningen må det spesifiseres om inndragningen gjelder utstyret og/eller filene.

5.3.2 Inndragningsgrunnlagene

5.3.2.1 Innledning og avgrensning av problemstilling

Loven oppstiller tre alternative grunnlag for å inndra "ting", jf. strl. 2005 § 69 første ledd bokstav a-c. Bestemmelsen gir hjemmel for å inndra

> "ting som
>
> a) er frembrakt ved,
> b) har vært gjenstand for, eller
> c) har vært brukt eller bestemt til bruk ved en straffbar handling."

Datafilene må oppfylle et av disse grunnlagene. Både strl. 2005 §§ 201 og 311 setter straff mot *produksjon, besittelse, anskaffelse og tilgjengeliggjøring* av henholdsvis skadelig dataprogram og overgrepsbilder. Lovbruddene er beskrevet i strl. 2005 § 201 og § 311 første ledd. Bestemmelsene lyder som følger:

Strl. 2005 § 201:

> "Med bot eller fengsel inntil 1 år straffes den som med forsett om å begå en straffbar handling uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen
>
> a) passord eller andre opplysninger som kan gi tilgang til databasert informasjon eller datasystem, eller
> b) dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem. På samme måte straffes den som uten forsett om å

[157] 'Exploits' kan både bety skadelig dataprogram og sårbarheter i datasystemet som kan misbrukes for inntrengning, se NOU 2007: 2 kapittel 3.4.1 s. 23, hvor det står at 'exploits' brukes "både om metoden og programmet som anvendes". I Bakdørsaken ble det benyttet om det skadelige dataprogrammet.
[158] Et annet ord for slike program er "trojaner". Se avhandlingen kapittel 3.3.3 og NOU 2007: 2 s. 24.
[159] Smlg. strl. 1902 § 35 annet ledd som lyder: " Det samme gjelder ting som har vært brukt eller bestemt til å brukes ved en straffbar handling."

begå en straffbar handling besitter et selvspredende dataprogram, og besittelsen skyldes uberettiget fremstilling eller anskaffelse av programmet.”[160]

Strl. 2005 § 311 første ledd:

”Med bot eller fengsel inntil 3 år straffes den som
a) produserer fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn,
b) utgir, tilbyr, selger, overlater til en annen, gjør tilgjengelig eller på annen måte søker å utbre fremstillinger som nevnt i bokstav a,
c) anskaffer, innfører eller besitter fremstillinger som nevnt i bokstav a, eller forsettlig skaffer seg tilgang til slikt materiale,
d) holder offentlig foredrag eller istandbringer offentlig forestilling eller utstilling av fremstillinger som nevnt i bokstav a.” [161]

Drøftelsen gjelder datafiler som har inngått som element i disse overtredelsene.

Som det fremgår av gjerningsbeskrivelsene rammes produksjon, anskaffelse, besittelse og tilgjengeliggjøring av skadelig dataprogram og overgrepsbilder. Strl. 2005 § 201 bruker ordet ”fremstiller” i stedet for ”produserer”, men betydningen er nok den samme.[162]

For overgrepsbilder finnes det ytterligere noen straffalternativer, henholdsvis tilgangsalternativet i strl. 2005 § 311 bokstav c, og utstillings- og foredragsalternativene i bokstav d. Jeg bort fra disse fordi de gjelder befatning med *meningsinnholdet* og ikke dataene som bærer innholdet. Overtredelse av de nevnte forbudene resulterer derfor ikke nødvendigvis i noen data hos domfelte som kan inndras.[163]

Tilgangsalternativet er nemlig overtrådt allerede når man ser på bildene på nettet, etter aktivt å ha oppsøkt dem. Ved nedlasting av filene rammes forholdet som anskaffelse og besittelse av data. Utstilling og foredrag forutsetter at lovbryteren allerede har rådigheten over det

[160] Som nevnt i kapittel 1.1 representerer strl. 2005 § 201 en reservasjonsløs gjennomføring av datakrimkonvensjonen art. 6.
[161] Den korresponderende bestemmelsen i strl. 1902 § 204 a lyder: ”Den som
a) produserer, anskaffer, innfører, besitter, overlater til en annen eller mot vederlag eller planmessig gjør seg kjent med fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn,
b) befatter seg med fremstillinger av seksuelle overgrep mot barn eller fremstillinger som seksualiserer barn, på annen måte som nevnt i § 204 første ledd.”
[162] Kanskje er det strl. 2005 § 311 som av språklige hensyn har valgt bort ”fremstiller”, fordi ordlyden da ville blitt ”den som fremstiller fremstilling…”.
[163] Se drøftelsen av forholdet mellom data og meningsinnhold i strl. 2005 § 311, i kapittel 9.1.

rettsstridige materialet (besittelsen), og bruker det som grunnlag for tilgjengeliggjøring.[164] Overtredelse av tilgangsalternativet i strl. 2005 § 311 bokstav c, og utstillings- og foredragsalternativene og bokstav d i elektronisk nettverk, gir derfor ikke data å inndra. Jeg kommer tilbake til spørsmålet om straffansvar uten å ha rådighet over mediet, i kapittel 9, hvor jeg behandler datafilenes betydning for å avgrense straffebudets objektive rekkevidde. En straffetrussel knyttet til befatning med meningsinnholdet rekker nemlig mye videre enn en trussel knyttet til befatning med datafilene. Det betyr at datafilen har karakter av å være en "ting" eller "gjenstand" med direkte relevans for straffansvaret.[165]

5.3.2.2 Datafiler som "er frembrakt ved" en straffbar handling

Det første inndragningsgrunnlaget krever at datafilen "er frembrakt ved" en straffbar handling, jf. strl. 2005 § 69 første ledd bokstav a. Dette grunnlaget omfatter ting som er "det direkte resultatet eller produktet av en straffbar handling".[166] Forarbeidene nevner eksemplene "hjemmebrent eller barnepornografi".[167]

Inndragningsgrunnlaget synes å korrespondere med produksjonsforbudet i strl. 2005 § 201 bokstav b ("fremstiller … dataprogram som er særlig egnet som middel…"), og strl. 2005 § 311 første ledd bokstav a ("produserer" overgrepsbilder). Spørsmålet er om datafiler som er rettsstridig produsert kan inndras etter dette grunnlaget. Det reiser i første omgang spørsmål om hva straffebudene mener med "fremstiller" og "produserer" og hva inndragningsregelens "er frembrakt ved" omfatter.

Man kan tale om "produksjon" både ved førstegangs frembringelse av en datafil og ved kopiering. Jeg behandler tilfellene hver for seg.

Førstegangsproduksjon av *skadelig dataprogram* innebærer at lovbryteren skriver en skadelig kildekode. Det kan også forstås å ramme kompileringen, dvs. at dersom vedkommende har

[164] En mulig variant er sanntidsoverføring av seksuelle overgrep mot barn. Det resulterer isolert sett ikke i noen data som lagres og besittes, og skal derfor ikke behandles i dette kapitlet. Men handlingen rammes nok både av anskaffelses- og tilgjengeliggjøringsalternativene i strl. 2005 § 311 bokstav b og c. Se mer om dette i kapittel 9.
[165] Datafilen har karakter av å være "ting/gjenstand" selv om strl. 2005 § 311 ikke bruker slike ord. Datafilens funksjon som konstituerende element i lovbruddet er likeverdig med en "gjenstand" som har uttrykkelig strafferettslig relevans blant annet i straffebudene om tyveri, underslag, skadeverk og ulovlig bruk. Dette omhandler den strafferettslige konseptualiseringen av data, som jeg behandler i del IV.
[166] Ot.prp. nr. 90 (2003-2004) kapittel 26.4.1 s. 346.
[167] Ot.prp. nr. 90 (2003-2004) kapittel 26.4.1 s. 346.

fått kildekoden fra en annen, men foretar den første kompileringen til skadelig objektkode, så har han fremstilt programmet.[168] Ytterligere kan det forstås å omfatte endringer i eksisterende programmer (kalles gjerne ”modifikasjon”). Det kan gjelde endring i et ”vennlig” program slik at det får en skadelig effekt det tidligere ikke hadde, eller en oppdatering av et skadelig dataprogram som resulterer i en ny generasjon av programmet.

Et reelt hensyn som støtter at modifikasjon anses som produksjon (jf. ”fremstiller” i strl. 2005 § 201), er at dersom det gjøres endringer i et skadelig dataprogram, fremstår det som nytt for de filtre som skal avdekke og blokkere det for å beskytte datasystemene. Ved endring i dataprogrammet endres *dataidentiteten* som er grunnlaget for gjenkjenning og blokkering. Et modifisert dataprogram kan rette seg mot de samme sårbarheter på datamaskinene som den eldre versjonen gjorde, men er nytt i henhold til identitetskriteriet. Da bør det også anses som et nyprodusert program. Reelt sett finnes det ikke noe annet kriterium enn dataidentiteten for å avgjøre om et dataprogram i objektkode er nytt eller ei. Programmet kan ikke enkelt observeres av mennesker selv om det finnes dataverktøy som kan hjelpe til med analyse. For å gjenkjenne programmet i det miljø hvor det virker, må den tekniske dataidentiteten legges til grunn. Det bør ikke ha betydning om programmets navn er det samme (bare tilføyd nye versjonsnumre), for eksempel ”Slammer 1”, ”Slammer 2” og ”Slammer 3”.[169] Det er jo ikke navneidentiteten, men den tekniske dataidentiteten som avgjør om programmet kan gjenkjennes. Motsatsen er at filene er ”den samme” dersom innholdet er likt, selv om filene har forskjellig navn.[170]

Etter forarbeidene er det klart at modifikasjon anses som produksjon, idet departementet med henvisning til Datakrimutvalgets forslag til straffebud sier at

> ”… modifisering vil i det vesentlige rammes som tilgjengeliggjøring, besittelse og/eller *fremstilling”* (min uth.).[171]

[168] Se om konvertering fra kilde- til objektkode i kapittel 4.4.
[169] Se omtale av Slammer i kapittel 3.3.3.
[170] *Aquilina* (2008) s. 205, sier om identifikasjon av “malware” ved hjelp av sjekksum: ”When a particular piece of malware already has been identified, hash analysis may identify other files with the same data but different names.” Identifikasjonen skjer følgelig på grunnlag av teknisk dataidentitet. Hva filen kalles har ingen betydning.
[171] Ot.prp. nr. 22 (2008-2009) kapittel 2.8.3.8 s. 39. Det er ”fremstilling” som er relevant. De andre alternativene som sitatet nevner, må bety at også et modifisert program kan tilgjengeliggjøres og besittes. Bestemmelsen rammer også det. Se også spesialmotivene som sier at ”«fremstiller» vil *blant annet* omfatte den som lager dataprogrammer av den typen loven nevner ” (min uth.). ”Blant annet” åpner for å inkludere endringer i eksisterende programmer, i fremstillingsalternativet.

Departementets uttalelse inngår i en redegjørelse om at man valgte en enklere utforming av straffebudet enn foreslått av Datakrimutvalget, uten at man dermed mente å innsnevre straffebudets rekkevidde. Utvalget hadde et eget alternativ for "modifiserer" som omfattet

> "at lovbryteren endrer et program … som er utviklet … av andre".[172]

Førstegangsproduksjon av *overgrepsbilder* innebærer fotografering eller filming av seksuelle overgrep eller posering.[173] Fra praksis kan det blant annet vises til:

Rt. 1997 s. 1994: Seksuelle overgrep utført mot 7-årig stedatter som ledd i opptak av videofilm. Opptaket fant sted "… ut fra rent profittmotiv. Hensikten var å distribuere videoen for salg." (s. 1996).

Rt. 2008 s. 1403: Domfellelse for en rekke seksuelle overgrep mot barn og unge gutter i Thailand. Overgrepene ble ansett begått på "særlig krenkende måte, fordi [de] ble filmet eller fotografert og også spredt videre på internettet" (avsn. 9). Foruten overgrepene, ble det domfellelse for produksjon og tilgjengeliggjøring av overgrepsbilder.

Rt. 2009 s. 140: Domfelte hadde blant annet forledet jenter i alderen 9-16 år, til å

> "å vise seg avkledd for ham ved hjelp av web-kamera og programmet MSN. Domfelte fikk også en del av pikene til å utføre seksuelle handlinger med seg selv mens han så på via MSN og til å sende ham seksuelt betonte bilder av seg selv … Materialet kan enkelt lagres hos mottakeren og distribueres videre." (avsn. 3).

For dette ble han domfelt for overtredelse av strl. 1902 § 200 annet ledd annet punktum. I tillegg ble han dømt for besittelse av filmer han hadde lagret og for ett tilfelle av viderespredning, jf. strl. § 1902 § 204a. Besittelsen gjaldt godt og vel 8 000 bildefiler og 1 741 filmfiler, som dels var materiale domfelte hadde skaffet seg på den nevnte måten (avsn. 29-31).

[172] NOU 2007: 2 kapittel 9.11 s. 160.
[173] Det omfatter også fremstilling av overgrepsbilder ved å endre (manipulere) eldre bilder, å skape datagenererte bilder, tegneserier og animasjoner, men slike har jeg altså holdt utenfor avhandlingens tema, se kapittel 1.1.

Men det er spørsmål om ikke handlingen også kan anses som *medvirkning til produksjon* av overgrepsbilder, jf. strl. 1902 § 204 a, jf. § 205. Det er jo på domfeltes oppfordring at barna lar seg filme, slik at bilder kan lagres og dermed anses å være produsert. Ved å anvende bestemmelsene i konkurrens får man frem det straffverdige i å produsere bilder som representerer en grov krenkelse av barnets personvern. Det supplerer *forledelsen* som rammes av strl. 1902 § 200 annet ledd annet punktum.

Spørsmålet kommer på spissen ved anvendelsen av de korresponderende bestemmelsene i straffeloven 2005. Strl. 2005 § 305 bokstav b som viderefører strl. 1902 § 200 annet ledd annet punktum, kommer nemlig til anvendelse "med mindre forholdet rammes av strengere bestemmelser".[174] Strafferammen etter denne bestemmelsen er fengsel inntil ett år, mens den etter strl. 2005 § 311 er fengsel inntil tre år. At også medvirkning til produksjon av overgrepsbilder er straffbart følger av den generelle medvirkningsbestemmelsen i strl. 2005 § 15, jf. strl. 2005 § 311 bokstav a. Men siden strl. 2005 § 311 ikke omfatter selve forledelsen, synes det mer korrekt å anvende bestemmelsene i konkurrens, fordi man da får frem alle sider ved den straffbare handlingen. Det betyr at produksjonsalternativet i strl. 2005 § 311 ikke konsumerer strl. 2005 § 305 bokstav b i disse tilfellene.

RG 2002 s. 1307: Domfelte hadde hatt kontakt med et barnehjem i Murmansk og invitert to av barna hjem for sommeren. Der ble de to jentene "ved flere anledninger fotografert nakne og i utfordrende stillinger …" Senere skannet han bildene på sin datamaskin og la dem ut på internett. Beslaget av overgrepsbilder var "et av de største som noen gang er gjort i Norge". Domfellelsen gjaldt seksuell omgang med barn under 14 år og befatning med overgrepsbilder, herunder produksjon og tilgjengeliggjøring.[175]

[174] Strl. 2005 § 305 *Seksuelt krenkende atferd mv. overfor barn under 16 år* lyder: "Med bot eller fengsel inntil 1 år straffes den som a) i ord eller handling utviser seksuelt krenkende eller annen uanstendig atferd i nærvær av eller overfor barn under 16 år. b) tvinger eller forleder et barn under 16 år til å utvise seksuelt krenkende eller annen uanstendig atferd, med mindre forholdet rammes av strengere bestemmelser".

[175] I tillegg kan nevnes: Rt. 2001 s. 1674: Voldtekt av 10-årig pike. To menn hadde planlagt "å innlede seksualforbindelser med småjenter for å fotografere hendelsene med sikte på omsetning av bildene. B skulle etablere kontakten, mens A skulle utføre handlingen." (s. 1675-76). Fotograferingen ble ikke noe av fordi A ikke fikk trengt inn "pga manglende ereksjon." I dette tilfellet ble altså ikke produksjonsforbudet overtrådt, men produksjon var motivet for handlingen. Se også LB-2005-132404; LB-2005-111057 og LB-2006-31596 som alle gjelder filming av mindreårige. Rt. 2000 s. 40 gjaldt seksuelt misbruk og fotografering av voksne kvinner. Fotografering rammes i dette tilfellet ikke av pornografiforbudet, idet strl. 1902 § 204 ikke rammer produksjon. Smlg. strl. 2005 § 317. Det kan reises spørsmål ved om det her foreligger en mangel ved loven, se drøftelsen i kapittel 5.4.2. LF-2006-159248 er en lignende sak.

Et annet spørsmål er om *kopiering av eksisterende materiale* rammes av produksjonsforbudet. Forbudet er begrunnet i faren for utbredelse av materiale: Når fysiske medier kopieres skapes det mer materiale med korresponderende økt spredningsfare.[176] Det er derfor ikke tvilsomt at kopiering for eksempel av CD- og DVD-plater med det rettsstridige innholdet, rammes av produksjonsforbudet. Da er man utenfor nettverkskonteksten og inndragningsobjektet er den fysiske bæreren, dvs. CD- og DVD-platene.

For datafilene sett uavhengig av lagringsmediet, synes situasjonen å være annerledes. Kopiering er *sekundærbefatning* som innebærer mangfoldiggjøring av dubletter. Forekomsten av dubletter i et beslag er gjerne forårsaket av *siktedes personlige behandling* av sine data.[177] Det kan også ha forekommet nedlasting av dubletter dersom vedkommende har vært aktiv på nettet. Dubletter på lovbryterens lagringsmedier utgjør imidlertid ikke noen økt spredningsfare og faller derfor noe på siden av begrunnelsen for produksjonsforbudet. I en viss forstand er det dessuten vanskelig å si at det blir *mer* av materialet når det bare kopieres lokalt. Dette syn kan påvises i en tendens i rettspraksis til anvendelse av et "nettoprinsipp" ved beregning av antallet overgrepsbilder. Et nettoprinsipp går ut på at identiske filer telles som én, i stedet for at man anvender den tellemetoden som er vanlig for fysiske objekter, dvs. at man summerer alle objektene ("bruttoprinsipp").

Høyesterett har således, i en sak om besittelse av overgrepsbilder, som gjaldt 10 videosnutter hvorav 3 var like, sagt at det dreide seg "i realiteten om 8 ulike filmer" (Rt. 2007 s. 422). De tre like filene ble altså regnet som én; det var "i realiteten" *ikke mer av materialet* når filene var like. Dersom de hadde vært talt som fysiske objekter skulle jo antallet vært 10.[178] Det finnes også underrettspraksis som anvender nettoprinsippet, noe jeg har belyst mer inngående i kapittel 11.5.2. Det kan derfor være naturlig å tolke det materielle produksjonsalternativet i straffebudene *innskrenkende* i slike tilfelle, dvs. at lokal kopiering ikke regnes som produksjon. Fortolkningen har gode reelle grunner for seg. Som forklart i kapittel 3.3.4, er kopieringen i slike tilfeller først og fremst et utslag av hvordan teknologien virker, og ikke av

[176] Se Ot.prp. nr. 22 (2008-2009) kapittel 2.8.3.8 s. 39, om skadelig dataprogram: "Kriminalisering av *fremstilling*, anskaffelse og besittelse er nødvendig for å hindre spredning, som er den befatningsformen som medfører størst fare for skade."
[177] Hvordan dette skjer, er beskrevet i kapittel 3.3.4.
[178] Smlg. saker med fysiske beslag, for eksempel Rt. 1980 s. 1532 som gjaldt beslag og inndragning av 97 000 pornoblader, 18 000 filmer og 20 videobånd. Domfelte var forretningsdrivende i pornobransjen, og ble dømt for omsetning av utuktige magasiner og filmer. Her må antas å ha vært noen like eksemplarer.

et ønske om å skape mer av materialet. Man unngår også å telle med dubletter som er rekonstruert under etterforskingen (se nedenfor).

Spørsmålet er om samme fortolkning skal anvendes for *inndragningsbestemmelsen* i strl. 2005 § 69 bokstav a. Situasjonen er altså at det er avdekket dubletter i beslaget, for eksempel at fil A forekommer 5 ganger, og forekomsten skyldes at lovbryteren har flyttet materialet rundt på sine egne lagringsmedier. Umiddelbart synes anvendelse av et nettoprinsipp å bære galt av sted, dersom konsekvensen er at bare én av de fem filene kan inndras. Det er jo behov for å inndra alle sammen. Jeg ser også bort fra muligheten for å inndra filene med hjemmel i strl. 2005 § 69 bokstav b, fordi de har "vært gjenstand for" straffbar besittelse. Det ville løse det praktiske, men ikke det prinsipielle problemet, nemlig den rettslige tilnærmingen til dublettene.

Et alternativ ved inndragning av lovbryterens dubletter er å telle med hver enkelt fil, selv om de er identiske. Da må inndragningen spesifisere brutto antall rettsstridige filer, dvs. fil A fem ganger (fil A, fil A, fil A, fil A og fil A). Fra et *teknisk* synspunkt er denne fremgangsmåten unødvendig. Hash programmet identifiserer alle dublettene på grunnlag av én identitet, og antallet har ikke noen betydning. Spørsmålet er hvorfor antallet dubletter skulle ha *rettslig* betydning. Etter min mening er det nærliggende å basere seg på den tekniske tilnærmingen ved løsningen av rettsspørsmålet, fordi man er avhengig av bruk av dataverktøy både for å konstatere dublettenes eksistens og kunne gjennomføre inndragningen. Da er det tilstrekkelig å kjenne *dataidentiteten*, den kan angis én gang og fanger opp alle dublettene i beslaget. Det innebærer i så fall at dublettene ses som én "ting", jf. strl. 2005 § 69, og rettslig sett eksisterer med referanse til en felles dataidentitet. Dermed er løsningen også i harmoni med rekkevidden av det materielle produksjonsforbudet.

Det kan reises spørsmål ved om sekundærbefatning med datafiler i det hele tatt kan anses som *produksjon* i strafferettslig forstand. Nær sagt enhver sekundærbefatning synes å lede til fremstilling av en dublett, slik er teknologien innrettet.[179] Fra et teknisk synspunkt er det *dataidentiteten* som har betydning, uansett hvor filen forekommer. Dersom dataidentiteten legges til grunn som rettslig relevant kriterium, er følgen at sekundærbefatning *ikke* anses som

[179] Se kapittel 3.3.4.

produksjon. Det gir også en klar avgrensning overfor anskaffelse og besittelse, hvoretter datafilene er *corpus delicti* og skal inndras med hjemmel i strl. 2005 § 69 bokstav b.

Analysen medfører at det også må reises spørsmål ved om kopiering av dubletter i det elektroniske nettverket, kan anses som "produksjon" i strafferettslig forstand. Også slike dubletter er resultat av sekundærbefatning som teknisk kan håndteres på grunnlag av én identitet. Dette spørsmålet har ikke betydning for inndragning av datafiler i beslaget, men for inndragning av dubletter i nettet, som jeg kommer til i del V.

5.3.2.3 Datafiler som har "vært gjenstand for" en straffbar handling

Det andre inndragningsgrunnlaget krever at datafilen har "vært gjenstand for" en straffbar handling, jf. strl. 2005 § 69 første ledd bokstav b. Grunnlaget kommer til anvendelse der

> "befatningen med gjenstanden tilsvarer gjerningsbeskrivelsen i det aktuelle straffebudet."[180]

Inndragningsgrunnlaget kan også beskrives ved en avgrensning mot de øvrige inndragningsgrunnlagene: Det omfatter ting som ikke er skapt ved den straffbare handlingen, og som heller ikke har vært brukt som middel til å begå handlingen. Tingen er i stedet en del av handlingen beskrevet i straffebudet (*corpus delicti*).

Inndragningsgrunnlaget synes å være aktuelt for straffalternativene *anskaffelse*, *besittelse* og *tilgjengeliggjøring* av skadelig dataprogram og overgrepsbilder, jf. strl. 2005 § 201 bokstav b ("anskaffer, besitter eller gjør tilgjengelig … dataprogram som er særlig egnet som middel …), og strl. 2005 § 311 første ledd bokstav c ("anskaffer … eller besitter" overgrepsbilder) og bokstav b ("… overlater til en annen, gjør tilgjengelig eller på annen måte søker å utbre …" overgrepsbilder).

Jeg kartlegger først rekkevidden av de materielle forbudene. Det synes enklest å innlede drøftelsen med *besittelsesalternativet*. Første spørsmål er om det stilles krav til *hvor dataene er lagret*, for å kunne si at de er i lovbryterens besittelse. Det er aktuelt å ha data lagret både lokalt og i nettet. Avgjørende er om lovbryteren har faktisk rådighet over dataene, ikke hvor

[180] Ot.prp. nr. 90 (2003-2004) kapittel 26.4 s. 346 flg., og kapittel 30.1 s. 463.

de er lagret, så det må være ganske klart at begge situasjonene anses som besittelse. Datakrimutvalget har sagt det slik:

> "«Besitter» betyr å ha [dataene] på et sted man selv kontrollerer. Besittelsens karakter er uten betydning. Det kan for eksempel være at …[dataene] … ligger lagret … på et nettsted på internett, som man selv kontrollerer. Det er uten betydning om nettstedet er på en norsk eller en utenlandsk server, eller om tjenesteyteren er norsk eller utenlandsk, så lenge [dataene] oppbevares under lovovertrederens direkte kontroll, eventuelt etter vedkommendes instruks."[181]

Også inndragningsreglene forutsetter at lovbryteren kan ha data lagret i "internettskyen", se strl. 2005 § 76 tredje ledd, som bestemmer at inndragning i slike tilfeller kan gjennomføres ved at tilbyderen sletter lovbryterens data.[182] Regelen sier ikke noe om hva som har vært inndragningsgrunnlaget, men gir god sammenheng med fortolkningen av det materielle besittelsesvilkåret.

Et annet spørsmål er om data som *er rekonstruert eller på annen måte gjort leselig* i forbindelse med dataetterforskingen, omfattes av besittelsesforbudet. Situasjonen kan for eksempel skyldes at lovbryteren har slettet dataene, gjort dem uleselige ved kryptering eller fjernet pekeren som søker opp filene på ordinært vis.[183] En lignende situasjon er at dataene har vært lagret på systemet, men at lovbryteren ikke har sett på dem fordi vedkommende manglet den nødvendige programutrustningen.

Til dette må det først konstateres at problemstillingen bare gjelder *slettede filer*. Filer som lovbryteren har sørget for å utilgjengeliggjøre for andre, for eksempel ved å fjerne "pekere" eller foreta kryptering, bør utvilsomt anses å være i vedkommendes besittelse, fordi filene er tilgjengelige for lovbryteren som kjenner nødvendige passord m.v.. Filer som lovbryteren mangler programutrustning til å fremvise må bedømmes på samme måte, såfremt forsettet omfatter at filene har rettsstridig innhold som nevnt. Illustrerende er en sak fra Eidsivating lagmannsrett (LE-2004-8204). Tiltalte hadde ikke hatt mulighet til å se på en del av bildene

[181] NOU 2007: 2 s. 158. Sitatet står i sammenheng med forbudet mot rettsstridig befatning med tilgangsdata, som er blitt strl. 2005 § 201 bokstav a. Smlg. uttalelse om besittelse av skadelig dataprogram, hvor Datakrimutvalget nøyer seg med å si at besittelse "vil for eksempel foreligge dersom lovbryteren har programmet lagret på sitt datasystem." (s. 161). Siden det bare er et eksempel, holdes det åpent at besittelsen også kan skje hos en nettvert. Datakrimutvalget behandlet ikke forbudet mot overgrepsbilder, men den første uttalelsen må antas å ha generell anvendelse. Dataenes innhold har jo ingen betydning for besittelsesspørsmålet, objektene er av identisk karakter ("*bits* er *bits*", jf. *Negroponte* (1997)).
[182] Se kapittel 5.6 om § 76 tredje ledd.
[183] Se kapittel 3.3.4 hvor dette er beskrevet.

som var omfattet av tiltalen for besittelse, fordi han manglet programvare til å få dem opp på skjermen. Lagmannsretten la imidlertid til grunn at domfelte

> "var klar over at han lastet ned videosnuttene, og at de på beslagstidspunktet lå lagret på hans maskin. Det kan da ikke være avgjørende at han manglet verktøy for å få se videoene. Slikt verktøy var enkelt å få tak i, og tiltalte har forklart at han var interessert i data".[184]

I alle disse tilfellene må besittelsesforbudet anses å være overtrådt og filene skal inndras med hjemmel i strl. 2005 § 69 bokstav b.

Men det gjenstår en problemstilling vedrørende slettede filer. Jeg drøfter bare under forutsetning om at slettingen har skjedd på en måte hvor siktede har ansett seg ferdig med filene. Det har imidlertid lykkes politiet å rekonstruere filene under etterforskingen.

For spørsmålet om straffansvar for besittelse er utgangspunktet at de slettede filene fysisk er på lovbryterens datautstyr. Men siden de er gjort utilgjengelige for ham selv, har han ikke glede av dem. Det må vel antas at utnyttelsesmuligheten er en relevant side av besittelsesvilkåret, noe som også synes å være lagt til grunn i uttalelsen fra lagmannsretten sitert over. I så fall leder slettingen til at besittelsen opphører.

Av dette følger at lovbryteren var i besittelse av filene før han slettet dem, og at gjerningstidspunktet ligger noe tilbake i tid. Det som da må vurderes er om besittelsen var forsettlig før filene ble slettet, jf. strl. 2005 § 21. For overgrepsbildene er det tilstrekkelig med uaktsomhet, jf. strl. 2005 § 311 tredje ledd.

Dersom anskaffelsen skjedde forsettlig er også besittelsen forsettlig. Problem oppstår bare dersom lovbryteren ufrivillig har kommet i besittelse av filene og slettet dem etter at han ble oppmerksom på det. Det er jo karakteristisk for elektroniske kommunikasjonstjenester at man er tilgjengelig for mottak av meldinger fra andre, for eksempel ved epost eller MMS (multimediamelding). Dermed kan man ufrivillig komme i besittelse av data med rettsstridig

[184] I denne saken ble hovedforhandling med dom opphevet av Høyesterett (Rt. 2004 s. 1580). Definisjonen av "barn" i strl. 1902 § 204 første ledd bokstav d, var blitt utvidet etter at de straffbare handlinger var begått, så det kunne ikke utelukkes at domfellelsen gjaldt mer materiale enn det som var rettsstridig på gjerningstidspunktet, dvs. et problem i forhold til strl. 1902 § 3, om at det er loven på gjerningstidspunktet som skal komme til anvendelse. Lagmannsrettens syn på besittelsen av de uåpnede filene har derfor uansett interesse.

innhold, for eksempel overgrepsbilder. Da må vedkommende oppfylle *handlingsplikten* for å unngå straffansvar.

Handlingsplikten går ut på å kvitte seg med dataene, eller gi dem til politiet i forbindelse med en anmeldelse. Både forarbeidene og praksis fra lagmannsretten legger til grunn en slik handlingsplikt. Blant avgjørelser fra Høyesterett har jeg ikke funnet noen som direkte behandler handlingsplikt i forhold til befatning med data, men plikten er omtalt i noen andre straffesaker.[185] Det er jo tale om et generelt strafferettslig prinsipp, og Datakrimutvalget har sagt følgende:

> "Besittelsesalternativet vil også ramme tilfeller hvor besittelsen har oppstått uforsettlig, men hvor besitteren unnlater å slette tilgangskodene etter at han ble oppmerksom på besittelsen … når vedkommende blir klar over [besittelsen] oppstår en umiddelbar sletteplikt".[186]

Uttalelsen er ikke kommentert i lovproposisjonen, men i rettspraksis finnes noen avgjørelser:

> RG 2004 s. 929: Spørsmål om overgrepsbilder som var midlertidig lagret som følge av nettleserens automatiske lagringsfunksjon, var straffbar besittelse. Lagmannsretten la til grunn at mellomlagringen kunne straffes som en forsettlig unnlatelseshandling, forutsatt at
>
> "en bruker kjenner til mellomlagringsfunksjonen og bevisst lar ulovlig materiale forbli lagret som [tempfiler] over tid … ved vurderingen av når en handlingsplikt inntrer vil tidsmomentet stå sentralt".
>
> I den nevnte saken hadde tiltalte fortløpende slettet tempfilene, og på den bakgrunn kom lagmannsretten til at handlingsplikten var oppfylt.
>
> RG 2007 s. 1345 (MMS): Domfelte hadde ufrivillig mottatt 13 overgrepsbilder via MMS på sin mobiltelefon. Det gikk to dager før han slettet bildene. Lagmannsretten sa følgende om handlingsplikten:

[185] Rt. 2002 s. 1717 (Orderud). Domfellelse for medvirkning til drap (strl. 1902 § 233). Domfelte hadde plikt til aktivt å avverge drap etter å ha mottatt to pistoler som skulle brukes til å begå ugjerningen. Rt. 1977 s. 513 (jaktloven). Høyesterett fastslo at en jeger hadde handlingsplikt til å hindre at dyr påføres unødige lidelser.
[186] NOU 2007: 2 kapittel 9.10 s. 159 (gjelder besittelse av tilgangskoder, jf. strl. 2005 § 201 bokstav a).

> ”ikke ethvert tidsforløp ville representere straffbar besittelse. En viss tid til å områ seg, etter ufrivillig å ha mottatt bildene, må innrømmes før besittelsen kan anses rettsstridig. Det må vurderes konkret hvor lang tid som kan tillates, og det må i denne sammenheng særlig vektlegges hva formålet med å unnlate å fjerne bildene er. Dersom vedkommende eksempelvis ønsker å politianmelde forholdet, vil det måtte ses hen til hvor raskt dette i praksis vil kunne gjøres.”
>
> Etter en konkret vurdering kom lagmannsretten til at handlingsplikten ikke var overholdt og det ble domfellelse for besittelsen.

Dersom personen handler i tide ved å slette dataene, virker det urimelig å legge ham til skade at politiet klarer å rekonstruere dem under etterforskingen. Loven rammer da heller ikke forholdet, fordi det subjektive vilkåret for straff mangler. Siden handlingsplikten effektivt var oppfylt mangler også det objektive vilkåret for straff. Strl. 2005 § 69 gjør som nevnt unntak for det subjektive vilkåret for straff, men ikke for det objektive, se første ledd tredje punktum, som viser til strl. 2005 § 67 tredje punktum (omtalt i kapittel 5.3.1). Strl. 2005 § 69 kan derfor ikke brukes som inndragningsgrunnlag for filene.

Dersom rekonstruksjonen gjelder *overgrepsbilder* er det utelukket å utlevere dem til personen som har vært utsatt for beslaget. Filene må inndras for å forebygge at de blir gjenstand for en straffbar handling, og hjemmelen er strl. 2005 § 70.[187] Siden filene kan legges i RDB og brukes som grunnlag for automatisert inndragning, er rekonstruksjon uansett hensiktsmessig og ønskelig med tanke på forebyggende inndragning. Den automatiserte inndragningen blir mer effektiv jo flere filer det er i RDB. Det kan følgelig reises spørsmål ved om det foreligger en inndragnings*plikt*, til tross for at loven bare taler om en *adgang*, jf. ”kan inndras”. Dette drøfter jeg i kapittel 5.7.

Dersom rekonstruksjonen gjelder *skadelig dataprogram*, stiller det seg noe annerledes. Befatning med slikt program er bare straffbart dersom det skjer med forsett om å begå en straffbar handling, jf. det subjektive overskuddet i strl. 2005 § 201. Forebyggende inndragning krever at det er ”nærliggende fare” for at tingen vil bli gjort til gjenstand for eller brukt ved en straffbar handling. Med mindre det siste alternativet er oppfylt avskjærer det subjektive vilkåret adgangen til å inndra utelukkende for befatning med det skadelige dataprogrammet, jf strl. 2005 § 201. Den store hovedregelen er jo at slik befatning er lovlig.

[187] Se mer om bestemmelsen i kapittel 5.4.

Men det er ikke lett å tenke seg at det vil oppstå situasjoner som setter dette spørsmålet på spissen, fordi beslaget gjerne skyldes at det er begått en datakriminell handling som etterforskes av politiet. De rekonstruerte programmene er slike som ikke ble benyttet ved lovbruddet og kan inndras med hjemmel i strl. 2005 § 69 bokstav c, smlg. hvordan man kunne gått frem i Bakdørsaken (Rt. 2004 s. 1619).[188]

De straffbare alternativene *"anskaffer"* og *"tilgjengeliggjør"* er interessante fordi de åpner for at dataene er i en dynamisk tilstand. Data anskaffes når de lastes ned over nett, og tilgjengeliggjøres når de for eksempel sendes med epost. Forbudet mot tilgjengeliggjøring kan overtres også ved at dataene legges opp på en web-side, og da er de lagret. Hvorvidt tilgjengeliggjøringen er dynamisk avhenger av om lovbryteren bruker "push" eller "pull" teknologi. Å sende en melding med epost eller til news, utnytter "push" teknologi, mens tilgjengeliggjøring på en web-side bruker "pull" teknologi (adressatene må hente selv).[189]

Når overtredelsen forutsetter en dynamisk tilstand hos dataene, åpner overtredelsens karakter for å anvende inndragningsgrunnlaget i strl. 2005 § 69 bokstav b, overfor data *under overføring*. Overgrepsbilder som er under overføring og skadelig dataprogram som overføres på en offentlig tjeneste som news, er elementer i straffbare handlinger.[190] Strl. 2005 § 69 bokstav b, gir etter ordlyden hjemmel for inndragning i slike tilfeller, jf. "ting" som har vært "gjenstand for" en straffbar handling. I slike tilfeller er jo ikke dataene tatt i beslag, men situasjonen er aktuell for automatisert inndragning.[191] Forutsetningen er at grunnlaget for tilgjengeliggjøringen er en datafil som er lagret, og har vært inndratt slik at den har en kjent identitet og kan gjenkjennes i filtrene.

Det er som nevnt et spørsmål om strl. 2005 § 69 annet ledd avskjærer muligheten for automatisert inndragning av data under overføring, jf. formuleringen "elektronisk *lagret*

[188] Se kapittel 5.3.1 og nedenfor i kapittel 5.3.2.4.
[189] *Andersen* (2005) kapittel 15.2.a s. 658 om "push" og "pull" teknologi ved elektronisk reklame. "Efter det ene princip henter den enkelte Internet-bruger selv sin information hos den erhvervsdrivende. Denne fremgangsmåde betegnes ofte som pull-teknologi. … Er der derimod tale om, at nettet anvendes på samme måde som tv og radio til at støde information frem mod forbrugeren, såkalt push-teknologi…". Teknologivalget har vært ansett som rettslig relevant ved jurisdiksjonsspørsmål på internett. Se for eksempel *Sieber* (2006), som sier: "The technical distinction between 'push techniques' …, and 'pull techniques' … is essential for determining the location where Internet documents are 'made accesible'. This difference … is decisive in the area of speech offenses…" (s. 200).
[190] På newsgruppene er innholdet lagret, men når meldingene distribueres på backbone nettet for å "mates" til de lokale newgruppene, er filene under overføring. Her ligger det vel til rette for bruk av filter med tanke på automatisert inndragning.
[191] Se drøftelsen av hvor i nettet filtreringen kan foregå, i kapittel 13.

informasjon" (min uth.). Det er for tidlig å besvare spørsmålet, fordi det både avhenger av den strafferettslige konseptualiseringen av data som "ting" (del IV) og hvordan loven behandler dubletter som fenomen (del V). Jeg nøyer meg derfor med å peke på problemstillingen her.

Med hensyn til data som er lagret (og tatt i beslag), synes ikke anskaffelse å representere et selvstendig alternativ for inndragning etter strl. 2005 § 69 bokstav b, i og med at også besittelsen er straffbar. Dersom dataene er i behold (herunder rekonstruerte filer m.v.) gir besittelsen grunnlag for inndragning. Og dersom de anskaffede filene effektivt er slettet på beslagstidspunktet, er det ingen data å inndra. Da må inndragningen begrenses til datautstyret.

En lignende problemstilling reiser seg for data som lovbryteren har tilgjengeliggjort i nettet, men som fortsatt er lagret hos vedkommende, og derfor tatt i beslag. Også disse datafilene er i vedkommendes besittelse, og i tillegg er de i nettet. Spørsmålet er hvordan man skal vurdere det, noe jeg har valgt å behandle i neste kapittel.

5.3.2.4 Datafiler som har vært "brukt eller bestemt til å brukes" ved en straffbar handling

Her er spørsmålet hva som er inndragningsgrunnlaget for data som er tilgjengeliggjort i nettet, men som er intakt hos lovbryteren. De beslaglagte dataene har således tjent som "kildefiler" eller "kopieringsgrunnlag" for tilgjengeliggjøringen i nettet. Tilgjengeliggjøringen leder til at det skapes dubletter i nettet. Inndragning av disse er et spørsmål om automatisert inndragning, som jeg behandler i del V flg.

Spørsmålet her er om dataene i beslaget skal anses å ha vært *gjenstand for* tilgjengeliggjøring, (jf. alternativ b), eller å ha vært *brukt til* tilgjengeliggjøring, jf. alternativ c "ting som har vært brukt ved en straffbar handling".

Forarbeidene til bestemmelsen sier ikke noe mer om inndragningsgrunnlaget i bokstav c, enn at det

> "forutsetter at det er en viss tilknytning mellom den straffbare handlingen og gjenstanden."[192]

[192] Ot.prp. nr. 90 (2003-2004) kapittel 25.4.1 s. 346. Smlg. *Matningsdal* (1987) s. 252.

Uttalelsen gjelder altså det såkalte "tilknytningskravet" mellom den straffbare handlingen og gjenstanden.[193] For å ta utgangspunkt i et tilfelle som ikke byr på tvil, så får dette grunnlaget anvendelse på ting som har vært brukt som verktøy eller middel til å begå lovbruddet. Forarbeidene nevner for eksempel

> "et jaktvåpen som har vært brukt til ulovlig jakt, eller en bil som har vært brukt til å smugle narkotika over grensen."[194]

Inndragningsgrunnlaget kommer derfor til anvendelse for skadelig dataprogram brukt som middel (verktøy) til å begå andre straffbare handlinger, som datainnbrudd, avlytting og driftshindring, jf. strl. 2005 §§ 204-206. Det er også dette grunnlaget som benyttes for å inndra det fysiske datautstyret.[195] Det samme gjelder dataprogram som var ment for slik bruk, men som rent faktisk ikke ble benyttet slik hendelsesforløpet utviklet seg, jf. "bestemt til bruk ved en straffbar handling" i bokstav c.

Det betyr at inndragning etter dette alternativet kunne vært anvendt i Bakdørsaken (Rt. 2004 s. 1619) som ble omtalt i kapittel 5.3.1. Saken gjaldt datainnbrudd og dataskadeverk over nett mot en rekke datasystemer i inn- og utland, og etterforskingen avdekket både "exploits" som hadde vært benyttet til å begå de straffbare handlingene og "exploits" som ikke var blitt brukt, men som de domfelte hadde i sin besittelse. Hjemmel for inndragning hadde i så fall vært strl. 1902 § 35 annet ledd. De "exploits" som faktisk var benyttet kunne vært inndratt som "ting som har vært brukt … ved en straffbar handling", mens de som ikke var brukt, kunne vært inndratt som "ting som har vært … bestemt til å brukes ved en straffbar handling" (smlg. strl. 2005 § 69 første ledd bokstav c).[196] Det som faktisk skjedde i saken var at *datautstyret* ble inndratt, og dataene som en konsekvens av det.

Men så gjenstår spørsmålet om hva som er inndragningsgrunnlaget for beslaglagte data som har vært *kildefiler for tilgjengeliggjøring*, men som ikke har inngått i noen annen straffbar handling. Disse rammes bare av forbudet i strl. 2005 § 201 bokstav b, og – for så vidt gjelder overgrepsbilder – av strl. 2005 § 311. Spørsmålet er om dataene rammes av

[193] Se *Matningsdal* (1987) s. 252; *Dyrnes* (2004) s. 94.
[194] Ot.prp. nr. 90 (2003-2004) kapittel 25.4.1 s. 346.
[195] Se eksempler på saker i kapittel 5.3.1.
[196] Etter strl. 2005 § 69 bokstav c lyder annet alternativ "ting som har vært … bestemt til bruk".

besittelsesforbudet, og skal inndras etter strl. 2005 § 69 bokstav b, eller om de rammes av tilgjengeliggjøringsforbudet og hva som da er inndragningsgrunnlaget.

Filene kan både anses å ha vært gjenstand for (besittelse) og å ha vært brukt ved en straffbar handling (tilgjengeliggjøring), så løsningen avhenger mye av hvordan man beskriver situasjonen. Hvis man sier at dataene har vært gjenstand for tilgjengeliggjøring, er motargumentet at det ikke er dataene *i beslaget* som er tilgjengeliggjort, de er jo intakte. Det er *dublettene* av kildefilen som er tilgjengeliggjort. Da er det nærliggende å anse dataene som *middel* til å overtre tilgjengeliggjøringsforbudet, slik at de skal inndras etter grunnlaget i bokstav c.

Hvis man derimot holder på *dataidentiteten* som det sentrale kriteriet også her, blir det avgjørende argumentet at dataene har tilgjengeliggjort *mer av seg selv.* Det er de samme datafilene som er på nettet som er kildefiler i beslaget. Siden dette resonnementet gir best konsistens med de øvrige drøftelsene, bør det være konklusjonen også her. Dvs. at datafilene i beslaget som har vært brukt som kopieringsgrunnlag for tilgjengeliggjøring i nettet, har *vært gjenstand for* en straffbar handling, og skal inndras med hjemmel i strl. 2005 § 69 bokstav b.

5.4 Strl. 2005 § 70 – forebyggende inndragning

5.4.1 Inndragning av ”ting” og ”informasjonsbærer”

Strl. 2005 § 70 om forebyggende inndragning lyder slik:

> ”En ting kan inndras når det på grunn av tingens art og forholdene for øvrig er en nærliggende fare for at den vil bli gjort til gjenstand for eller brukt ved en straffbar handling. Er tingen egnet til bruk ved legemskrenkelser, er det tilstrekkelig at det er fare for slik bruk. Inndragning av en informasjonsbærer, jf. § 76, kan bare foretas når det er fare for uopprettelig skade.
>
> Istedenfor å inndra tingen kan det påbys tiltak for å forebygge at tingen blir brukt til lovovertredelser.
>
> § 69 annet ledd gjelder tilsvarende.
>
> Inndragning etter første ledd kan foretas uansett hvem som er eier.”

Begrepet ”ting” brukes i inndragningsgrunnlagene i første ledd første og annet punktum. Tredje ledd bestemmer at ”§ 69 annet ledd gjelder tilsvarende”. Dermed omfatter ”ting” i strl. 2005 § 70 også data. Inndragningsalternativet i første ledd annet punktum er imidlertid lite

aktuelt for data, fordi det forutsetter at tingen er "egnet til bruk ved legemskrenkelser". En karakteristisk egenskap ved data er som kjent at de ikke direkte kan oppfattes av mennesker.

Etter første alternativ kan imidlertid data (jf. "ting") inndras når det

> "på grunn av tingens art og forholdene for øvrig er en nærliggende fare for at den vil bli gjort til gjenstand for eller brukt ved en straffbar handling."

Dette er ikke det eneste grunnlaget for forebyggende inndragning av data; også alternativet i tredje punktum er aktuelt. Det gjelder inndragning av en "informasjonsbærer, jf. § 76", og § 76 første ledd definerer "informasjonsbærer" slik:

> "Med informasjonsbærer menes i denne bestemmelse trykt skrift eller annet som formidler en skriftlig, visuell, auditiv eller *elektronisk lagret informasjon."* (min uth.).

Her bruker loven det samme uttrykket som i strl. 2005 § 69 annet ledd. Også alternativet om forebyggende inndragning av "informasjonsbærer" virker følgelig aktuelt for data. Vilkårene er strengere enn for forebyggende inndragning av "ting", jf. første punktum; det kan "bare foretas når det er fare for uopprettelig skade", jf. tredje punktum. Begrunnelsen for de strenge inngrepskriteriene er at alternativet hjemler inngrep i ytringsfriheten, hvor det blant annet må tas hensyn til forbudet mot forhåndssensur.[197]

Spørsmålet er om data er "informasjonsbærer", jf. "elektronisk lagret informasjon" i strl. 2005 § 76 første ledd, siden det tilsvarende uttrykket i strl. 2005 § 69 annet ledd omfatter data.[198] I utgangspunktet er det rimelig å anta at de to bestemmelsene anvender begrepet likt. Antakelsen styrkes ved at det er tale om bestemmelser som står i samme kapittel, hvor formuleringen "elektronisk lagret informasjon" kom inn i bestemmelsene på samme tid.[199]

Men ved ettersyn synes ikke dette utgangspunktet å kunne opprettholdes. I strl. 2005 § 76 første ledd er "elektronisk lagret informasjon" nevnt på linje med "skriftlig, visuell [eller]

[197] Ot.prp. nr. 90 (2003-2004) kapittel 26.5.3 s. 348, og kapittel 26.6.4 s. 349.
[198] Se kapittel 5.3.1.
[199] Den siste presiseringen er ikke så selvsagt som man kanskje skulle tro fordi § 69 og § 76 ble vedtatt samtidig i lov om straff av 20. mai 2005 nr. 28. Men siden straffeloven 2005 viderefører inndragningsreglene i straffeloven 1902 kunne man tenkt seg at "elektronisk lagret informasjon" også var brukt tidligere, og at det var brukt flere steder i den nye loven, for eksempel i strl. 2005 § 351 annet ledd, hvor lovgiver imidlertid har valgt å bruke ordet "data" i stedet (se kapittel 5.3.1). Men begrepet er nytt og ble tatt i bruk med straffeloven 2005, samtidig for § 69 og § 76.

auditiv … informasjon". Adjektivene "skriftlig", "visuell" og "auditiv" beskriver "informasjon" som mennesker kan oppfatte. Dette er meningsinnhold, dvs. innhold som er en del av en ytring.[200] Det understrekes av at bestemmelsen bruker ordet "formidler"; en ytring er nettopp meningsinnhold som formidles, dvs. presenteres, for et menneske. Det betyr at i denne bestemmelsen refererer ordet "informasjon" seg til det *innhold som bæres* av mediet, jf. begrepet 'informasjonsbærer'. Uttrykket "elektronisk lagret" viser bare at bestemmelsen også omfatter meningsinnhold i elektronisk form, dvs. det jeg har kalt "databasert informasjon".[201]

Dermed har "elektronisk lagret informasjon" *forskjellig* betydning i strl. 2005 § 69 og § 76. I den førstnevnte bestemmelsen betyr det "data", og i den andre "databasert informasjon". De to bestemmelsene bruker samme formulering om to forskjellige fenomener, som hører hjemme på hvert sitt nivå i modellen i kapittel 2.1, henholdsvis i midten og øverst i modellen. Den begrepsmessige inkonsistensen må anses uheldig, men skaper ikke noe nevneverdig problem for fortolkningen av reglene.

Det ligger likevel et poeng her av mer generell art, som gjelder om lovgiver har vært konsekvent ved reguleringen av data, eller om man har vekslet mellom data og meningsinnhold. Spørsmålet har betydning for drøftelsen av data som strafferettslig objekt (del IV) og som objekt for inndragning. Og i det nettopp nevnte tilfellet bruker ikke loven "elektronisk lagret informasjon" på en innholdsmessig konsistent måte.[202]

Spørsmålet om strl. 2005 § 76 første ledd omfatter *data* gjenstår. Legaldefinisjonen omfatter både trykt skrift og andre medier, jf. "trykt skrift eller annet" som "formidler" innhold som nevnt. Ved å slutte tilbake fra de innholdsvarianter som bestemmelsen nevner, følger det av alternativet "elektronisk lagret informasjon" at bæreren må være data. Data må dermed henføres under alternativet "eller annet". Det betyr at *fysiske medier og data er likestilte* i legaldefinisjonen av informasjonsbærer. Forarbeidene til bestemmelsen eksemplifiserer

[200] Se kapittel 4.2 om ytringsbegrepet.
[201] Se kapittel 2.2.
[202] Se *Eckhoff* (2001) kapittel 13 om betydningen av hensynene til konsekvens og harmoni i lovtolkingen. *Mestad* (2009) s. 7, sier at i "lovspråket er stilistisk variasjon en uting." Her poengterer han at lovteksten bør tilstrebe koherens. Forskjellige ord i en lovtekst har derfor normalt forskjellig betydning, selv om ordene brukes om hverandre i dagligtale. Som tidligere nevnt bruker strl. 2005 § 69 annet ledd og § 351 annet ledd (dataskadeverk) bruker *forskjellige* ord om det samme, henholdsvis "elektronisk lagret informasjon" og "data" om data. Det bryter hensynet til språklig koherens. Motstykket er at *like ord og uttrykk* betyr det samme. Men som vi har sett er det ikke tilfelle for "elektronisk lagret informasjon" i strl. 2005 §§ 69 og 76. Det bryter med hensynet til innholdsmessig koherens.

riktignok ”eller annet” som ”CDer, harddisker og disketter for lagring av elektronisk informasjon”, men det utelukker jo ikke at også data omfattes av ”eller annet”.[203] Det skaper også best sammenheng med strl. 2005 § 69 annet ledd, som behandler data som en selvstendig bærer.

For så vidt gjelder legaldefinisjonens anvendelse på avhandlingens *innholdstyper*, må det være klart at skadelig kildekode og overgrepsbilder omfattes av alternativene ”skriftlig” og ”visuell” informasjon. Skadelig objektkode har imidlertid ikke noen av de oppregnede karakteristika (skriftlig, visuell, auditiv), annet enn at den selvsagt er ”elektronisk”. Men *det* er ikke tilstrekkelig for en informasjonsbærer, fordi innholdet da må bestå av meningsinnhold. Situasjonen henger selvsagt sammen med at skadelig objektkode ikke er en ytring, men et verktøy som er en ”ting”. Skadelig objektkode omfattes altså ikke av begrepet informasjonsbærer.

For å gå tilbake til spørsmålet om grunnlagene for forebyggende inndragning av data, har drøftelsen vist at lovens ordning går ut på at både første og tredje punktum i strl. 2005 § 70 hjemler inndragning av data. Data er både ”ting” (første punktum) og ”informasjonsbærer” (tredje punktum). Innholdets karakter avgjør subsumsjonen. I kapittel 4 la jeg til grunn at skadelig kildekode og overgrepsbilder er ytringer, mens skadelig objektkode er et verktøy – en ”ting” – i form av data. Det betyr at forebyggende inndragning av skadelig objektkode (verktøy) skal skje i medhold av bestemmelsens første punktum, og skadelig kildekode og overgrepsbilder etter tredje punktum.

I forhold til overgrepsbildene innebærer dette en endring i forhold til rettstilstanden etter straffeloven 1902. Bilder har vært ansett som ”ting” og inndratt med hjemmel i strl. 1902 § 37 b (se lovsitat i fotnote her).[204] Det er lagt til grunn i Rt. 2000 s. 40, som gjaldt seksuelle overgrep begått overfor kvinner som var neddopet av domfelte. Etter overgrepene, mens de fremdeles var bevisstløse, hadde domfelte fotografert kvinnene i naken tilstand i svært integritetskrenkende positurer. I tillegg hadde han mange tilsvarende bilder av kvinner som han ikke var domfelt for å ha begått straffbare forhold overfor.

[203] Ot.prp. nr. 90 (2003-2004) kapittel 26.6.2 s. 349.
[204] Strl. 1902 § 37 b lyder:
”Selv om vilkårene etter §§ 34-36 ikke foreligger, kan en ting inndras når det på grunn av dens art og forholdene for øvrig er fare for at den vil bli brukt til en straffbar handling. Dette gjelder uansett hvem som er eier og uansett om straffansvar kan gjøres gjeldende mot noen. § 35 siste ledd gjelder tilsvarende.”

Spørsmålet var om de sistnevnte bildene kunne inndras med hjemmel i strl. 1902 § 37 b om forebyggende inndragning av "ting" (smlg. strl. 2005 § 70 første ledd første punktum). Førstvoterende fastslo at det er "… ikkje tvilsamt at bilete er «ting» etter straffelova § 37 b", og bildene ble inndratt. Høyesterett kan ikke ha ment at *meningsinnholdet* var "ting", så uttalelsen må forstås å referere seg til *fotografiene*, dvs. bilde på papir.[205] For databaserte bilder er *dataene* mediet og korresponderer med papiret, og er derfor "ting" (smlg. strl. 2005 § 69 annet ledd). Det samme følger av at inndragningspraksis i pornosaker har anvendt strl. 1902 § 35 om inndragning av "ting", og ikke hjemmelen for inndragning av "trykt skrift", jf. strl. 1902 § 38.[206] Etter straffeloven 2005 ville § 70 tredje punktum ("informasjonsbærer") vært korrekt hjemmel, ikke første punktum om "ting".

5.4.2 Nærmere om inndragningsgrunnlagene

Forebyggende inndragning er et preventivt tiltak og kan anvendes overfor et bredt spekter objekter siden "ting" favner vidt. I rettspraksis knyttet til strl. 1902 § 37 b som bare krever "fare" for at tingen vil bli brukt til en straffbar handling, er det lagt til grunn at det bør utvises tilbakeholdenhet ved bruk av bestemmelsen.[207] For bedre å reflektere rettspraksis krever strl. 2005 § 70 første ledd "nærliggende fare".[208]

Etter bestemmelsens første punktum skal vilkåret om "nærliggende fare" vurderes i lys av "tingens art og forholdene for øvrig" med tanke på om den "vil bli gjort til gjenstand for eller brukt ved en straffbar handling." I forhold til avhandlingens innholdstyper er denne vurderingen bare relevant for skadelig objektkode. Overgrepsbilder og skadelig kildekode inndras jo etter tredje punktum om "informasjonsbærer".

Forutsetningen for forebyggende inndragning er at det ikke er begått en straffbar handling. Siden skadelig objektkode ikke er noe politiet kan finne og inndra på samme vis som fysiske

[205] Av slutningen til Larvik herredsrett gjengitt i Høyesteretts avgjørelse, fremgår det at inndragningen gjaldt "513 enkeltfotografier med tilhørende negativer", dvs. at det ikke var tale om datafiler.
[206] Jeg kommer nærmere inn på denne praksis i kapittel 11.4.3.4.
[207] Se Rt. 1997 s. 27 (inndragning av våpen); Rt. 1998 s. 2006 (inndragning av motorsykkel) og Rt. 2000 s. 40 (inndragning av integritetskrenkende fotografier). Se også Ot.prp. nr. 90 (2003-2004) kapittel 30.1 s. 465: "Likeledes vil det ofte være nærliggende fare for at en person benytter et virusprogram til å begå dataskadeverk hvis han ikke har en plausibel grunn til å ha laget et slikt program."
[208] Ot.prp. nr. 90 (2003-2004) kapittel 26.5.3 s. 348.

objekter, for eksempel et farlig våpen, synes ikke inndragningsgrunnlaget å være særlig praktisk i dette tilfellet.[209]

Realistisk sett kan inndragningsspørsmålet bare komme opp dersom politiet alt har foretatt et beslag og avdekket skadelig objektkode i den forbindelse.[210] Dersom saken gjelder datakriminalitet er det mest nærliggende at objektkoden kan inndras med hjemmel i strl. 2005 § 69 bokstav c. For at det skal bli tale om forebyggende inndragning må tilknytningsvilkåret mellom objektkoden og lovbruddet mangle. Det betyr at lovbruddet gjelder et forhold hvor den skadelige objektkoden ikke kan ha noen relevans.

Etter sin art kan objektkoden brukes til å begå lovbrudd, så spørsmål er om "forholdene for øvrig" gjør det til en nærliggende fare. Det må vurderes i forhold til situasjonen og det må foreligge konkrete holdepunkter for faren. Det bør tas i betraktning at til tross for det omfattende forbudet mot befatning med skadelig dataprogram, jf. den objektive gjerningsbeskrivelsen i strl. 2005 § 201, er lovens utgangspunkt at befatningen er *lovlig.* Det følger av at straffebudet krever at befatningen skjer med "forsett om å begå en straffbar handling", dvs. et såkalt subjektivt overskudd. Det er lovlig å være i besittelse av skadelig dataprogram selv om man er klar over dets skadeevne, og man behøver ikke dokumentere en god grunn for befatningen. Forutsetningen er at det ikke foreligger forsett om å begå en straffbar handling.[211]

Dessuten kan det foreligge aktverdige motiver for befatningen med skadelig dataprogram. Både i forskningsmiljøer og datasikkerhetsforetak kan befatningen skyldes behov for å analysere koden. Også en viss privat utveksling kan skje. Det skal for eksempel være vanlig at datasikkerhetsforetak utveksler skadelig dataprogram med hverandre, som ledd i bransjesamarbeidet. Det gir rask mulighet til å analysere programmene, gi dem en unik identitet og oppdatere filtrene i nettet.[212] Det er egentlig bare den offentlige

[209] Smlg. konklusjonen i kapittel 5.3.2.3 om inndragning av skadelig dataprogram som lovbryteren besitter.
[210] Se kapittel 5.3.2.3.
[211] Det bevismessige problemet med å dokumentere et slikt forsett, uten at det foreligger befatning med en annen straffbar handling, er stort. Anvendelse av strl. 2005 § 201 alene synes derfor ikke som en meget praktisk mulighet.
[212] Ifølge opplysninger fra en "malware"-ekspert i datasikkerhetsbransjen er det vanlig praksis at datasikkerhetsforetak utveksler skadelige dataprogram med hverandre for å kunne utføre analyse. Foretakets teknologi for å detektere og blokkere det skadelige programmet i nettet, er imidlertid proprietær, dvs. bedriftens egen eiendom. (*Fagerland*, epost 16.05.2007, i arkiv hos meg).

tilgjengeliggjøringen av skadelig dataprogram i nettet som ubetinget er straffbar. Men da er inndragningshjemmelen strl. 2005 § 69.

Dersom en ansatt i et foretak som nevnt, begår underslag eller ryker ut i et slagsmål i helgen, og straffes for legemskrenkelse, kan det neppe konstateres nærliggende fare for at vedkommende vil bruke objektkoden til en straffbar handling. Denne inndragningshjemmelen for skadelig dataprogram som er tatt i beslag synes derfor å være lite praktisk. Hvis programmene ikke kan inndras etter strl. 2005 § 69 foreligger neppe grunnlag for inndragning i det hele tatt.

Et annet spørsmål er om forebyggende inndragning kan skje overfor den skadelige objektkoden som spres i nettet. Spørsmålet blir hypotetisk fordi politiet ikke er i stand til å foreta inndragningen. Som vanlig bruker kan ikke politiet gripe inn i datastrømmene på nettet. Hvis man likevel tenker seg muligheten, støter man på problemet med manglende ekspertise til å avgjøre hva som er skadelig dataprogram. Ytterligere er skadelig dataprogram på nettet så vidt spredt så det er vanskelig å se hvordan inndragning skulle skje uten å ta i bruk filtrering. Det forutsetter en beslutning *på forhånd* om hvilke dataprogram som skal filtreres slik at inndragningen kan skje automatisk. Derfor er det nødvendig å ta inndragning av beslaglagte data som utgangspunkt for inndragning i nettet. Siden tilgjengeliggjøringen er straffbar antas inndragningsgrunnlaget å være strl. 2005 § 69 bokstav b, jf. drøftelsen i kapittel 5.3.2.4.

For *overgrepsbilder og skadelig kildekode* er hjemmel for forebyggende inndragning strl. 2005 § 70 tredje punktum. Da må det være fare for "uopprettelig skade", noe som tar sikte på skade av ikke-økonomisk karakter, for eksempel krenkelse av æren, privatlivets fred og andre aspekter av personvernet.[213]

Det er vanskelig å se hvordan kildekoden kan forårsake denne type skade, så inndragningshjemmelen er ikke så velegnet for slikt innhold. På den annen side er det klart at en skadelig kildekode til et selvspredende program har stort skadepotensiale og sterke reelle hensyn taler for at det inndras før det spres med i praksis uopprettelig skade på nettet. Sannsynligvis er man hjulpet av strl. 2005 § 69 i dette tilfellet, som må ses i sammenheng med forbudet mot forsettlig besittelse av selvspredende dataprogram, jf. strl. 2005 § 201

[213] Ot.prp. nr. 90 (2003-2004) s. 465.

bokstav b annet punktum. Behovet for forebyggende inndragning av skadelig kildekode er derfor som for objektkoden, liten.

Også med hensyn til overgrepsbilder som er tatt i beslag er det vanskelig å tenke seg at ikke vilkårene for inndragning allerede etter strl. 2005 § 69 er oppfylt. Bestemmelsen kommer til anvendelse også om de subjektive vilkår ikke er oppfylt, så det er lite behov for forebyggende inndragning av overgrepsbilder som er tatt i beslag. Et unntak gjelder rekonstruerte filer hvor besittelsen ikke representerer noe lovbrudd. De må inndras etter strl. 2005 § 70.[214] Dersom situasjonen unntaksvis skulle oppstå, må det uten videre være klart at vilkåret om "fare for uopprettelig skade" er oppfylt. Bildene er en alvorlig krenkelse av barnets personvern som må bringes til opphør.

Som en liten ekskurs her, tilføyer jeg at det samme må anses å gjelde for "voksenpornografi" som lovbryteren har produsert uten samtykke fra personene på bildet. Slik pornografi er det lovlig å besitte, men ikke å spre. I den tidligere omtalte saken i Rt. 2000 s. 40, hadde domfelte tatt integritetskrenkende bilder av kvinner som han hadde bedøvet og forgrepet seg på seksuelt. Disse bildene ble inndratt med hjemmel i strl. 1902 § 35. Spørsmålet gjaldt om lignende bilder av kvinner han ikke var dømt for å ha begått overgrep mot, kunne inndras med hjemmel i strl. 1902 § 37 b om forebyggende inndragning. Høyesteretts mindretall mente at det ikke var konkrete holdepunkter for spredningsfare, og besittelsen var ikke straffbar. Etter flertallets vurdering forelå spredningsfare, så resultatet ble at bildene ble inndratt.

Her synes det å foreligge en mangel ved loven. Det må være åpenbart at retten til respekt for privat liv etter EMK art. 8, må pålegge myndighetene en plikt til å destruere slike bilder, selv om de misbrukte og avbildete kvinnene ikke selv har mulighet til å fremsette kravet.[215] Det må gjelde selv om det ikke er avklart om det er domfelte som har tatt bildene. Av Rt. 2000 s. 40 fremgår det at

> "… bileta av eit titals andre jenter som domfelte ikkje har vilja seie namna på, og som ikkje er identifiserte. Alle er av same karakter, idet jentene verker medvetslause eller i djup søvn … Lagmannsretten har kome til at fotografia er av ein slik art at dei fotograferte kvinnene sikkert ikkje ville samtykt til attgjeving eller i offentleg visning."

[214] Se kapittel 5.3.2.3.
[215] EMK art. 8 er sitert i kapittel 12.1.

Det strider mot rettsfølelsen å anse overgriperens besittelse av bildene som rettmessig fordi forbudet mot "voksenpornografi" ikke rammer forholdet. Både fotograferingen og besittelsen må anses å være i strid med EMK art. 8, og i henhold til EMK art. 1, plikter myndighetene å sikre de konvensjonsbaserte rettighetene for sine borgere, dvs. sørge for at retten til privatliv er effektiv. Siden selve det forhold at lovbryteren besitter bildene må anses å representere en krenkelse av kvinnenes rett til privatliv, kan ikke en konkret vurdering av spredningsfaren anses å gi et tilstrekkelig effektivt vern. Det synes følgelig å være behov for en lovendring her.

For så vidt gjelder kildekode og overgrepsbilder som er *spredt i nettet*, blir situasjonen som for den skadelige objektkoden. Politiet er avskåret fra å foreta inndragning med mindre det kan gjøres automatisert.

5.5 Spesifikasjonen i inndragningsbeslutningen

Inndragningsbeslutningen må vise til hjemmelsgrunnlaget, dvs. strl. 2005 §§ 69 eller 70, jf. § 76. Det er bare ved inndragning av skadelig objektkode at det ikke skal vises til strl. 2005 § 76. I tillegg må beslutningen spesifisere de datafiler som er inndratt.

Et spørsmål er om det er praktisk gjennomførbart å spesifisere filene, særlig i saker om overgrepsbilder hvor antallet ofte kommer opp i tusenvis av filer. Hvordan skulle man for eksempel ha spesifisert de 32 000 filene dersom datainndragning hadde blitt anvendt i Rt. 2005 s. 1058?[216] Under etterforskingen utferdiges imidlertid en politirapport som spesifiserer de rettsstridige filene i beslaget. Rapporten som kalles "analyse av databeslag", inngår i sakens dokumenter, er omfattet av mistenktes og forsvarerens innsynsrett, jf. strpl. § 242, og således undergitt kontradiktorisk behandling. Rapporten gir grunnlaget for opplysningene i tiltalen om overtredelsens omfang, og kan dokumenteres under hovedforhandlingen sammen med et representativt utvalg av bilder og videosnutter. Inndragningsbeslutningen kan dermed utformes med en henvisning til listen i rapporten. Det vil være i samsvar med praksis ved inndragning av fysiske ting, når omfanget er for stort til at det hensiktsmessig kan spesifiseres i selve beslutningen, se for eksempel Rt. 1980 s. 1532. Saken gjaldt omsetning av utuktige skrifter m.v., jf. strl. 1902 § 211. Beslaget hadde en anslått totalvekt på "vel 16 tonn".

[216] Saken er omtalt i kapittel 5.3.1.

Tingretten inndro ca 97 000 pornoblader, 18 000 filmer og 20 videobånd, og viste til beslagsrapporten. Fremgangsmåten ble opprettholdt av Høyesterett.

Med henvisning til analyserapporten gir datainndragning *en helt presis spesifisering* av de inndratte datafiler, selv om antallet skulle være stort. Dermed oppfylles vilkåret i strl. 2005 § 76 annet ledd første punktum om at det ved

> "inndragning av en informasjonsbærer skal […] angis hvilke deler av innholdet som begrunner inndragningen."

På denne måten gis det et *entydig grunnlag* for å bestemme hvilke datafiler som skal overføres til RDB, dersom det er aktuelt å gå videre med inndragning av dubletter i nettet. Den senere inndragningen av dubletter innebærer ikke noe spesifikasjonsproblem, den er bare en funksjon av de "svartelistede" datafilene i RDB. Den presise spesifiseringen er også i godt samsvar med lovens regler for *gjennomføringen* av datainndragningen, som jeg behandler i neste kapittel.

På bakgrunn av konklusjonen om at dublettene teller som én ved inndragning, bør beslutningen bare angi totalt antall unike filer. Filene kan overføres til RDB hvor hver enkelt representerer en unik dataidentitet.

Inndragningsbeslutningen bør ikke spesifisere dataidentiteten som sådan, fordi den er avhengig av tekniske kriterier. Jeg har vist til hash teknologi som egnet verktøy for tildeling av identiteter.[217] Over tid kan det bli utviklet ny teknologi som beregner identiteten til de samme filene på en annen måte. Dublettene vil likevel ha felles identitet. Det vesentlige er hvilke filer som er inndratt, og man må kunne kontrollere en "match" mellom de inndratte filene i analyserapporten som ligger til grunn for inndragningen, og filene i RDB. Det kan gjøres ved bruk av saks- og løpenummer for filene.[218]

Jeg kan her nevne at man i *amerikansk rett* har hatt en diskusjon om bruk av automatiserte søk etter rettsstridig innhold i nettet i henhold til et predefinert grunnlag. Det er slik jeg mener at inndragningsbeslutningen kan fungere for dublettene. Diskusjonen har vesentlig angått

[217] Se kapittel 3.3.3.
[218] I kapittel 14.4 har jeg behandlet spørsmålet om hemmelighold av sjekksummen er forenlig med informasjonsplikten overfor borgerne, jf. EMK art. 8, og funnet at EMK art. 8 ikke er til hinder for dette.

spørsmålet om metoden er forenlig med fjerde tillegg (”Fourth Amendment”) til den amerikanske konstitusjonen. Det er en bestemmelse som har et visst slektskap med G § 102 (forbud mot husinkvisisjoner) og EMK art. 8.[219]

I den amerikanske diskursen har den kjente jusprofessor i ”internettets forfatningsrett”, *Lessig,* konkludert med at metoden kan godtas dersom teknologien oppfyller bestemte krav. Disse kravene er at algoritmens funksjon må være kontrollert, og det må foreligge garanti for sikker ”match” ved bruk av programmet.[220]

Det betyr per i dag at hash teknologien som jeg har redegjort for i kapittel 3.3.3, kan brukes. Men rettslig sett kan man ikke binde seg til én spesifikk teknologi. Kanskje utvikles det ny teknologi som er enda mer presis og sikker og da må det være adgang til å beregne dataidentitetene til filene i RDB på nytt, slik at man hele tiden kan bruke den teknologien som er best. Derfor bør inndragningsbeslutningen vise direkte til filene som er spesifisert i analyserapporten.

5.6 Gjennomføring av datainndragning

I strl. 2005 § 76 annet og tredje ledd gis det bestemmelser om gjennomføring av inndragning av informasjonsbærer. Disse delene av bestemmelsen lyder slik:

> ”Ved inndragning av en informasjonsbærer skal det angis hvilke deler av innholdet som begrunner inndragningen. Den som må tåle inndragningen, kan mot å dekke utgiftene kreve å få en kopi av den del av innholdet som ikke omfattes av inndragningen.

[219] Fourth Amendment lyder slik: “The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated; and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”. *Hubbard* (2005) s. 8.

[220] *Lessig* (2006) s. 222-224. Diskusjonen har sitt opphav i en artikkel skrevet av *Adler* om en metode han kalte ”Net- Wide Search”, *Adler* (1995). Artikkelen synes å ha generert synspunkter i to retninger. Den ene gjelder muligheten for å misbruke RDB ved å legge inn annet materiale enn det som er formålet. Dette later til å ha vært *Adlers* største innvending mot metoden. Jeg antar at inndragningsprosedyren for å bygge opp RDB sikrer mot innlegging av annet materiale, og *Adler* drøftet ikke denne muligheten. Den andre hovedinnvendingen gjelder hvordan man sikrer seg at innholdet i RDB virkelig rammes av loven. Se *Salgado* (2005) s. 46, som påpeker at sjekksummene som sådan ikke er omfattet av forbudet: “The definition of child pornography cannot be set out as a chemical formula, unlike drug contraband, and no legislative body has declared particular images to be contraband, much less blessed a hash set.” Det er dog et poeng som ligger noe på siden av saken, fordi den rettslige vurderingen gjøres i forhold til innholdet av dataene. *Kerr* (2006) s. 316, er således mer positiv. Han sier at hvis ”a dozen of defendants have been convicted of possessing or distributing a particular image of child pornography, isn’t that equivalent to a legal determination that the particular image is contraband?” Også her fyller inndragningsprosedyren som jeg foreslår, rettssikkerhetshensynene.

Dersom lovbryteren ikke er rettighetshaver til en informasjonsbærer på et datasystem som kreves inndratt, rettes kravet mot tilbyderen av datasystemet. Tilbyderen kan pålegges å stenge lovbryterens tilgang til informasjonsbæreren og slette innhold som tilhører lovbryteren. Er lovbryteren rettighetshaver til informasjonsbæreren, kan tilbyderen pålegges å stenge tilgangen til informasjonsbæreren og slette innholdet."[221]

Reglene kommer til anvendelse uavhengig av om inndragningen er skjedd med hjemmel i strl. 2005 §§ 69 eller 70 tredje punktum, såfremt dataene bærer meningsinnhold. Det er imidlertid nærliggende å reise spørsmål om reglene bør anvendes analogisk på skadelig objektkode. Reglene er utformet med særlig henblikk på elektroniske forhold. Spesifikasjonskravet i annet ledd første punktum, og reglene om stenging og sletting i tredje ledd, er like hensiktsmessige for skadelig dataprogram som for data som bærer ytringer. Dette er analogi til gunst for den som utsettes for inndragningen, fordi det påser at inndragningen skjer så presist som mulig. Jeg antar derfor at denne fortolkningen er forsvarlig.[222]

Strl. 2005 § 76 annet ledd regulerer situasjonen hvor bare *deler av* innholdet på en informasjonsbærer skal inndras. Inndragningsbeslutningen skal da angi "hvilke deler av innholdet som begrunner inndragningen." Dette lar seg enkelt oppfylle ved inndragning av datafiler, ved henvisning til analyserapporten som beskrevet i kapittel 5.5. Bare filene på listen inndras.

Dersom ikke hele databeslaget skal inndras, oppstår spørsmålet om hvordan man effektivt sletter de inndratte filene. Hvis de kan rekonstrueres, bør også den fysiske bæreren inndras.[223]

[221] Strl. 2005 § 76 første og annet ledd ble vedtatt sammen med de øvrige bestemmelsene i straffelovens alminnelige del ved lov 20. mai 2005 nr. 28. Forarbeidene er Ot.prp. nr. 90 (2003-2004) kapittel 26 og utredningene som leder opp til denne. I Ot.prp. nr. 22 (2008-2009) ble strl. 2005 § 76 annet ledd annet punktum foreslått endret, og tredje ledd tilføyd. Det er bestemmelsen i denne ordrakt som er sitert i brødteksten. Bakgrunnen for endringene var Datakrimutvalgets arbeid som ble utført i tiden mellom de to proposisjonene, jf. NOU 2007: 2 kapittel 5.12 (rettighetstap, inndragning og vilkår for betingete dommer). Opprinnelig lød strl. § 2005 § 76 annet ledd annet punktum slik: "Den som må tåle inndragningen kan mot å dekke utgiftene kreve informasjonsbæreren tilbakelevert etter at det ulovlige innholdet er fjernet." Begrunnelsen for at regelen ble snudd om, var problemet med "effektiv sletting av lagret informasjon, som dermed også innebærer en mulighet for tilbakelevering av ulovlig materiale." (Ot.prp. nr. 22 (2008-2009) s. 397).

[222] Se kapittel 5.2.2 om utgangspunkter for fortolkning og analogispørsmålet.

[223] Se Rt. 1987 s. 49, inndragning av videokassetter med utuktige filmer. Inndragning var besluttet gjennomført ved sletting av det utuktige materialet (avmagnetisering), og videokassettene skulle deretter tilbakeleveres, jf. strl. 1902 § 35 fjerde ledd. Etter påtalemyndighetens anke fant Høyesterett at " det ikke er grunnlag for å bestemme dette i medhold av straffelovens § 35 fjerde ledd. Her hvor tiltalte har gjort seg til næring ulovlig å kopiere videofilmer, kan det ikke være tilstrekkelig "tiltak for å forebygge at tingen blir brukt til nye lovovertredelser"… at han får tilbakelevert "rene" kassetter. Disse vil han i så fall ha mulighet for å nytte i ny ulovlig virksomhet." Smlg. RG 2007 s. 169: Domfellelse for overtredelse av personopplysningsloven for å ha lagret 60 000 amerikanske navn, adresser og epostadresser og over 650 000 epostadresser, uten å rapportere til Datatilsynet. Tingretten hadde besluttet inndragning ved å slette de nevnte data. Med henvisning til Rt. 1987 s. 49 fant lagmannsretten at inndragningen måtte skje i det fysiske utstyret, men begrenset det til "maskinenes

De lovlige data kan i så fall tilbakeleveres på et nytt rent lagringsmedium til den berettigete. Loven åpner for denne muligheten, jf. strl. 2005 § 76 annet ledd annet punktum, mot at den berettigete dekker kostnadene. Men det er uansett viktig å foreta datainndragningen, for å bygge opp referansegrunnlaget i RDB.

Spesifikasjonen er også viktig ved *asymmetriske rettighetsforhold*, hvor eieren av lagringsmediet ikke er part i straffesaken. Dette omfatter nokså forskjellige situasjoner, fra private forhold hvor farens PC er misbrukt av "hacker-sønnen", en bedriftsserver som er misbrukt av en ansatt, til nettvertstjenester som kan ha mange tusen tjenestemottakere som leier sine egne brukerområder. Dersom servere til bedrifter og nettverter er involvert, er inndragning av den fysiske bæreren normalt utelukket. Da er det mulig å inndra rettigheten til brukerområdet, og å inndra domenet (for eksempel skurk.no), men dette er ikke det samme som å inndra *dataene*.[224] Domeneinndragning fratar heller ikke lovbryteren rådigheten over dataene, det bare vanskeliggjør tilgjengeliggjøringen, fordi nettstedet ikke lenger er søkbart på navnet.[225]

Dataene er "ting" uavhengig av de *rettigheter* som legger grunnlaget for at man disponerer et brukerområde eller et domene. Web 2.0-situasjonen utløser altså mulighet for *to typer gjenstandsinndragning,* både av *data* og *rettigheter*, jf. strl. 2005 § 69 annet ledd første og tredje alternativ. I begge tilfeller må tilbyder bistå for å gjennomføre inndragningen. Dersom dataene og retten til brukerområdet inndras, må gjennomføringen skje ved at nettverten sletter dataene og stenger tilgangen til brukerområdet. Inndragning av domenet må gjennomføres ved "svartelisting" av NORID, som administrer ordningen med nettadresser i Norge.[226] Dette

harddisker". Se også strl. 2005 § 70 annet ledd: "I stedet for å inndra tingen kan det påbys tiltak for å forebygge at tingen blir brukt til lovovertredelser.". Men i lys av de nevnte avgjørelsene er det neppe tilstrekkelig å nøye seg med å slette dataene, dersom meningen er at siktede skal får igjen det fysiske utstyret. Annerledes blir det selvsagt ved inndragning på brukerområder i nettet. Da må sletting skje, jf. str. 2005 § 76 tredje ledd.

[224] I Rt. 2009 s. 1011 (joyzone.no) ble det fastslått at det kunne tas beslag i et domenenavn som var brukt for ulovlig virksomhet, for å sikre et senere inndragningskrav.

[225] Ved søk på domenenavn finner man nettstedet via tjenesten til navnetjenerne, dvs. datamaskiner som sammenholder domenenavn med IP-adresser. Dersom domenenavnet er inndratt, kan IP-adressen fremdeles være i bruk.

[226] Inndragning resulterer i at *domfelte* varig fratas retten til bruk av domenenavnet. Et spørsmål er imidlertid hva som skjer med *domenenavnet* på sikt. Dersom det ikke skal kunne brukes av andre for lovlig virksomhet i fremtiden, vil inndragning representere et varig inngrep i ytringsfriheten på nettet, og kunne lede til en reduksjon i tilgjengelige domenenavn. Et domenenavn som har vært utnyttet for ulovlige formål, kan jo ha en verdi for lovlige formål senere, i hvert fall dersom det ikke hefter en varig "badwill" ved navnet. Ved henvendelse til NORID har jeg fått opplyst at inndragning resulterer i "svartelisting" av domenenavnet for en viss tid, inntil det på nytt blir frigitt for bruk.

kan skje ved pålegg fra politiet med henvisning til inndragningsbeslutningen, jf. strpl. § 455 annet ledd som bestemmer at fullbyrdingen iverksettes av politiet.[227]

Strl. 2005 § 76 tredje ledd berører spørsmålet om å få bistand fra tilbyder til å gjennomføre datainndragning. Bestemmelsen regulerer både situasjonen hvor "lovbryteren ikke er rettighetshaver til en informasjonsbærer på et datasystem som kreves inndratt" (jf. første punktum), og hvor lovbryteren *er* "rettighetshaver til informasjonsbæreren" (jf. tredje punktum). I begge tilfeller kan tilbyderen pålegges å stenge tilgangen til informasjonsbæreren og slette innholdet. Siden også det førstnevnte alternativet forutsetter at lovbryteren har brukerrettigheter til nettstedet (i forarbeidene kalt "brukerprofil"), synes det ikke å være noen forskjell mellom dem, så jeg behandler dem under ett.[228]

Den løsning lovgiver følgelig har lagt opp til er at lovbryterens personlige tilgang til et brukerområde i nettet, kan stenges og innholdet slettes av tilbyder, jf. strl. 2005 § 76 tredje ledd. Stengning av tilgangen innebærer det samme som å gjennomføre inndragning av *retten* til brukerområdet, jf. strl. 2005 § 69 annet ledd første alternativ ("rettigheter").[229]

Etter strl. 2005 § 76 tredje ledd er stengningen knyttet til et krav om å inndra en *informasjonsbærer* som lovbryteren er rettighetshaver til. En informasjonsbærer kan som vi har sett, være den fysiske bæreren og dataene som er lagret på den fysiske bæreren.[230] I nettverkskonteksten er det naturlig å tolke uttrykket slik at det betyr brukerområdet på nettvertens server, jf. "eller annet" i strl. 2005 § 76 første ledd. Sammenhengen i lovens

[227] Smlg. *Dyrnes* (2004) s. 242.
[228] Ot.prp. nr. 22 (2008-2009) kapittel 16.1 s. 398. Her står det at alternativet i tredje ledd første punktum omfatter at "lovbryteren ikke eier eller er rettighetshaver til nettstedet, men hvor vedkommende kun har tilgang til nettstedet og har lagret ulovlig materiale der. For disse tilfellene er det ikke adgang til å be tjenesteyteren om å stenge ned nettstedet slik at det blir utilgjengelig for enhver bruker, men kun å pålegge tjenesteyteren å forhindre at lovbryteren fortsatt har tilgang til nettstedet. I tillegg kan tjenesteyteren pålegges å slette materiale som tilhører lovbryteren. Dette vil for eksempel kunne gjøres ved at tjenesteyteren sletter lovbryterens brukerprofil på et nettsted som inneholder seksualiserte skildringer av barn. Bilder eller annet ulovlig materiale med tilknytning til denne brukerprofilen vil kunne slettes."
[229] Ytterligere en mulighet er å bruke rettighetstap, jf. strl. 2005 § 56, som er en mer inngripende reaksjon, fordi det formelt sett er straff, jf. strl. 2005 § 29 bokstav d, og fordi det kan lede til tap av retten til å ha internettaksess i det hele tatt. I hvert fall er det lagt til grunn av Datakrimutvalget, se NOU 2007: 2 kapittel 5.12.3 s. 119. På den andre siden har man Rt. 1995 s. 1872 (PINkode) hvor Høyesterett avslo påtalemyndighetens krav om tap av retten til "å være telefonabonnent". Høyesterett kunne ikke se tilstrekkelig grunn for en slik reaksjon og lot det "stå hen" om det var hjemmel til det. Av departementets bemerkninger i Ot.prp. nr. 90 (2003-2004) s. 321 synes det å fremgå at strl. 2005 § 56 gir hjemmel for rettighetstap av denne art, men at det sjelden vil være "tilstrekkelig tungtveiende grunner til å forby enhver form for bruk av telenettet." Det vises videre til at strl. 2005 § 57 om kontaktforbud også gjelder på "immaterielle steder", dvs. på nettet, og kan komme til anvendelse i en del praktiske tilfeller, se proposisjonen kapittel 24.3 og 24.4 særlig s. 321 og 324.
[230] Se kapittel 5.4.1.

hjemmelsrekke later altså til å være at *retten til brukerområdet* inndras med hjemmel i strl. 2005 § 69 annet ledd første alternativ (”rettigheter”), jf. strl. 2005 § 76 første, jf. tredje ledd. Da har man dekning for krav om inndragning av retten til brukerområdet og for stengning av tilgangen. Dersom *dataene* også ønskes inndratt må det hjemles i strl. 2005 § 69 annet ledd tredje alternativ (”elektronisk lagret informasjon”), jf. strl. 2005 § 76 første, jf. tredje ledd, hvoretter tilbyderen kan pålegges å slette dataene på brukerområdet.

Det synes som om reglene kunne vært forenklet ved å innskrenke tredje ledd til ett alternativ for stengning av brukerkonto og sletting av data. Det har også oppstått et uklart forhold mellom objektet for inndragning etter strl. 2005 § 69 og spesialreglene for fullbyrdelse. De sistnevnte reglene synes med henvisningen til ”informasjonsbærer” å forutsette at det kun er tale om datainndragning, mens rettighetsinndragning er like aktuelt. Og dermed oppstår også spørsmålet om det er behov for reglene i strl. 2005 § 76 tredje ledd i det hele tatt. I annen sammenheng regulerer ikke loven nøyaktig hvordan man skal gå frem for å fullbyrde krav om gjenstandsinndragning, politiet iverksetter fullbyrdingen med en henvisning til inndragningsbeslutningen.

5.7 Om det er adgang eller plikt til å foreta inndragning

Bruken av inndragning etter strl. 2005 § 69 er fakultativ, jf. ”kan inndras” i bestemmelsens første ledd. Utgangspunktet er altså motsatt av det som gjelder for utbytte av straffbar handling, hvor loven pålegger inndragningsplikt, jf. ”skal inndras” i strl. 2005 § 67 første punktum.

Ved avgjørelsen av ”om inndragning skal foretas” skal det tas hensyn til ”en effektiv håndheving av straffebudet”, og om inndragningen ”er forholdsmessig”, jf. strl. 2005 § 69 tredje ledd.

For overgrepsbilder kan det åpenbart ikke være rom for noe skjønn over *om* inndragning skal skje, det må være klart at alt materiale (alle datafiler) med slikt innhold *skal* inndras fordi all befatning er ulovlig. Det er ikke mulig å tenke seg at inndragningen av datafilene skulle være uforholdsmessig. Videre er det klart at inndragning er nødvendig for å effektivisere forbudet. Dersom man ikke foretok inndragning ville konsekvensen bli at man lot den straffbare besittelsen vedvare. Det må også tas i betraktning at subjektiv skyld ikke er et vilkår for

inndragning etter bestemmelsen, til tross for ordlyden som sier at det må foreligge "en straffbar handling".[231] Med hensyn til overgrepsbilder som er tatt i beslag er derfor konklusjonen at det foreligger *inndragningsplikt*, ikke bare en *adgang* slik bestemmelsens ordlyd indikerer.

Likevel finnes det tilfeller i rettspraksis hvor man har unnlatt å inndra overgrepsbilder. Muligens skyldes det at man bare har vurdert inndragning av *det fysiske utstyret*, noe som kan ha vært ansett som uforholdsmessig inngripende i tillegg til straffen. Men det synes klart at det likevel forelå en plikt til å inndra de rettsstridige datafilene.[232] Se følgende saker til illustrasjon:

> Rt. 2007 s. 422: Dom for besittelse av overgrepsbilder. Her ble spørsmål om inndragning ikke nevnt. En tenkelig grunn kan være at saken gjaldt besittelse av et lite antall bilder (8 filmsnutter, 37 bilder). Kanskje det medførte at inndragning av datautstyret fortonte seg som et uforholdsmessig inngrep i tillegg til fengselsstraffen. Men da ville det vært i god pakt med hensynet til rettshåndhevelsen å ha inndratt de ulovlige datafilene.
>
> RG 2007 s. 1345 (MMS): Domfelte hadde mottatt 13 overgrepsbilder på mobiltelefonen, og ble domfelt for å ha unnlatt å slette dem raskt nok (brudd på handlingsplikten). Mobiltelefonen ble ikke påstått inndratt, noe som kan skyldes at forgåelsen fremsto som liten. Bildene var tilsendt uoppfordret, antallet var lite og besittelsen hadde bare vart i to dager. Men man kunne altså inndratt bildene og latt domfelte beholde mobiltelefonen.

For skadelig dataprogram som er produsert av lovbryteren synes vurderingen å måtte bli tilsvarende som for overgrepsbilder. Det samme gjelder dersom det har vært brukt eller bestemt til å brukes ved en straffbar handling. Når ett av inndragningsgrunnlagene i strl. 2005 § 69 bokstav a eller c er oppfylt, må det således antas å foreligge inndragningsplikt. I andre tilfeller er utgangspunktet at programmet er å anse som *lovlig materiale* i den forstand at den private befatning og utveksling er lovlig. Det leder også til at det er lite rom for å anvende

[231] Se kapittel 5.3.1.
[232] Det som har skjedd er antakelig at bildene er blitt slettet av politiet før tilbakelevering av utstyret, men det er en ordning som ligger på siden av lovens bestemmelser.

forebyggende inndragning i disse tilfellene. I disse tilfellene innebærer lovens ord om at inndragning "kan" foretas, en realitet.

Drøftelsene av skadelig dataprogram har vært vanskelige fordi det er et spenningsforhold mellom lovens utgangspunkt om at befatningen er lovlig, og at loven på den annen side ikke krever subjektiv skyld for inndragning. Det er lite rimelig å inndra fordi hjemmelen nærmest har objektiv karakter, dersom tingen i utgangspunktet er lovlig på grunn av det subjektive overskuddet som må foreligge. Man må følgelig holde seg til muligheten for forebyggende inndragning hvor en konkret vurdering av faren blir avgjørende.

Hovedkonklusjonen er imidlertid at når ett av inndragningsgrunnlagene i strl. 2005 § 69 er oppfylt, foreligger det inndragnings*plikt* både for skadelig dataprogram og overgrepsbilder.

5.8 Hvorvidt inndragning er adekvat reaksjon for overgrepsbilder

For overgrepsbilder er lovens forbud så strengt at de ikke har noe lovlig anvendelsesområde (annet enn i en referansedatabase for politiet). Det gir grunn til å reise spørsmål ved om inndragning er den adekvate reaksjon etter loven.

Spørsmålet melder seg fordi inndragning som hovedregel skal utbringe et proveny, enten skal det skje til inntekt for statskassen, jf. strl. 2005 § 75 første ledd, eller til dekning av skadelidtes erstatningskrav, jf. strl. 2005 § 75 annet ledd. Det henger sammen med forutsetningen om at inndragning er et inngrep i eiendomsretten og i utgangspunktet må anses som et inngrep i formuesgoder.[233] Det er imidlertid åpenbart at inndragning av overgrepsbilder og skadelig dataprogram ikke kan gi slikt proveny.

En tilsvarende situasjon foreligger for narkotika, som også er undergitt totalforbud, jf. strl. 2005 § 231. Da foretas det inndragning av stoffet som deretter destrueres. Det er riktignok opplyst at man i praksis tar stoffet i beslag, og destruerer det umiddelbart uten å avvente inndragningsbeslutningen. Praksisen er begrunnet med at politiet dermed slipper å bruke

[233] Se mer om dette i avhandlingen del IV.

ressurser på å lagre stoffet til inndragningsdommen foreligger, når det under enhver omstendighet er klart at stoffet er ulovlig og må destrueres.[234]

Denne praksis har vært kritisert, men ikke fordi man mener at det ikke er tale om inndragning. Tvert imot later det til å være enighet om at materiale uten legal verdi må bringes under kontroll og destrueres med hjemmel i inndragningsreglene. For å kunne holde på den etablerte praksis i lovlige former, er det derfor gitt en bestemmelse i strpl. § 214 b, som delegerer inndragningskompetansen til påtalemyndigheten når slike "ting" avdekkes og "verken eieren, besitteren eller lovbryteren er kjent".[235] Bestemmelsen korresponderer med strl. 2005 § 74, som gir tingretten adgang til å beslutte inndragning uten at noen er gjort til saksøkt, når verken lovbryteren eller besitteren har kjent oppholdssted i Norge.

På denne bakgrunn må det antas at inndragning er den adekvate reaksjon overfor overgrepsbilder, til tross for manglende legal verdi. Det støttes av en kommentar i forarbeidene til strpl. § 214 b, om at politiet i kraft av bestemmelsen, vil

> "kunne inndra barnepornografisk materiale som ikke kan knyttes til noen bestemt person."[236]

I del IV behandler jeg spørsmålet om eiendomsrett til data. Eiendomsretten eksisterer selv om den utsettes for store inngrep, fordi det er en residualrett. Selv om man er farlig nær en fiksjon kan man si at eiendomsretten eksisterer i en formell rettslig forstand, også for materiale som nevnt i strl. 2005 §§ 201 og 311. Man har eiendomsretten om enn i meget uthult form, inntil den opphører, for eksempel ved inndragning. Det er dette perspektivet som må anlegges på inndragning av det rettsstridige materialet som avhandlingen behandler.

[234] Ot.prp. nr. 90 (2003-2004) kapittel 26.12.3.3 s. 358. "I dag destrueres normalt beslaglagt narkotika uten at det reises inndragningssak, noe som ikke er formelt riktig. … Effektivitetshensyn tilsier derfor at påtalemyndigheten gis adgang til å beslutte inndragning." Se også *Dyrnes* (2004) s. 91 som skriver at: "Ofte fattes ikke noe formelt inndragningsvedtak for slike produkter. Det tas som en selvfølge at tingene fratas lovbryteren. Det er sjelden lovbryteren protesterer mot slik «uformell inndragning»."

[235] Strpl. § 214 b lyder: "Påtalemyndigheten kan beslutte inndragning av en beslaglagt ting dersom inndragning kan skje etter straffeloven § 74 og verken eieren, lovbryteren eller besitteren er kjent. Beslutningen skal være skriftlig og begrunnet. Eieren eller besitteren kan kreve saken forelagt for retten innen 6 måneder etter at vedtak om inndragning er fattet." Bestemmelsen ble vedtatt samtidig med straffeloven 2005, dvs. 20. mai 2005 nr. 28.

[236] Ot.prp. nr. 90 (2003-2004) kapittel 30.4 s. 492.

5.9 Refleksjon over reglene – hjemmel for inndragning av dublettene

Drøftelsene har vist at strl. 2005 § 69 er den viktigste hjemmelen for inndragning av overgrepsbilder og skadelig dataprogram som er tatt i beslag. Et vesentlig formål med inndragningen er å effektivisere håndhevingen av straffebudet, noe som fremgår av bestemmelsens tredje ledd, som sier at ved vurderingen av om inndragning skal foretas og hvilket omfang den skal ha, skal det

> "særlig legges vekt på om inndragning er påkrevd av hensyn til *en effektiv håndheving av straffebudet,* og om det er forholdsmessig. Når forholdsmessigheten vurderes, skal det blant annet legges vekt på andre reaksjoner som ilegges, og konsekvensene for den som inndragningen rettes mot." (min uth.).

De inndratte data er vanligvis dubletter av data som finnes på nettet, enten fordi de er anskaffet derfra eller fordi lovbryteren har tilgjengeliggjort dem. I lys av inndragningsplikten for skadelig dataprogram og overgrepsbildene, er spørsmålet om det kan utledes noe mer av effektiviseringsformålet enn hensynet til den konkrete saken. På grunn av sammenhengen mellom datafilene i saken og dublettene i nettet, bør effektivitetsvurderingen også ta hensyn til dublettene i nettet.

Hensynene til den konkrete straffesaken og til nettet, korresponderer i noen grad med hensynene til individual- og allmennprevensjon. Mens forholdsmessighetsvurderingen i tredje ledd er knyttet opp til individuelle forhold, åpner effektivitetsbetraktninger også for å ta allmennpreventive hensyn. Effekten utenfor den konkrete saken, dvs. til dublettene i nettet, bør derfor trekkes inn i vurderingene.

Hvis man bare ser på forholdene i den konkrete saken, er datainndragning hensiktsmessig for å oppnå en reaksjon i tilfeller hvor man er avskåret fra å inndra den fysiske bæreren. På den annen side kan lovbryteren enkelt *gjenanskaffe* materialet ved å laste det ned fra nettet på nytt. Den store overførings- og lagringskapasiteten, samt den enkle tilgjengeligheten, gjør at det går raskt, og det koster lite.[237] Det er selvfølgelig utelukket å tilbakelevere det rettsstridige

[237] Materialet er i stor grad fritt tilgjengelig på nettet. Ved bruk av betalingstjenester viser praksis at det oppnås ubegrenset tilgang til nettstedet for et lite beløp per måned: Rt. 2004 s. 215, USD 29/mnd. (*Landslide*, hvor bakmennene, et ektepar fra Texas, tjente mellom 4 og 12 millioner norske kroner i løpet av de åtte månedene tjenesten pågikk, *Sunde* (2006) s. 244): RG 2006 s. 595, USD 40-60/mnd.; LA-2005-111640, for to måneder med tilgang til tre nettsteder betalte domfelte ca 1000 kroner; LB-2006-51173, USD 5/mnd., for medlemskap i

materialet, men inndragningen isolert sett kan neppe anses å virke *effektiviserende* for håndhevelsen.

Unntak gjelder for *materiale som lovbryteren selv har produsert, men ennå ikke rukket å tilgjengeliggjøre.* Det kan være overgrepsbilder han selv har tatt eller selvspredende dataprogram vedkommende har programmert.[238] Det kan også være bilder som lovbryteren har medvirket til å produsere ved å forlede mindreårige til å posere nakne m.v., foran webkamera.[239] Fra et effektiviseringssynspunkt er det påkrevet å foreta inndragning i disse tilfellene, for å avverge det varige problemet som forårsakes av tilgjengeliggjøring.[240] Begrunnelsen for inndragning av data som lovbryteren har produsert, ligger altså i *det forebyggende*, til tross for at strl. 2005 § 70 ikke er inndragningsgrunnlaget.

Men *vanligvis* består beslaget av dubletter som også finnes på nettet, og inndragning vil være et langt mer effektivt virkemiddel om den også omfattet disse. Derfor er det behov for å la inndragningen av de beslaglagte data få virkning for dublettene i nettet. Med forbehold for materiale som lovbryteren har produsert, men ikke rukket å tilgjengeliggjøre, er den viktigste begrunnelsen for datainndragning at det kan legge grunnlaget for presis sjekksumbasert filtrering i nettet.

Ved inndragning av datafilene i beslaget rettes inndragningskravet mot lovbryteren, jf. strl. 2005 § 71 tredje ledd (”inndragning etter § 69 foretas overfor lovbryteren …”). Forebyggende inndragning rettes mot den som ”besitter eller eier gjenstanden”, jf. strl. 2005 § 71 fjerde ledd.

Neste steg er å konstatere at datafilens identitet er unik og identifiserer dublettene. Av grunner som jeg forklarer i del VI, kan imidlertid ikke automatisert inndragning rettes mot person. Automatiseringen er en fullbyrdelse av inndragning som alt er besluttet. Beslutningen må derfor rettes mot ukjent lovbryter eller besitter, noe det er hjemmel for i strl. 2005 § 74 tredje ledd, som lyder:

---

en newsgruppe med overgrepsbilder; LE-2004-8204, USD 7,50/mnd.: ”… som medlem av nyhetsgruppen [fikk siktede] tilgang til om lag 150.000 bilder ukentlig. Nye bilder ble fortløpende lagt ut på nettstedet.” Til tross for de lave beløpene tjener bakmennene millioner. Av dette forstår man flere ting: 1) At barna anses som verdiløse, fordi som det er sagt: ”De er små og billige og lette å få tak i” se *Sunde* (2006) s. 217 med videre henvisninger; 2) At markedet er enormt; og 3) At online business hvor ytelsen består i dubletter er en enkel måte for å skape stor profitt.

[238] I slike tilfeller er inndragningsgrunnlaget strl. 2005 § 69 første ledd bokstav a, se kapittel 5.3.2.2.

[239] Se Rt. 2009 s. 140 omtalt i kapittel 5.3.2.2.

[240] Se kapittel 3.3.4.

> ”Har verken lovbryteren eller besitteren kjent oppholdssted i Norge, kan tingretten beslutte inndragning på de vilkår som er nevnt i annet ledd, uten at noen er gjort til saksøkt.”

Bestemmelsen har som nevnt en parallell i strpl. § 214 b som gir påtalemyndigheten kompetanse til å beslutte inndragning i slike tilfeller. Men siden saken alt er brakt inn for retten er det mest nærliggende å treffe en beslutning i samme sak, i medhold av strl. 2005 § 74 tredje ledd. Det er altså tale om å beslutte inndragning uten at noen er gjort til saksøkt.

Det kan ikke antas at strl. 2005 § 74 tredje ledd krever at det først gjøres anstrengelser for å avdekke lovbryterens eller besitterens identitet. Det ville avskjære inndragningsmulighetene, fordi man ikke kan forhåndsidentifisere besitteren av dublettene. Det bør ikke være til hinder for en praktikabel rettshåndhevelse ved bruk av inndragning.[241] Vilkåret om at det må foreligge en straffbar handling er oppfylt for dublettene. For overgrepsbildene er vilkåret oppfylt uansett hvor de finnes i nettet. For skadelig dataprogram er det oppfylt overalt hvor det er offentlig tilgjengeliggjort, mens det må gjøres en reservasjon for dataprogram som håndteres privat, siden det kan være lovlig. Dette kan man ta hensyn til ved hvordan man innretter filtreringen som utfører inndragningen. Privat befatning med skadelig dataprogram holder jeg derfor utenfor spørsmålet om automatisert inndragning, se kapittel 13 i del VI.

Strl. 2005 § 74 tredje ledd forutsetter også at tingen må være tatt i beslag. Det følger av henvisningen til ”de vilkår som er nevnt i annet ledd”, som blant annet nevner ”beslaget”. Dersom man kan basere seg på beslaget som er gjort i straffesaken og på det grunnlag inndra datafilen med tilhørende dataidentitet, er vilkårene i strl. 2005 § 74 oppfylt. Det sentrale spørsmålet synes derfor å være om loven åpner for inndragning på grunnlag av identiteten. Dette spørsmålet behandler jeg i del V. Forutsatt at loven åpner for denne ordningen, kan beslutningen treffes i straffesaken mot lovbryteren, ved å tilføye et punkt om det i slutningen.

[241] I tilknytning til den tilsvarende inndragningsbestemmelsen i strl. 1902 § 37 c, trekker *Matningsdal* (1987) frem hensynet til en praktikabel retthåndhevelse ved bruk av inndragning uten at noen gjøres til saksøkt, se s. 495-496.

For å bringe drøftelsen ned på *et helt konkret plan*, kan inndragningsbeslutningen i straffesaken for eksempel utformes slik:

1. Dom på straff overfor NN.

2. I tillegg dømmes NN til å tåle inndragning av 75 360 datafiler som spesifisert i analyserapport datert DDMMÅÅ, jf. strl. 2005 § 69 første ledd bokstav b, jf. § 76, annet ledd første punktum, jf. § 71 tredje ledd.

3. I tillegg inndras dublettene av datafilene nevnt i punkt 2, jf. strl. 2005 § 69, jf. § 76 annet ledd første punktum, jf. § 74 tredje ledd.

5.10 Oppsummering

I dette kapitlet har jeg gjennomgått inndragningsgrunnlagene for skadelig dataprogram og overgrepsbilder. For så vidt gjelder data som er tatt i beslag, er strl. 2005 § 69 den praktiske hjemmelen, fordi det da vanligvis vil foreligge en straffbar handling. I disse tilfellene hersker det en inndragningsplikt, ikke bare en adgang.

I forbindelse med inndragningen av lovbryterens data i straffesaken, kan det treffes beslutning om inndragning av dublettene med hjemmel i strl. 2005 § 74 tredje ledd.

Et gjennomgående funn er at dataidentiteten har materiell betydning ved fortolkningen av alternativene i den objektive gjerningsbeskrivelsen i strl. 2005 §§ 201 og 311, og ved fortolkningen av inndragningsgrunnlagene i strl. 2005 § 69. Det generelle poenget er at dataidentiteten er det relevante kriteriet ved anvendelsen av reglene, ikke antallet filer. Det har til følge at dublettene i nettet kan inndras sammen med filene i beslaget. Det materielle grunnlaget for å tillegge dataidentiteten denne betydningen for automatisert inndragning, er dog ikke behandlet i dette kapitlet. Spørsmålet behandles i del V. Men såfremt det materielle grunnlaget viser seg å foreligge, gir reglene *de lege lata* hjemmel for å foreta automatisert inndragning.

Inndragningen av datafilene spesifiseres med henvisning til analyserapporten som ligger i sakens dokumenter. De inndratte filene kan deretter overføres til RDB, tildeles en teknisk identitet og brukes som grunnlag for automatisert inndragning.

Et funn av mer regelteknisk art gjelder manglende innholdsmessig konsistens ved lovens bruk av "elektronisk lagret kommunikasjon". I strl. 2005 § 69 annet ledd betyr det "data", og i § 76 første ledd betyr det "databasert informasjon", dvs. meningsinnhold. Det skaper imidlertid ikke noe problem for automatisert inndragning. Begrepsmessig inkonsistens av språklig, men ikke innholdsmessig art, finnes også mellom strl. 2005 § 69 annet ledd "elektronisk lagret informasjon" og strl. 2005 § 351 annet ledd "data", som begge steder betyr data.

Til sist, og nærmest som en sidevirkning av den øvrige kartleggingen, synes det å foreligge et behov for å se på lovverket når det gjelder beskyttelsen av personvernet ("privat liv", jf. EMK art. 8) for så vidt gjelder ærekrenkende bilder som er tatt uten den avbildedes samtykke. Den skjønnsmessige adgangen til forebyggende inndragning kan ikke anses å være et tilstrekkelig tiltak for å etablere et effektivt personvern for en voksen fornærmet i slik sammenheng. Barnets rett til personvern er bedre ivaretatt fordi det gjelder et absolutt befatningsforbud mot overgrepsbilder.

IV Data som strafferettslig objekt

6 Forming av temaet

6.1 Problemstilling

I det foregående har jeg gjennomgått reglene for inndragning av data tatt i beslag, og avsluttet med å antyde muligheten for å inndra dublettene med henvisning til én felles identitet. Denne drøftelsen følger jeg opp i del V. Men selve konseptet, dvs. fullbyrdelse av inndragning i nettet rettet mot dubletter med en kjent identitet, synes å avhenge av om data har en selvstendig strafferettslig status som "ting". Jeg kaller det et spørsmål om den strafferettslige konseptualiseringen av data, og dette er temaet for del IV.

Siden strl. 2005 § 69 annet ledd forutsetter at dataene må være "lagret", oppstår det en usikkerhet ved om inndragningsbestemmelsen virkelig anser data for å være et selvstendig objekt, en "ting". Kanskje er bestemmelsen et utslag av læren om det funksjonelle gjenstandsbegrepet, dvs. at data ikke er et selvstendig objekt, men en del av det fysiske lagringsmediet som er "gjenstanden".[242] Når det også tas i betraktning at straffeloven i stedet for å la data omfattes av generelle begreper som "ting" og "gjenstand", bruker forskjellige andre uttrykk, oppstår det en viss usikkerhet med hensyn til hvilken strafferettslige status data egentlig har. Jeg tenker for eksempel på følgende straffebud som alle mener data, men bare sier det direkte i ett tilfelle: Det gjelder strl. 2005 § 69 annet ledd ("elektronisk lagret informasjon"), § 201 ("databasert informasjon"), § 206 ("informasjon") og § 351 annet ledd ("data").[243]

Spørsmålet er hva slags type gode loven regulerer. Dersom data er et objekt i seg selv, hvorfor oppstilles vilkår om at dataene må være lagret, og hvorfor brukes flere forskjellige begreper om data? Hvorfor ikke bare bruke "ting" eller "gjenstand"?

[242] Se om denne læren i kapittel 7.6.3.
[243] Strl. 2005 § 69 er sitert i kapittel 5.3.1. Strl. 2005 § 201 ble sitert i kapittel 1.1 og 5.3.2.1. Strl. 2005 § 206 (fare for driftshindring) lyder: "Med bot eller fengsel inntil 2 år straffes den som ved å overføre, skade, slette, forringe, endre, tilføye eller fjerne *informasjon* uberettiget volder fare for avbrudd eller vesentlig hindring av driften av et datasystem"; strl. 2005 § 351 (skadeverk) lyder: (første ledd) "Med bot eller fengsel inntil 1 år straffes den som skader, ødelegger, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen." (annet ledd) "For skadeverk straffes også den som uberettiget endrer, gjør tilføyelser til, ødelegger, sletter eller skjuler andres *data*" (mine uth.).

Tekniske betingelser bør vektlegges ved fortolkningen av loven, fordi muligheten for å utrette noe overfor data, enten det er en straffbar handling, beslag eller inndragning, krever bruk av dataverktøy. Dersom inndragning skal skje i nettet må man innrette seg under hensyn til at det har en komplisert og dynamisk struktur, med en stadig varierende tjenestesammensetning. Da er det neppe praktikabelt med en tilnærming som kategorisk forutsetter at dataene må være "lagret" på en bestemt bærer.

For automatisert inndragning som er basert på forhåndsidentifikasjon av rettsstridige filer, bør det være irrelevant om inndragningen skjer mens dataene er lagret eller overføres. Filenes innhold er uansett det samme. I tillegg er databehandlingen i "internettskyen" i ferd med å bryte ned skillet mellom data som er lagret og data som overføres. Data som fra et brukersynspunkt antas å være lagret, kan hyppig flyttes mellom servere, og data under overføring blir lagret et utall steder underveis. Rettshåndhevelsen bør derfor ikke nødvendigvis baseres på kriterier som har med lagring – overføring å gjøre.

De straffeprosessuelle reglene om utlevering av post viser at begrepet "besittelse", som kan synes å være nært beslektet med "lagret", ikke er så lett å anvende i nettet. I den såkalte "epostkjennelsen" (RG 2008 s. 1477) var spørsmålet om epost lagret på siktede konto hos eposttilbyder, skulle utleveres med hjemmel i den alminnelige regelen om utleveringspålegg, jf. strpl. § 210, hvoretter vitneplikt er tilstrekkelig, eller etter regelen om postbeslag, jf. strpl. § 211, som oppstiller strengere vilkår for utlevering. Begge bestemmelser anvender vilkåret "besitter", og lagmannsretten kom til at eposten var i tilbyders besittelse slik strpl. § 210 bruker ordet, men ikke slik strpl. § 211 bruker det. Utlevering skulle følgelig skje med hjemmel i strpl. § 210.

Retten gjorde det klart at "besitter" *ikke* er ensbetydende med "lagret", og uttalte blant annet at tilbyderen "må også *under forsendelsen* anses å ha besittelsen av sendingen" (min uth.). Etter analogi med brevpost ble eposten ikke ansett for å være i tilbyderens besittelse etter at den var kommet frem til epostkontoen, i hvert fall ikke i den forstand strpl. § 211 bruker besittelsesbegrepet.

Retten ga altså uttrykk for et dynamisk besittelsesbegrep på tvers av sondringen lagres – overføres. Men retten kunne like gjerne tatt utgangspunkt i at "besitter" i strpl. § 211 refererer seg til *faktisk rådighet* over eposten. Da skulle strpl. § 211 vært anvendt, fordi eposttilbyderen

hadde mulighet til å foreta utleveringen selv om den var kommet frem til kontoen, siden eposten fysisk var lagret på serveren. I RG 1998 s. 1155 ga retten strpl. § 211 et noe videre anvendelsesområde i forhold til epost som er lagret, for da ble eposten ansett for å være i tilbyders besittelse inntil den faktisk var "hentet opp og fjernet" av mottakeren.

Uavhengig av avgjørelsene kan man si at det ikke ville vært noe i veien for å anse eposten for å være *både* i siktedes *og* i tilbyderens besittelse etter at den er kommet inn til epostkontoen. At posten *enten* er i postverkets *eller* mottakeren besittelse er et konsept utviklet for fysiske goder, mens for data kan man gjerne si at den som har faktisk mulighet til råde over dataene har dem i sin besittelse. I "internettskyen" kan det fort være tale om flere aktører på samme tid, både avsender, mottaker og tilbyder av overførings- og lagringstjenester. I så fall burde utleveringshjemmelen være strpl. 211, fordi det tar hensyn til det spesielle vernet om fortrolig kommunikasjon som den bestemmelsen er ment å sikre.[244]

For inndragning i nettet synes sondringen offentlig – privat å være mer sentral enn sondringen lagres – overføres, for så vidt gjelder den rettslige statusen til konkrete datafiler. En grunn er at materielle forbud mot bestemte ytringer gjerne er av relativ karakter, dvs. at den offentlige fremsettelsen er gjort straffbar, men ikke det å fremsette den samme ytringen privat. Det kategoriske totalforbudet mot overgrepsbilder representerer i så måte et unntak. Og prosessuelt går det et viktig skille mellom offentlige og private områder. Mens offentlige områder kan utsettes for rettshåndhevende tiltak av generell karakter, må inngrep i den private sfære ha hjemmel i lov og skje på grunnlag av konkret mistanke.

Dersom data virkelig anses som et selvstendig objekt byr loven slik jeg ser det, på følgende tolkingsmulighet: Utgangspunktet er at "lagret" i strl. 2005 § 69 annet ledd omfatter de data som er tatt i beslag. Men den automatiserte inndragningen av dublettene må skje med referanse til filenes dataidentitet, og da er spørsmålet om *dataidentiteten* er "ting", noe som løses ved en fortolkning av strl. 2005 § 69 *første* ledd. Dette spørsmålet behandler jeg i del V. I så fall er det av underordnet betydning rettslig sett om datafilene (dublettene) er lagret eller er under overføring når de blokkeres ved den automatiserte inndragningen. Siden datafilene prinsipielt bør ses uavhengig av det fysiske lagringsmediet, bør også datafilen som objekt

[244] Bestemmelsen er foreslått opphevet av Metodekontrollutvalget, jf. NOU 2009: 15 kapittel 19 s. 213-215. Domstolens sentrale rolle som kontrollør er ikke hensiktsmessig på grunn av det store omfanget epost som må kontrolleres.

betraktet kunne henføres direkte under ”ting” etter inndragningsbestemmelsens første ledd. Dermed er ”lagret” i annet ledd en veiledende presisering for data tatt i beslag, og begrenser ikke adgangen til å foreta automatisert inndragning, for eksempel av dubletter under overføring.

6.2 Eiendomsrettens betydning for inndragning av data

Inndragning er et inngrep i eiendomsretten. Tingen som inndras må følgelig være undergitt eiendomsrett.[245] Det gjenspeiles også i at inndragningsobjektet gjerne omtales som ”formuesgjenstand” og at fullbyrding skjer ved salg til fordel for statskassen, jf. strl. 2005 § 75. Prinsipielt gjelder dette også ting uten legal verdi, som overgrepsbilder, jf. drøftelsen i kapittel 5.8.

”Ting” i inndragningsreglene har derfor en parallell i begrepet ”gjenstand” som brukes i straffebud til vern om eiendomsretten, nemlig bestemmelsene om tyveri, underslag, ulovlig bruk og skadeverk. Men da byr rettstilstanden på nok et usikkerhetsmoment. På den ene siden sier loven at ”som ting regnes også … elektronisk lagret informasjon”, jf. strl. 2005 § 69 annet ledd. På den andre siden sies det i forarbeidene i tilknytning til gjenstandsbegrepet i straffeloven 2005, at

> ”Informasjon i datasystemer mv. skal fortsatt ikke regnes som gjenstand.”[246]

Formuleringen ligger nokså nær den som står i strl. 2005 § 69 annet ledd, som nettopp klargjør at data er ”ting”. Data er ifølge disse rettskildene henholdsvis en formuesgjenstand som kan inndras, men ikke en formuesgjenstand som kan utsettes for skadeverk (smlg. inndragning ved sletting). Det gir grunn til å avklare om data er et selvstendig strafferettslig objekt eller ei.

Det kan være at rettssetningen om at *informasjon* ikke kan eies, har influert på uttalelsen om gjenstandsbegrepet.[247] I kommentaren til strl. 1902 § 6 som presiserer gjenstandsbegrepet,

[245] Ot.prp. nr. 90 (2003-2004) kapittel 26 s. 341. Se også *Andenæs/Matningsdal/Rieber-Mohn* (2004) s. 512 flg., *Eskeland* (2006) s. 390-393, *Hov* (2007) s. 22 og Bjerke (2001) s. 55.
[246] Ot.prp. nr. 90 (2003-2004) kapittel 12.2.4 s. 165 (gjenstand). Forarbeidene til straffeloven 2005 behandler begrepene ”gjenstand” og ”ting” i Ot.prp. nr. 90 (2003-2004). I kapittel 12.2.4 sies det at begrepet ”gjenstand” ikke omfatter informasjon i datasystemer, jf. sitatet over, og i kapittel 26.4.3, at elektronisk lagret informasjon er ”ting” som kan inndras (s. 351). Det er jo også kommet til uttrykk i loven, jf. strl. 2005 § 69 annet ledd. Forarbeidene kommenterer ikke forholdet mellom de to standpunktene.

opplyses det således at ordet "gjenstand" ikke omfatter "opplysninger i en datamaskin".[248] Det er i så fall ikke til hinder for at *data* kan være gjenstand for eiendomsrett, i hvert fall må det legges til grunn som et utgangspunkt. Det synes således å være et spørsmål om strafferettslige resonnementer har holdt data og informasjon fra hverandre, når "informasjon" er brukt på en måte som også kan dekke data, jf. uttalelsen i forarbeidene til straffeloven 2005 (*"informasjon* i datasystemer skal fortsatt ikke regnes som gjenstand" (min uth.)).

Reglene om beslag og inndragning, som henholdsvis er midlertidig og permanent inngrep i eiendomsretten, speiler de nevnte straffebud som er satt *til vern* om eiendomsretten.[249] Siden eiendomsretten er den sentrale underliggende verdi eller rettighet, tilsier harmoni- og konsekvenshensyn at alle bestemmelsene gjelder samme type objekt. Det må være et objekt som kan eies. Begrepene brukes ikke andre steder i straffeloven enn i bestemmelser som berører eiendomsretten.[250] Jeg ser da bort fra tilfeller med det språklige uttrykket "å ha vært gjenstand for noe", som forekommer både i og utenfor inndragningsbestemmelsene.[251] Hvorfor loven bruker "ting" når objektet er utsatt for inngrep (beslag, inndragning) og "gjenstand" når det nyter strafferettslig vern, har jeg ikke greid å finne ut. Ut fra en alminnelig språklig forståelse betyr ordene det samme og det synes som man kunne greid seg med ett av dem.[252] For øvrig brukes "gjenstand" også i en av inndragningsbestemmelsene, se strl. 2005 § 71 fjerde ledd, som lyder:

---

[247] Se kapittel 7.3.

[248] *Matningsdal* (2003) s. 31.

[249] Dette følger nå tydelig av overskriften til straffeloven 2005 kapittel 27, som gjelder "Vinningslovbrudd og liknende *krenkelser av eiendomsretten"* (min uth.). Kapitlet inneholder blant annet straffebudene mot tyveri (§ 321), underslag (324) og ulovlig bruk (§ 343). Bestemmelsen mot skadeverk, jf. § 351, står i kapittel 28 om "Skadeverk og fremkalling av fare for allmennheten". Men bestemmelsen inneholder vilkåret "tilhører en annen", slik som de nevnte vinningsforbrytelsene. Av forarbeidene fremgår det at straffebudene i kapittel 28 "ivaretar til dels ulike interesser", og at hovedformålet med de alminnelige skadeverksbestemmelsene er "å verne den private økonomiske og ideelle interesse i at gjenstander ikke utsettes for skade fra utenforstående." Straffansvaret er derfor knyttet til at gjenstanden tilhører en annen. (Ot.prp. nr. 22 (2008-2009) kapittel 9.1. s 302).

[250] "Ting" brukes også i straffeloven 2005 kapittel 15 om foreldelse mv., jf. strl. 2005 § 100 om bortfall av straff og inndragningsansvar ved den skyldiges eller ansvarliges død. Også her brukes det i forbindelse med (bortfall av) inndragning.

[251] Se strl. 2005 § 69 første ledd bokstav b og § 70 første punktum, og i strl. 2005 § 106 bokstav d (krigsforbrytelse). Når loven for eksempel har bestemmelser som setter straff for den som "borttar … en gjenstand fra et lik", og om minstestraff for voldtekt ved "innføring av gjenstand i skjede- eller endetarmsåpning", kunne det like gjerne stått "ting" i stedet, se strl. 2005 § 195 annet ledd (likskjending) og § 292 bokstav c (voldtekt, minstestraff). Det er dessuten helt klart at de nevnte "gjenstandene" er "ting" som kan inndras, jf. strl. 2005 § 69 første ledd, fordi de har vært "gjenstand for" (sic) en straffbar handling (likskjending), og "brukt ved en straffbar handling" (voldtekt).

[252] Den alminnelige språklige forståelse er utgangspunktet for fortolkningen. Se *Eckhoff* (2001) kapittel 2 om lovtekstene, s. 39. Se også for eksempel *Andenæs/Matningsdal/Rieber-Mohn* (2004) s. 112 om tolking av straffelover, hvor det står at utgangspunktet for tolkingen "er den naturlige forståelse av bestemmelsene etter vanlig språkbruk."

> ”Inndragning etter § 70 foretas overfor den som besitter eller eier *gjenstanden*” (min uth.).

Av disse grunner skulle man som utgangspunkt tro at de to begrepene har likt innhold.

Verken ”ting” eller ”gjenstand” er legaldefinert, så lovgiver har ikke løst de fortolkningsmessige spørsmålene på den måten.[253] Men siden objektet uansett må tilfredsstille kravet til eiendomsrett, er det et sentralt spørsmål *om data kan eies*.

Jeg har derfor valgt å gi meg i kast med en analyse av de strafferettslige begrepene ”gjenstand” og ”ting” (”gjenstand/ting”). Siden formålet er å komme frem til en avklaring med hensyn til om begrepene omfatter *data* som selvstendig objekt, oppstår det også spørsmål om betydningen av hensynet til teknologinøytralitet. Hensynet har utspring i problemstillinger knyttet til digitalisering og konvergens i ekomsektoren, og er relevant for den rettslige tilnærmingen til data. ”Teknologinøytralitet” som uttrykk synes nettopp å tilsi at hvorvidt grunnkomponenten er *bits* eller *atomer* ikke er rettslig relevant, noe som i så fall leder til at data kan være ”gjenstand/ting” selvstendig sett på linje med fysiske objekter. Men for å avklare om rettstilstanden er slik, er det behov for å ta rede på hva hensynet til teknologinøytralitet mer konkret går ut på. Jeg foretar denne kartleggingen først, i forlengelsen av en beskrivelse av rettskildesituasjonen for de rettsspørsmål som skal behandles (kapittel 6.3). Jeg er ikke kjent med noen annen fremstilling om teknologinøytralitet i strafferetten, så jeg har ikke kunnet unngå denne ekskursen ved å vise til et annet arbeid.

Deretter gjennomgår jeg begrepene ”gjenstand/ting” (kapittel 7-8). I kapittel 9 analyserer jeg data som objekt ved overtredelse av strl. 2005 §§ 201 og 311. I kapittel 10 foretar jeg en oppsummering.

[253] En legaldefinisjon skal normalt legges til grunn overalt hvor begrepet forekommer i den aktuelle lov, *Eckhoff* (2001) s. 337.

6.3 Rettskildesituasjonen og hensynet til teknologinøytralitet

6.3.1 Tolkingsproblem og rettskildesituasjon

Fortolkningen må forholde seg til at det er tale om å henføre et nytt fenomen (data) under eldre regler, hvor deler av forarbeider og teori stammer fra tidlig på 1900-tallet.[254] Flere av rettskildene kan derfor med god margin henføres til den såkalte "pre internett æraen". Straffeloven 2005 representerer hovedsakelig bare en videreføring av rettstilstanden i straffeloven 1902 på de områdene som avhandlingen behandler, så eldre rettskilder er fremdeles relevante. I utredningen om datakriminalitet i 1985 anbefalte Straffelovrådet å anvende de eldre regler på data, med supplering av noen få spesialregler, og dette ble fulgt opp av lovgiver.[255] I straffeloven 2005 er tilnærmingen langt på vei den samme. Selv om lovgiver har gitt spesialregler for "Vern om informasjon og informasjonsutveksling", jf. strl. 2005 kapittel 21, har man også søkt å anvende de tradisjonelle bestemmelsene der det har vært mulig.[256]

Problemstillingen med anvendelse av eldre regler på "gjerningstyper som blir muliggjort ved ny teknikk", ble kommentert av Straffelovrådet i 1985.[257] Utgangspunktet er at en regel kan dekke nye forhold; det er nettopp kjennetegnet ved en regel, den virker generelt over tid. Det problematiske er at man ikke kan være sikker på om eldre regler dekker nye forhold på en fullstendig og adekvat måte.[258] På strafferettens område settes problemet på spissen på grunn av det strenge klarhetskravet, jf. legalitetsprinsippets vilkår om klar lovhjemmel for idømmelse av straff og strafferettslig reaksjon.[259]

På den annen side er både "ting" og "gjenstand" tidløse begreper og det kommer ikke mye ut av en ren ordfortolkning. Det historiske utgangspunktet er at de omfatter fysiske objekter,

[254] Med "nytt" fenomen tenker jeg på data i henhold til avhandlingens begrepsbruk, som er forklart i kapittel 2 og beskrevet som faktisk fenomen i kapittel 3. Som generelt begrep er jo data svært gammelt, jf. det latinske utspringet *datum*, se kapittel 2.3.2.
[255] NOU 1985: 31 s. 28 flg. De bestemmelser som ble innført spesielt med tanke på data, var strl. 1902 § 145 annet ledd (uberettiget tilgang), § 151b (sabotasje), § 261 (ulovlig bruk og forføyning), § 270 nr. 2 (databedrageri). Se *Sunde* (2006) s. 91-96.
[256] Se Ot.prp. nr. 22 (2008-2009) s. 20.
[257] NOU 1985:31 kapittel 4.1 s. 28.
[258] Straffelovrådet sa således i utredningen om datakriminalitet at "det kan bero på tilfeldigheter om de gamle bestemmelser passer på nye forhold". Men uttalelsen viser at muligheten for at de gjør det, ble holdt åpen, se NOU 1985: 31 s. 28.
[259] Se kapittel 5.2.2.

men samfunns- og teknologiutviklingen har ledet til at de omfatter mer enn som så. Både elektrisk strøm og enkle fordringer er således omfattet.[260]

"Gjenstand/ting" kan karakteriseres som "elastiske" begreper, dvs. begreper som tillater en gradvis utvikling i rettstilstanden.[261] Med *Eckhoff* kan man si at "foranderligheten [er] på en måte bygget inn i selve lovteksten."[262] Utviklingen er tilrettelagt av *lovgiver* ved bruk av de generelle begrepene, og innføring av presiserende bestemmelser i strl. 2005 §§ 12 og 69 annet ledd, som bidrar til å utfylle innholdet i dem. Det er ikke meningen at bestemmelsene skal leses antitetisk.[263] Lovgiver har dermed lagt til rette for en utvikling skapt av *domstolene*, som for eksempel har kommet til at "gjenstand" omfatter enkle fordringer. Slike fordringer er følgelig vernet mot underslag (som "løsøregjenstand", jf. strl. 1902 § 255 første alternativ).[264] Det viser at begrepene er elastiske og preges av samfunns- og teknologiutviklingen.

Jeg tror det interessante problemet for fortolkningen er å identifisere *de kriterier* som "gjenstand/ting" hviler på. Det må antas at det hefter fellestrekk ved fysiske objekter, elektrisitet og enkle fordringer som begrunner hvorfor de omfattes av de samme begrepene. Disse kriteriene må sies å representere lovgiverviljen, eller lovens mening, med begrepene "gjenstand/ting".[265] Som elastiske begreper ligger det i sakens natur at de kan omfatte goder som lovgiver ikke hadde foranledning til å tenke på da loven ble gitt. Det innebærer også at et gode som oppfyller kriteriene omfattes av loven, fordi det kan henføres direkte under ordlyden ("gjenstand/ting").

Siden hovedspørsmålet gjelder om data omfattes av begrepene, er det som nevnt nærliggende å trekke inn hensynet *teknologinøytralitet.* For å vite om og hvordan det har betydning på strafferettens område, herunder det foreliggende tolkningsspørsmålet, er det behov for ha mer kunnskap om hva det går ut på, noe jeg skal redegjøre for i det følgende.

[260] Elektrisk strøm omfattes bare av begrepet "gjenstand", men det er nok fordi elektrisitet løpende forbrukes og derfor etter sin art ikke kan inndras ("ting").
[261] Se *Eckhoff* (2001) s. 187 flg. som bruker "elastisk" begrep for eksempel om moralske vurderinger som "ærbarhet" og "god forretningsskikk", og om et verdinøytralt ord som "skip", som for så vidt kan sammenlignes med "gjenstand/ting". De såkalte "passbåtdommene" illustrerer godt hvor elastisk begrepet "skip" er.
[262] *Eckhoff* (2001) s. 187.
[263] Se kapittel 7.1.
[264] Se kapittel 7.6.4.
[265] Se *Eckhoff* (2001) s. 148-151 om det subjektive og det objektive fortolkningsprinsipp. I dette tilfellet oppstår det ikke noe spenn i valget mellom lovgivers eller lovens mening med begrepene. På grunn av begrepenes tidløse karakter har det nok vært lovgivers mening at de skal fastlegges i lys av samfunnsutviklingen.

6.3.2 Hensynets utspring og anvendelsesområde

6.3.2.1 Ekomsektoren: Digitalisering og konvergens

Teknologinøytralitet som et eksplisitt formulert prinsipp, har utspring i reguleringen av ekomsektoren. Men prinsippet – eller *hensynet* som jeg velger å kalle det – har også fått betydning på andre områder, blant annet innen opphavsretten, strafferetten og straffeprosessen. I utgangspunktet er teknologinøytralitet et direktiv til lovgiver, men det står også på egne ben som et reelt hensyn. Da betegner det en vurdering av om et tilfelle som man vurderer å henføre under regelen, *er funksjonelt likeverdig* med et tilfelle som klart omfattes av regelen.[266] Sentralt blir derfor spørsmålet om data fungerer likeverdig med andre objekter innenfor den aktuelle regelen.

Teknologinøytralitet vokste frem på 1990-tallet som et reguleringsprinsipp for ekomsektoren innen det europeiske indre markedet, på linje med prinsippene om minimumsregulering og ikke-diskriminering av markedsaktører.[267] Teknologinøytralitet skal bidra til å integrere de historisk atskilte områdene tele, data og kringkasting i ett felles område (ekomsektoren). Foranledningen er endringene forårsaket av *digitalisering og konvergens*, som betyr at datateknologien overtar som lagrings- og overføringsteknologi, dvs. at innhold (tekst, lyd, bilde) behandles og overføres i sifferformater.[268] Teknologien behandler innhold som tall, og er "blind" for hva innholdet betyr for mottakeren, smlg. begrepet "elektronisk kommunikasjon" i ekomloven § 1-5 nr. 1 som gjelder dataene, ikke innholdet.[269]

Konvergens betyr "å løpe sammen, nærme seg hverandre" og betegner i denne sammenheng at de teknologibetingede skillene mellom tele, data og kringkasting er i ferd med å forsvinne fordi alt baseres på data.[270] Høyesterett har karakterisert fenomenet slik:

[266] *Eckhoff* (2001) om reelle hensyn som rettskildefaktor på s. 371 flg.; *Mestad* (2009) om reelle hensyn som "[v]urderinger under rettsanvendelsen" s. 27.
[267] Se NOU 1999: 26 kapittel 4.1.1.4 s. 72. "Reguleringer bør utvikles i retning av teknologinøytralitet". Ikke-diskriminering av markedsaktører er noe annet enn det fellesskapsrettslige ikke-diskrimineringsprinsippet med hensyn til nasjonalitet, jf. *EØS-rett* (2004) om EFT art. 12 på s. 67. Ikke-diskriminering av markedsaktører gjelder mellom store og små, private og statlige aktører, og har med liberaliseringen og privatiseringen av ekomsektoren å gjøre.
[268] Se forklaringen om *bits* i kapittel 3.3.1. Se også *Seipel* (2004) s. 49 som skriver at "termen *digitalisering* syftar på att alla slag av information (text, bild, ljud) återges i *sifferform* vid behandling i datorer och vid överföring via telekommunikationer. Ettor och nollor bär altså informationen vare sig det är fråga om telefonsamtal, distribution av musikk, handel med värdepapper, filmvisning, virtuella bibliotek, konstruktion av ett hus eller någonting annat. Digitalskriften är långt mer kraftfull än den traditionella bokstavskriften."
[269] Se kapittel 2.3.4.
[270] Den språklig betydningen er forklart i Kunnskapsforlagets tjeneste ordnett.no, under "Fremmedord".

> ”Særleg det siste tiåret har det skjedd ei nedbryting av skiljet mellom sektorane kringkasting, tele og data, jf. Konvergensutvalget i NOU 1999: 26, sjå til dømes punkt 1.1.1. Det er illustrerande for farten på utviklinga dei seinare åra at ved lova om elektronisk kommunikasjon av 4. juli 2003 nr. 83 vart den relativt nye lova om telekommunikasjon av 23. juni 1995 oppheva. I denne perioden har utviklinga av internettet stått sentralt, og i tilknyting til det også ei aukande samansmelting ikkje minst av telefoni og data.”[271]

At digitalisering og konvergens hører nært sammen lar seg illustrere med noen eksempler: Taletelefoni som utføres digitalt innebærer at lyden bæres av datapakker og ikke av analoge signaler som tidligere. Lyden er digitalisert og overføres elektronisk, tele og data konvergerer. Et annet eksempel gjelder følgen av at innholdets karakter er uten betydning for dataoverføringen. Dermed forsvinner den tekniske begrunnelsen for å operere med en telesektor som er spesialisert mot overføring av lyd, separat fra datasektoren.

Utviklingen leder til at man kan tilby og selv få tilgang til, innhold uavhengig av typen elektronisk utstyr. For eksempel er TV-sendinger en fra punkt til multipunkt-tjeneste, og basert på prinsipp om samtidighet, dvs. at sendingen går samtidig til alle seerne.[272] Men utviklingen har medført at programmer legges tilgjengelige på internett, og kan utnyttes av brukerne som kan koble seg opp både via datamaskin og mobiltelefon. Teknisk sett er det ikke lenger en betingelse for å se ”TV-programmer” at man har et TV-apparat. Også dette er konvergens. En annen sak er at et rettslig krav om samtidighet kan sette begrensninger for hva slags sendinger man mener at hører til kringkastingssektoren.[273]

---

[271] Rt. 2006 s. 813 avsnitt 26 (i en sak om eiendomsskatt). Konvergens er ellers ikke noe vanlig uttykk i rettsspråket, ved søk i Lovdata har jeg bare funnet det i to høyesterettsavgjørelser. I det ene tilfellet gjaldt det beskrivelse av kuttskader i en sak om legemsbeskadigelse, hvor ansiktet til fornærmede var skadet med kniv både på venstre og høyre side. Skaden ble blant annet beskrevet slik: ”På høyre side er det to tilsvarende kutt som konvergerer mot høyre munnvik…” (Rt. 1992 s. 1219). I det andre tilfellet siteres det fra den danske oversettelsen av EUs femte motorvognforsikringsdirektiv, som har til formål ”… «at afhjælpe mangler og skabe klarhed om visse definitioner i direktiverne og dermed sikre øget konvergens i medlemsstaternes fortolkning og anvendelse heraf».” (Rt. 2005 s. 1365 (Finanger II)).

[272] Kringkastingsloven § 1-1 definerer ”kringkasting” som ”utsending av tale, musikk, bilder og likende med radiobølger eller over tråd, ment eller egnet til å mottas direkte og *samtidig* av allmennheten.” (min uth.).

[273] Konvergensutvalget (1999) identifiserte 4 forskjellige former for konvergens: Tjeneste-, nettverks-, terminal- og markedskonvergens. Se NOU 1999: 26 kapittel 3, oppsummert på s. 11. Se også *Seipel* (2004) s. 50-51. Nettverks- og terminalkonvergens kalles iblant plattformkonvergens, se for eksempel Datakrimutvalget som kommer inn på betydningen av EUs TV direktiv (direktiv 89/552/EØF, endret ved direktiv 97/36/EF) ved en diskusjon av jurisdiksjon på internett. I lys av at direktivet er foreslått endret (jf. forslag 2005/0260 (COD)), skriver utvalget: ”Konvergens mellom ulik teknologi og medier, gjør direktivet også relevant for andre innholdstjenester enn tv-tjenester, blant annet for internettjenester. EU-kommisjonen ønsker ikke at reguleringen skal forskjellsbehandle ulike *teknologiske plattformer* som leverer lignende innhold. Endringsforslaget innebærer derfor bl.a. en utvidelse av virkeområdet til alle typer audiovisuelle medietjenester uansett hvilken *plattform* de leveres fra.” (mine uth.), se NOU 2007: 2 kapittel 8.5 på s. 144. Markedskonvergens er et økonomisk

De fellesskapsrettslige prinsippene ble nedfelt i en rekke rettsakter som ble gjennomført i norsk rett ved ekomloven i 2003.[274] Forarbeidene gir uttrykk for at teknologinøytralitet har stor betydning, og sier blant annet at ekomloven:

> "viderefører et reguleringsregime som er mest mulig teknologinøytralt. Dette vil si at reguleringen ikke skal favorisere én teknologi fremfor en annen. Reguleringen skal ikke legge opp til/favorisere bruk av bestemte teknologier, men overlate teknologivalg til markedet."[275]

Konvergens er en vedvarende utfordring. I "IKT-meldingen" fra 2007 opplyses det at den politiske målsettingen for ekomsektoren etablert på 1990-tallet, stadig er fastholdt, og at vi

> "… blir stadig stilte overfor nye regulatoriske utfordringar på grunn av den teknologiske utviklinga og utbreiinga av nye tenester. Det blir jamleg prøvd å handtere utfordringane i norsk lovgiving."[276]

Det slås fast at myndighetene til enhver tid må bidra med regulatoriske rammevilkår som legger til rette for en markedsstyrt utvikling uten diskriminering av teknologier og tjenester.[277]

6.3.2.2 Strafferettslig og prosessuelt

I *straffeprosessen* kan behovet for teknologinøytrale regler spores i lovforarbeider fra 1990-tallet som gjaldt endringer i reglene om bruk av tvangsmidler m.v.. Som følge av Sikkerhets- og Metodeutvalgenes utredninger, ble det i 1999 gjort lovendringer som vesentlig gjaldt tvangsmiddelbruk.[278] Med hensyn til kapitlet om telefonkontroll, ble overskriften endret til "Avlytting og annen kontroll av kommunikasjonsanlegg (kommunikasjonskontroll)", jf. strpl. kapittel 16a. I motivene er det presisert at

---

utviklingstrekk, som innebærer at de ulike bransjene flyter sammen, på grunn av de nevnte tre tekniske konvergensformene. Eksempler er at forlag engasjerer seg i online-levering av litteratur; koblingen mellom underholdnings- og internettbransjen m.v.

[274] Den fellesskapsrettslige "reguleringspakke på området for elektronisk kommunikasjon" består av rammedirektivet 2002/21/EF, tillatelsesdirektivet 2002/20/EF, tilgangsdirektivet 2002/19/EF, USO-direktivet 2002/22/EF, frekvensvedtaket 2002/676/EF og kommunikasjonsverndirektivet 2002/58/EF. Se Innst.S. nr. 223 (2003-2004) s. 2: "Bakgrunn/Beslutninger i EØS-komiteen".

[275] Ot.prp. nr. 58 (2002-2003) kapittel 4.3.

[276] St.meld. nr. 17 (2006-2007) kapittel 6.3.8 s. 102.

[277] St.meld. nr. 17 (2006-2007) kapittel 6.3.8 s. 102.

[278] Endringslov nr. 82/1999 på bakgrunn av utredningene NOU 1993: 3 Strafferettslige regler i terroristbekjempelsen (Sikkerhetsutvalget) og NOU 1997: 15 Etterforskingsmetoder for bekjempelse av kriminalitet (Metodeutvalget). Lovproposisjonen er Ot.prp. nr. 64 (1998-1999).

> ”[t]empoet i den teknologiske utviklingen gjør det sannsynlig at [avlytting som metode] raskt vil utvikles ytterligere. I tillegg vil det antagelig også dukke opp nye, hittil ukjente metoder for avlytting. Avlyttingsadgangen er derfor gjort *uavhengig av hvilken teknologi som benyttes*. Det avgjørende er om avlyttingen retter seg mot *kommunikasjon.*” (min uth.).[279]

Sitatet gir uttrykk for behovet for teknologinøytrale regler, selv om man den gang ennå ikke benyttet betegnelsen ”teknologinøytralitet”. Men i 2005 brukes ”teknologinøytralitet” i straffeprosessen. Det kommer til syne i forarbeidene til endringen i strpl. § 216b annet ledd bokstav c, som gir politiet hjemmel til å bruke teknisk utstyr for å identifisere telefoner, datamaskiner og andre anlegg for elektronisk kommunikasjon.[280] I den forbindelse påpekte flere høringsinstanser at ”regelen bør gjøres så teknologinøytral som mulig”, og departementet sa seg enig i dette.[281]

Teknologinøytralitet ble her brukt i samme *snevre forstand* som i ekomsektoren, dvs. at det begrunnet straffeprosessuell likestilling av forskjellige kommunikasjonsteknologier. Straffeprosessloven var også nylig blitt endret for å innføre ekomlovens begrep ”elektronisk kommunikasjon” og derivatformer, blant annet ”elektronisk kommunikasjonstjeneste”, se strpl. §§ 118, 211 og 216a.[282]

Med forbehold for datakriminalitet har ikke teknologinøytralitet vært et uttalt hensyn innen *strafferetten*, før man kommer til de innledende overveielsene i siste delproposisjon til straffeloven 2005. Men da går lovgiver inn for teknologinøytralitet *i mye videre forstand* enn for ekomsektoren og i straffeprosessloven. Før disse bemerkningene i en sen fase i lovgivningsarbeidet, er hensynet bare å spore i forbindelse med datakriminalitet. Konvergens i betydningen *mediekonvergens* ble imidlertid nevnt i delutredning VII, ved omtalen av redaktøransvar m.v., i forbindelse med plassering av ansvar for ytringer på nett.[283]

---

[279] Ot.prp. nr. 64 (1998-1999) s. 156. Om endringen i overskriften til strpl. kap. 16a, se proposisjonen s. 168.
[280] Endringslov nr. 87/2005.
[281] Se Ot.prp. nr. 60 (2004-2005) kapittel 8.5.1 s. 108 flg., om høringsinstansenes ønske om teknologinøytral regel; og i de spesielle motivene står det: ”I dag er problemstillingen særlig aktuell i forhold til GSM […] Regelen er imidlertid gitt en teknologinøytral utforming, og hjemler også tiltak med sikte på å identifisere andre kommunikasjonsanlegg” (kapittel 13.1). Se Ot.prp. nr. 72 (2006-2007) kapittel 6.6 s. 31 om teknologinøytralitet i ekomloven.
[282] Ekomloven ble innført ved lov 4. juli 2003 nr. 83. Ved samme lov ble det gjort endringer i straffeprosessloven slik at strpl. § 118 bruker ”tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, elektronisk kommunikasjonsinstallatør”; strpl. § 211 ”sending som besittes av […] en tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste”; strpl. § 216a tredje ledd ”anlegg for elektronisk kommunikasjon”.
[283] NOU 2002: 4 kapittel 9.7.2. til punkt § 21-7. Det er vist til Konvergensutvalget og Ytringsfrihetskommisjonens betraktninger om teknologiutviklingens betydning for ansvarsbestemmelsene.

I Datakrimutvalgets første utredning fastslås det at begrepet "«computer system» er ment å være teknologinøytralt".[284] Det vises til at det er i samsvar med begrepsbruken i ekomsektoren.[285] Utvalget påpeker også behovet for en

> "oppdatering av begrepsbruken i straffelovgivningen, blant annet på bakgrunn av den tekniske utviklingen".[286]

Legaldefinisjonen av "informasjonsbærer" i strl. 2005 § 76, er en respons på behovet for nye begreper. Bestemmelsen kom uavhengig av Datakrimutvalgets uttalelse fordi strl. 1902 § 38 helt tydelig var utdatert. Den gjelder "trykt skrift", jf. bestemmelsens første ledd, og utstyr brukt til gammeldags grafisk produksjon av bøker, jf. "plater og former" i bestemmelsens tredje ledd.[287] Legaldefinisjonen av "informasjonsbærer" er teknologinøytral i meget vid betydning fordi den omfatter *ethvert medium, fysiske og data*, bare det bærer et meningsinnhold.[288]

I sin andre delutredning la Datakrimutvalget frem forslag til straffebud om datakriminalitet.[289] Utredningen ligger til grunn for departementets videre arbeid med kapittel 21 "Vern av informasjon og informasjonsutveksling" i straffeloven 2005.[290] Utvalget gikk inn for "prinsipper om teknologi- og innholdsnøytralitet", og uttalte at

> "Spørsmål om hva slags type «IKT-system» det er tale om og hva slags innhold dataene har, er ikke relevante for reglenes anvendelsesområde. Straffebudene omfatter «IKT-systemer», uansett om teknologien gjelder tele-, IT- og media (herunder kringkasting)."[291]

Uttalelsen viser at teknologinøytralitet ble brukt på samme måte som i ekomsektoren, noe som betyr at hensynet *bare gjelder fenomener innen den elektroniske konteksten*. Dette er

[284] NOU 2003: 27 kapittel 1.4 s. 10.
[285] NOU 2003: 27 s. 10. Utvalget skriver at " [E]n slik forståelse er i tilfelle i tråd med forståelsen nasjonalt innenfor området for elektronisk kommunikasjon slik den fremstilles i Ot.prp. nr. 58 (2002-2003) Om lov om elektronisk kommunikasjon. Utvalget finner det hensiktsmessig å legge til grunn en teknologinøytral forståelse av begrepet «computer system» og bruker i det følgende det norske begrepet «datasystem»."
[286] NOU 2003: 27 kapittel 1.4 s. 12.
[287] *Bing* (2008) kapittel 5.2 s. 121-131 om de problemer vilkåret "trykt skrift" avstedkommer for redaktøransvaret på nett.
[288] Se kapittel 5.4.1.
[289] NOU 2007: 2 kapittel 11 s. 175.
[290] Ot.prp. nr. 22 (2008-2009) kapittel 2 s. 17 flg.
[291] NOU 2007: 2 kapittel 5.2.1 s. 59 om utvalgets forståelse av teknologinøytralitet, og s. 61 om at forståelsen er i samsvar med datakrimkonvensjonen begrepsbruk.

teknologinøytralitet i *snever* forstand. Anskaffelse av skadelig dataprogram kan tjene som eksempel på hva en slik forståelse av teknologinøytralitet innebærer. Det tilsier at anskaffelse bør være straffbart både når det skjer via datamaskinen (data) og ved en multimediamelding på mobiltelefonen (tele). Hva slags overføringstjeneste som benyttes bør være uvesentlig, forutsatt at den hører til ekomsektoren.[292] Men hensynet i snever forstand strekker ikke til for å straffe anskaffelse av skadelig kildekode *skrevet på et stykke papir*, fordi det er en representasjonsform som faller utenfor ekomsektoren. Dersom lovgiver likevel ønsker å ramme det, må loven utformes teknologinøytralt i bredere forstand enn "ekomversjonen", eller loven må suppleres med regler om de spesielle tilfellene.

Lovgiver valgte på strafferettens område å gå inn for en *vesentlig videre* anvendelse av teknologinøytralitet enn på ekomområdet. Det kommer til uttrykk i siste delproposisjon, i departementets kommentar til Datakrimutvalgets utredning. Departementet slutter seg til prinsippet om teknologinøytralitet, men presiserte det slik:

> "Hvor straffverdig en handling er, beror normalt ikke på hvilket teknologisk utstyr som er benyttet eller hvilken teknologisk innretning som er gjenstand for den straffbare handlingen. Der det har vært mulig, har departementet strukket prinsippet om teknologisk nøytralitet enda lenger, slik at enhver informasjon og informasjonsutveksling – uavhengig av om den er elektronisk eller ikke – i utgangspunktet nyter samme vern. Et eksempel er forslaget til § 202 om identitetskrenkelse. Etter forslaget gjelder bestemmelsen uavhengig av om utnyttelsen av en annens identitet skjer ved hjelp av elektronisk utstyr eller på annen måte, for eksempel i bankskranken eller per brev."[293]

I tråd med dette syn unnlot lovgiver å ta i bruk de legaldefinisjoner som Datakrimutvalget hadde foreslått. Legaldefinisjonene var teknologinøytrale i snever forstand, smlg. ekomsektorens begrepsbruk, og bandt straffebudenes virkeområde til en spesifikt elektronisk kontekst.[294] I lys av uttalelser fra flere høringsinstanser gikk departementet imot forslaget om bruk av legaldefinerte begreper, fordi:

[292] Nøyaktig hva som konvergerer kan det oppstå spørsmål om, og mot eksemplet kan det innvendes at MMS-meldinger også er datateknologi (ikke tele). Uansett er det et eksempel på tjenestekonvergens, nemlig at en datatjeneste leveres integrert i et teleprodukt.
[293] Ot.prp. nr. 22 (2008-2009) s. 21.
[294] Som nevnt i kapittel 2.1, var det tale om legaldefinisjon av fem begreper, jf. lovforslaget § 1 bokstav a – e, dvs. datasystem, data, dataprogram, databasert informasjon og elektronisk kommunikasjonsnett. Se NOU 2007: 2 s. 59.

> ”det er vanskelig å utforme presise og dekkende definisjoner som samtidig er føyelige nok … Departementet mener imidlertid at begrepene ikke bør «låses» i en legaldefinisjon, men i den grad det er nødvendig og mulig forklares i motivene og utvikles i takt med teknologien”.[295]

Det prinsipielle strafferettslige synspunktet er altså en preferanse for *teknologinøytralitet i vid forstand*, noe som for eksempel viser seg i den nettopp nevnte definisjonen av ”informasjonsbærer”. Det fremkommer også i legaldefinisjonen av offentlig handling som består i fremsettelse av et budskap, jf. strl. 2005 § 10 annet ledd annet punktum. Forarbeidene understreker at legaldefinisjonen er medienøytral, og det gjelder i vid forstand. Det betyr at budskap som fremsettes elektronisk er likestilt med budskap som fremsettes fysisk, det avgjørende kriteriet er om budskapet er ”egnet til” å nå et større antall personer, anslagsvis minst 20-30 personer.[296]

Hensynet til teknologinøytralitet virker to veier. *I den ene retningen* innebærer det at straffebud som har et viktig virkeområde i en elektronisk kontekst, også kan anvendes i fysisk kontekst. Strl. 2005 § 311 er et godt eksempel på dette. Selv om det viktigste funksjonsområdet for forbudet mot overgrepsbilder i dag er internett og mobilnettverk, er det klart at også bilder i blader og på DVD-plater omfattes.[297] Lovgivers målsetting om nulltoleranse innebærer at enhver manifestasjon av overgrepsbilder rammes, noe som i realiteten gjør spørsmål om teknologi irrelevant.[298]

For så vidt gjelder forbudet mot skadelig dataprogram, jf. strl. 2005 § 201, ligger det litt annerledes an. For at programmet skal fungere som et direkte anvendelig skadelig verktøy, må det foreligge som data. Da er det et

> ”dataprogram … som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem”, jf. § 201 bokstav b.

[295] Ot.prp. nr. 22 (2008-2009) kapittel 2.3.2 s. 21.
[296] Ot.prp. nr. 90 (2003-2004) kapittel 12.2.2 s. 164. Bestemmelsen er sitert i avhandlingen kapittel 4.2. Se også kapittel 11.2.1.
[297] *Andenæs/Andorsen* (2008) s. 187, sier at ”internett er i dag den enkleste og mest utbredte måten” å anskaffe og planmessig gjøre seg kjent med overgrepsbilder. *Sunde* (2006) kapittel 8.4.1 s. 226-230 redegjør for at det er bred enighet om behovet for nulltoleranse på dette området, og at blant annet ønsket om en holdningsskapende effekt, ligger bak lovens strenge regulering.
[298] Se for eksempel Ot.prp. nr. 28 (1999-2000) (seksuallovbrudd) hvor det i spesialmotivene til strl. 1902 § 204 bokstav d om overgrepsbilder, uttales: ”I utgangspunktet er målsettingen at all befatning med barnepornografi skal være straffbar.”

Ifølge forarbeidene omfattes også skadelig kildekode, og den kan jo etter omstendighetene foreligge i utskrift.[299] For sin mest praktiske overtredelsesmåte, må imidlertid straffebudet anses å være teknologispesifikt, noe som skyldes de elektroniske omgivelser dataprogrammet er beregnet på.

I den andre retningen innebærer teknologinøytralitet at regler som ut fra historiske premisser er utformet primært med tanke på "den fysiske verden", også kan omfatte fenomener i "den virtuelle verden". Spørsmålet om begrepene "gjenstand/ting" kan fortolkes slik at data likestilles med fysiske objekter m.v., hører hjemme i denne kategorien.[300] I språkbruken om teknologinøytralitet er dette formulert i frasen "what holds offline should also hold online", se kapittel 6.4.2.

6.3.3 Teknologinøytralitet som reelt hensyn: Napster-dommen

Teknologinøytralitet kan også være et selvstendig reelt hensyn. Napster-dommen (Rt. 2005 s. 41) viser dette. Saken gjaldt erstatningsansvar for å ha lagt lenker på internett som pekte til nettsteder hvor man kunne laste ned musikkfiler uten rettighetshavernes samtykke. Det oppsto spørsmål om tilgjengeliggjøringsbegrepet i åvl. § 2 omfatter lenker som nevnt. Mer generelt gikk problemet ut på om regler som var blitt til lenge før internett, var anvendelige på handlinger utført ved bruk av ny teknologi (avsn. 49). Forarbeidene var fra 1959-1960, og opplyste at tilgjengeliggjøringsbegrepet omfatter enhver måte å gjøre allmennheten kjent med verket på.[301] Høyesterett presiserte deretter at tilgjengeliggjøringsbegrepet er "teknologinøytralt" (avsn. 42), og konkluderte med at å legge ut slike lenker var tilgjengeliggjøring i åndsverklovens forstand.

De forarbeider som Høyesterett viste til benytter *ikke* ordet "teknologinøytralitet". Karakteristikken ble gitt av Høyesterett selv, noe som indikerer at uttrykket har gått inn i det alminnelige rettsspråket.[302] Høyesterett brukte teknologinøytralitet for å begrunne rettslig

[299] Se kapittel 4.4.
[300] Se kapittel 7-8.
[301] Ot.prp. nr. 26 (1959-1960) Om lov om opphavsrett til åndsverk.
[302] Like etter Høyesteretts avgjørelse kom proposisjonen til endringene i åndsverkloven, som blant annet implementerte opphavsrettsdirektivet i norsk rett. Proposisjonen er datert 11. februar 2005, mens Napster-dommen er avsagt 27. januar 2005. Lovendringene skjedde ved lov 97/2005, i kraft 1. juli 2005. I Ot.prp. nr 46 (2004-2005) s. 19 er ordet "teknologinøytralt" benyttet om tilgjengeliggjøringsbegrepet. *Rognstad* (2009) presiserer at både eksemplarbegrepet og tilgjengeliggjøringsbegrepet er teknologinøytrale begreper, s. 152 og 155. I dansk rett har *Frost* mer generelt satt fokus på teknologinøytralitet ved informasjonsanskaffelser (*Frost*

likestilling av teknisk forskjellige metoder for å gi adressereferanser. Informasjon om nettsteder gitt i form av lenker på internett, ble ansett likeverdig med for eksempel, å gi en tilsvarende opplysning i en avis (avsn. 48). Høyesterett uttalte at:

> ”… avgjørende må være hvordan teknikken virker – om og hvordan tilgang gis” (avsn. 47).

I Napster-dommen likestilte man teknologier som i det ytre er svært forskjellige. Det avgjørende var at *funksjonaliteten* sett i forhold til lovens kriterium var den samme, nemlig å gi tilgang til musikk. Det ga grunnlag for å anvende teknologinøytralitet i vid forstand, og det hadde ikke betydning at teknologien var av yngre dato enn regelen. Fortolkningsmetoden har fått støtte i teorien, jf. *Bing* som konstaterer at man dermed ser:

> ”direkte på funksjonaliteten uten å gå omveien om mer eller mindre adekvate metaforer for hva som skjer.”[303]

6.4 Teknologinøytralitet, ”ting” og ”gjenstand”

6.4.1 Innledning

Gjennomgangen har vist at teknologinøytralitet kan ha vid og snever betydning. Innen strafferetten er utgangspunktet at det er teknologinøytralitet i vid forstand som gjelder. Det er naturlig siden straffebudene ofte mer er rettet mot handlemåten enn karakteren av objektet som er involvert. Departementet har eksplisitt fremhevet dette hensynet, jf. den tidligere siterte uttalelsen om at

> ”Hvor straffverdig en handling er, beror normalt ikke på hvilket teknologisk utstyr som er benyttet eller hvilken teknologisk innretning som er gjenstand for den straffbare handlingen.”[304]

(2002)). Han poengterer betydningen av teknologinøytralitet (medieuavhengighet) for så vidt gjelder kjøpsrettslige informasjonsanskaffelser, se *Frost* (2002) kapittel II, 4.1, sammenholdt med s. 157: ”Således er det ikke selve den omstændighed, at en ydelse foreligger i digitalt format som en fil eller blot som mer fritstående bits, som er afgjørende for den retlige bedømmelse. Digitaliseringsteknologien har afstedkommet en øget fokusering på *informationsydelsen som sådan* uafhengigt af det format, denne konkret måtte forefindes i”, og s. 274, hvoretter en grunnidé i *Frosts* kjøpsrettslige verk er at ”det ikke er den *måde,* en informationsydelse præsteres på, men derimot hvilken *form* for information, der skal præsteres, som er udslagsgivende for retsgrundlaget”. *Frost* fokuserer mer på rettighetene til innholdet enn til mediet, og mener at det ikke skal gjøre en forskjell om informasjonen kjøpes online eller over disk. Smlg. avhandlingen kapittel 6.4.2. Jeg mener at det rettslige skillet mellom medium og innhold uansett må opprettholdes innen strafferetten, fordi det er relevant om krenkelsen forøves eller retter seg mot noe som er ytret, eller om det gjelder mediet.

[303] *Bing* (2008) s. 102.

Hvis begrepene ”gjenstand/ting” skal anses som teknologinøytrale i vid forstand, er spørsmålet hvilke fenomener som kan omfattes og følgelig rettslig likestilles i bestemmelser som bruker begrepene. Her gir jeg en beskrivelse av tolkingsproblemet med bruk av eksempler, for å legge grunnlaget for drøftelsen av gjeldende rett i kapittel 7 flg..

Det må uten videre antas at fysiske objekter omfattes fordi straffeloven tradisjonelt har rettet seg mot slike, for eksempel tyveri av en lommebok eller skadeverk på en bil. Det samme gjelder beslag og inndragning, for eksempel av drapsvåpen, utstyr til å begå pengefalsk, sprøyter og annet utstyr som kan inngå i narkotikalovbrudd m.v.. Men så oppstår spørsmålet om fast eiendom omfattes. En fast eiendom er muligens ”gjenstand/ting” etter en naturlig språklig forståelse, men kan ikke stjeles fordi den ikke kan borttas.

Så finnes det andre typer formuesgoder som det kanskje ikke er så enkelt å klassifisere i forhold til ”gjenstand/ting”, for eksempel tellerskritt ved telefonbruk og elektrisitet som også har en pris per enhet.[305] Noe veiledning finnes i straffelovens egne bestemmelser, særlig strl. 2005 § 12 som bestemmer at med gjenstand menes også ”elektrisk energi og annen energi”, og strl. 2005 § 69 annet ledd, som bestemmer at som ting regnes også ”rettigheter, fordringer og elektronisk lagret informasjon”. Da foreligger det etter loven et bredt spekter av objekter utover de fysiske. Energi er evnen til å utføre arbeid, mens rettigheter og fordringer kan anses som abstrakte goder.[306] Data er et objekt for datamaskinen, og kan ikke sanses direkte av et menneske.

Denne bredden tatt i betraktning kan det konstateres at begrepene ”gjenstand/ting” utvilsomt er teknologinøytrale *i vid forstand*. Spørsmål er om hensynet til teknologinøytralitet har noe selvstendig å tilføre ved fortolkningen av ”gjenstand/ting” for så vidt gjelder data. Ligger det noe mer i hensynet enn at begrepene presumeres å ha vid betydning?

Koops har spaltet opp hensynet til teknologinøytralitet slik at det kort oppsummert er tale om (i) hva slags fenomener som skal likestilles; (ii) hvordan likhetshensynet slår ut i forhold til

[304] Ot.prp. nr. 22 (2008-2009) s. 21. Uttalelsen står i et avsnitt om gjelder utforming av straffebud mot datakriminalitet, som jeg siterte i kapittel 6.3.2.2.
[305] Se *Andenæs/Andorsen* (2008) som er inne på dette problemet på s. 305.
[306] Med ”abstrakt gode” mener jeg et objekt som kan være undergitt eiendomsrett, men som ikke har en fysisk representasjon, se kapittel 7.2.

det konkrete problemet; (iii) om teknologinøytralitet kommer i strid med legalitetsprinsippets klarhetskrav; og (iv) om loven unødig binder opp teknologiutviklingen.[307] Jeg utnytter disse punktene i en avsluttende diskusjon i tilknytning til begrepene ”gjenstand/ting”.

6.4.2 ”What holds offline should also hold online”

Hensynet til teknologinøytralitet er et saklighetskrav, som tilsier at forskjellige fenomener bør være rettslig likestilte dersom det ikke er saklig grunn til forskjellsbehandling. Slagordet har vært ”what holds offline should also hold online”.[308] Det gir uttrykk for likestilling på tvers av miljøer, men har ikke noen særlig eksakt betydning. Noen ganger gis det en snever avgrensning, for eksempel at programanskaffelser over disk (offline) likestilles med programanskaffelser over nett (online). Andre ganger gjelder det i vid forstand, for eksempel at en elektronisk signatur (data / ”online”) skal ha samme rettsvirkning som en håndskrevet signatur (fysisk / ”offline”).[309] Spørsmålet om data er ”gjenstand/ting” omhandler likestilling på tvers av miljøer i vid forstand, fordi det rettslige uttrykket i utgangspunktet gjelder fysiske objekter (offline), mens data er elektroniske signaler (”online”).[310]

At ”gjenstand/ting” er teknologinøytrale i vid forstand følger alt av straffelovens forarbeider og de presiserende bestemmelsene i strl. 2005 §§ 12 og 69 annet ledd. Om ikke annet kan det konkluderes med at strafferettens tilnærming er i samsvar med en vanlig utlegning av dette hensynet, til tross for at det opprinnelig er snevert formulert på grunn av utspringet i ekomsektoren.

6.4.3 Likestilling – men hva definerer likhet og forskjell?

Dersom det er spørsmål om å besørge rettslig likestilling av fenomener, må man som utgangspunkt mene at de er forskjellige. Hvis de er like er det jo intet å likestille. Bedømmelsen av fellestrekk og forskjeller hviler på oppfatninger om faktum, og for å gi en

[307] *Koops* (2006) s. 83 flg.
[308] *Koops* (2006) s. 85.
[309] Se esignaturloven § 6 om rettsvirkninger av elektronisk signatur. Bestemmelsen lyder: ”Rettsvirkninger av elektronisk signatur: Dersom det i lov, forskrift eller på annen måte er oppstilt krav om underskrift for å få en bestemt rettsvirkning og disposisjonen kan gjennomføres elektronisk, oppfyller en kvalifisert elektronisk signatur alltid et slikt krav. En elektronisk signatur som ikke er kvalifisert, kan oppfylle et slikt krav.”
[310] Det er denne form for teknologinøytralitet som ligger bak drøftelsen til *Frost* for informasjonsanskaffelser, se kapittel 6.3.3.

rettslig relevant faktumbeskrivelse må de egenskaper loven krever identifiseres. Når de relevante egenskapene er kartlagt vet man hva begrepene generelt omfatter.

Deretter må man vurdere hvordan begrepene fungerer i den enkelte regel hvor de skal virke. Det kan jo tenkes at konteksten viser at begrepene skal avgrenses noe ulikt i forskjellige regler. Dersom det hersker tolkningstvil kommer hensynet til teknologinøytralitet inn som et *saklighetskrav*, hvor man må vurdere om data er funksjonelt likeverdig med andre objekter som omfattes av regelen, jf. Høyesteretts fremgangsmåte i Napster-dommen. Et relevant moment er *behovet* for å utføre automatisert inndragning i nettet uavhengig av om dublettene er lagret eller overføres. Da bør data anses som "ting" selvstendig sett. Dermed blir spørsmålet om det er noen saklig grunn til å behandle data annerledes enn fysiske objekter, dersom de uansett oppfyller kriteriene som ligger til grunn for "gjenstand/ting".

6.4.4 Legalitetsprinsippet - kontrollevnens betydning

Koops påpeker at dersom teknologinøytralitet drives for langt i lovgivningsarbeidet, kan lovens uttrykk bli så abstrakte og generelle at de mister sin veiledende funksjon.[311] I så fall risikerer man å krenke legalitetsprinsippets klarhetskrav.

En sak for seg er at hvorvidt klarhetskravet er oppfylt, må vurderes konkret i forhold til den enkelte bestemmelse. Et annet spørsmål gjelder holdbarheten av påstanden om at det gjelder et spenningsforhold mellom et generelt begrep og klarhetskravet. Den bør ikke ukritisk legges til grunn.

Det kan i hvert fall ikke tas som utgangspunkt at et begrep er vagt og uklart fordi det er generelt. Vaghet gjelder forholdet mellom begrepets meningsinnhold og den virkelighet det

[311] *Koops* (2006) s. 100 "What level of legal certainty is required?" skriver at : "[L]egislation that is too focused on sustainability and hence abstracts too much away from technology will result in vague laws that provide little legal certainty." Koops bruker trafikkdata som eksempel, og kritiserer regler som ikke binder begrepet til spesielle kommunikasjonstjenester, slik man tidligere gjorde (i nederlandsk rett) for "plain old telephony". Jeg synes kanskje ikke eksemplet med trafikkdata er så godt. Det er snarere uheldig å binde reglene til spesifikke kommunikasjonstjenester, som i praksis brukes om hverandre. For den som inngrepet gjelder har det ingen betydning om inngrepet gjelder mobiltelefonbruk eller andre kommunikasjonstjenester (fast telefon, epost, internettoppkobling m.v.). Derimot er esignaturloven et eksempel på et rettslig abstraksjonsnivå som har gått så langt at det er vanskelig å forstå innholdet, se definisjonslisten i esignaturloven § 3 for eksempel nr. 6: "Signaturfremstillingssystem: "programvare eller maskinvare som benyttes til å fremstille elektronisk signatur ved hjelp av signaturfremstillingsdata.", og nr. 7: "Signaturverifikasjonsdata: unike data, som for eksempel koder eller offentlige nøkler, som benyttes til å verifisere en elektronisk signatur."

skal regulere.[312] Både ”gjenstand” og ”ting” er generelle begreper som kan omfatte meget og fungere som overbegrep. Fordi de er generelle er de *tidsbestandige* og kan ta opp i seg nye fenomener som har de nødvendige karakteristika for å være ”gjenstand/ting”. Det gir begrepene karakter av å være fleksible og dynamiske, dvs. at de er ”elastiske” som tidligere nevnt.[313] Her synes det også å ligge et dynamisk tolkingselement som gjelder menneskets *økende evne til å kontrollere sine omgivelser*. Det må antas at dersom fenomenet kan kontrolleres og individualiseres, så er det ”gjenstand/ting”, fordi det hører sammen med forutsetningen om at objektet kan eies. Følgelig må det som et generelt utgangspunkt antas å være slik at jo flere fenomener man kan underkaste kontroll, jo flere fenomener kan henføres under begrepene.

Derfor synes problemet snarere å være hvordan man skal gi en relevant beskrivelse av data.[314] Klarhetskravet leder ikke i dette tilfellet til at det må utvises tilbakeholdenhet med hensyn til hva de rettslige begrepene anses å omfatte; det som må undersøkes er om godet oppfyller de kriterier som lovens begrep krever. Med hensyn til IKT har nok den generelle forståelsen på kort tid økt betraktelig. Mens man tidligere vektla at data var noe nytt og annerledes, er utgangspunktet i dag kanskje motsatt. I stedet for å beskrive data som ”en serie et-tall og nuller” som i datakrimutredningen fra 1985, synes nå en beskrivelse av data som et gode som kan spesifiseres og konkretiseres, som mer relevant.[315] Ethvert fenomen kan oppløses i sine minste partikler, som atomer, *bits*, fotoner (lyspartikler), eller endog kvarker. Men partiklene er ikke rettslig relevante; de må manifestere seg som et større fenomen, og det er dette som skal vurderes i forhold til lovens krav til egenskaper. På denne bakgrunn kan en fortolkning som utelukker objekter fordi de består av *bits*, anses som vilkårlig.

En lignende situasjon har man for det generelle begrepet ”informasjonsbærer” som omfatter medier generelt.[316] Begrepet vil omfatte nye medier i takt med at utviklingen lanserer stadig nye måter å formidle ytringer på. Dette må anses som rettslig uproblematisk, og det vil fremstå som vilkårlig dersom et medium ble utelukket fordi det var basert på ny teknologi.

[312] *Kolflaath* (2004) s. 25; *Jacobsen* (2008) s. 304.
[313] Se kapittel 6.3.1.
[314] Se kapittel 3.2 om beskrivelsesproblemet vedrørende data.
[315] Straffelovrådets utredning om datakriminalitet NOU 1985: 31 s. 8 viser til *Torvund*, Complex 6/83 s. 147-148, hvor data er beskrevet som ”en serie et-tall og nuller”. Med tanke på strafferettslige problemstillinger er det i dag naturlig med en noe fyldigere beskrivelse, jf. kapittel 3.
[316] Jf. strl. 2005 § 76. Omtalt i kapittel 5.4.1.

Dersom uklarheten reelt sett ikke knytter seg til faktum, slik jeg hittil har drøftet, har man med et alminnelig harmoniseringsproblem knyttet til de aktuelle rettskildefaktorene å gjøre. Det er en vanlig situasjon i juridisk arbeid og betyr ikke at loven er spesielt uklar.

Ut fra en bred teknologinøytral tilnærming, må situasjonen for data være som for andre objekter, nemlig et utgangspunkt om at data omfattes av "gjenstand/ting", og dermed av de regler som bruker disse begrepene. Men dersom det er konkrete holdepunkter for noe annet, kan det bli tale om å tolke begrepene innskrenkende, slik at data faller utenfor regelen. Dette er i samsvar med den tolkningsmetode som Høyesterett brukte i Napster-dommen (Rt. 2005 s. 41). Dommen gjaldt riktignok krav om erstatning, ikke straff, men det er vanskelig å se at tolkingsresultatet skulle blitt et annet dersom saken hadde omhandlet krav om straff. Det man i så fall kunne ha gjort var å anvende fortolkningen, men frifinne på grunn av unnskyldelig rettsvillfarelse.[317] Med Napster-dommen må tolkingsspørsmålet anses avgjort og legges til grunn i fremtidige saker uavhengig av om det er tale om idømmelse av straff eller en annen reaksjon.

Hovedkonklusjonen er derfor at går man til verks ved fortolkningen med en analyse først på det generelle plan hvor de kriterier som begrepet hviler på identifiseres, og så går over på det på det spesielle plan, er ikke generelle begreper nødvendigvis uklare.

6.4.5 Reglene bør ikke hindre teknologiutvikling

Hensynet til teknologinøytralitet tilsier også at loven ikke bør hindre teknologiutvikling. Dette er et teknologivennlig standpunkt som også kan tuftes på argumentet om at teknologi ikke kan være "god" eller "ond", bare mer eller mindre nyttig. En moralsk karakteristikk kan derfor bare rettes mot *bruken* av teknologien. Uansett må det antas å være vanskelig for politikerne (lovgiver) å forutsi hva som blir nyttig teknologi, noe som tilsier varsomhet med å gripe inn for å styre utviklingen via regelverket. Utviklingen kan fort lede til at lovgitte restriksjoner fremstår som utidsmessige og vilkårlige , noe som bør unngås for å gi innovasjon best mulige kår.

[317] Høyesterett var inne på forsvarets anførsel om unnskyldelig rettsvillfarelse. Retten fant at domfeltes lenking til musikk som var lagt ut nettet var "forsettlige og meget klanderverdige medvirkningshandlinger" (avsn. 67), og domfelte "har utvilsomt vært klar over at musikken var opplastet uten rettighetshavernes samtykke. Han har handlet forsettlig og kan ikke høres med at han befant seg i rettsvillfarelse med hensyn til at han har medvirket til et straffbart forhold" (avsn. 68).

For avhandlingens analyse er situasjonen at lovbestemmelsene alt foreligger, så spørsmålet er om teknologihensynet gjør seg gjeldende ved fortolkningen *de lege lata*, eventuelt i en vurdering *de lege ferenda.*

Hensynet til å unngå bindinger på teknologiutviklingen kan komme opp ved fortolkningen på følgende måte: Det er behov for teknologiutvikling for å ta i bruk automatisert inndragning i nettet. Tekniske løsninger kan selvsagt bare brukes innen de rammer som følger av hjemmelskrav og individenes grunnleggende rettigheter. Men *nøyaktig* hva slags tekniske løsninger som er hensiktsmessige, er det ikke nødvendig for loven å bestemme. Blant flere mulige tolkningsalternativer bør man derfor gå inn for det som gir minst binding med tanke på den praktiske gjennomføringen. Dermed foreligger et argument for å koble adgangen til automatisert inndragning til strl. 2005 § 69 første ledd, som ikke krever at dataene er "lagret".

6.5 Oppsummering

Jeg har nå stilt problemet, nemlig om data omfattes av begrepene "gjenstand/ting" som selvstendig objekt. Jeg har også avklart at "gjenstand/ting" er teknologinøytrale begreper i vid forstand som på et generelt grunnlag må antas å omfatte data. I de videre drøftelsene bygger jeg på disse utgangspunktene.

7 Kriterier til grunn for "gjenstand" og "ting"

7.1 Problemstilling

I dette kapitlet kartlegger jeg hvilke kriterier begrepene "gjenstand/ting" er basert på. Til slutt vurderer jeg om data oppfyller kriteriene. Nedenfor følger først en oversikt over de bestemmelser som er sentrale i analysen. Jeg inkluderer også bestemmelser i straffeloven 1902, fordi de eldre rettskildene refererer seg til disse. Deretter foretar jeg kartleggingen.

7.1.1 Straffebestemmelsene (”gjenstand”)

Jeg konsentrerer meg om følgende straffebestemmelser som bruker ordet ”gjenstand” eller ”løsøregjenstand”:[318]

- Tyveribestemmelsen, som rammer uberettiget tilegnelse ved å ”bortta” eller ”ta” en ”gjenstand” (strl. 1902 § 257 / strl. 2005 § 321);[319]
- Underslagsbestemmelsen, som rammer rettsstridig tilegnelse av en ”løsøregjenstand” som man alt besitter (strl. 1902 § 255 første alt. / strl. 2005 § 324 bokstav a);[320]
- Bestemmelsen om ulovlig bruk, som rammer ulovlig bruk eller forføyning over en ”løsøregjenstand” (strl. 1902 § 261 / strl. 2005 § 343);[321] og
- Skadeverksbestemmelsen, som rammer det å ødelegge (m.v.) en ”gjenstand” (strl. 1902 § 291 / strl. 2005 § 351).[322]

Alle bestemmelsene forutsetter at gjenstanden ”tilhører en annen” enn lovbryteren. Dermed må jeg behandle spørsmålet om data kan være gjenstand for eiendomsrett.[323]

Straffebudene veksler mellom å bruke ”gjenstand” og ”løsøregjenstand”. Jeg bruker bare ”gjenstand” fordi det ikke synes å være noen rettslig relevant forskjell mellom begrepene. Det viser seg i forholdet mellom tyveri- og underslagsbestemmelsen, hvor ”løsøregjenstand” brukes ved underslag og ”gjenstand” ved tyveri. Dersom ordvalget hadde hatt reell betydning burde begrepsbruken vært motsatt, fordi en løsøregjenstand kan borttas og følgelig utsettes for

[318] Det finnes flere, se strl. 1902 § 150 bokstav b; strl. 1902 § 267/ 2005 § 327 (ran); strl. 1902 Salgspant § 278; strl. 1902 § 317 / 2005 §§ 332 og 337 (heleri og hvitvasking).
[319] *Strl. 1902 § 257 første ledd* bruker ”borttar” og lyder: ”For tyveri straffes den som borttar eller medvirker til å bortta en gjenstand som helt eller delvis tilhører en annen, i hensikt å skaffe seg eller andre en uberettiget vinning ved tilegnelsen av gjenstanden.”; *strl. 2005 § 321 første ledd* bruker ”tar” og lyder: ”For tyveri straffes den som tar en gjenstand som tilhører en annen, med forsett om å skaffe seg eller andre en uberettiget vinning ved å selge, forbruke eller på annen måte tilegne seg den.”
[320] *Strl. 1902 § 255 første straffalternativ* lyder: ”For underslag straffes den som i hensikt derved å skaffe seg eller andre en uberettiget vinning rettsstridig avhender, pantsetter, forbruker eller på annen måte tilegner seg en løsøregjenstand som han besitter, men som helt eller delvis tilhører en annen…”; *Strl. 2005 § 324 første ledd bokstav a* lyder: ”For underslag straffes den som med forsett om en uberettiget vinning for seg selv eller andre rettsstridig selger, forbruker eller på annen måte tilegner seg en løsøregjenstand eller pengefordring som han besitter, men som tilhører en annen.”
[321] *Strl. 1902 § 261 første punktum* lyder: ”Den som rettsstridig bruker eller forføyer over en løsøregjenstand som tilhører en annen, og derved skaffer seg eller andre betydelig vinning eller påfører den berettigete betydelig tap straffes med fengsel inntil 3 år.”; *Strl. 2005 § 343* lyder: ”Med bot straffes den som ulovlig bruker eller forføyer over en løsøregjenstand som tilhører en annen, slik at den berettigete påføres tap eller ulempe.”
[322] *Strl. 1902 § 291 første ledd* lyder: ”For skadeverk straffes den som rettsstridig ødelegger, skader, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen.”; *Strl. 2005 § 351 første ledd* lyder: ”Med bot eller fengsel inntil 1 år straffes den som skader, ødelegger, gjør ubrukelig eller forspiller en gjenstand som helt eller delvis tilhører en annen.”
[323] Se kapittel 7.5. Smlg. *Andenæs/Andorsen* (2008) s. 306-308 om eiendomsbegrepets betydning ved tyveri.

tyveri, mens fast eiendom er en gjenstand som kan underslås, men ikke stjeles.[324] Videre avgrenses "gjenstand" ulikt i forhold til fast eiendom. I tyveribestemmelsen kan ikke begrepet omfatte fast eiendom på grunn av kravet om besittelsesforrykkelse. Derimot kan fast eiendom utsettes for skadeverk.[325]

Etter en naturlig språklig forståelse er "gjenstand" et videre begrep enn "løsøregjenstand", fordi det også omfatter fast eiendom. Eksemplene viser imidlertid at begrepene ikke er brukt på dette vis i loven.[326] Det fremgår også at det konkrete innholdet i begrepet "gjenstand" i stor grad bestemmes av konteksten som dannes av straffebudenes øvrige vilkår.

Både straffeloven 1902 og 2005 inneholder en bestemmelse som presiserer gjenstandsbegrepet i forhold til energi (elektrisitet). Strl. 2005 § 12 viderefører strl. 1902 § 6 i litt enklere orddrakt og lyder:

> "Med gjenstand menes også elektrisk energi eller annen energi".[327]

Formuleringen "menes også" viser både at gjenstandsbegrepet har vid betydning og at bestemmelsen ikke er en legaldefinisjon. Det kan derfor ikke uten videre legges til grunn at energi er omfattet av alle straffebudene som bruker "gjenstand".[328] Også her må det bero på en fortolkning hvor bestemmelsens øvrige vilkår får stor betydning. Man kan for eksempel tenke seg at elektrisitet kan være gjenstand for tyveri, underslag og ulovlig bruk, men neppe for skadeverk. Et strømbrudd leder jo ikke til at elektrisitet forspilles eller skades. Derimot er ødeleggelse av strømkabelen et skadeverk.[329]

[324] Mer om dette, se *Sunde* (2006) s. 108. Det er tilfelle for tyveri- og underslagsbestemmelsene både etter den eldre og den nye straffeloven, fordi straffeloven 2005 viderefører den eldre ordbruken.
[325] *Sunde* (2006) s. 108. I Rt. 1953 s. 462 ble graving på annen manns eiendom ansett som skadeverk.
[326] Se også *Matningsdal* (1995) som i relasjon til strl. 1902 § 257 sier at det ikke er noen realitetsforskjell mellom begrepene, s. 676; smlg. *Andenæs/Andorsen* (2008) s. 305.
[327] Smlg. strl. 1902 § 6. "Under Uttrykket Løsøregjenstand indbefattes i denne Lov, ogsaa enhver til Frembringelse af Lys, Varme eller Bevægelse fremstillet eller opbevaret Kraft."
[328] Se kapittel 6.2 om betydningen av at bestemmelsene ikke er legaldefinisjoner, med henvisning til *Eckhoff* (2001) s. 337.
[329] Ved Odelstingsforhandlingene i 1902, da man diskuterte det strafferettslige vernet for elektrisk strøm, var man innom alle alternativene unntatt ulovlig bruk. Indst.O. I-1901/1902, s. 29.

7.1.2 Inngrepsbestemmelsene (”ting”)

Beslag og inndragning karakteriseres som midlertidig og permanent inngrep (”berøvelse”) i eiendomsretten.[330] Inngrepshjemlene speiler tyveri- og skadeverksbestemmelsene, men betegner objektet som ”ting”, ikke som ”gjenstand”.[331]

Reglene om gjenstandsinndragning ble gjennomgått i kapittel 5, og jeg viser til de fullstendige lovsitatene der vedrørende strl. 2005 §§ 69, 70 og 76.[332] Beslagsbestemmelsen i strpl. § 203 bør imidlertid siteres. Den lyder slik:

> ”Ting som antas å ha betydning som bevis, kan beslaglegges inntil rettskraftig dom foreligger i saken. Det samme gjelder ting som antas å kunne inndras eller å kunne kreves utlevert av fornærmede.”

Som kjent inneholder inndragningsreglene en presiserende bestemmelse av ”ting”, jf. strl. 2005 § 69 annet ledd, som lyder:

> ”Som ting regnes også rettigheter, fordringer og elektronisk lagret informasjon.”[333]

Bestemmelsen knytter an til hovedregelen om at ”ting” som er produktet av, har vært gjenstand for eller bestemt til å brukes ved en straffbar handling kan inndras, jf. strl. 2005 § 69 første ledd.[334] Bestemmelsen er av samme karakter som strl. 2005 § 12. Med ”regnes også” gis det uttrykk for at ”ting” er et vidt begrep. Loven presiserer også at data omfattes av begrepet, jf. ”elektronisk lagret informasjon” og spørsmålet er stadig om de kriterier som ligger til grunn for ”ting” tilsier at data anses som et selvstendig objekt, uavhengig av den fysiske bæreren, og når de overføres.

Straffeprosessloven har ikke noen lignende bestemmelse, men på grunn av sammenhengen mellom beslags- og inndragningsreglene må ”ting” forstås å bety det samme. Forarbeidene til inndragningsreglene i straffeloven 2005 legger uten videre til grunn at utvidet adgang til forebyggende inndragning vil

[330] Se kapittel 6.2 med videre henvisninger.
[331] Jeg har avgrenset mot inndragningsbestemmelsenes bruk av formuleringen ”gjenstand for”, som jeg ikke ser at har noen betydning for drøftelsen. Se kapittel 6.2.
[332] Str. 2005 § 69 er sitert i kapittel 5.4.1, § 70 i kapittel 5.5.1 og § 76 i kapittel 5.5.2 og 5.7.1.
[333] Smlg. strl. 1902 § 35 første ledd annet punktum: ”Som ting regnes også rettigheter og fordringer”. Tilføyelsen av ”elektronisk lagret informasjon” i strl. 2005 § 69, regnes som en presisering av gjeldende rett, dvs. skal innfortolkes i ”ting”, jf. strl. 1902.
[334] Fullstendig lovsitat i kapittel 5.3.1.

> ”automatisk utvide adgangen til å ta beslag. Det skyldes at det etter straffeprosessloven § 203 første ledd annet punktum er adgang til å beslaglegge ting som antas å kunne inndras”.[335]

Begrepsidentiteten følger også av at beslag for å sikre et inndragningskrav i objektet, bare kan tas når man skal bruke gjenstandsinndragning (ikke verdiinndragning). Loven krever nemlig at det er identitet mellom det objekt som er involvert i den straffbare handling og som skal inndras, og beslagsobjektet.[336] Vilkåret har betydning dersom objektet er blitt konvertert eller blandet sammen med andre verdier i tiden mellom den straffbare handling og beslagstidspunktet. Dersom identitetsvilkåret ikke er oppfylt, må verdiinndragning anvendes og da er lovens ordning at *heftelse* skal brukes for å sikre inndragningskravet, jf. strpl. § 217, ikke beslag.[337]

Konvertering er ikke noe problem i forhold til den fremgangsmåten som belyses i avhandlingen. Den starter med beslag av data som stammer fra en straffbar handling, jf. strl. 2005 §§ 201 eller 311, jf. strl. § 203. Disse dataene inndras, jf. strl. 2005 § 69 flg. Det oppstår imidlertid et identitetsspørsmål som gjelder om dublettene i nettet kan identifiseres med dataene som inndras i straffesaken. Spørsmålet drøftes i kapittel V.

7.2 Mange ulike objekter

Spørsmålet er hvilke kriterier som ligger til grunn for begrepene ”gjenstand/ting”. Ifølge hevdvunnen lære er utgangspunktet at ”gjenstand/ting” er basert på det ”tingsrettslige tingsbegrepet”.[338] Men det er nokså selvsagt siden de straffebud som bruker ”gjenstand” er

[335] Ot.prp. nr. 90 (2003-2004) kapittel 26.5.3 s. 348. Smlg. *Andenæs/Myhrer* (2009) s. 317 ”Om slik inndragning kan skje, beror på inndragningsbestemmelsene i strl. Kap. 2 og i spesiallovgivningen.”

[336] Se Rt. 1995 s. 1583, fulgt opp i Rt. 2002 s. 133 og s. 136. Se også NOU 1996: 21 Mer effektiv inndragning av vinning kapittel 4.3 og 4.8.1; Ot.prp. nr. 8 (1998-1999) s. 64-66; *Dyrnes* (2004) s. 48 og s. 176.

[337] Se *Dyrnes* (2004) som gjennomgår noen tilfeller av konvertering og sammenblanding på s. 177. Hvorvidt det leder til at objektets identitet er endret, må undersøkes nærmere og er et eget tema i finansiell etterforsking. Konvertering av penger til fysiske objekter som bil og bolig, endrer ikke identiteten. Men hvis det for eksempel er klart at et beløp på konto kommer fra en lovlig transaksjon, kan det ikke tas gjenstandsinndragning i kontoen, selv om beløpet er like stort som utbyttet fra en straffbar handling begått av kontohaver. Da må det foretas heftelse og verdiinndragning.

[338] *Matningsdal* (1987) s. 242 sier at ”«ting» refererer seg til det alminnelige tingsrettslige tingsbegrep”. Det har også vært vanlig å kalle inndragning av ting for ”gjenstandsinndragning”, se *Dyrnes* (2004) s. 48. Men for inndragning kan det være litt vanskelig å holde styr på begrepsbruken så ”det er en relativt utbredt misforståelse at gjeldende bestemmelse om inndragning av ting, bare hjemler gjenstandsinndragning, og at bestemmelsen om inndragning av utbytte bare gjelder verdiinndragning. Imidlertid gir begge bestemmelsene adgang til både gjenstands- og verdiinndragning”, se Ot.prp. nr. 90 (2003-2004) kapittel 26.4.3 s. 347. Uansett er inndragning av ting i medhold av strl. 2005 §§ 69 flg., gjenstandsinndragning så lenge det er ting som inndras, så jeg problematiserer ikke dette.

satt til vern om eiendomsretten, og inndragning er et permanent inngrep i eiendomsretten. Da må både gjenstanden og tingen kunne eies. For ”ting” kommer forutsetningen også til syne ved at objektet iblant kalles ”formuesgjenstand”.[339] Det burde utelukke objekter uten legal verdi, men som tidligere påvist skal også slikt som narkotika og overgrepsbilder inndras, så man kan ikke trekke altfor kategoriske slutninger av karakteristikken.[340]

Henvisningen til en tingsrettslig avgrensning av den gruppe objekter som omfattes av bestemmelsene, er ikke helt selvforklarende.[341] Det er tale om en nokså uensartet gruppe objekter så det kan være hensiktsmessig med en sortering i henhold til modellen i kapittel 2.1.

Nederst finner vi *fysiske objekter*, som fast eiendom og fysiske løsøregjenstander som bøker, sykler, pengesedler og levende dyr. Dette er ”materielle ting” eller *håndfaste verdier*, for å følge *Falkangers* språkbruk.[342]

På øverste nivå finner vi *abstrakte goder.* Rettigheter og enkle fordringer hører til her.[343] De omfattes av strl. 2005 § 69 annet ledd og er følgelig ”ting”. Kjennelsen i Rt. 2009 s. 1011 (”joyzone.no”) fastslår adgangen til å ta beslag i domenenavn (”joyzone” m.fl.) for å sikre et krav på gjenstandsinndragning, jf. strpl. § 203, jf. strl. 1902 §§ 35 og 37 b. Rett til domenenavn er således et eksempel som faller inn under dette alternativet. Det samme må antas å gjelde rett til et brukerområde hos en nettvert. Dessuten har rettspraksis fastslått at enkle fordringer kan være gjenstand for underslag, som ”løsøregjenstand”.[344]

Jeg bruker uttrykket ”abstrakte goder” for å skille mot immaterialrettighetene, dvs. opphavsrettighetene, nærstående rettigheter, vernet om bedriftshemmeligheter osv.

[339] Ot.prp. nr. 90 (2003-2004) kapittel 26 s. 343 (nederst) og s. 346.
[340] Se kapittel 5.8.
[341] *Falkanger* (2007) påpeker at ”tingsretten” er en referanse til en systematikk for behandling av eiendomsrettslige spørsmål hvor man er nokså pragmatisk med grenseoppgangen mot andre rettsområder (s. 31).
[342] *Falkanger* (2007) s. 31. Også fast eiendom kan inndras, se *Matningsdal* (1987) s. 242-243.
[343] *Falkanger* (2007) s. 31. Selv om ”materielle ting” er tingsrettens objekter, inkluderes også fordringer, og i en viss utstrekning rettigheter. Den strafferettslige hjemmelen er strl. 2005 § 69 annet ledd ”som ting regnes også rettigheter, fordringer”, smlg. strl. 1902 § 35 første ledd annet punktum. Om bakgrunnen for presiseringen om at rettigheter og fordringer kan inndras, skriver *Matningsdal* (1987) s. 243, at ”Man fant det derfor riktig å ta inn [strl. 1902 § 35 annet punktum] for å gjøre det klart at en fordring ikke bare kan inndras når den er knyttet til et dokument, men at inndragning også kan foretas «når det gjelder muntlige fordringer eller rettigheter av annen art enn en pengefordring»”.
[344] Se utviklingen i rettspraksis fra Rt. 1997 s. 1760, hvor spørsmålet ble reist, men ikke avgjort; Rt. 2003 s. 1243, hvor det under dissens ble lagt til grunn at en enkel fordring kunne underslå som ”løsøregjenstand”; og Rt. 2008 s. 1582 hvor rettssetningen i 2003-avgjørelsen uten videre ble lagt til grunn i en sak om underslag av pengeoverføring fra Aetat. Sakene er omtalt i kapittel 7.6.4.

Immaterialrettighetene faller etter vanlig oppfatning utenfor det tingsrettslige tingsbegrepet. Men av dette kan man ikke trekke den slutning at det er et vilkår for å være undergitt eiendomsrett at objektet har en fysisk representasjon. Det vitner jo eiendomsretten til rettigheter og enkle fordringer om. Skillet overfor immaterialrettighetene er begrunnet i karakteren av det *regelsystem* som regulerer dem. Mens eiendomsretten anses som en såkalt residualrett, anses immaterialrettighetene som et sett med positivt avgrensede rettighetsbeføyelser (se mer om dette i kapittel 7.3). For å unngå misforståelser bruker jeg derfor *abstrakte goder* om rettigheter og fordringer, slik at de ikke forveksles med de egentlige immaterialrettighetene.

Rettigheter og fordringer eksisterer i kraft av rettsstiftende disposisjoner, og har ikke en fysisk manifestasjon. Det gjelder selv om ytelsen er av fysisk karakter når den presteres, for eksempel en gjeld som betales i kontanter. Dersom en fordring er knyttet til et gjeldsbrev er imidlertid objektet fysisk, og hører til på modellens nederste nivå. Det som her er sagt er i samsvar med en uttalelse i forarbeidene til straffeloven 2005 i tilknytning til tyveribestemmelsen, hvor det står at

> ”penger er eksempelvis en gjenstand, mens immaterielle rettigheter ikke er det.”[345]

Pengene det er tale om hører til på nederste nivå i modellen, når de består i kontanter. Og de immaterielle rettighetene anses ikke som eiendomsrettigheter, så de faller utenfor gjenstandsbegrepet. Men eiendomsrett til en enkel fordring kan man ha, så dette ”abstrakte godet” er ”gjenstand”.

Jeg avgrenser ellers drøftelsene mot ”rettigheter”, fordi det er en stor og uensartet gruppe. Det må uansett antas at allemannsrettighetene ikke omfattes av gjenstandsbegrepet, de tilkommer jo alle i kraft av loven. Alternativet ”rettigheter” kan omfatte individuelle rettigheter, for eksempel jakt- og fiskerettigheter som man har kjøpt. Nøyaktig hvilke rettigheter som omfattes har ikke noen betydning for analysen, så jeg ser ikke mer på dette.

Et viktig spørsmål er imidlertid hvordan man skal plassere *informasjon* i forhold til det tingsrettslige tingsbegrepet. Informasjon bæres av et medium og er et immaterielt objekt som dermed hører til på modellens øverste nivå. Et annet spørsmål er om informasjon kan eies.

[345] Ot.prp. nr. 22 (2008-2009) kapittel 8.3.1 s. 280.

Her er vi tilbake til forholdet mellom data og databasert innhold, og jeg behandler spørsmålet i drøftelsen av forholdet mellom eiendomsretten og de immaterielle rettigheter, jf. nedenfor.

I området mellom fysiske objekter og abstrakte goder finner vi objekter som har en faktisk konstaterbar manifestasjon (i motsetning til abstrakte goder), men hvor *befatningen er indirekte* fordi den må skje ved bruk av verktøy (i motsetning til fysiske objekter). Her finner vi elektrisitet, jf. strl. 2005 § 12, og data, jf. strl. 2005 § 69 annet ledd. Jeg kan gi enda et eksempel på et objekt som hører til her, og det er *gass.* I forarbeider og teori er det lagt til grunn at gass omfattes av gjenstandsbegrepet. Det fremgår alt ved Odelstingsforhandlingene i 1902 ved straffelovens tilblivelse. Man behandlet gjenstandsbegrepet i en diskusjon som gjaldt hvordan man skulle gi elektrisitet adekvat strafferettslig vern som formuesgode, noe som endte med innføringen av strl. 1902 § 6, som er videreført i strl. 2005 § 12.[346] Det ble sagt at begrepet ”«gjenstand» forudsætter en fast, en flydende eller gasartet aggregatform”.[347] Uttalelsen viser at det ikke har vært noe absolutt vilkår at gjenstanden kan påvises fysisk uten bruk av hjelpemidler. I 1930 skrev *Kjerschow* følgelig at gass var ”gjenstand”.[348]

Det at det tingsrettslige tingsbegrepet inkluderer de abstrakte godene, elektrisitet og gass, samt at data anses som ”ting”, står i et spenningsforhold til den rettssetning som det iblant vises til, om at begrepet ’gjenstand’ forutsetter at objektet er av *legemlig* karakter. Straffelovrådet viste til denne læren i 1985, da det konkluderte med at data ikke var gjenstand. På den bakgrunn ble det uttalt følgende:

> ”Etter alminnelig språkbruk må en gjenstand være av fysisk beskaffenhet, slik at immaterielle objekter faller utenfor begrepet. Rent fysisk er lagrede data bare magnetiske impulser, og den informasjon dataene representerer, er selvsagt av utpreget immateriell karakter.”[349]

Men som jeg har antydet er det ikke helt entydig hva ”immaterielle objekter” betyr. Åndsverk omfattes ikke, med det gjør jo et abstrakt gode som en enkel fordring.

Som en oppsummering har gjennomgangen vist at ”gjenstand/ting” inkluderer objekter som fordeler seg på alle tre nivåer i modellen i kapittel 2.1. I den videre fremstilling av begrepet

[346] Se lovsitatene i kapittel 7.1.1.
[347] Indst. O. I-1901/1902, s. 29. Forhandlinger i Odelstinget nr. 55 (1901-1902) s. 435.
[348] *Kjerschow* (1930) s. 632, s. 901.
[349] NOU 1985: 31 kapittel 4.3.3 s. 9.

tar jeg først opp avgrensningen mot immaterialrettighetene fordi det har betydning for å forstå forskjellen i rettighetsforholdene til data og databasert informasjon.

7.3 Eiendomsrett vs. positivt avgrensede rettsposisjoner

Nordisk rettvitenskap har hatt en diskusjon om immaterialrettighetene kan kalles eiendomsrett, eller om de kjennetegnes av å være et sett positivt avgrensede rettigheter, såkalte "rettsposisjoner".[350] Det er redegjort for diskusjonen i en rekke andre fremstillinger, så jeg nøyer meg med å konstatere konklusjonen.

Konklusjonen er at eiendomsretten og de immaterielle rettigheter er forskjellige og at man følgelig ikke kan karakterisere immaterialrettighetene som eiendomsrettslige. Grunnen er som alt indikert, at immaterialrettighetene består av positivt avgrensede rettigheter og beføyelser, mens eiendomsretten er residuell, dvs. en "restrett". Med det menes at når eiendomsrett til et objekt først er etablert, så har man samtlige positive og negative eierbeføyelser, med mindre det er gjort inngrep i dem. Motsatt kjennetegnes immaterialrettighetene av å være de rettigheter loven har valgt å etablere på grunn av ens rolle i forhold til godet, for eksempel opphavspersonens enerett til tilgjengeliggjøring av verket, jf. åvl. § 2. Eiendomsretten derimot er som utgangspunkt komplett.

Det er den korrekte rettslige karakteristikken av *åndsverket* som later til å ha tiltrukket seg størst oppmerksomhet, men diskusjonen er også relevant for informasjon som ikke er åndsverk, for eksempel patentrettigheter, vernet om bedriftshemmeligheter, personopplysninger osv.[351] Diskusjonen er således videreført i spørsmålet om *informasjon* kan eies, og da later det til å være enighet i nordisk teori om at svaret er negativt.[352] Informasjon

[350] Uttrykket "rettsposisjoner" kommer så vidt jeg forstår fra *Koktvedgaards* doktoravhandling "Immaterialretspositioner" fra 1965.
[351] *Irgens-Jensen* (2008) har i kapittel 1.2 en liste over forskjellige immaterialrettsgoder, som gir oversikt over hvordan rettsreglene overlapper og utfyller hverandre.
[352] For så vidt gjelder den nordisk rettstilstand gir *Lau Hansen* (2001) en god oppsummering. Forskjellen går mellom å ha en *rettsposisjon* som er uttrykkelig avgrenset, kontra å ha *eiendomsrett* som er residuell. Dette ble inngående analysert i *Ross'* kritikk av *Vinding-Kruses* opphavsrettslige arbeid, og videreutviklet i *Koktvedgaard* "Immaterialretspositioner" (1965). *Lau Hansen* konkluderer med at det ikke ville være korrekt å anse rettigheter til informasjon som eiendomsrett, slik man for eksempel gjør i amerikansk rett, men redegjør for en rekke omstendigheter som gjør at forskjellen likevel blir liten. Helt sentralt er imidlertid at diskusjonen gjelder *informasjon,* ikke den fysiske bæreren. Med andre ord har ikke diskusjonen tatt opp spørsmålet om eiendomsretten til *mediet*, som er sentralt for mitt tema. Om rettighetsforholdet til personopplysninger skriver *Schartum* (2004) s. 40: "Vi tror ikke at analogien med eiendomsrettsbegrepet er særlig brukbar som et teoretisk utgangspunkt, bl a fordi det kan gi assosiasjoner om en langt videre råderett enn det som normalt er tilfellet.".

er altså ikke et gode som etter gjeldende rett er gjenstand for eiendomsrett, men man kan ha rettigheter til informasjon på en rekke forskjellige positivt oppregnede grunnlag.

Det betyr at man ved spørsmålet om *data* kan være gjenstand for eiendomsrett, må skille ut spørsmålet om *informasjon* kan være gjenstand for eiendomsrett. Informasjon kan ikke det. Men dermed er det ikke sagt hva løsningen er for mediet.

Drøftelsene i kapittel 2 viser at det kan skilles mellom data som medium og databasert informasjon. Forholdet dem imellom har sin parallell i opphavsrettens sondring mellom eksemplaret og åndsverket. Opphavsrettighetene gjelder åndsverket, mens eksemplaret er et fysisk objekt. *Rognstad* skriver således at opphavsretten

> ”relaterer seg til det åndsverk eksemplarene *er bærere av.”* (min uth.). [353]

Og videre at:

> ”Åndsverket er ikke en fysisk størrelse. Riktignok kan det fremstilles fysiske *eksemplarer* av åndsverket, som for eksempel en bok, et maleri, en CD osv. Disse eksemplarene vil være gjenstand for *eiendomsrett* på samme måte som bilder, møbler, vaskemaskiner og andre løsøregjenstander.” [354]

Data som ”gjenstand/ting” er på nivå med de nevnte eksemplarene, som altså er undergitt eiendomsrett selv om åndsverket de bærer ikke er det. Det er også klart at man i opphavsretten anser *datafiler* som *eksemplarer*, på linje med fysiske bærere. Da faller de i kategorien ”middelbare eksemplar”. Jeg viser nok en gang til *Rognstad*, som sier at de ”middelbare eksemplar” er

> ”eksemplar der verksinnholdet ikke kan iakttas umiddelbart (slik tilfellet er for bøker og andre trykksaker, malerier, skulpturer, brukskunst, bygningskunst etc.), men der det kreves en innretning i form av avspillingsutstyr e.l. for å ta del i verket. Denne – helt selvsagte – presiseringen klargjør at fysiske bærere som CDer og DVDer omfattes av åndsverklovens eksemplarbegrep. Men det gir også

Han mener altså at personopplysninger ikke er gjenstand for eiendomsrett, dvs. at han uttrykker en oppfatning om innholdet, ikke om mediet. Det samme gjør *Udsen* (2009) s. 71-73, som behandler spørsmålet om eiendomsrett til åndsverk og personopplysinger, og naturlig nok, konkluderer med at de ikke kan eies.

[353] *Rognstad* (2009) s. 35. Det å kalle åndsverket ”immaterielt” er farlig språkbruk, fordi det etter rådende teori anses som en fiksjon. Men det står fast at åndsverket ikke er en fysisk størrelse, og i teorien reflekteres tanken om at eksemplarene og verket befinner seg på forskjellige nivåer, noe sitatet av *Rognstad* viser. Se også *Rognstad* (2009) kapittel 3.1 og 6.1. Smlg. *Stuevold Lassen* (2009) s. 485-487.

[354] *Rognstad* (2009) s. 35.

> rom for å medta *elektroniske eksemplarer* i en datamaskin (herunder mobiltelefoner, mp3-spillere, etc.) under det samme eksemplarbegrepet."[355]

Det kan ikke trekkes direkte slutninger av de opphavsrettslige løsninger over i strafferetten. Men de viser jo at det er konseptuelt uproblematisk å skille mellom medium (data) og informasjon, og dette skillet legger jeg som sagt til grunn at gjelder innen strafferetten også, som et utgangspunkt for de rettslige vurderingene. De strafferettslige reglene behandler ikke data og informasjon likt, og derfor må det i hvert tilfelle undersøkes hva loven mener når man er inne på spørsmål om vern eller inngrep mot disse godene.

Jeg har med dette etablert det *teoretiske utgangspunktet* for at man ved spørsmålet om eiendomsrett må konsentrere seg om datafilen, og se bort fra rettighetene til innholdet. Det utelukker ikke at det i annen sammenheng kan være hensiktsmessig å behandle data og informasjon under ett, noe jeg redegjør for i kapittel 8.2. Men i strafferetten kan det bære galt av sted.

Til slutt bør det nevnes at "eksemplar" er et begrep som har vesentlig betydning i opphavsretten, men det er ikke er et strafferettslig begrep. Dette er det viktig å ha med seg ved inndragning av dublettene som "ting", som drøftes i del V, og jeg kommer spesielt tilbake til det i kapittel 11.3.4. Innen strafferetten gjelder fortolkningen hele tiden begrepene "gjenstand/ting".

7.4 Spesifisering, konkretisering og kontroll

7.4.1 Kriterier som følger av handlingen beskrevet i lovbestemmelsene

Objektet må være av en slik art at det kan utsettes for den handling som lovbestemmelsene beskriver. *Straffebudene* beskriver handlinger rettet mot individualiserbare objekter, jf. borttar, tilegner seg, bruker/forføyer eller beskadiger en "gjenstand". *Beslag og inndragning* går ut på å frata lovbryteren rådigheten over objektet. Den permanente løsningen for objekter uten legal verdi, er at de destrueres. For data betyr det at de slettes.

[355] *Rognstad* (2009) s. 152.

Alle bestemmelsene forutsetter at objektet kan *spesifiseres* i de beslutninger som det gjøres bruk av i rettshåndhevelsen. Det mest presise spesifikasjonskravet finnes nok i strpl. § 207 første ledd som sier at ”beslaglagte ting skal opptegnes nøyaktig og merkes på en slik måte at forveksling unngås.” Videre gjelder det spesifikasjonskrav for det faktiske grunnlaget i tiltalebeslutning, dom og forelegg.[356] Beslutningene skal vise hva saken gjelder og hva som konkret omfattes av beslutningen.[357] For spesifikasjonen av datafilene i inndragningsbeslutningen, viser jeg til fremstillingen i kapittel 5.5, hvor det fremgår at det kan gjøres helt presist. Det kan gjøres på tilsvarende vis i de øvrige beslutningene.

For unike objekter, for eksempel verdigjenstander som malerier og smykker, eller biler som er registrert med unike kjennetegn, er spesifikasjonen tilstrekkelig. For andre objekter kreves en nærmere *konkretisering*, for eksempel med verdi- og mengdeangivelser.[358] Med hensyn til pengesedler må det kreves opplysning om beløp, mens andre objekter kan spesifiseres ved antall, kilo, liter eller kubikkmeter (for eksempel antall spritflasker, eller kilo hasjisj). Også dette kan gjøres for datafiler, ved angivelse av antall, mengde *bytes,* og andre opplysninger som jeg har redegjort for i kapittel 3.3.2 og 3.3.3. Data lar seg med andre ord *konkretisere.*

Spesifikasjon og konkretisering er relatert til *kontroll*. Dersom objektet ikke kan kontrolleres kan det ikke kan utsettes for de handlinger som bestemmelsene gir anvisning på, og heller ikke eies. Den frie luft kan ikke spesifiseres og konkretiseres på noen meningsfylt måte i forhold til bestemmelsene, og kan heller ikke eies, så her svikter begge forutsetningene for å være ”gjenstand/ting”. Det er annerledes for luft på flaske, for eksempel dykkerflasker. Da er

[356] Strpl. § 252 nr. 4 som sier at tiltalebeslutningen skal inneholde ”en kort, men så vidt mulig nøyaktig beskrivelse av det forhold tiltalen gjelder”, smlg. strpl. § 256 nr. 4 om forelegg. Se strpl. § 38 om kravene til en dom.

[357] Det er et eget spørsmål hvor detaljert lovens spesifikasjons- og konkretiseringskrav er. Spørsmålet ble drøftet i Rt. 1997 s. 266 i forhold til et krav om utlevering av dokumenter i medhold av utleveringsregelen i strpl. § 210, som gjelder ”ting”. Høyesterett fastslo at det gjaldt krav til spesifisering og konkretisering, og at detaljeringsnivået måtte fortolkes i lys av formålet, dvs. slik at den som skal etterkomme kravet har mulighet for å vite hva han skal framlegge. Konklusjonen var at opplysningene måtte være slik at ”adressaten … med rimelighet kan finne frem dokumentet”, s. 268. Smlg. argumentasjonen i Rt. 1999 s. 1944, hvor påtalemyndigheten fikk medhold i at opplysning om IP-adresse og tidspunkt var tilstrekkelig presisering og konkretisering til at Telenor (internettilbyder) måtte utlevere opplysning om telefonnummer brukt ved internettoppkobling. Løsningen ble fulgt opp i Rt. 2000 s. 169. Disse sakene gjelder utleveringsplikten etter ekomloven § 2-9 (tidligere teleloven § 9-3), men prinsippet for å bestemme hvor spesifikk opplysningen som gis må være, må bli det samme som for utlevering etter straffeprosessloven. Krav om utlevering av større dokumentbeslag reiser egne problemer, fordi det kan være vanskelig på forhånd å spesifisere konkret hvilke dokumenter som er relevant for etterforskingen. Se Rt. 1986 s. 1149 og Metodekontrollutvalgets redegjørelse i NOU 2009: 15 s. 212.

[358] For sedler nevner *Dyrnes* også at det kan være verdt å notere serienummer, for å vite når de var i omløp. *Dyrnes* (2004) s. 180.

luften under kontroll, og kan borttas dersom den først er gjenstand. Som alt nevnt anses gass for å være omfattet av gjenstandsbegrepet.

Kontroll kan være en aktiv handling (man kontrollerer et objekt) eller en passiv tilstand (et objekt er under kontroll). Med tanke på objektet er spørsmålet om det er brakt under kontroll. Dersom det er ukontrollert faller det utenfor gjenstandsbegrepet, men hvis det først er kontrollert, er det gjenstand. Mange objekter finnes både i ukontrollert og kontrollert form, for eksempel vann i naturen kontra vann i et damanlegg, energi generelt kontra strøm i kabel, og gass som naturforekomst kontra gass per kubikkmeter. Det kan derfor ikke sies generelt at energi er gjenstand; det er *kontrollert* energi som er gjenstand.

Konklusjonen er at "gjenstand/ting" forutsetter at objektet kan *spesifiseres* og om nødvendig, *konkretiseres* i form av verdi- eller mengdekriterier. Objekter som er ukontrollerbare i fri tilstand, kan oppfylle vilkårene dersom de bringes over i en tilstand hvor de kontrolleres. *Kontrollmuligheten* synes derfor å være viktigere enn hva objekter *er* etter naturvitenskapelige kriterier, for eksempel om det er fast, flytende eller gass. Det samme må gjelde om godet består av atomer eller *bits* fordi begrepene er teknologinøytrale i vid forstand.[359] Dette fremgår både av den brede gruppen goder som inngår i begrepene "gjenstand/ting" og av de kriteriene som nettopp er gjennomgått. Det fremstår ikke som problematisk å henføre data som gode betraktet inn under begrepene.

7.4.2 Eiervilkåret

Neste spørsmål gjelder betydningen av vilkåret om at objektet må kunne eies. Eiendomsretten har to sider, kalt de positive og negative eierbeføyelsene.[360] De positive eierbeføyelsene omfatter retten til å bruke og forføye over objektet både faktisk og rettslig. Straffebudene om tyveri, underslag, ulovlig bruk og skadeverk, verner om de positive eierbeføyelsene (borttakelse, tilegnelse, bruk/forføyning, beskadigelse av "gjenstand"). Forutsetningen er at gjenstanden "tilhører en annen", fordi man ikke skal kunne straffes for å ha foretatt disse

[359] Se kapittel 6.4.1.
[360] *Falkanger* (2007) s. 41.

handlingene mot sitt eget objekt.[361] Som eier kan man nettopp behandle objektet slik man vil, også ødelegge objektet og la det gå til grunne.[362]

Et annet spørsmål er om eiervilkåret kan tilføre beskrivelsen av objektet noe mer enn at det må kunne individualiseres og konkretiseres, slik jeg alt har vært inne på. Her synes de *negative* eierbeføyelsene å utgjøre et supplement. Retten til å nekte andre å utnytte objektet innebærer at objektet etter sin art må kunne kontrolleres slik at andre bare kan nyte det etter tillatelse fra eieren. Man må altså kunne ekskludere andre fra bruken, dersom man ikke ønsker å tillate den. Kriteriene som kjennetegner ”gjenstand/ting” blir altså de samme enten man tar utgangspunkt i *handlingen* beskrevet i bestemmelsen, eller i *eiendomskriteriet*. Det er tale om *spesifisering, konkretisering og kontroll*.

Dermed leder ikke eiendomskriteriet til at det som utgangspunkt må antas å være noe problem å henføre data under ”gjenstand” i de nevnte straffebudene. Hvorvidt det er noe spesielt med data som problematiserer denne vurderingen, for eksempel om evnen til å generere dubletter har betydning for eiendomsretten, tar jeg opp i kapittel 7.5.

Med hensyn til *beslag og inndragning* (”ting”) er det tradisjonelle utgangspunktet at inngrepet anses å ramme eiendomsretten.[363] Beslag skjer ved borttakelse, et inngrep som overfor fysiske objekter korresponderer med den objektive gjerningsbeskrivelsen i tyveribestemmelsen. Den permanente berøvelsen av eierrådigheten (inndragning) gjennomføres ved salg til inntekt for statskassen eller skadelidte, eller destruksjon dersom objektet ikke har noen lovlig omsetningsverdi.[364] Disse handlingene korresponderer med ulovlig forføyning og skadeverk. *Spesifikasjons- og konkretiseringskriteriene* er de samme som for straffebestemmelsene. Videre forutsetter både beslag og inndragning at objektet bringes under politiets *kontroll*, dvs. at lovbryteren fratas den faktiske rådigheten over objektet.

For *beslag* er situasjonen noe mer komplisert, noe som skyldes at inngrepet både kan foretas for å sikre bevis, og for å sikre et krav på inndragning. Dersom inndragning er det endelige

[361] Forståelsen av vilkåret ”tilhører en annen” ble drøftet i Rt. 2008 s. 1582, med hensyn til beløp som var feilinnbetalt på konto. Høyesterett fant at eiendomsretten til beløpet ikke hadde gått over til kontoeier i kraft av overføringen.
[362] Det ses bort fra at en mengde offentligrettslige regler modifiserer denne posisjonen, f.eks. for retten til å foreta bygningsendringer, vern om fredete bygninger, plikter overfor dyr man eier osv.
[363] Se kapittel 6.2.
[364] Se kapittel 5.6.

formålet med beslaget, er det klart at lovbryteren må fratas rådigheten over tingen. For *data* betyr det at dersom man ikke kan frata rådigheten ved å beslaglegge det fysiske datautstyret, må dataene slettes hos lovbryteren. Det gjelder for eksempel overgrepsbilder funnet på en bedriftsserver.[365]

Hvis derimot *bevissikring* er formålet, jf. strpl. § 203 første ledd første punktum om at ting som "antas å ha betydning som bevis, kan beslaglegges", oppstår det en situasjon som er spesiell for data, fordi bevissikringen kan skje ved å ta en kopi. Det betyr at lovbryteren beholder de opprinnelige dataene. Ved kopieringen sikrer politiet seg de *opplysningene* som ligger i dataene. En annen sak er at bevisforspillelseshensyn kan tilsi at det også er nødvendig å frata lovbryteren *rådigheten over dataene*, fordi vedkommende ellers kan tilpasse forklaringen nokså nøye i forhold til de opplysningene han vet at politiet har skaffet seg. I så fall må politiet også ta med datautstyret eller stenge tilgangen til brukerområdet. Effektiv sletting av dataene er i hvert fall utelukket før det eventuelt er truffet en rettskraftig beslutning om det.[366]

I tillegg brukes "beslag" om opplysninger som utleveres fra tredjemann i henhold til utleveringspålegg, jf. strpl. § 210 flg., og postbeslag, jf. strpl. § 211. I Rt. 1992 s. 904 som gjaldt utlevering med påfølgende beslag i Televerkets utskrift av trafikkdata registrert til og fra siktedes mobilnummer, sa Høyesterett at:

> "Bestemmelsene i straffeprosessloven kap 16 om beslag og utlevering av ting som antas å ha betydning som bevis, er av generell karakter. Beslagsadgangen og utleveringsplikten omfatter ikke bare legemlige gjenstander, men også opplysninger som lagres på data og som i tilfelle må gjøres tilgjengelige ved utskrifter, som f eks opplysninger om bankkonti. Begrensninger i lovens alminnelige adgang til beslag og krav om utlevering, ut over det som er fastsatt i straffeprosessloven, krever særskilt hjemmel." (s. 906).

Denne lovforståelsen er lagt til grunn senere.[367] Avgjørelsen viser for det første at beslagsadgangen *ikke* er begrenset til *legemlige* objekter, her omfattet den opplysninger, dvs. informasjon. For det annet indikerer den at karakteristikken av beslag som et inngrep i

[365] Loven gir som kjent også anvisning på inndragning av rettigheter, og dermed kan man i resultatet oppnå det samme, nemlig utestenge lovbryteren fra vedkommendes egne data, ved å inndra retten til et brukerområde.
[366] En mulighet er å slette dataene hos lovbryteren etter at de er sikret av politiet ved kopiering. Da kan de om nødvendig tilbakeleveres på et senere tidspunkt.
[367] Rt. 1992 s. 928; Rt. 1997 s. 470; Rt. 1998 s. 309; RG 1998 s. 1155; RG 2008 s. 1477 (epostkjennelsen).

eiendomsretten er utsatt for et visst press, fordi beslagshjemmelen ble ansett å være anvendelig på ”ting” som etter sin art *ikke* kan eies, nemlig opplysninger (informasjon). Presset skyldes at de historiske betingelser for beslag har endret seg. Teknologiutviklingen har gjort det mulig å rette inngrep både mot data og opplysninger som objekter i seg selv, og samfunnsutviklingen mer generelt har ledet til at innhenting av opplysninger fra tjenesteytere innen ekom- og finanssektoren, er blitt meget viktige etterforskingsskritt. Selv om beslagshjemmelen anses å være anvendelig, må *opplysninger* sies å være av en ganske annen karakter som objekt betraktet enn de fysiske, og de er ikke undergitt eiendomsrett.[368]

Politiets praksis med å ta beslag i data ved kopiering synes derfor ikke umiddelbart å representere noe inngrep i eiendomsretten. Lovbryteren har jo fremdeles sine data og kan utøve sine eierbeføyelser over dem. Dermed er det et spørsmål om lovens vilkår om at beslaget må gjelde ”ting”, er oppfylt.

I *amerikansk teori* har man påpekt at denne form for beslag likevel kan anses som et inngrep i eiendomsretten. Kopieringen leder nemlig til at man berøver lovbryteren muligheten til å endre eller slette dataene med virkning for omverdenen. Selv om det kan gjøres etter beslaget, har det ingen hensikt, fordi politiet ved sin handling effektivt og sikkert har ”frosset” datasituasjonen på beslagstidspunktet. Under eiendomsretten hører retten til å behandle objektet slik man vil, også retten til å bestemme om man vil eksponere det for andre, eller ødelegge det slik at ikke andre får tilgang til det. Dermed er konklusjonen at beslaget antakelig kan anses som et inngrep i eiendomsretten. [369]

Jeg legger ikke med dette til grunn at det norske eiendomsrettsbegrepet nødvendigvis er likt det amerikanske. Men den amerikanske analysen følger det samme rettighetsskjemaet som norsk rett, dvs. et sett av positive og negative beføyelser (”a bundle of rights”). I henhold til det norske begrepsapparatet kan kopieringen derfor anses som et inngrep i de positive eierbeføyelsene, nemlig i retten til å råde over og slette dataene med virkning for omverdenen.

[368] Med rettsinformatikkens begreper er opplysninger som utleveres av tredjeperson *fleksibel informasjon,* mens objekter er *integrert informasjon* og faller som sådan utenfor det egentlige informasjonsbegrepet. Se kapittel 4.4 og *Udsen* (2009) s. 40.

[369] I amerikansk rett har *Ohm* (2005) reist spørsmålet i forhold til fjerde tillegg til konstitusjonen (”Fourth Amendment”), som blant annet beskytter mot inngrep i private eiendeler (”seizure”). Jeg har sitert bestemmelsen i kapittel 5.5. *Ohms* syn er at inngrepet rammer eiendomsretten, slik at det foreligger ”seizure” (beslag) ved kopieringen. Se også *Kerr* (2006) s. 316 med videre henvisninger.

Som en oppsummering så langt, har det fremgått at spesifikasjon, konkretisering og kontroll er vesentlig enten man analyserer handlingen som er beskrevet i lovbestemmelsen (både straffebudene og inngrepsbestemmelsene), eller tar utgangspunkt i vilkåret om eiendomsrett. Vi har også sett at det i utgangspunktet er rimelig å anta at data oppfyller vilkårene. Det må påvises spesielle omstendigheter dersom det skulle vise seg likevel ikke å være tilfelle. I det følgende ser jeg nærmere på spørsmålet om eiendomsretten til data.

7.5 Eiendomsrett til data

Siden "gjenstand/ting" omfatter objekter som kan eies, skal jeg drøfte hva det vil si å kunne utøve eierbeføyelser over data. Jeg kan ikke se at spørsmålet har vært behandlet i forbindelse med forarbeidenes uttalelse om at "informasjon i datasystemer" ikke skal regnes som gjenstand.[370] Eiendomsretten er imidlertid en forutsetning for anvendelsen både av de straffebud og de inngrep som avhandlingen drøfter. Det har betydning for adgangen til automatisert inndragning fordi inndragning ikke kan brukes mot eierløse objekter.[371] Spesielt med tanke på datafilene på internett er det derfor behov for å konkretisere grunnlaget for eiendomsretten, slik at man kan ta stilling til om man generelt kan gå ut fra at vilkåret er oppfylt med tanke på de dubletter som det er tale om å inndra.

Når det er sagt, må det tilføyes at Høyesterett har gitt uttrykk for en viss skepsis overfor vekten av eiendomsrettslige betraktninger ved fortolkningen av straffebud som er satt til vern om eiendomsretten.[372] I tillegg har jeg påvist at *beslag* er utsatt for et visst press i forhold til å arte seg som et inngrep i eiendomsretten, siden det anvendes som tvangsmiddel for å skaffe informasjon.[373] Det tyder på at man ikke nødvendigvis skal forstå vilkåret helt kategorisk.

Jeg tar utgangspunkt i at data kan *spesifiseres, konkretiseres og kontrolleres*. Muligheten for å kontrollere data bør utdypes. Data kan som en del andre goder foreligge både i kontrollert og ukontrollert form. De data avhandlingen først og fremst interesserer seg for er dubletter av

[370] Se kapittel 6.2.
[371] *Matningsdal* (1987) s. 297 nevner at politiet som andre, kan okkupere eierløse objekter (derelinkvert gods). Men dette er som jeg kommer til, neppe et praktisk grunnlag for inngrep på internett.
[372] Uttalelsen falt i en sak om underslag av feilinnbetalt beløp til bankkonto i Rt. 2008 s. 1582. Førstvoterende uttalte med tilslutning fra de øvrige dommerne: "Etter mitt syn strider det mot alminnelig språkbruk å anse penger som ved en feil er overført til en bankkonto, for å tilhøre kontoinnehaveren. Jeg slutter meg til lagmannsretten når den påpeker at «…'eiendomsrett' ikke er noe entydig begrep. Det er sammensatt og omfatter forskjelligartede beføyelser og rettsvirkninger. Begrepet som sådan er da ikke vel egnet til å fastslå innholdet i straffeloven § 255»". (avsn. 16).
[373] Se kapittel 7.4.2.

datafiler som er inndratt, ”svartelistet” og tildelt en unik identitet. Dublettene kan gjenkjennes av filtrene i nettet og blokkeres. Fra et rettshåndhevelsessynspunkt kan de derfor kontrolleres. Men spørsmålet er om dublettene er undergitt eiendomsrett når de finnes på nettet, slik at blokkeringen arter seg som et inngrep i eiendomsretten.

Siden eiendomsretten er en ”restrett” behøver man ikke nødvendigvis å kunne utøve et komplett sett av eierbeføyelser. For data er begrensninger gjerne knyttet til *innholdet*, for eksempel opphavsrettigheter som er til hinder for fri kopiering av musikkfiler. For overgrepsbilder er denne begrensningen særlig tydelig, siden det gjelder et totalforbud mot befatning med datafilen. Men som tidligere nevnt er ikke slike begrensninger til hinder for å ha eiendomsrett i formell rettslig forstand, den er bare lite eller ingenting verdt.[374]

I et mer generelt perspektiv kan det kanskje reises spørsmål ved om data som er elektroniske signaler, har det preg av å være ”formuesgode” som er eiendomsrettens objekt og formål. Det kan innvendes at data ikke har noen egenverdi, fordi verdien ligger i informasjonen. Men det gjelder ikke bare data, verken papiret i en bok eller plastskiven til en DVD-film har en økonomisk verdi av betydning. De er likevel objekter som kan eies. Dessuten kan argumentet snus rundt, ved å fremholde at data som andre medier er av *uvurderlig verdi* for omsetning og tilgjengeliggjøring av innhold, så i realiteten er informasjonen lite verdt uten mediet. Data kan ses som en innsatsfaktor for produksjon og utnyttelse av informasjon, og er i den forstand et formuesobjekt.[375]

Det skilles mellom tre former for etablering av eiendomsrett, nemlig originære, derivative og ekstinktive erverv. Jeg avgrenser mot de ekstinktive erverv som gjelder spørsmål om konkurrerende eiendomsrett til et objekt, fordi at da er eiendomsretten alt etablert. Jeg tar bare opp spørsmålet om hva som skal til for å få og utøve eiendomsrett til data.

Originære erverv er okkupasjon og produksjon. *Okkupasjon* innebærer total overtakelse av et eierløst objekt. Overfor data som er lagret i nettet lar det seg vanskelig gjøre uten å overta kontrollen med vertsmaskinen. I stedet for okkupasjon skjer *erverv av en kopi* ved nedlasting av data som er tilgjengeliggjort på et nettsted, og da taler vi om derivativt erverv (se

[374] Se kapittel 5.8 hvor det er konstatert at inndragning kan brukes også overfor ting uten legal verdi.
[375] En annen sak er at det koster lite *å spre* data, noe spamproblemet er et tydelig uttrykk for, se NOU 2007: 2 kapittel 3 s. 34 og s. 36 flg., om phishing og spam.

nedenfor). Et annet spørsmål er om data kan okkuperes mens de er under overføring. Igjen blir det spørsmål om total overtakelse. Det betyr at man må plassere seg som en falsk kommunikasjonspart ("stjele" en IP-adresse).[376] Dette virker lite praktisk og man har heller ingen måte å avgjøre om dataene er eierløse i utgangspunktet. Som jeg kommer til må utgangspunktet snarere være det motsatte, nemlig at det må presumeres å herske eierrådighet til dataene på nettet. Jeg ser derfor bort fra okkupasjon av data i nettet som grunnlag for eiendomsrett.

Produksjon er derimot en meget praktisk atkomstmåte til data. Under forutsetning om at det er tale om data som selvstendig objekt uavhengig av lagringsmediet, kan bare *førstegangsproduksjon* være produksjon i eiendomsrettslig betydning, dvs. den som tar et overgrepsbilde eller lager et skadelig dataprogram. Dubletter er kopier hvor eiendomsretten må bygge på derivativt grunnlag.[377]

Derivativt erverv innebærer overdragelse av eiendomsrett til et objekt. Siden data ikke kan forflyttes, forblir overdragerens kildedata under vedkommendes eierrådighet. Det overdrageren kan overføre er *eiendomsretten til en dublett* (dvs. en kopi av kildedataene). Det kan gjøres overfor stadig nye erververe.

Derivativt erverv ved nedlasting av data er vanlig på nettet. Tilgjengeliggjøringen i nettet innebærer ikke oppgivelse av eiendomsretten til kildedataene, men eieren må ta stilling til om det skal gis mulighet for fri nedlasting og utnyttelse av dublettene, om det skal forlanges vederlag i form av betaling eller bytte, eller settes andre avtalerettslige restriksjoner på utnyttelsen.[378]

Eieren kan også for eksempel legge opp tjenesten slik at dataene bare kan beskues ved *streaming*. Da er det innholdet (informasjonsleveransen) som er det vesentlige, og det skjer

[376] Dette kalles IP-spoofing, og kan være et såkalt "man i in the middle" angrep.
[377] Kopiering av CD- og DVD-plater med digitalt innhold holder jeg utenfor. Smlg. fortolkningen av produksjonsalternativet i strl. 2005 §§ 69 bokstav a, § 201 og § 311 bokstav a, i kapittel 5.3.2.2. Smlg. også grunnlaget for inndragning av dubletter på grunnlag av én dataidentitet, i kapittel 11.
[378] Se *Rognstad* (2009) s. 365; og *Rognstad* (2008), særlig på s. 532 flg. om begrensninger til å utnytte åndsverk som er lagt tilgjengelige på nettet. *Rognstad* mener at man ikke kan ta som utgangspunkt at tilgjengeliggjøring er samtykke til fri utnyttelse. Utnyttelsesretten som følger av tilgjengeliggjøringen må fastlegges ved en fortolkning ut fra avtale- og tingsrettslige regler, samt av situasjonen som sådan. I det siste ligger at internett er et annet miljø enn det fysiske, som skaper sin egen kontekst som også influerer på hvilke rettslige slutninger man kan trekke av at verket er tilgjengeliggjort. Ifølge *Rognstad* må det kreves særlig klare holdepunkter for å kunne legge til grunn at det er samtykket til fri kommersiell utnyttelse av det tilgjengeliggjorte verket.

ingen varig nedlasting eller erverv av eiendomsrett til dataene.[379] Eieren kan altså beholde kontroll mot spredning ved å bruke en teknisk beskyttelse som tillater fremføring, men hindrer nedlasting.

Dersom eieren tilbyr nedlasting av dataene, erverves eiendomsrett til dubletten. Det fortrenger ikke innehaverens eiendomsrett til kildedataene. Eiendomsretten til dubletten oppstår hos erververen fordi anskaffelsen er lovlig og kopien bringes under vedkommendes kontroll. Dersom data ligger fritt tilgjengelig kan enhver erverve dem ved nedlasting. Eieren har ikke dermed oppgitt eiendomsretten til kildedataene, men kan ha forskjellige grunner til å unnlate å kreve vederlag for dublettene som lastes ned. For eksempel kan en inntekt alt være oppnådd gjennom reklamebannere på nettstedet. I andre tilfeller kan innehaveren være interessert i størst mulig spredning, kanskje av et religiøst eller politisk budskap, og ønsker ikke at et vederlagskrav skal være til hinder for det.

En annen sak er at det kan være vanskelig på nettet å henføre data til en bestemt eier, noe som skyldes gode muligheter for anonymitet.[380] Men anonymitet i seg selv er ikke ensbetydende med at en datafil på nettet er eierløs. Også med tanke på illegalt gods i fysisk form (sprit, narkotika) vil eieren gjerne forsøke å holde seg anonym. Hvorvidt man reelt sett er anonym på nettet avhenger av mange omstendigheter, blant annet hvilken ressursbruk politiet skal sette inn på å analysere elektroniske spor, og innhente og utveksle opplysninger i internasjonalt politisamarbeid m.v., for å bli ført tilbake til en kilde som er eier. Videre er det klart at dersom man hadde brakt kildens identitet på det rene, ville man også tillagt vedkommende eiendomsretten til den meldingen som vedkommende postet. Det betyr at man ikke enkelt kan oppgi eiendomsretten til meldinger på nettet, noe som har gode grunner for seg med tanke på

[379] Smlg. *Frost* (2002) om filbaserte og adgangsbaserte informasjonsytelser, s. 64-68. Om adgangsbaserte ytelser skriver han: “Det karakteristiske for den adgangsbaserede digitale ydelse er således at informationsindholdet *fremføres for brugeren* […] Det centrale er imidlertid, at brugeren ikke opnår verken en *faktisk* eller en *retlig råden* over selve den ydelse, der udgør formålet for den konkrete *fremføringstjeneste.* Det er alene ydelsens *informative element,* der kan rådes over, og da kun med respekt af eventuelle immaterielle begrænsninger.” (s. 67-68).

[380] Internettets anonyme karakter er et moment som ble vektlagt av EMD i *K.U.* (2008). Saken gjaldt statens positive forpliktelse til å sikre privatliv etter EMK art. 8, i dette tilfelle ved å sørge for at loven ikke gjør teletilbydernes taushetsplikt så absolutt at den hindrer oppklaring av krenkelser begått på internett. EMD sa at ”it was well-known that the Internet, precisely because of its anonymous character could be used for criminal purposes” (avsn. 48). Finland ble dømt for overtredelse av EMK art. 8. Men det er selvsagt også slik at anonyme tjenester kan brukes for å poste lovlig innhold.

muligheten for å utøve rettshåndhevelse i form av automatisert inndragning. Det er åpenbart uheldig om inngrepet avskjæres fordi eiendomsretten presumeres å være oppgitt.[381]

Jeg tror derfor det må tas utgangspunkt i at førstegangs tilgjengeliggjøring på nettet skjedde av en person som hadde eierrådighet over datafilen. Anonym tilgjengeliggjøring kan forstås som et samtykke til at andre erverver dublettene. Det betyr at både den opprinnelige innehaveren (som er anonym) og erververne, er eiere av datafilene (dublettene). Både den lovbryter som får inndragningskravet rettet mot seg i straffesaken, og de som utsettes for fullbyrdingen i nettet, er derfor – på generelt grunnlag – å anse som eiere av datafilene. Løsningen gir også en klar ansvarsplassering for tilgjengeliggjøring av innhold på nettet, noe som er i samsvar med de regler som er utviklet for tilbydernes ansvarsfrihet for innhold på nettet, jf. ehl. §§ 15-18.

7.6 Kravet til legemlighet

7.6.1 Problemstilling

Konklusjonen i det foregående er at data oppfyller de generelle kriteriene som ligger til grunn for "gjenstand/ting". Disse kriteriene er utledet av ordlyden i de aktuelle bestemmelsene. "Legemlighet" var ikke blant de kriterier som ble identifisert. Dette har likevel vært oppstilt som et kriterium for å være "gjenstand". Det behøver ikke nødvendigvis å være et problem i forhold til data, fordi de elektroniske signalene er fysiske fenomener, og kan således sies å ha en "legemlig" representasjon.[382] På den annen side har data vært oppfattet som noe "uhåndgripelig" og da har man et problem i forhold til legemlighet. I dette kapitlet drøfter jeg kravet til legemlighet.

[381] Se også Personvernkommisjonen om retten til å være anonym, NOU 2009:1 kapittel 13.3.8. Kommisjonen sier at det er "viktig for personvern i mediene at den omtalte til enhver tid har et ansvarssubjekt som kan kontaktes for å få løst personvernkrenkelser i minnelighet, eller som kan gjøres strafferettslig eller sivilrettslig ansvarlig dersom krenkelsen ikke kan løses på annen måte." Her synes kommisjonen å benytte ordet "ansvarssubjekt" om det som i realiteten bare kan være et kontaktorgan for klager. Skadevolder er ansvarlig og EMD har uttrykkelig avvist at en kompensasjonsordning fra tredjeperson er tilstrekkelig som substitutt for strafforfølgning, se *K.U.* (2008) pkt. 47. Tilsvarende kan man tenke om eiendomsrett på nettet. Noen eier datafilen selv om man ikke vil vedkjenne seg eierskapet. Myndighetene kan etablere ordninger som reduserer ofrenes problemer på grunn av anonymiteten, med det fjerner verken ansvaret eller innehaverens eiendomsrett.
[382] Se kapittel 3.3.1.

7.6.2 Det historiske utgangspunktet

Forutsetningen om at gjenstandsbegrepet omfattet noe som var av legemlig karakter, kan spores til de tidligere omtalte Odelstingsforhandlingene i 1902, da man diskuterte den beste måten å gi elektrisitet strafferettslig vern. Problemet gjaldt å få bukt med ”tyvtapping” av strøm. Man støtte på problemer med å anse det som tyveri, underslag, eventuelt skadeverk, fordi man mente at gjenstandsbegrepet var begrenset til fysiske objekter, mens elektrisitet ikke var ”noget, som man kan tage og føle paa”.[383] Man viste til at objektet måtte kunne foreligge i en av de tre aggregattilstander, dvs. fast, flytende eller gass.[384]

Siden elektrisitet ikke oppfylte disse kriteriene, gjorde lovgiverne noe som i ettertid må sies å være ganske interessant: Med bestemmelsen i strl. 1902 § 6 inkluderte man elektrisitet i gjenstandsbegrepet samtidig som man passet på å holde energi ”frit i naturen” utenfor.[385] Det ble gjort ved å oppstille vilkår om at kraften måtte være ”fremstillet” eller ”opbevaret”, jf. strl. 1902 som lyder:

> ”Under Udtrykket Løsøregjenstand indbefattes i denne Lov ogsaa enhver til Frembringelse af Lys, Varme eller Bevægelse *fremstillet* eller *opbevaret* Kraft.” (min uth.).

Det betyr at bare energi som er produsert og kan overføres via kraftledninger eller lignende, er ”gjenstand”. Med ordene ”fremstillet” og ”opbevaret” sørget man i 1902 for *teknologinøytralitet i vid forstand*.[386] Lovgiver likestilte et ikke-legemlig objekt (energi) med legemlige objekter ved å inkludere vilkår som opphevde forskjellen mellom objektene. Dermed fjernet man den rettslige relevansen av at objektene var forskjellige i sin fundamentale karakter. Det som således følger av ordlyd og forarbeider er at elektrisitet er gjenstand, men bare hvis den er *kontrollert, kvantifisert og prissatt*. Enkelt sagt er det elektrisitet per kilowattime som omfattes av gjenstandsbegrepet. Dette følger også eksplisitt av forarbeidene fra 1902, hvor det sies at det er det ”aftalte kvantum” elektrisitet som er relevant.[387]

[383] Indst. O. I-1901/1902, s. 29. Forhandlinger i Odelstinget nr. 55 (1901-1902) s. 435.
[384] Indst. O. I (1901/1902), s. 29.
[385] Indst. O. I (1901-1902) s. 29-30. Energi finnes i alle ting. Definisjonsmessig er energi evnen til å utføre arbeid.
[386] Se kapittel 6.3, særlig 6.3.2.2.
[387] Forhandlinger i Odelstinget nr. 55 (1901-1902) s. 433.

Vilkårene ”fremstillet” og ”opbevaret” er nøkkelopplysninger for å forstå gjenstandsbegrepet. De indikerer at dersom objektet kan spesifiseres og kontrolleres er det å anse som gjenstand. Den språklig sett enklere formuleringen i strl. 2005 § 12 er ikke like opplysende på dette punkt, men i forarbeidene fremgår det at språkendringen ikke innebærer noen rettslig endring.[388]

Grunnen til at spesifikasjon og kontroll er viktige, er at bestemmelsens formål nettopp er å verne mot krenkelser av eiendomsretten. Lovgiverne har derfor ikke hatt til hensikt å avgrense gjenstandsbegrepet på en måte som medfører at objekter som etter sin art kan eies, faller utenfor det strafferettslige vern. Hvorvidt et objekt kan underkastes eiendomsrett beror mye på utviklingen i teknologien, så det må anses å være i samsvar med lovgivernes historiske utgangspunkt når et nytt gode som data anses som ”gjenstand”. På den annen side er den åpenbare innvendingen at dersom gjenstandsbegrepet skal forstås på denne måte, hadde det ikke vært nødvendig med presiseringen i strl. 1902 § 6 (strl. 2005 § 12).

Jeg tror en slik innvending er for enkel. I 1902 var det antakelig behov for presiseringen fordi elektrisitet var et nytt fenomen, og forskjellige teknologiske hjelpemidler var ikke som i dag, en alminnelig del av tilværelsen for de fleste. Men i dag fremstår bestemmelsen som en anakronisme. Man er vant til å bruke teknologi, og å betrakte det gode som derigjennom behandles, som sitt. Det synes derfor ikke å foreligge noe behov for å presisere at data er et objekt som kan eies. Det er noe man har en tilvant forestilling om og reflekteres i at det er vanlig å tale om ”sine” data, smlg. også strl. 2005 § 351 annet ledd som bruker uttrykket ”andres data”.

[388] Strl. 2005 § 12 lyder slik: ”Med gjenstand menes også elektrisk energi eller annen energi”, og ifølge opplysningene på s. 164 i Ot.prp. nr. 90 (2003-2004) viderefører bestemmelsen gjeldende rett. Dette må også få betydning for fortolkningen av alternativet ”eller annen energi” i strl. 2005 § 12. Ifølge forarbeidene omfatter det blant annet ”oppvarmingsenergi fra fjernvarmeanlegg” (Ot.prp. nr. 90 (2003-2004) s. 165). Hvis problemet man mener å regulere, gjelder uberettiget tilkobling til rørsystemet som legges ut fra slike anlegg, er energien i en form hvor man *har kontroll med leveransen*. Det er altså ikke energi i en ubestemt betydning som omfattes, men en leveranse av en målbar ytelse med økonomisk verdi. Dermed korresponderer forutsetningene for begge alternativene i strl. 2005 § 12, og det kan stilles spørsmål ved om det kunne vært innskrenket til ett noe mer generelt formulert alternativ.

7.6.3 Det funksjonelle gjenstandsbegrepet

I 1985 beskrev Straffelovrådet data som ”en serie et-tall og nuller” og som ”magnetiske impulser”.[389] Man sa blant annet at:

> ”Rent fysisk er lagrede data bare magnetiske impulser, og den informasjon dataene representerer, er selvsagt av utpreget immateriell karakter.”[390]

Beskrivelsen ble holdt opp mot et utgangspunkt om at det strafferettslige gjenstandsbegrepet krevde at objektet var av:

> ”fysisk beskaffenhet, slik at immaterielle objekter faller utenfor begrepet”.[391]

Dette ledet til at man mente at data falt utenom det strafferettslige gjenstandsbegrepet. Dermed fikk man et problem med det strafferettslige vernet for data, for eksempel mot skadeverk, hvor straffebudet verner en ”gjenstand”. Problemet ble løst ved å anvende læren om det funksjonelle gjenstandsbegrepet, som sørget for at data ble ansett som en del av en fysisk gjenstand, nemlig lagringsmediet. Dermed var kravet til legemlighet oppfylt.

Læren om det funksjonelle gjenstandsbegrepet går ut på at det objekt straffebudet verner, skal vurderes som *en helhet*. Læren er utledet av en kjennelse i Rt. 1930 s. 1005 (Damluke).[392] Domfelte hadde stengt en luke i et damanlegg med den følge at anlegget stoppet. Spørsmålet var om handlingen kunne anses som skadeverk, jf. strl. 1902 § 291. Forsvareren hadde innvendt at domfeltes forhold ikke innebar at han hadde ødelagt, beskadiget, ubrukbargjort eller forspilt noen gjenstand slik loven krevet. Høyesterett tok avstand fra en slik lovforståelse og sa:

> ”«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.”

[389] NOU 1985: 31 s. 8-9.
[390] NOU 1985: 31 s. 9.
[391] NOU 1985: 31 s. 9.
[392] Kjennelsen er ved en feil kalt ”dom” i avgjørelsens innledende opplysninger.

I utredningen om datakriminalitet fra 1985 viste Straffelovrådet til kjennelsen og sa at den ga uttrykk for "et funksjonelt syn" på begrepet "gjenstand". Selv om data isolert sett ikke var "gjenstand", nøt *lagrete* data likevel strafferettslig vern fordi de måtte ses i sammenheng med lagringsmediet. Begrunnelsen var at etter uberettiget endring eller sletting av data:

> "er lagringsmediet for eieren ikke det samme som før endringen eller slettingen".[393]

Dette synet ble gjentatt av Datakrimutvalget i den første delutredningen, men uten noen selvstendig vurdering av lærens holdbarhet eller formålstjenlighet for data.[394] Synspunktet ble imidlertid også gjentatt av departementet i siste lovproposisjon til straffeloven 2005. I redegjørelsen for gjeldende rett i de generelle motivene om skadeverk, står det at

> "Elektronisk lagret informasjon (data) er ikke en gjenstand, men endring og sletting av den vil som regel likevel være straffbart, fordi handlingene er skadeverk mot lagringsmediet, jf. Rt. 2004 side 1619."[395]

Som det fremgår bygger departementets syn på en uttalelse i Rt. 2004 s. 1619 (Bakdør) som jeg kommenterer nedenfor.

Det helhetlige syn på objektet som læren legger til grunn, innebærer at man kan slå ned på handlinger som setter objekter ut av funksjon, eller vesentlig forringer funksjonsdyktigheten, selv om de ikke er fysisk beskadiget og må repareres. Dermed kan hindringer bedømmes som skadeverk. I rettspraksis gir saker om stolper lagt over veibanen (Rt. 1966 s. 905), og endring av sporveksleren til trikken (Rt. 1986 s. 571), uttrykk for dette syn. I dataverdenen kan et overbelastningsangrep over nettet som midlertidig lammer det angrepne datasystem, anses på samme måte.[396] Strl. 1902 § 291 (skadeverk) har vært anvendt på slike tilfeller.[397]

[393] NOU 1985: 31 s. 10.
[394] NOU 2003: 27 kapittel 2.4 s. 17.
[395] Ot.prp. nr. 22 (2008-2009) kapittel 9.2.1 s. 303.
[396] Slike handlinger kalles Denial-of-Service, dvs. DOS-angrep (eller tjenestenektangrep). Se NOU 2007: 2 kapittel 3.4.9 s. 29. Straffeloven 2005 har en egen bestemmelse som rammer slike handlinger, nemlig fare for driftshindring i strl. 2005 § 206. Bestemmelsen lyder slik: "Med bot eller fengsel inntil 2 år straffes den som ved å overføre, skade, slette, forringe, endre, tilføye eller fjerne informasjon uberettiget volder fare for avbrudd eller vesentlig hindring av driften av et datasystem." Etter strl. 2005 § 206 er allerede farefremkallelsen en fullbyrdet forbrytelse, se begrunnelse i Ot.prp. nr. 22 (2008-2009) s. 63. Handlingene innebærer ikke fysiske skader eller direkte inngrep i datasystemet, men resulterer i funksjons- og driftshindring. Siden det blir satt ut av funksjon er handlingen skadeverk, jf. rettssetningen som kom til uttrykk i Damlukekjennelsen (Rt. 1930 s. 1005). Bestemmelsen supplerer den alminnelige skadeverksbestemmelsen i strl. 2005 § 351. Om forholdet mellom bestemmelsene, se Ot.prp. nr. 22 (2008-2009) kapittel 2.15, særlig departementets merknader i kapittel 2.1.5.5. s.

Selv om læren kan være hensiktsmessig for fysiske objekter, kan den vanskelig sies å gi vern om *data*. Det som følger av læren er at *datamaskinen* har beskyttelse mot skadeverk, selv om den ikke fysisk er beskadiget. En krenkelse av dataene rammer jo ikke datamaskinen fysisk sett. Men også her foreligger det to problemer.

For det første er ikke datamaskinen beskadiget dersom det innholdet som datamaskinen brukes til å behandle (de ”brukergenererte” data), er slettet. Det blir som å ødelegge bokser som oppbevares på et lager. Lageret er ikke ødelagt som følge av handlingen. Endring eller sletting av brukergenererte data, som for eksempel arbeidsnotater og utkast til phd-avhandlinger, rammer ikke datasystemet. Isolert sett kan verdien av lagringsmediet sies å ha økt på grunn av kapasiteten som er frigjort.[398] Da synes ikke læren om det funksjonelle gjenstandsbegrepet å begrunne hvorfor handlingen skulle anses som skadeverk. Siden det er foretatt en kanskje uopprettelig skadevoldende handling overfor dataene, er det mer naturlig å si at *dataene* er den ”gjenstand” som er rammet. De kan beskrives helt konkret, med henvisning til filnavn, hvor de var lagret m.v., så det fremgår at dataene var målet for handlingen, og hvilke data det gjaldt.

Derimot kan datamaskinen anses for å være beskadiget dersom operativsystemet er rammet. Da kan endring og sletting ha konsekvenser for datasystemets funksjonalitet. Ved endringer i operativsystemet, for eksempel ved å legge inn feilfunksjoner i form av ”logisk bombe”, er systemets funksjonalitet endret.[399] Men da er det naturlig å gå rett på sak, og si at datamaskinen er beskadiget, slik at den som ”gjenstand” har vært utsatt for skadeverk.[400]

---

62 flg. Strl. 2005 § 351 annet ledd bruker ”data”, også det et avvik fra strl. 2005 § 69 annet ledd (”elektronisk lagret informasjon”) og § 206 (”informasjon”)

[397] Ringerike herredsretts dom av 13. desember 2001, omtalt i *Sunde* (2006) s. 202-203, se også s. 69 om DOS-angrep; *Bing* (2008) kapittel 3.7 s. 53 flg.

[398] Synspunkt jeg også har fremført i *Sunde* (2006) kapittel 4.3 s. 101 flg.

[399] NOU 1985: 31 kapittel 4.3.1 s. 9 om logisk bombe. Se *Aquilina* (2008) s. 61, som omtaler en amerikansk sak fra 2008, hvor en systemadministrator (ansvarlig for datasystemet og har de mest omfattende privilegiene) ble dømt til fengsel i 30 måneder, for å ha lagt inn en ”logisk bombe” som hadde funksjonalitet for å slette ”critical data” på mer enn 70 servere. Logisk bombe er beskrevet som ”event-driven” ”malicious code”.

[400] Men også i slike tilfeller er det mulig å se dataprogrammet alene som beskadiget, nemlig hvis endringen utføres i et program i en database som brukes for oppdatering av datasystemer. Jeg har omtalt en slik sak i norsk rett, se *Sunde* (2006) s. 84, 194 og på 197-198, hvor en programmerer ble dømt for skadeverk for å ha gjort endringer i et dataprogram som ville gi ”45 avvik fra normalprosedyren i [dataprogrammet] fra og med årsskiftet 2001/2002” (RG 2003 s. 858). Programmet var foretakets produkt, som ble levert til en rekke andre bedrifter som var avhengige av jevnlige oppdateringer av programmet. På grunn av den uberettigete endringen som var lagt inn, kunne de andre systemene blitt oppdatert med den logiske bomben. Forholdet ble avdekket før feilen var blitt spredt til kundene.

Bakdørsaken (Rt. 2004 s. 1619) som departementet viste til i sin uttalelse om at data ikke var gjenstand, illustrerer de problemer som kan oppstå. De tiltalte hadde lagt inn "bakdører" og nye brukere, ved å foreta endringer i programoppsett og det administrative systemet. *Lagmannsretten* hadde frifunnet for tiltalepunktet om skadeverk, og vist til at endringene:

> "ikke innebærer noen endring i funksjonaliteten som andre brukere vil merke ved ordinær bruk av systemet" (sitert i høyesterettsavgjørelsen avsn. 25).

Handlingene hadde konsekvenser for "den tillit systemeieren har hatt til maskinene", men dette kunne ikke anses som "et kriterium for straffbarhet etter skadeverksbestemmelsen" (avsn. 26). Lagmannsretten tok altså funksjonalitetslæren på ordet, og vurderte om *datamaskinen* var å anse som beskadiget.

Lagmannsretten mente imidlertid at en endring som rammet sikkerheten på systemet uten at *brukerne* merket det, ikke var å anse som en skade. Lagmannsretten så derfor helt bort fra den interesse *eieren* av et datasystem har i at systemet er sikkert.[401] Det kan sammenlignes med ødeleggelse av en lås i en dør. Huset kan fint brukes, men man er ikke i særlig tvil om at det foreligger et skadeverk.

Høyesterett kom til at det forelå skadeverk, og viste til at:

> "det må ha vekt at det i lovforarbeider nå i snart 20 år er uttalt at straffelovens bestemmelser om skadeverk kan få anvendelse på uberettiget endring eller sletting av elektronisk lagrete data. Jeg legger også vekt på at det allerede i Rt-1930-1005 ble gitt uttrykk for et funksjonelt syn på skadeverksbestemmelsen" (avsn. 30).

Resultatet ble at handlingen skulle bedømmes som skadeverk, og *begrunnelsen* hvilte på at det var tilstrekkelig at handlingen hadde rammet dataene. Høyesterett gikk altså langt i å gi data selvstendig strafferettslig vern som gjenstand.

Høyesterett sa imidlertid også at "[d]ata er i seg selv ikke en «gjenstand»" (avsn. 27). Men uttalelsen fungerer bare som et utgangspunkt for resonnementet, og var ikke nødvendig for å

[401] Datakrimutvalgets slår fast at "Utgangspunktet er at eieren av datasystemet har rett til å bestemme hvem som skal benytte det og til å sette regler for bruken." NOU 2007: 2 kapittel 4.6.2 s. 52. Uttalelsen står i en redegjørelse for integritetshensynet, som et av de viktige sikkerhetskriterier for IKT (sammen med konfidensialitet, tilgjengelighet og uavviselighet).

begrunne resultatet. I realiteten reiste ikke saken spørsmålet om data var gjenstand, fordi datamaskinen var målet for den skadevoldende handlingen. Uttalelsen har derfor karakter av å være et *obiter dictum*, og har liten vekt.[402]

Det funksjonelle gjenstandsbegrepet kommer også til kort i den meget praktiske situasjon som gjelder *asymmetriske rettighetsforhold*. Læren tjener bare formålet dersom rettighetene til dataene og til lagringsmediet er på samme hånd. Det støttes av 1985-utredningen, hvor det sies at endring og sletting leder til at lagringsmediet *”for eieren”* ikke er det samme som før. Eierens situasjon blir imidlertid ikke påvirket uten at det er hans data som endres eller slettes. Dersom dataene tilhører en annen, er det jo den personen som rammes. Læren gir således ikke noe vern for data som er lagret hos en nettvert (web 2.0).[403] Eieren av serveren (nettverten) er ikke krenket selv om en av tjenestemottakerne har fått slettet sine data. Nettverten kan være krenket av et forutgående datainnbrudd på vertsmaskinen, men ikke av slettingen av dataene til tjenestemottakeren. Dermed strekker ikke det funksjonelle gjenstandsbegrepet til.

Læren gir heller ikke vern dersom eieren av dataene (tjenestemottakeren) utsettes for en krenkelse *begått av nettverten selv*, for eksempel i form av underslag (uberettiget kopiering) eller sletting av data. Det følger av vilkåret ”tilhører en annen”, som ikke er oppfylt siden nettverten eier vertsmaskinen.

Konklusjonen på denne drøftelsen er at bruken av det funksjonelle gjenstandsbegrepet fremstår som unødvendig (tidligere ville man kanskje benyttet uttrykket ”et kunstgrep”), for å gi data et direkte strafferettslig vern. I realiteten har det skjøvet spørsmålet om et strafferettslig vern for data ut av det rettslige synsfeltet. I stedet har man konsentrert seg om å etablere et strafferettslig vern for datamaskinen. Det er hensiktsmessig med tanke på å verne datamaskinen mot krenkelser, men det har ikke etablert et strafferettslig vern for data. Bruken av læren på datarelaterte spørsmål har heller ikke resultert i en klar rettstilstand som går ut på at data ikke har et selvstendig strafferettslig vern. Snarere synes rettskildene å trekke i retning

[402] *Eckhoff* (2001) s. 172 om obiter dicta. *Eckhoff* gir eksempler på at *obiter dicta* – ”uttalelser som ikke har vært nødvendige for å begrunne resultatet” – har blitt tillagt en viss vekt. Men utgangspunktet er at de har liten eller ingen vekt, fordi de nettopp ikke tjener som argument for det resultat eller den rettssetning som dommen uttrykker. I Rt. 2004 s. 1619 fremstår uttalelsen som et pliktmessig nikk til det strafferettslige tradisjonelle utgangspunktet for data, men representerer verken i argumentasjonen eller resultatet noen reell videreføring av dette syn. I de saker hvor *obiter dicta* tillegges vekt, representerer de nettopp noe nytt.. Det sier seg selv at såkalte ”mainstream” oppfatninger i *obiter dicta* ikke har synderlig rettskildemessig verdi.
[403] Se kapittel 3.3.5.

av at data behandles som selvstendig objekt. Problemet er bare at det stadig vises tilbake til en uttalelse fra 1985, uten at det foretas en selvstendig vurdering av synspunktets holdbarhet.

Bakdørsaken gir i realiteten støtte for at data har et selvstendig strafferettslig vern. Videre taler sterke reelle hensyn for en slik fortolkning, gitt det store behovet for vern ved asymmetriske rettighetsforhold.

7.6.4 Enkle fordringer

Rettsutviklingen for enkle fordringer viser at "gjenstand" ikke innebærer noe ubetinget krav til legemlighet. Slike fordringer er *abstrakte goder*, og de er ikke nevnt i strl. 1902 § 6 (smlg. 2005 § 12). Men fordi bruk av banktjenester er blitt et viktig og selvfølgelig samfunnstrekk, har det oppstått behov for å ramme rettsstridige beføyelser over bankinnskudd som underslag. Siden beløpet registrert på konto ikke er "penger" i den betydning som menes i underslagbestemmelsens annet alternativ, er spørsmålet om fordringen er "løsøregjenstand", jf. første alternativ.

Opprinnelig ble ikke enkle fordringer omfattet av underslagsbestemmelsen, en rettsoppfatning som bygget på *Kjerschows* tolkning av en utrykt høyesterettskjennelse av 29. september 1928. Den gjaldt en herredskasserer som overførte en fordring fra herredskassens konto til sin egen. Høyesterett kom til at handlingen ikke kunne være underslag fordi fordringen ikke var løsøregjenstand.[404] Siden kjennelsen er utrykt er det ikke godt å vite hva som lå i bunnen av resonnementet. To tilnærminger er mulige, den ene er å vektlegge at handlingen består av forskjellige kredit- og debetføringer i bokholderiet. Det reduserer handlingen til enkeltaktiviteter og gir ikke fornemmelse av at man har rådet over et konkret *objekt* (fordringen). Den andre tilnærmingen er nettopp å fastslå at det ble forføyd over et objekt som var en fordring, og at gjerningspersonen hadde rådigheten over denne, og forøvrig legge mindre vekt på detaljene i hvordan det skjedde. Da rettes fokus mot formuesgodet. Man kan ane en parallell her til betraktningsmåten for data, er det tale om å behandle uhåndgripelige signaler, eller å råde over identifiserbare filer, meldinger, bilder osv.?

Det gikk nesten 70 år før et sammenlignbart underslagsspørsmål på nytt kom opp for Høyesterett i Rt. 1997 s. 1760 (dissens). Da ble det ikke satt på spissen fordi flertallet

[404] Se *Kjerschow* (1930) ss. 632 og 901; *Sunde* (2006) s. 104.

avgjorde saken på annet grunnlag.[405] Reelt ble spørsmålet først behandlet i Rt. 2003 s. 1243 (dissens 3-2), og deretter i Rt. 2008 s. 1582. I den sistnevnte saken sluttet Høyesterett seg til fortolkningen i 2003-saken.

Rt. 2003 s. 1243 gjaldt feilinnbetalt beløp til konto. Spørsmålet var om domfeltes unnlatelse av å tilbakebetale beløpet som han var klar over at var feilinnbetalt, var uberettiget tilegnelse av løsøregjenstand. I stedet for å tilbakeføre beløpet hadde han overført det til en annen konto. Høyesteretts flertall sluttet seg til lagmannsrettens lovanvendelse, hvorfra det sentrale lød som følger:

> ”I dagens samfunn er overførsel fra en konto til en annen en helt ordinær måte å betale på. Selv om begrepet løsøregjenstand ikke umiddelbart assosieres med en betalingsform hvor penger ikke flyttes fysisk, må også et tilfelle som det foreliggende rammes av straffeloven § 255 som tilegnelse av en løsøregjenstand. Etter lagmannsrettens vurdering er det her – hensett til sakens realitet – ikke tale om noen utvidende tolking av straffeloven § 255 til ugunst for tiltalte” (avsn. 19).

I saken fra 2008 ga et enstemmig Høyesterett tilslutning til anvendelse av underslagsbestemmelsen på et tilfelle hvor domfelte tilegnet seg et beløp som var feilinnbetalt fra Aetat til hans konto. Da ble uten videre lagt til grunn at beløpet på konto var ”løsøregjenstand”.[406] I lys av denne praksis inntar strl. 2005 § 324 bokstav a, alternativet ”eller pengefordring” ved siden av ”løsøregjenstand”, noe som ifølge forarbeidene er ”en presisering av gjeldende rett”.[407]

Rettsutviklingen for enkle fordringer viser at det ikke gjelder noe ubetinget vilkår om legemlighet for å være løsøregjenstand. Enkle fordringer eksisterer i kraft av at man kjenner til partene i skyldforholdet og beløpet. Det foreligger med andre ord spesifikasjon og konkretisering av objektet, samt en viss kontroll fordi man vet hvem som er skyldner og kan inndrive kravet. Det er tilstrekkelig for å henføres under gjenstandsbegrepet. Videre viser eksemplet at behov som følge av samfunns- og teknologiutviklingen har blitt tillagt stor vekt ved fortolkningen av ”gjenstand”. Det må man kunne regne med at gjør seg gjeldende for data

[405] Det ble vist til at forholdet ikke var straffbart fordi det var ”et regulært mislighold av en sivilrettslig pengeforpliktelse” (Rt. 1997 s. 1760 på s. 1763).
[406] Diskusjonen gjaldt kriteriet ”tilhører en annen”, dvs. betydningen av eiendomsvilkåret i underslagsbestemmelsen.
[407] Ot.prp. nr. 22 (2008-2009) kapittel 8.4.2 s. 285. Jeg er skeptisk til slike ”presiseringer”, fordi man mister treningen i å anvende de generelle begrepene. Jeg tror lovteknikken kan bidra til å skape usikkerhet der hvor man ellers ikke hadde tenkt at loven var uklar. Loven er ikke uklar hvis man kan holde seg til de generelle begrepene, såfremt man kjenner til de kriterier som må være oppfylt.

også, så sentralt som bruken av IKT er i dag. Som det fremgår av Rt. 2003 s. 1243, i sitatet fra lagmannsretten, var det ikke en gang tale om utvidende fortolkning av underslagsbestemmelsen, og det til tross for at man anvendte "gjenstand" på et abstrakt gode.

8 Data vs. informasjon

8.1 Problemstilling

I dette kapitlet går jeg tilbake til forarbeidenes uttalelse om at "informasjon i datasystemer skal fortsatt ikke regnes som gjenstand".[408] Spørsmålet er hva uttalelsen betyr. Mange tolkingsmomenter taler nå for at data omfattes av "gjenstand". Det som etter hvert fremtrer som en mulighet er at uttalelsen tar sikte på *databasert informasjon*, dvs. opplysninger og annet innhold som bæres av data. Det er nettopp dette som står i kommentarutgaven til straffeloven 1902, hvor det til § 6 sies at "opplysninger i en datamaskin" ikke omfattes av gjenstandsbegrepet.[409] Dersom man med "informasjon" primært mener innholdet i data, byr ikke uttalelsen i forarbeidene på noe problem i forhold til om *data* anses som "gjenstand". Informasjon oppfyller som nevnt ikke de kriterier begrepet 'gjenstand' hviler på, men det gjør data.

8.2 "Informasjonssamfunnet"

Utviklingen i IKT har skjedd så raskt og medført så store endringer at det har vært tale om "paradigmeskifte" og "informasjonsrevolusjon". Det har dannet en kontekst for lovgivers overveielser.

Med "informasjonssamfunnet" menes at IKT har gjort *informasjon* allment globalt tilgjengelig og mer økonomisk verdifull enn noen gang tidligere. "Informasjon" har blitt brukt i en bred betydning som både omfatter data og meningsinnhold, dvs. *databåren informasjon*. Diskursen har ikke nødvendigvis hatt behov for å skille mellom data og meningsinnhold, selv om det er rettslig relevant for forholdet mellom eiendomsretten og andre rettigheter. At data er undergitt eiendomsrett synes å ha kommet i skyggen av fokuset på andre rettigheter som knytter seg til informasjonen, nemlig opphavsrettigheter, regler til vern om hemmeligheter (bedrifts- og statshemmeligheter), vern om personopplysninger osv.. Hvis "informasjon"

[408] Se kapittel 6.2.
[409] *Matningsdal* (2003) s. 31. Se avhandlingen kapittel 6.2.

brukes om data og informasjon under ett, får man ikke frem at rettsspørsmålene er forskjellige for de to fenomenene.

I en kjent artikkel fra 1989 stilte den innflytelsesrike tyske strafferettsjuristen *Sieber* spørsmålet om informasjon representerte et nytt *grunngode*.[410] Inspirert av *Wiener* tok han *nettverk* som et kriterium for å identifisere "grunngoder" ("Grundgröße"). Han la til grunn at som utgangspunkt må fysiske objekter og energi anses som grunngoder som overføres med hver sin type nettverk.[411] Således fantes det før informasjonsrevolusjonen *nettverk* for å transportere fysisk gods langs land- og sjøvei, og for å transportere energi ved strømkabel.[412] Med kommunikasjonsteknologien overføres *informasjon* i elektroniske kommunikasjonsnettverk.[413] Siebers poeng ble anskueliggjort ved uttrykket "the information super-highway" på 1990-tallet.[414] Informasjon er følgelig en tredje type grunngode ved siden av fysiske objekter og elektrisitet.

Senere påpekte sosiologen *Castells* at nettverksteknologien transformerte *informasjon* til et økonomisk gode i seg selv. *Castells* tok *Negropontes* tanker om *bit*forflytning et skritt videre.[415] *Bit*forflytning gir grunnlag for et økonomisk produkt, nemlig *den elektroniske informasjonen.*[416] *Castells* konkluderte således med at:

[410] Se *Sieber* (1989) kapittel II.1 "Information als «Grundgröße» neben Materie und Energie" (s. 2572 flg.). Sieber har vært en sentral rådgiver for Europarådet i arbeidet med datakriminalitet og Datakrimkonvensjonen. I 1996 publiserte han "Memorandum on a European Model Penal Code (EMPC)" for Europarådet (Committee on Legal Affairs and Human Rights, Parliamentary Assembly). I situasjonsrapporten *Europarådet* (2004) har han skrevet kapittel 3: The threat of cyber crime, s. 81-218. Her beskriver han blant annet de seks "bølgene" i trusselbildet mot IKT og konvensjonens tilnærming til dem. For en oversikt over hans mange publikasjoner, se http://www.mpicc.de/ww/en/pub/home/sieber/sieber_publ.htm (besøkt 20. februar 2010).

[411] I artikkelen henviser *Sieber* til *Wiener* (se *Wiener* (1988)). *Wiener* teoretiserte rundt styringssystemer (kybernetikk) og for ham var det sentrale at man via kommunikasjon kan påvirke andre. En melding skaper en lomme av orden i en virkelighet preget av kaos og oppløsningstendenser (entropi). Kommunikasjon er en motkraft til entropi, som effektiviseres via teknologi. *Wiener* (1988) er et opptrykk av utgaven fra 1954. Ideene var alt publisert i det mer tekniske arbeidet "Cybernetics or Control and Communication in the Animal and the Machine" (1948). *Wieners* tanker hadde således hatt innflytelse over lengre tid da *Sieber* skrev sin artikkel.

[412] Smlg. *Sieber* (1989), kapittel II.1; Wiener (1988) særlig s. 96-98.

[413] *Sieber* (1989) bruker her informasjon i vid betydning, slik at det også omfatter data. Hos *Sieber* er kommunikasjonsteknologien er forutsetning for resonnementene, og ved beskrivelsen av informasjon som grunngoder det *elektronisk informasjon* som beskrives, uten å problematisere skillet mellom data og informasjon.

[414] Den forklarende rapporten til datakrimkonvensjonen benytter formuleringen "the information super-highways and networks, including Internet" " i pkt. 8.

[415] Se kapittel 3.3.1 om Negropontes budskap.

[416] *Negroponte* (1997) illustrerer poenget med en anekdote på s. 20. Han ble en gang spurt om verdien av sin gamle computer, og svarte: "Et eller annet sted mellom en og to millioner dollar (dansk oversettelse)". Forklaringen var at selv om datamaskinen bare var verdt USD 2000, var innholdet av uvurderlig verdi.

> ”The emergence of a new technological paradigm organized around new, more powerful, and more flexible information technologies makes it possible for information itself to become the product of the production process.”[417]

Den elektroniske informasjonen blir altså et produkt i seg selv. Dette har vært mye omtalte fenomener og en vesentlig årsak til behovet for å etablere et strafferettslig vern mot anslag mot elektronisk basert informasjon. Man ser også at dersom ikke formuleringen ”informasjon i datasystemer” presiseres, kan den både bety

- data (*bits* og *bit*forflytning),
- databasert informasjon (informasjon), og
- begge deler under ett (data og informasjon smelter sammen til ett økonomisk gode).

Innen rettsinformatikken finnes det teoretiske posisjoner som tar utgangspunkt i en sammensmeltning mellom av elektroniske data og informasjon. I utgangspunktet gjelder det klassiske skillet mellom data og informasjon, hvor tegn og signaler er data, mens informasjon er meningsinnholdet som utledes av slike tegn og signaler (fortolkningen).[418] Herfra kan det foretas en slutning over til IKT, hvor ”tegn og signaler” brukes om de elektroniske signalene som bare datamaskinen kan forstå. Det er slike impulser som er kalt ”et-tall og nuller”, ”magnetiske signaler” og ”elektroniske signaler" i forarbeidene til straffeloven.[419] Så går man videre og sier at disse signalene representerer informasjon.

Alt dette er korrekt, men det er viktig å være klar over at så lenge informasjonen bare er under behandling, lagring eller overføring hos datamaskinen, er den ikke informasjon som kan forstås av mennesker.[420] I slike tilfeller brukes ”informasjon” på en bred måte som omfatter data (i betydningen elektroniske signaler). Jeg har avgrenset mot en slik måte å bruke informasjonsbegrepet på i strafferettslig sammenheng, og har introdusert begrepet *presentasjon* (dvs. databasert informasjon i objektiv forstand) for å danne overgangen mellom data og informasjon i subjektiv forstand (dvs. det fortolkede innholdet). Jeg viser til kapittel 2 om dette.

[417] Sml. *Castells* (2000) s. 78.
[418] Se kapittel 2.
[419] Straffelovrådet brukte uttrykkene ”et-tall og nuller” og ”magnetiske signaler”, jf. NOU 1985: 31 s. 8-9. Datakrimutvalget brukte ”elektroniske signaler” i annen delutredning, NOU 2007: 2 kapittel 5.2.2 s. 61.
[420] Uttrykket ”magnetiske impulser” er egentlig ikke riktig, det er tale om elektromagnetiske impulser siden det er elektrisitet som skaper impulsene.

Både i norsk og dansk rettsinformatisk teori bygges det iblant på sammensmelting av elektroniske data og elektronisk båret informasjon. *Bing* har tatt denne posisjonen for å utvikle det nye begrepet "funksjonell ytring". Det brukes om *elektronisk kommunikasjon* som har datamaskinen som endepunkt, dvs. " ytringer fra mennesker til maskiner".[421] En funksjonell ytring er således en kommunikasjonsstrøm som består av elektroniske signaler. I utgangspunktet klargjør *Bing* at han bruker "ytring" som

> "en felles betegnelse for enhver form for melding, utsagn eller formidling av data uansett form – det omfatter altså tekst og tale, musikk og signaler, bilder og bevegelser, alt som er egnet til å formidle et meningsinnhold. Dermed brukes uttrykket «ytring» med en betydning som ligger nær «data»."[422]

På den måten blir meningsinnhold (ytring) og data (i tradisjonell forstand) nærmest synonyme begreper. *Bing* sier så at:

> "datamaskinteknologien har gjort det mulig å formidle i nettet ytringer, typisk i form av datamaskinprogrammer, som styrer datamaskiner slik at det får konsekvenser … [D]enne ytringen … henvender seg [ikke] primært til mennesker, men tar sikte på å bli lest, tolket og reagert på av datamaskinbaserte systemer."[423]

Dermed har man begrepet "funksjonell ytring", det smelter sammen elektroniske signaler (data) og informasjon.[424]

Man ser noe tilsvarende i dansk teori som har "fusjonert" data og informasjon i begrepet "medieavhengig informasjon" når informasjonen er digitalisert.[425] Også her tas det

[421] *Bing* (2008) s. 25.
[422] *Bing* (2008) s. 22. Se avhandlingen kapittel 4.2 om begrepet "ytring", smlg. beskrivelsen i sitatet av *Bing*.
[423] *Bing* (2008) s. 25-26.
[424] *Bing* eksemplifiserer med DOS-angrep, dekodingsprogrammer og lenker som brukes på webben, se *Bing* (2008) s. 53-56, 71, 98. Forskjellen fra "ytring" i vanlig forstand, er at den funksjonelle ytring ikke er beregnet på mennesker. Ytringer i form av "tegn og signaler" som er beregnet på mennesker, kan altså ikke ha datamaskinen som endelig adressat. *Bing* viser til at "informative" ytringer kan formidles fra datamaskiner til mennesker, for eksempel informasjon som hentes opp fra elektroniske databaser. Han nevner *Z* (1988) som et eksempel. Saken gjaldt om betingelsene for adgang til den østerrikske "Lovdata-tjenesten", krenket retten til informasjonsfrihet (retten til å anskaffe informasjon), et spørsmål som ble ansett å falle inn under EMK art. 10 (ikke krenkelse). Også saken *Times* (2009) om ærekrenkende artikler som lå tilgjengelig i avisen *Times'* internettarkiver falt innenfor området for EMK art. 10 ("such archives fall within the ambit of the protection afforded by Article 10") se pkt. 27. Også denne saken viser at innholdet i databaser tilgjengelige over nett representerer informative ytringer når innholdet først er av en slik karakter at det er beregnet på å informere et menneske. Det er mulig at *Bing* ser 'funksjonell ytring' som motsatsen til den 'informative ytring', som utvilsomt er en ytring i klassisk forstand. Temaet later til å inneholde flere interessante spørsmål, men det faller utenfor avhandlingens prosjekt å drøfte dem her.

utgangspunkt i det klassiske skillet mellom data og informasjon.[426] Dette overføres til digitaliserte medier hvor informasjonen representeres i sifferformat og dermed blir *medieavhengig* (eller snarere medie*bunden*). For å kunne holde på det definisjonsmessige utgangspunktet for data, skriver *Udsen* som sammenfatter mye av dansk teori på området, at forutsetningen om

> ”at data kan erkendes af den menneskelige hjerne, afskærer ikke de data, der behandles af computere, fra at være omfattet af begrepet. Al data, der behandles af en computer, kan teoretisk undergives tilsvarende behandling i den menneskelige hjerne og vil derfor være omfattet af definitionen. Forskellen består i den hastighed, hvormed behandlingen sker.”[427]

Dermed kommer det ut på ett - teoretisk sett - om man taler om data eller informasjon.[428]

I strafferettslig sammenheng bør, etter mitt syn, skillet mellom data og informasjon opprettholdes. Data må behandles av datamaskiner, noe som er en forutsetning for automatiserte prosesser og for at strafferettslige normer kan virke i nettet uten at mennesket ”ser på” det som til enhver tid foregår.

Et budskap er for eksempel ”egnet til å nå et større antall personer” når det er lagt opp på en web-adresse, selv om ingen har sett på det ennå. Dermed er vilkåret i strl. 2005 § 10 annet ledd annet punktum oppfylt. Tilsvarende er overgrepsbilder tilgjengeliggjort om de er lagt ut på nevnte måte, selv om ingen har sett på dem ennå. Og det samme gjelder skadelig objektkode, enda koden bare er ment for datamaskinen og ikke for mennesker. I alle disse tilfellene er den strafferettslig relevante omstendighet hvordan man har behandlet *data.*

---

[425] *Medieavhengig* informasjon skal holdes atskilt fra *fleksibel* informasjon, som er informasjon som utveksles uten tilknytning til noe bestemt medium, for eksempel samtale mellom mennesker, og fra *integrert* informasjon, som er slikt man kan utlede av å se på formen på en gjenstand. For eksempel at formen på et dørhåndtak sier noe om dets funksjon. Integrert informasjon skal holdes helt utenfor informasjonsbegrepet.

[426] *Udsen* (2009) ss. 33-34.

[427] *Udsen* (2009) s. 35 (petit).

[428] Dette gir problemer for den rettslige regulering, som *Udsen* (2009) konstaterer på s. 36: ”Denne medieafhengighed bevirker, at information altid optræder i en kombination af noget materielt (mediet) og noget immaterielt (informationen). Sondringen er central for den retlige regulering. Mediet kan uden videre placeres inden for de regler, som regulerer fysiske genstande, mens det ofte er vanskelig at afklare, hvordan disse regler skal tilpasses informationsfaktummet. Mens tyveri af et fysisk medium eksempelvis utvivlsomt er undergivet straffelovens almindelige bestemmelser om tyveri, har det været et vanskeligere spørgsmål, om ulovlig tilegnelse af information også skulle behandles efter tilsvarende regler.” Etter min mening blir komplikasjonene unødig store fordi data og informasjon ikke holdes atskilt, til tross for at man innleder med å si at så er tilfelle. Jeg ser for eksempel ikke hvorfor loven ikke kan ha et straffebud mot datatyveri, se drøftelsen i avhandlingen kapittel 8.5

Som det fremgår er ikke det strafferettslig relevante poeng nødvendigvis hvordan man har behandlet meningsinnholdet (informasjonen), ofte er det *dataene som objekt betraktet* som står i forgrunnen for interessen. Dette har jeg redegjort nærmere for i kapittel 9. Dessuten er det behandlingen av *data* som ligger til grunn for at man kan si at rettshåndhevelsen foregår automatisert. Dette har jeg redegjort for i kapittel 11.2. Det at mennesker kan lese innhold som presenteres for dem, ligger i forlengelsen av data som fenomen. Det kan ha strafferettslig relevans, for eksempel dersom man ser på overgrepsbilder på dataskjermen, men det er ikke det samme som å ha befatning med dataene i seg selv.

8.3 Strafferettslige beskrivelser av data

I likhet med teoretiske posisjoner som behandler data som "tegn og signaler", og dermed anser data for å være informasjon, beskrev Straffelovrådet data som "en serie et-tall og nuller" og som "magnetiske impulser".[429] I forhold til spørsmålet om data var gjenstand, konstaterte man at kravet til legemlighet ikke var oppfylt. Selv om det forelå en viss rettskildenød, antok man at det gjaldt et slikt krav, på bakgrunn av uttalelsen til *Kjerschow* som bygget på den utrykte høyesterettskjennelsen fra 1928, og fordi enkle fordringer (den gang) ikke var ansett som "løsøregjenstand" i underslagsbestemmelsen.[430]

Straffelovrådets beskrivelse etterlater et inntrykk av data som et diffust og "uhåndgripelig" fenomen. Her har man ikke vært alene. I den svenske utredningen "Information och den nya InformationsTeknologin" fra 1992, var man blant annet inne på spørsmålet om *data* kan eies, i en drøftelse av om *informasjon* kan eies.[431] Utvalget tok utgangspunkt i at det må skille mellom tre nivåer, hvor man holder den fysiske bæreren, data og informasjon fra hverandre. Utvalget skrev:

> "Viktig är att hålla i sär information och informationsbärare. Information er något immaterielt medan informationsbärare er fysiska föremål. Data er något däremellan. De ger en fysisk representation av information men de er inte påtagliga; de har som vi ofta återkommer till en kvasimateriell karaktär."[432]

[429] NOU 1985: 31 s. 8-9. Karakteristikken "en serie et-tall og nuller" er hentet fra *Torvund*, Complex 6/83 s. 147-148. Straffelovrådets uttrykk "magnetiske impulser" er ikke riktig, det er tale om elektromagnetiske impulser siden det er elektrisitet som skaper impulsene.
[430] NOU 1985: 31 s. 9.
[431] SOU 1992: 110 kapittel 4.6.2 s. 155 flg.
[432] SOU 1992: 110 s. 156.

Den svenske betegnelsen av data som et "inte påtagliga" og "av kvasimateriell karakter" føyer seg inn i rekken av svake beskrivelser som også finnes i norsk rett. Konklusjonen ble at *dersom data* betraktes som eiendom, blir konsekvensen at *informasjon* i seg selv kunne bli omfattet av vern mot tyveri ("stöldsskydd").[433] Dette vek man tilbake for, siden lovgiver alt hadde tatt stilling til informasjonsvernet gjennom regler i "datalagen, sekretesslagen och senast lagen om företagshemligheter". Utvalget slo fast at hvorvidt det finnes behov for "ett allment och längre gående skydd för information ankommer inte på oss att pröva."[434]

I forhold til spørsmålet om data kan eies, fremstår det som en svakhet at utvalget ikke tok stilling til om dette alt fulgte av generelle tingsrettslige regler. Det er samme svakhet som har gjort seg gjeldende i norsk strafferettsteori vedrørende data. Dersom spørsmålet hadde vært stilt på den måten, ville neste spørsmål vært om det fantes grunner *de lege ferenda* for hvorfor data likevel *ikke burde* være undergitt eiendomsrett. Da kunne man pekt på betenkeligheter med kontroll over informasjon som et mulig hensyn, selv om det er vanskelig å se hvorfor det er et større problem når informasjon bæres av data, enn når den bæres av bøker. Det er jo ikke tvilsomt at bøker eies.

Straffelovrådets drøftelse og konklusjon fra 1985 er ikke blitt analysert senere.[435] Datakrimutvalget har ikke diskutert data i forhold til det strafferettslige gjenstandsbegrepet. I utvalgets første delutredning (2003), ble Straffelovrådets syn lagt til grunn ved beskrivelsen av gjeldende rett, uten nærmere vurderinger.[436] I annen delutredning (2007) hadde ikke utvalget behov for å komme inn på diskusjonen, fordi det foreslo særbestemmelser om datakriminalitet basert på egne legaldefinerte begreper. Utvalget brukte uttrykket "elektroniske signaler" synonymt med data.[437] Legaldefinisjonene skilte mellom data og databasert informasjon, men som nevnt besluttet departementet ikke å bruke legaldefinisjonene i loven.[438]

[433] SOU 1992: 110 s. 157."Gör man detta [dvs. anser data for å være undergitt eiendomsrett] leder detta emellertid till den konsekvensen att information i sig kan komma att bli omfattad av stöldsskydd." (min klamme).
[434] SOU 1992: 110 s. 157.
[435] Jeg ser da bort fra min egen drøftelse i *Sunde* (2006) kapittel 4. I denne avhandlingen har jeg hatt anledning til å gå grundigere inn på temaet.
[436] NOU 2003: 27 kapittel 2.4.2 (gjeldende rett) og 2.4.3 (utvalgets vurderinger) på s. 17.
[437] NOU 2007: 2 kapittel 5.2.2 "data" og "dataprogram" s. 61.
[438] Se kapittel 6.3.2.2.

I det øvrige utredningsarbeidet til straffeloven 2005, har man forlatt bruken av ordet "data", og gått over til å bruke andre uttrykk med mer ubestemt betydning, for eksempel "informasjon i datasystemer" og "elektronisk lagret informasjon". Straffelovkommisjonens utredning fra 2002 som har lagt sterke føringer for utformingen av straffeloven 2005, anvendte således ikke distinksjonen mellom data og informasjon. Følgende formulering er illustrerende:

> "Det kan virke rimelig at informasjon som overføres elektronisk, bør ha det samme vernet som informasjon som er lagret, enten elektronisk […] eller på papir […] Kommisjonen har vurdert om [bestemmelser] som verner lagret informasjon mot endring eller sletting, også bør beskytte informasjon som er under overføring ved elektroniske midler."[439]

I tillegg kan det som nevnt konstateres at straffeloven 2005 bruker mange forskjellige uttrykk om data, "elektronisk lagret informasjon", "databasert informasjon", "informasjon" og "data" (dette er beskrevet i kapittel 6.1).[440] Og "elektronisk lagret informasjon" brukes også om informasjon, se strl. 2005 § 76 første ledd (databasert informasjon) og drøftelsen i kapittel 5.4.1.

8.4 Oppsummering

For å oppsummere har den sentrale problemstillingen vært om data omfattes av det strafferettslige begrepet "gjenstand". Ordlyden er generell og begrepet er elastisk og tidsbestandig. Analysen i kapittel 7 viste at begrepet "gjenstand" omfatter fenomener som kan spesifiseres, kontrolleres og eies. Det ble konstatert at data oppfyller disse vilkårene.

[439] NOU 2002: 4 kapittel 9.9.1 s. 319.

[440] *Bygrave* (2006) har påpekt behovet for å forstå data bedre. Han skriver blant annet at "the legal community has often vague and somewhat inconsistent views of core information concepts" (s. 120.) Han påpeker at det er nødvendig med en mer presis forståelse siden "legal rules are increasingly being formulated such that their scope does turn on the ambit of basic information concepts" (s. 122). Strafferettslige og -prosessuelle spørsmål har ellers ikke vært gjenstand for større interesse blant rettsinformatikere, hvor spørsmål om personvern, immaterialrett og utvikling av elektronisk forvaltning synes å ha stått i forgrunnen. Det foreligger selvsagt betydelige vitenskapelige bidrag som systematiserer feltet, utvikler kommunikasjonsteori og anvendt søketeori for oppbygning av rettslige informasjonssystemer m.v, se her hjemme blant annet *Bing* (1982). Men i sitt betydelige systematiserende arbeid innen "computer and law" streifer *Seipel* (1977) bare så vidt innom strafferettslige spørsmål, og nevner ikke prosessuelle. Problemet med "protection against unauthorized access and manipulation of information in computer systems" nevnes (s. 77), og det skilles mellom tilsiktede og utilsiktede trusler (s. 84), men "general problems of criminal liability associated with computer abuse" anses å falle utenfor disiplinen (s. 135). I klassifikasjonssystemet på s. 311 flg., er temaet fordelt på underpunktene 2.4.3 (Law enforcement, criminal justice) 3.5.3 (Computer abuse, criminal law aspects); *Andersen* (2005) omfatter alle felt og er et oversiktsverk. Innen straffe- og prosessretten bygger meg bekjent, ikke noe verk hittil i Norden på rettsinformatiske innsikter. Men å klandre rettsinformatikerne ville jo være å rette baker for smed, det er mer til poenget å konstatere at informasjonsrettslige spørsmål har hatt liten interesse blant strafferettsteoretikerne.

Ut fra lovgiverviljen er det naturlig at data er gjenstand, fordi begrepet brukes i bestemmelser som verner eiendomsretten mot krenkelser. Det kan sies å stride imot lovens formål om begrepet avgrenses slik at et objekt som etter sin art kan eies, faller utenfor. Rent språklig er det ikke noe problem å henføre data under "gjenstand". *Forutsetningen* er at man med 'data' mener elektroniske signaler, og at det er elektroniske signaler som kan identifiseres og som man har under kontroll, for eksempel en konkret fil i filsystemet under "mine dokumenter", med en bestemt plass rent fysisk på serveren, med et filnavn, og med en størrelse (*bytes*). Data i betydningen "tegn og signaler som mennesker kan oppfatte" faller utenfor dette databegrepet. En datafil kan tilhøre en person, og det må antas vanligvis å være tilfelle. Den kan følgelig være "gjenstand" i henhold til de kriterier som bestemmer begrepets innhold.

Det må følgelig anses å være i samsvar med den opprinnelige lovgiverviljen fra 1902 å henføre data under lovens ordlyd "gjenstand". Spørsmålet er om det nå hersker en *ny* lovgivervilje, som er introdusert med virkning for straffeloven 2005.

Det som har skjedd i straffeloven 2005 er at man har tilføyd alternativet "eller annen energi" i den presiserende bestemmelsen i strl. 2005 § 12. Forøvrig har man ikke rørt ved gjenstandsbegrepet, men videreført rettstilstanden etter straffeloven 1902.

Analysen i det foregående har vist at oppfatningen om at data ikke var gjenstand, første gang ble uttrykt av Straffelovrådet i 1985. Det baserte seg på en meget utilstrekkelig beskrivelse av data. Videre forelå det rettskildenød, så konklusjonen var ikke særlig bastant.[441] For det tredje hvilte begrunnelsen på at gjenstandsbegrepet krevde legemlighet. Denne oppfatningen var koblet til rettstilstanden for enkle fordringer, men denne har senere endret seg.[442] Gjenstandsbegrepet krever ikke legemlighet. Derimot synes *kontroll* å være viktig. Det må for eksempel ha vært en forutsetning for *Kjerschows* opplysning om at gass var gjenstand.[443] Kanskje det fremsto som så opplagt at han ikke fant grunn til å nevne det, for han kan ikke ha ment at gass i fri form var omfattet. Det ville være å stille gass likt med energi "frit i naturen". Men selve forestillingen om at det er mulig å ha kontroll over konkrete data, blir fjern dersom de beskrives som uhåndgripelige magnetiske signaler.

[441] NOU 1985: 31 s. 9.
[442] Se kapittel 7.6.4.
[443] *Kjerschow* (1930) s. 632, s. 901.

Siden man i forberedelsene til straffeloven 2005 ikke har analysert tilstanden for data i forhold til gjenstandsbegrepet, er Straffelovrådets konklusjon bare blitt repetert.[444] Det er imidlertid mulig å spore en tendens til å frigjøre seg fra denne oppfatningen, jf. Rt. 2004 s. 1619, hvor Høyesterett går langt i å behandle data som gjenstand, enda det ikke var nødvendig for å konkludere med at det forelå skadeverk mot datamaskinen.[445]

Det som i ettertid synes å ha skjedd er at siden bruken av ordet "informasjon" ble en vanlig betegnelse både for data og informasjon, har resonnementene dreiet seg om meningsinnholdet, dvs. "opplysninger" i datasystemer, eller "lyd, tekst, bilde" som det står i ekomloven § 1-5 nr. 1. Men også her betyr det *data*, fordi det ekomloven prøver å klargjøre er at uansett hvilken karakter innholdet har, er det *dataene* (den elektroniske kommunikasjonen) som loven regulerer, se redegjørelsen i kapittel 2.3.4. Med hensyn til uttalelsene i strafferettslig teori og forarbeider, synes fokuset på innholdet å ha blitt dominerende, smlg. straffelovskommentaren som sier at strl. 1902 § 6 ikke omfatter "opplysninger i en datamaskin".[446] Dermed er det nærliggende at uttalelsen om at "informasjon i datasystemer mv skal fortsatt ikke regnes som gjenstand", betyr *opplysningene* i datasystem. Det gir god mening ved fortolkningen av lovens bestemmelser.

Konklusjonen er dermed at data er "gjenstand" slik straffeloven 1902 bruker begrepet, og denne begrepsbruken er videreført i straffeloven 2005.

8.5 Vurdering av tolkningsresultatet

Straffeloven 2005 innfører flere nye bestemmelsen til vern om data. På den bakgrunn kan man si at behovet for å henføre data under gjenstandsbegrepet er mindre enn etter den eldre loven.

[444] Slike uttalelser finnes blant annet i Ot.prp. nr. 90 (2003-2004) på s. 165, i tilknytning til strl. 2005 § 12: " Informasjon i datasystemer mv. skal fortsatt ikke regnes som gjenstand." En lignende uttalelse står i siste delproposisjon, hvor det sies at: "[e]lektronisk lagret informasjon (data) er ikke en gjenstand, men endring og sletting av den vil som regel likevel være straffbart, fordi handlingene er skadeverk mot lagringsmediet, jf. Rt-2004-1619." Se Ot.prp. nr. 22 (2008-2009) kapittel 9.2.1 s. 303, se også s. 60.
[445] Se kapittel 7.6.3.
[446] Se kapittel 8.1.

Datakrimutvalget foreslo imidlertid en bestemmelse som vernet uberettiget tilegnelse av data ved kopiering (datatyveri).[447] Departementet fulgte ikke opp forslaget og nøyde seg med å innføre en bestemmelse om datainnbrudd, jf. strl. 2005 § 204 som lyder:[448]

> "Med bot eller fengsel inntil 2 år straffes den som ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystem eller del av det."

I forarbeidene til straffeloven 2005 uttaler departementet at bestemmelsen om datainnbrudd bare gir indirekte vern for "informasjon", fordi det som "direkte straffes er den uautoriserte inntrengningen i datasystemet."[449] Videre konstateres det at bestemmelsen

> "har berøringspunkter med en rekke andre bestemmelser … bruk av systemet, eksempelvis søk etter og kartlegging av informasjon som finnes på en datamaskin, vil kunne rammes som ulovlig bruk. Endring eller sletting av data og informasjon som finnes på systemet kan rammes av skadeverkbestemmelsene (se forslaget til § 206 og § 351)."[450]

Spørsmålet om straff for uberettiget tilegnelse av data som er lagret fremstår derfor som strafferettslig *uregulert*. Forklaringen ligger kanskje i det synet på kopiering som fremkommer i høringsuttalelsen fra Elektronisk Forpost Norge (EFN), som er sitert i lovproposisjonen. Her fremholdes det at et eventuelt

> "vern mot uberettiget kopiering bør adresseres særskilt og medienøytralt."[451]

Uttalelsen retter seg i realiteten mot en annen problemstilling enn det som gjelder det rene datatyveri. Datakrimutvalget foreslo å kriminalisere den uberettigete kopiering eller overføring av data, noe som ofte skjer etter et datainnbrudd. I utredningen vises det til en sak fra Oslo tingrett hvor

> "en ledende ansatt … var i ferd med å gå over i stilling som administrerende direktør i et konkurrerende selskap. Før han sa opp stillingen … kopierte han innholdet på den såkalte "produksjonsserveren" til 5-7 cd-er som han tok med seg ut av bedriften. Det var tale om ca. 23 000 datafiler. I tillegg tilegnet han

[447] Gjerningsbeskrivelsen i forslaget til straffebud (§ 6 Datatyveri) lød slik: "For datatyveri straffes den som uberettiget kopierer, overfører eller på annen måte tilegner seg data", se NOU 2007: 2 s. 175.
[448] Se Ot. prp. nr. 22 (2008-2009) kapittel 2.11.2 s. 50.
[449] Se Ot. prp. nr. 22 (2008-2009) kapittel 2.11.4 s. 51.
[450] Se Ot. prp. nr. 22 (2008-2009) kapittel 2.11.4 s. 51-52.
[451] Se Ot. prp. nr. 22 (2008-2009) kapittel 2.11.3 s. 51.

> seg arbeidsgiverens hemmelige anbud på et prosjekt verd ca. 200 millioner kroner, ved å overføre datafilen med anbudet til sin private frisurf e-postkonto."[452]

Når det som i ovennevnte sak kopieres noe man ikke eier, som det verken er samtykket til kopiering av, eller foreligger noen grunn til å anta at er frigitt som et offentlig gode, er det lite nærliggende å søke hjelp i opphavsrettens vern. Man har med en annen problemstilling å gjøre enn den som gjelder kopiering av digitaliserte åndsverk, som har vært et hovedspørsmål i den rettspolitiske debatten om utnyttelsen av digitalisert informasjon, og som EFN kan ha tenkt på. Det å kopiere en musikk-CD eller en DVD-film man har kjøpt, reiser spørsmål om forholdet mellom de opphavsrettslige enerettigheter og allmennhetens rett til å utnytte eksemplarer av verket. Da blir hensynet til medienøytral regulering et vektig argument, jf. også at de opphavsrettslige regler som utgangspunkt er teknologinøytrale.[453] Siden det ikke er straffbart å kopiere sider i en bok, hvorfor skulle det være straffbart å kopiere data? Dermed har lovgiver vegret seg for å innføre en bestemmelse om datatyveri.

Men hvis man sier at situasjonen er en helt annen; det er for eksempel tale om et datainnbrudd på en server til en nettvert, hvor mange tusen brukere lagrer sine data. Ved datainnbruddet kopieres det fra disse dataene. Bør eierne av dataene være henvist til vern etter opphavsrettslige regler for å ivareta sine interesser? Hvilket vern har arbeidsnotater, excel-ark med utregninger, utkast til phd-avhandlinger, private bilder osv.. Bør det i slike tilfeller stilles krav om verkshøyde for å ha et strafferettslig vern mot kopiering? Er det databasevernet som skal tre inn? Men det verner bare nettverten og omfatter ikke nødvendigvis brukerens interesser. Eller skal innholdet henføres under vernet om personopplysninger? Og hva hvis nettverten selv tilegner seg kopi av utvalgte deler av innholdet, for eksempel i forbindelse med sikkerhetskopiering. Burde man ikke ha et strafferettslig vern mot en slik handling? Data må anses som en privat eiendel, og det burde ikke være nødvendig å bevise at innholdet er av en spesiell karakter for å nyte strafferettslig vern om eiendomsretten. Her bryter følgelig straffelovgivningen med hensynet til teknologinøytralitet. Tyverivernet ytes både gamle og slitte gjenstander som ikke har noen økonomisk verdi av betydning, men altså ikke til data som kan bære store verdier.

[452] Oslo tingretts dom av 10. mars 2005 (TOSLO-2004-84792). Omtalt i NOU 2007: 2 s. 70-72.
[453] Se kapittel 6.3.3 om Napster-dommen og teknologinøytralitet i åndsverkloven.

Det er mulig at Datakrimutvalget gikk noe langt i sine bestrebelser fordi man foreslo også en straffebestemmelse om *informasjonstyveri*.[454] Departementet har lagt til grunn at det er tilstrekkelig med en bestemmelse om datainnbrudd, og har på den måten bevisst gått inn for å gi informasjon bare et indirekte vern. Men om det kanskje var å gå noe langt å foreslå en generell bestemmelse om informasjonstyveri, er det behov for vern mot *datatyveri*, jf. eksemplet i saken fra Oslo tingrett. For gjerningspersonen har det en egenverdi å råde over dataene (mediet) fordi man vanskelig kan huske innholdet i omfattende datamengder. Men som drøftelsen har vist, mangler det strafferettslig vern mot uberettiget kopiering av lagrete data.

Det er lite nærliggende å ta opp en drøftelse av om lagrete data har vern som "gjenstand", etter tyveribestemmelsen. Vilkåret om besittelsesforrykkelse kan vanskelig oppfylles. I tillegg har lovgiver nylig konkludert negativt vedrørende tyverispørsmålet. Data under overføring derimot, er beskyttet mot kopiering, jf. regler om beskyttelse av tilgangskontrollerte fjernsynssignaler og av personlig kommunikasjon, jf. strl. 2005 §§ 203 og 205.

Det synes å stille seg annerledes for handlinger som kan bedømmes som underslag. Tilegnelsesbegrepet er ikke på samme måte som borttakelse, knyttet til et vilkår om besittelsesforrykkelse. For data som er betrodd en nettvert, synes derfor bestemmelsen om underslag å kunne gi vern om data fordi de er "gjenstand". Nettverten som forsettlig unnlater å slette deler av sikkerhetskopierte data for å utnytte dem selv, gjør seg derfor skyldig i underslag av data. Men uberettiget kopiering som følge av datainnbrudd oppstiller loven altså ikke noe vern mot. Dette synes som en mangel ved straffeloven 2005.

Ved å konstatere at "gjenstand" omfatter data, ytes altså data strafferettslig vern på et område som må antas å kunne være praktisk (web 2.0-situasjonen). Bortsett fra for tyverisituasjonen, synes straffeloven 2005 å ha et godt vern om data. Det virker imidlertid unødvendig å anvende et eget ledd for å verne data mot skadeverk slik strl. 2005 § 351 annet ledd gjør. Det hadde vært enklere og konseptuelt klarere å henføre vernet direkte under første ledd, som rammer skadeverk mot "gjenstand".

[454] NOU 2007: 2 s. 175, § 5 Informasjonstyveri, se omtale i utredningen kapittel 5.5 s. 70-73.

For fortolkningen av loven er det uansett fordelaktig å ha plassert sentrale begreper på en klar måte. Hovedkonklusjonen er at "gjenstand" omfatter data. Det er ikke nødvendig å se data i sammenheng med lagringsmediet for å la det være objekt for rettsreglene. Dette synes å påvirke forståelsen av "ting" i inndragningsreglene, på grunn av det nære slektskapet mellom "gjenstand" og "ting". Presiseringen av at ting omfatter "elektronisk lagret informasjon", gjelder data som er tatt i beslag. Men data som overføres kan være objekt for automatisert inndragning, fordi det etter loven kan betraktes som et selvstendig fenomen. Da går man rett på strl. 2005 § 69 første ledd.[455]

9 Data som element i lovbruddet

9.1 Problemstilling

I dette kapitlet behandler jeg konseptualiseringen av data som "gjenstand/ting" med utgangspunkt i hvordan data fungerer som objekt ved overtredelser av straffebud som er særlig praktiske for overtredelser på internett. Diskusjonen føres for strl. 2005 §§ 201 og 311 som begge rammer det å produsere, anskaffe, besitte og tilgjengeliggjøre det rettsstridige materialet.

[455] Det er mulig lovgiver har hatt et noe uavklart forhold til fenomen som det er behov for å anvende teknologi for å kontrollere. Det gjelder ikke bare data, men også energi. Begrunnelsen for alternativet "eller annen energi", jf. strl. 2005 § 12, er nemlig tankevekkende. Ifølge forarbeidene: "klargjør [bestemmelsen] det spørsmål som har voldt tvil i praksis, nemlig om borttakelse av energi i telefon- og TV-kabler omfattes av gjenstandsbegrepet." (Ot.prp. nr. 90 (2003-2004) s. 165.). Her vises det både til energi i form av elektrisitet, verdienheter i form av tellerskritt, og TV-signaler data. Objektene som tilegnelsen gjelder er altså helt forskjellige. Dersom man uberettiget tilegner seg elektrisitet, gjelder hovedalternativet "elektrisk energi" i strl. 2005 § 12, og tilfellet skal bedømmes som tyveri, jf. Rt. 1985 s. 1138. Dersom man tilegner seg beskyttede TV-signaler, rammes handlingen direkte av strl. 2005 § 203 uten å gå veien om gjenstandsbegrepet, og da er definisjonstillegget i strl. 2005 § 12 overflødig. Med hensyn til telefoni består problemet i uberettiget tilegnelse av tellerskritt, noe som er en økonomisk størrelse, ikke "annen energi", jf. definisjonstillegget. I "gamle dager", før GSM-standarden - ble det gjort ved å bruke "klonede" mobiltelefoner som var utstyrt med ulovlig kopierte SIM-kort. Det representerte også dokumentfalsk. Rette innehaver av telefonnummeret ble belastet tellerskrittforbruket fra den "klonede" telefonen. Vanligvis uttrykkes den økonomiske konsekvensen av handlingen som et "tap" og et krav om vinnings forsett. Energiforbruket ved telefonmisbruk fremstår som uvesentlig og er heller ikke målet for handlingen. Tellerskrittene som man nettopp tilegner seg, omfattes ikke av ordlyden i strl. 2005 § 12. For å ramme telefonmisbruk må man gå rett på en fortolkning av aktuelle straffebud. Tellerskrittmisbruk kan være databedrageri, jf. strl. 2005 § 371 bokstav b, og det er ikke nødvendig å misbruke apparatet for å begå bedrageriet. Smlg. PIN-kodedommen Rt. 1995 s. 1872 (PINkode). Ved misbruk av PIN-kode kan man dessuten si at man misbruker en identitet, jf. strl. 2005 § 202. Dersom man misbruker selve telefonen kan bestemmelsen om ulovlig bruk anvendes direkte, jf, strl. 2005 § 343 (for eksempel leieboeren som ringer venner i Australia med utleiers telefon), smlg. Rt. 1989 s. 980 og Rt. 1992 s. 790, se også *Sunde* (2006) s. 213-215. Tilføyelsen "eller annen energi" synes derfor bare å være nødvendig for å kunne ramme uberettiget tilegnelse av fjernvarme, som ikke omfattes av alternativet "elektrisk energi", men her kunne man kanskje samordnet alternativene til ett (se kapittel 7.6.2).

Jeg undersøker om sondringen mellom data og informasjon er relevant for fortolkningen av bestemmelsene. Har man for eksempel overtrådt anskaffelsesforbudet dersom man har sett på et bilde i et blad gjennom et utstillingsvindu? Og har man overtrådt besittelsesforbudet ved å ha synsinntrykkene i sitt hode?

Videre undersøker jeg om det er rimelig å likestille data med fysiske objekter ved fortolkningen. Kan man for eksempel si at nedlasting av en datafil med et overgrepsbilde er en tilsvarende overtredelse som anskaffelse av et pornoblad? Eller at besittelse av et skadelig dataprogram er likestilt med å ha besittelse av fysiske objekter som piratdekoderkort m.v.?

Hvis straffetrusselen er knyttet til befatning med *data* på samme vis som fysiske objekter, og befatning med meningsinnholdet alene ikke er tilstrekkelig for straff, behandler straffeloven data på linje med et fysisk objekt. I så fall spiller det ingen rolle hva slags *ting* befatningen gjelder, bare den bærer *fremstilling* som nevnt i strl. 2005 § 311 eller har *egenskaper* som nevnt i strl. 2005 § 201. Det betyr at straffeloven mer gjennomgående behandler data som et selvstendig objekt. Det taler i så fall for at data kan inndras på selvstendig grunnlag, også i nettet.

9.2 Overgrepsbilder

9.2.1 Innledning

Strl. 2005 § 311 første ledd lyder:

> ”Med bot eller fengsel inntil 3 år straffes den som
> a) produserer fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn,
> b) utgir, tilbyr, selger, overlater til en annen, gjør tilgjengelig eller på annen måte søker å utbre fremstillinger som nevnt i bokstav a,
> c) anskaffer, innfører eller besitter fremstillinger som nevnt i bokstav a, eller forsettlig skaffer seg tilgang til slikt materiale,
> d) holder offentlig foredrag eller istandbringer offentlig forestilling eller utstilling av fremstillinger som nevnt i bokstav a.” [456]

[456] Den korresponderende bestemmelsen i strl. 1902 § 204 a lyder: ”Den som
a) produserer, anskaffer, innfører, besitter, overlater til en annen eller mot vederlag eller planmessig gjør seg kjent med fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn,
b) befatter seg med fremstillinger av seksuelle overgrep mot barn eller fremstillinger som seksualiserer barn, på annen måte som nevnt i § 204 første ledd.”

For så vidt gjelder overgrepsbildene i strl. 2005 § 311, er det klart at følgende handlinger nevnt i bokstav a-c – produksjon, anskaffelse, besittelse og tilgjengeliggjøring – er overtrådt dersom befatningen gjelder blader, VHS-kassetter eller DVD-filmer med det rettsstridige materialet. Det finnes mye rettspraksis som viser dette i tilknytning til det vanlige pornografiforbudet, men få avgjørelser for overgrepsbilder fordi det vesentlig foregår ved bruk av internett.[457] Men noen eksempler finnes, se for eksempel:

> Rt. 1995 s. 1894: De domfelte hadde solgt VHS-kassetter med overgrepsfilmer.
>
> RG 2006 s. 595: Foruten å ha overgrepsbilder lagret på datautstyret, hadde domfelte "en full ringperm av ordinær A4-størrelse inneholdende bilder som i all hovedsak åpenbart er grov barneporno."
>
> LG-2006-3339: Dom for besittelse av 10 000 bilder.
> "Samlingen var bygd opp gjennom datautskrifter, men er ikkje lagra som datafiler med tilhøyrande spreiingsfåre."

Etter ordlyden er imidlertid befatning med *meningsinnholdet* tilstrekkelig for overtredelse, jf. "fremstilling som seksualiserer barn…" i bokstav a. En fremstilling er noe som vises og som man oppfatter. En fremstilling som bæres av et medium, er en *presentasjon,* dvs. databasert informasjon i objektiv forstand (se kapittel 2). Og etter å ha sett på slike bilder kan man for eksempel si at man tenker på fremstillinger av seksuelle overgrep mot barn. Det betyr ikke at man tenker på å begå seksuelle overgrep, ei heller at man har bildet fysisk. Man kan for eksempel ha sett det på en skjerm (databasert informasjon i objektiv forstand). Deretter lagres fremstillingen i hukommelsen, noe som kan anses som en form for besittelse.

Likevel er det, som jeg kommer til, klart at alternativene produserer, anskaffer, besitter og tilgjengeliggjør, *ikke* rammer befatning med meningsinnholdet alene. Det gjelder et mulig unntak for anskaffelse og tilgjengeliggjøring av fremstillinger i sann tid, som jeg behandler til slutt.[458] Men *hovedregelen* er at de nevnte alternativene krever befatning med mediet. At

[457] Rt. 1979 s. 863 og Rt. 1979 s. 1418: Begge avgjørelsene gjaldt salg av utuktige magasiner og filmer; Rt. 1980 s. 1532: Omsetning av utuktige bildemagasiner, filmer og videobånd; Rt. 1985 s. 569: Utleie og salg av utuktige videokassetter, filmer og blader; Rt. 1987 s. 1194: Omsetning av utuktige blader, videokassetter og filmer.
[458] Kapittel 9.2.5.

loven er slik å forstå, viser jeg nedenfor, men først er det grunn til å spørre hvorfor loven er slik innrettet.

9.2.2 Rettspolitiske overveielser

Hvis man vender blikket mot *markedet* er et viktig formål med forbudet mot overgrepsbilder nettopp å hindre tilgang til *meningsinnholdet,* fordi det kan inspirere til å foreta slike overgrep som man har sett på bildene. Denne delen av begrunnelsen mot overgrepsbilder gjelder ikke hensynet til barnet på bildet, men til *andre barn* som er i brukerens "risikosone". I den forklarende rapporten til datakrimkonvensjonen (185 ETS) sies det således at

> "it is widely believed that such material and online practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging or facilitating sexual offences against children" (pkt. 93).[459]

Dette er gjentatt i pkt. 134 i den forklarende rapporten til Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk (201 ETS).

Ordlyden i strl. 2005 § 311 åpner for at de fire befatningsformene kan anses å være oppfylt ved kontakt med meningsinnholdet. Meningsinnholdet fremkalles ved en prosess; man kan si at man "produserer" ved å forestille seg innholdet, og "anskaffer" og "besitter" etter å ha sett på det. "Tilgjengeliggjøring" kan skje ved å lese opp slike fremstillinger (også tekst rammes av "fremstilling"), men det holder jeg utenfor siden jeg har avgrenset til bilder.[460]

Når de kognitive handlingene ikke rammes til tross for dekningen i ordlyden og det ville fremme det legislative formålet, skyldes det at man ikke har villet risikere at straffetrusselen skulle slå for bredt. *Skadefølgeprinsippet* som er et generelt prinsipp for straffelovgivningen, sier at straff forutsetter en handling. Lovgiver bør ikke kriminalisere det å tenke "onde tanker", for eksempel å fantasere om seksuelle overgrep mot barn. Det ville lede til en såkalt "sinnelagsstrafferett", hvor det er vanskelig å knytte ansvaret til ytre konstaterbare forhold med en påviselig skadelig effekt. I noen tilfeller kan det også oppstå problemer med den

[459] Se mer om hensynene bak straffebudet i *Sunde* (2006) kapittel 8.4 s. 226 flg., bl.a. om skadefølgeprinsippets to sider; på den ene siden hensynet til vern om barna på bildene, og på den andre hensynet til barna som kommer i risikosonen som følge av inspirasjonen fra bildene.
[460] Se kapittel 1.1.

moralske begrunnelsen for bruk av straff, men det slår ikke til her siden fremstillingene *er* en farlig inspirasjonskilde.

I overveielsene over prinsipper for kriminalisering ved forberedelsen av straffeloven 2005, står det blant annet at:

> "en psykisk innstilling, dvs. planer eller ønsker om å begå straffbare handlinger, ikke kan danne grunnlag for straffansvar, selv ikke av planer av utpreget kriminelt slag. I tillegg til subjektiv skyld må det kreves at det er foretatt en handling…".[461]

Når meningsinnholdet bæres av fysiske medier er handlingen enkel å konstatere, fordi befatningen gjelder mediet. Problemer oppsto da internett ble tatt i bruk for å skaffe materialet. Det kan skyldes at man ikke hadde tatt stilling til om det var tilstrekkelig for straff at man hadde sett på bilder, eller om det måtte kreves rådighet over dataene også. Videre var det et spørsmål om det var tilstrekkelig for straff at vedkommende hadde dataene på sin datamaskin, uten å ha åpnet dem for eksponering på sin egen skjerm.

På internett kan man skaffe seg tilgang til meningsinnholdet uten å skaffe seg varig rådighet over dataene. Separasjon av medium og innhold er vanlig, fordi nettet tilrettelegger for et "nærvær" til tross for fysisk fravær. Det gjelder ikke noe krav om *samtilstedeværelse* slik som i den fysiske verden. Derfor er det blitt en selvfølge at man kan anskaffe og tilby hva man vil når man vil på nettet. Teknologien besørger samhandling og konstant tilgang til ressurser, herunder overgrepsbilder, mens behovet for å ha rådigheten over mediet (dataene) forsvinner.[462]

For overgrepsbildene på nettet har dette betydning på den måten at innholdet er tilgjengelig selv om man ikke har mediet (dataene). Man kobler seg opp til et aktuelt nettsted, for eksempel preteensex.com, betaler en månedsavgift på 30 dollar og har fri tilgang til materialet som der er lagret. Dersom preteensex.com er en adgangsbasert tjeneste som ikke tillater nedlasting (for eksempel en "streaming"-tjeneste) er det følgelig "ydelsens *informative element"* som er det sentrale, slik *Frost* formulerer det, og brukeren får innholdet, men ikke

[461] Ot.prp. 90 (2003-2004) s. 88- 89. På s. 88 beskrives skadefølgeprinsippet slik: "Skadefølgeprinsippet bør være utgangspunkt og grunnvilkår for kriminalisering: Atferd bør bare gjøres straffbar dersom den fører til skade eller fare for skade på interesser som bør vernes av samfunnet".
[462] Opphevelse av samtidighetskravet mellom tid og sted er et dominerende kjennetegn ved modernitet, se for eksempel *Giddens* (1990) og avhandlingen kapittel 10.

dataene.[463] Formålet bak straffebestemmelsen tilsier straffansvar, noe som kunne vært oppnådd ved å gi anskaffelsesalternativet anvendelse på tilfellet. Men da har man antakelig ment at argumentene for straffansvar krysses av skadefølgeprinsippet. Man har lagt til grunn at befatningen med meningsinnholdet ikke er ytre konstaterbar slik at vilkåret om *handling* ikke har vært oppfylt.

Mellomlagringsfunksjonen i nettleseren leder til at kopier av bildene man har klikket på hos preteensex.com, legges i mellomlagringsområdet på datamaskinen. Slike filer blir kalt "tempfiler" ("Temporary Internet Files"). Brukeren har altså sett på bildene, men – teknisk sett – ikke fra de datafiler som var lagret på vedkommendes maskin. Den rådigheten man får som følge av mellomlagringen, er ikke ønsket og heller ikke årsaken til at man har sett på bildene (anskaffet seg meningsinnholdet). Også her har skadefølgeprinsippet vært ansett til hinder for straffansvar, noe som er synlig i den manglende vilje til å domfelle i disse situasjonene.[464]

9.2.3 Tilgangsalternativet rammer befatning med informasjonen

Ved innføring av *tilgangsalternativet* i strl. 2005 § 311 bokstav c, har lovgiver gitt klar hjemmel for straff i disse tilfellene. Alternativet rammer den som "forsettlig skaffer seg tilgang til" materiale som nevnt.[465] Dersom alternativet sammenholdes med lovens beskrivelse av det rettsstridige materialet, "fremstilling som seksualiserer barn…", er det klart at det i denne sammenheng *bare kan bety meningsinnholdet.* Tilgangsalternativet er nettopp ment å ramme befatning *uten* at man har rådighet over mediet. Tilføyelsen av tilgangsalternativet vitner om en utvikling i problemforståelsen. Det viste seg at lovgivers

[463] *Frost* (2002) s. 67-68. Se også avhandlingen kapittel 7.5.
[464] LE-2002-242, frifinnelse, besittelse av Temporary Internet Files, lagmannsretten konkluderte med at tingretten hadde anvendt for streng aktsomhetsnorm da man domfelte for uaktsom besittelse; RG 2004 s. 689, frifinnelse, logger på tiltaltes datamaskin viste 12 752 treff på «Lolita», "som er ei adresse med klar barnepornografisk profil". Videre var det slettet 52 bilder fra harddisken, og "i dei sletta filene blei funne fleire bilete med barnepornografisk innhald". Tempfilene ble ansett å være i besittelse objektivt sett, men det subjektive vilkåret var ikke oppfylt, verken forsett eller uaktsomhet. Dommen sier imidlertid ikke noe om hva tiltalte faktisk visste om mellomlagringsfunksjonen, så den konkrete bevisvurderingen fremstår som noe ufullstendig. RG 2004 s. 929, frifinnelse, tiltalte "forklarte at han stort sett hadde søkt bevisst" etter overgrepsbilder. Han var klar over den automatiske mellomlagringen. "Etter som tiltalte ikke ønsket at pornografiske bilder skulle være lagret på hans pc, slettet han tempfilene. Slettingen foretok han etter hver gang han hadde sett på bildene på internett"; RG 2005 s. 246, dom for besittelse av tre bilder og en film som tiltalte hadde sett på før han slettet dem. Men frifinnelse for flesteparten av bildene som hadde vært på tiltaltes datamaskin, i alt 2 250 bilder, fordi tiltalte etter at han ble klar over mellomlagringsfunksjonen stilte den "slik at lagringstiden ble redusert til 0 dager."
[465] Alternativet viderefører i noe videre form alternativet "den som mot vederlag eller planmessig gjør seg kjent med" overgrepsbilder, jf. strl. 1902 § 204 a bokstav a.

valg ikke var begrenset til å kriminalisere befatning med meningsinnholdet generelt eller å avstå fra kriminalisering. Det forelå også mulighet for å ramme handlinger som rettet seg mot meningsinnholdet, men som forutsatte aktivitet for å klikke seg inn på relevante tjenester.

Dermed løste lovgiver flere problemer. For det første fikk man klar hjemmel for å ramme reelt straffverdige handlinger, og dermed effektivisere barns beskyttelse mot seksuelle overgrep. Alternativet overholder skadefølgeprinsippets krav til handling, fordi det forutsetter aktivitet for å skaffe seg tilgang. Aktive søk for å skaffe seg tilgang til det rettsstridige materialet på nettet, er handlinger som kan registreres i logger hos lovbryteren og innholdsleverandøren, samt hos kredittkortselskapet dersom tjenesten er betalingsbelagt. Søk og bruk av slike tjenester materialiserer seg derfor på en ytre sett påviselig måte. Forarbeidene er dessuten klare med hensyn til at alternativet ikke skal ramme den som "uforvarende kommer i kontakt med" slikt materiale.[466]

Ved å skaffe seg tilgang til meningsinnholdet skaffer lovbryteren seg farlig inspirasjon som kan gå ut over barn i vedkommendes "risikosone". I tillegg er handlingen reelt straffverdig fordi den markerer etterspørsel overfor den kriminelle tilbyderen på nettet. Det stimulerer til nye overgrep mot barn som kontrolleres av produsentene for å dekke "behovet" i markedet. Etterspørselen på nettet er faktisk konstaterbare handlinger, jf. skadefølgeprinsippet.

9.2.4 Handlinger som gjelder data og fysiske medier

Med innføring av tilgangsalternativet ble det også klart at alternativene produserer, anskaffer, besitter og tilgjengeliggjør gjelder *mediet* som bærer det rettsstridige innholdet. Ellers ville det ikke vært behov for tilgangsalternativet. For internettrelaterte handlinger betyr det at de fire befatningsformene gjelder *data* som bærer det rettsstridige innholdet.

Data er altså et medium som straffebudet rangerer likt med fysiske bærere som blader, VHS-kassetter og DVD-filmer. Dersom straffebudene hadde brukt begrepet "gjenstand" ville data

[466] "Alternativet vil typisk ramme oppsøking av slikt materiale på internett. Derimot er det ikke meningen å ramme den som uforvarende kommer over slikt materiale, heller ikke ved uaktsomhet", se Ot.prp. 22 (2008-2009) s. 266. Det fremgår at bestemmelsen tar særlig hensyn til artikkel 20 nr. 1 bokstav f i Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk (201 ETS). Bestemmelsen forplikter staten til å kriminalisere "bevisst å skaffe seg tilgang til barnepornografi gjennom informasjons- og kommunikasjonsteknologi". Ifølge den forklarende rapporten til konvensjonen (pkt. 140) vil forsett om å skaffe seg tilgang til overgrepsbilder særlig kunne påvises ("may notably be deduced"), dersom handlingen har skjedd flere ganger ("recurrent") eller tilgang er skaffet mot betaling.

helt klart vært omfattet på lik linje med de fysiske objektene.[467] Forskjellen mellom data og fysiske bærere er bare at man må bruke datamaskinen for å skaffe seg den rådigheten som straffebudet beskriver, de kan kalles "middelbare" medier.[468]

Straffebudet lener seg ikke på det funksjonelle gjenstandsbegrepet, fordi det er helt klart at rådigheten over det fysiske lagringsmediet ikke er det sentrale i en elektronisk kontekst. Det avgjørende er om *data* er håndtert på en måte som loven beskriver. Besittelsesvilkåret er oppfylt både for data som er lagret lokalt hos lovbryteren og for data vedkommende har rådighet over i "internettskyen".[469]

Siden besittelsesvilkåret er oppfylt også når dataene er lagret annet sted enn på eget utstyr, skiller bestemmelsen prinsipielt mellom det fysiske utstyret og dataene, og dataene behandles som et objekt i seg selv.

Overgrepsbilder *produseres og besittes* ved å ta bilde av et seksuelt overgrep og lagre det. Disse datafilene er "ting" som kan inndras, se kapittel 5. Når det gjelder alternativene *anskaffelse* og *tilgjengeliggjøring*, har jeg tidligere bemerket at de tilføyer handlingene et preg av dynamikk, fordi de åpner for å inkludere *overføring* av data mellom datamaskiner i nettet. Logisk sett burde lovteksten ha plassert tilgjengeliggjøring før anskaffelse, fordi tilgjengeliggjøringen kommer først, men selve tingen som den straffbare befatningen gjelder, er altså underveis. Strl. 2005 § 311 rammer derfor befatningen med data som selvstendige objekter uavhengig av den fysiske bæreren, ikke bare når dataene er lagret, men også når de er under overføring.

Lovgiver har bevisst gitt straffebudet teknologinøytral utforming i vid forstand, fordi formålet har vært nulltoleranse mot overgrepsbilder, såfremt grunnleggende kriminaliseringsprinsipper samtidig overholdes.[470] Den vide teknologinøytraliteten gjelder *medier*, om mediet er en fysisk bærer eller data er irrelevant, og slik utviklingen har båret av sted er data blitt det viktigste mediet for bestemmelsens befatningsformer. På samme måte som pornoblader er

[467] Det er jo "gjenstand" som ellers brukes i straffebudene, jf. fremstillingen i det foregående.
[468] Smlg. opphavsrettens "middelbare" eksemplar, se kapittel 7.3.
[469] Se kapittel 5.3.2.3 om besittelsesvilkåret.
[470] Se for eksempel Ot.prp. nr. 28 (1999-2000) (seksuallovbrudd) hvor det i spesialmotivene til strl. 1902 § 204 bokstav d om overgrepsbilder, uttales: "I utgangspunktet er målsettingen at all befatning med barnepornografi skal være straffbar." Smlg. *Sunde* (2006) s. 226 flg., hvor det også redegjøres for den internasjonale målsettingen om nulltoleranse.

gjenstander som selges, anskaffes og besittes, er datafiler gjenstander som selges, anskaffes og besittes. Det er ikke noen konseptuell strafferettslig forskjell mellom mediene.

Denne analysen viser at data behandles som "gjenstand" også i strl. 2005 § 311, som *ikke* bruker begrepet. Og data som gjenstand ses atskilt fra den fysiske bæreren.

Det betyr også at straffebudets formulering om at befatningen må gjelde "fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn", er en forenkling. For så vidt gjelder de fire hovedbefatningsformene må det innfortolkes krav om at befatningen gjelder et *medium*. En mer presis, men språklig sett tyngre formulering av lovteksten, ville for eksempel vært som følger (for produksjonsforbudet):

> a) den som produserer medium med fremstilling av seksuelle overgrep av barn …,

Tilsvarende kunne man gjøre med alternativene anskaffer, besitter og tilgjengeliggjør.

Direkte kan lovens formulering sies å være en fiksjon fordi fremstillingene *qua meningsinnhold,* ikke kan produseres, anskaffes, besittes eller tilgjengeliggjøres. Fiksjonen er ikke ment å føre noen bak lyset. Det er bare en enkel uttrykksform og en arv fra den gang befatning med fysiske medier var det vanlige. Tidligere fungerte ordlyden fint for de praktiske tilfellene og det var neppe foranledning til å drøfte strafferettslige konsekvenser av separasjon mellom medium og meningsinnhold før internett gjorde situasjonen vanlig.

9.2.5 Sanntidsoverføringer

Alternativene "anskaffer" og "tilgjengeliggjør" gjenstår stadig som litt kompliserte tilfelle, og jeg tenker da på *sanntidsoverføringene.* Man kan nemlig overføre seksuelle overgrep på nettet ved bruk av web-kamera *mens overgrepene pågår*. Man kan også forlede mindreårige til å utføre seksuelle handlinger med seg selv mens man ser på i sann tid. Et eksempel på det siste har man i Rt. 2009 s. 140, hvor lovbryteren hadde forledet jenter i alderen 9-16 år til å filme seg selv i sann tid ved bruk av web-kamera og MSN. For dette ble han domfelt for overtredelse av strl. 1902 § 200 annet ledd annet punktum som rammer den som forleder barn under 16 år til å utvise seksuelt krenkende eller annen uanstendig atferd. Den korresponderende bestemmelsen i strl. 2005 § 305 bokstav b presiserer at den gjelder såfremt

forholdet ikke rammes av strengere bestemmelser. Jeg har sitert bestemmelsen i kapittel 5.3.2.2. Der har jeg tatt til orde for at strl. 2005 § 305 bokstav b bør anvendes i konkurrens med, og ikke anses å konsumere, forbudet mot å medvirke til produksjon av overgrepsbilder, fordi man da både får frem forledelsen og fremstillingen av personvernkrenkende bilder.

Men etter ordlyden er også tilgjengeliggjørings- og anskaffelsesalternativene anvendelige på sanntidsoverføringer. Jeg ser da bort fra eventuell lagring av filmene, som er anskaffelse og besittelse av data. Lagring er ikke nødvendig for å foreta overføringen. Overføringen av filmen slik at mottakeren ser på mens filmingen skjer, er tilgjengeliggjøring/anskaffelse av den rettsstridige "fremstilling" som nevnt i strl. 2005 § 311 bokstav a. Man får tilgang på *meningsinnholdet* uten å ha rådighet over mediet. Det underbygger at "fremstilling" betyr meningsinnholdet.

Fortolkningen slår ikke bena under den tidligere konklusjonen om at anskaffelse og tilgjengeliggjøring forutsetter befatning med mediet. Poenget er at vilkåret om befatning med mediet må innfortolkes, unntatt ved sanntidsoverføring. Da kan man holde seg direkte til ordlyden.[471]

Ved sanntidsoverføring skjer det ingen "tingliggjøring" av data. Slike overføringer kan ikke gjenkjennes ved sjekksumidentifikasjon, for de har jo ikke vært lagret og man er avskåret fra å gi dem en forhåndstildelt identitet. Men dette viser bare at data kan foreligge i ukontrollert og kontrollert form.[472]

9.3 Skadelig dataprogram

Også her skal jeg behandle spørsmålet om data fungerer som en gjenstand i forbindelse med overtredelsen av straffebudet, og om det er nærliggende å likestille data med fysiske

[471] Forarbeidene behandler sanntidsoverføringer i forhold til strl. 20005 § 305 bokstav b, se Ot.prp. nr. 22 (2008-2009) kapittel 7. 14 og 16.7. Det kan også anses som en "fremvisning", jf. strl. 2005 § 310, dvs. "live" overgrepsforestilling med barn. Bestemmelsen er "i hovedsak ment å ramme publikum eller «kunden» " og bestemmelsen rammer "også den som får slike fremvisninger direkte overført gjennom elektronisk kommunikasjon", se Ot.prp. nr. 22 (2008-2009) s. 447. I så fall har man fremdeles et problem med ansvaret for den som tilgjengeliggjør. Uttalelsen om at den elektroniske overføringen rammes av strl. 2005 § 310 bryter med systematikken ellers i forholdet mellom § 310 og § 311, hvor nettopp den ene gjelder fremvisning og den andre gjelder fremstilling. Overføring er en fremstilling.
[472] Se kapittel 7.4.1 og 7.6.2.

gjenstander ved fortolkning av bestemmelsen. Jeg konsentrerer meg om skadelig dataprogram som står nevnt i bokstav b i strl. 2005 § 201.

Strl. 2005 § 201 lyder:

> ”Med bot eller fengsel inntil 1 år straffes den som med forsett om å begå en straffbar handling uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen
>
> a) passord eller andre opplysninger som kan gi tilgang til databasert informasjon eller datasystem, eller
>
> b) dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem. På samme måte straffes den som uten forsett om å begå en straffbar handling besitter et selvspredende dataprogram, og besittelsen skyldes uberettiget fremstilling eller anskaffelse av programmet.”[473]

Skadelig *objektkode* er beregnet på å bli ”lest” og behandlet av datamaskiner, og er data i hele sitt livsløp.[474] Programmet kan anses som et fungerende verktøy med skadeevne, og det er et klart formål med straffebudet å ramme nettopp slike dataprogram som det finnes mye av i nettet. De går under navn som ”virus”, ”orm”, ”malware” og ”exploits”. Derfor omfatter ”dataprogram” i strl. 2005 § 201 bokstav b *data.* Produksjon, anskaffelse, besittelse og tilgjengeliggjøring gjelder altså data, på samme vis som for overgrepsbildene.

I henhold til alternativet ”eller annet ” som er inntatt ved siden av ”dataprogram” i bokstav b, rammes også befatning med fysiske innretninger. Skadelig objektkode og fysiske innretninger er således likestilt i forhold til de straffbare befatningsformene. Dette er helt klart både etter ordlyd (”dataprogram eller annet”) og forarbeider. I forarbeidene sies det at

> ”Bestemmelsen vil typisk ramme forskjellige former for datavirus og hackerverktøy. Uttrykket «eller annet» må forstås vidt, og omfatter enhver logisk eller fysisk innretning som er særlig egnet som middel til å begå straffbare handlinger rettet mot databasert informasjon og datasystem.”[475]

[473] Strl. 1902 § 145b er mindre omfattende enn strl. 2005 § 201. Strl. 1902 § 145b første ledd lyder: ”Den som uberettiget gjør tilgjengelig for andre passord eller andre data som kan gi tilgang til et datasystem, straffes for spredning av tilgangsdata med bøter eller fengsel inntil 6 måneder eller begge deler”. Etter annet ledd øker strafferammen til fengsel inntil 2 år ved grov overtredelse. Se Ot.prp. nr. 40 (2004-2005) om bakgrunnen for bestemmelsen. Det finnes noen andre bestemmelser som innenfor sine områder svarer til strl. 2005 § 201. Den ene er strl. 1902 § 262 første ledd som avløses av strl. 2005 § 203 første ledd. Den andre er åvl. § 53a annet ledd og § 53c, jf. § 54. Forholdet mellom bestemmelsene reiser noen harmoniseringsspørsmål som man har bemerket, men ikke løst ved arbeidet med straffeloven 2005, se omtale av problemet i avhandlingen kapittel 1.1 med videre henvisninger.

[474] Se kapittel 4.4.

[475] Ot.prp. nr. 22 (2008-2009) kapittel 16.2 s. 401. Smlg. Datakrimutvalget som sier at bestemmelsen ”likestiller skadelig utstyr med skadelig dataprogram.”, se NOU 2007: 2 kapittel 9.11 s. 160.

Datakrimutvalget nevner piratdekoderkort og fysisk tastetrykksregistrator som eksempler på slikt fysisk utstyr.[476] Piratdekoderkort er fysiske smartkort som kan dekode krypterte signaler. Rt. 1995 s. 35 (Smartkort) involverer slike piratdekoderkort.[477] I Rt. 1994 s. 1610 (BetalTV) som er nevnt i forbindelse med drøftelsen av databegrepet i kapittel 2.3.2, var såkalte "piratfiltere" brukt. Også filtre er fysiske innretninger som omfattes av "eller annet" i strl. 2005 § 201 bokstav b. Hvilke fysiske innretninger som til enhver tid rammes av loven, avhenger av utviklingen i tjenestetilbudet, beskyttelsesmekanismene og omgåelsesteknologien.

En *fysisk* tastetrykksregistrator er en gjenstand som festes i forlengelsen av tastaturkabelen (og som kan se ut som en ordinær del av denne). Gjenstanden registrerer og lagrer signaler som sendes fra tastaturet til datamaskinen.[478] En tastetrykksregistrator kan også være et dataprogram som er installert på datamaskinen. Programmet kopierer og sender signalene som skrives til maskinen, til sin "oppdragsgiver" som er en annen maskin i nettet.[479] I dette tilfellet omfattes tastetrykksregistratoren av alternativet "dataprogram". Et annet eksempel på en fysisk innretning som omfattes av "eller annet" i bokstav b, kan kanskje være en såkalt "falsk basestasjon" ("IMSI-catcher") som kan fange opp identiteten til en mobiltelefon som er i området.[480]

[476] NOU 2007: 2 s. 160.
[477] I Smartkortdommen ble salg av piratdekoderkort for å få tilgang til betalingsbelagte fjernsynssignaler ikke ansett straffbart etter strl. 1902 § 145 annet ledd eller åvl. § 2, jf. § 54. Ved innføringen av strl. 1902 § 262 kom det hjemmel for å ramme slike handlinger (tilføyd ved lov nr. 15/1995). I Nedenes herredsretts dom 1. juli 1998. (Sak nr. 98-00235) ble en mann dømt til fengsel i 8 måneder for salg og koding av av 29 000 piratdekoderkort og ilagt kr. 1, 8 millioner i inndragning av utbytte. Saken er omtalt hos *Sunde* (2006) s. 182.
[478] *Caloyannides* (2004) s. 54 kap. 4.3. "Commercial hardware keystroke loggers".
[479] *Caloyannides* (2004) s. 57 kap. 4.4 om "Commercial software keystroke loggers".
[480] Metoden omfattes av strpl. § 216b bokstav c "å identifisere [elektronisk kommunikasjonsanlegg] ved hjelp av teknisk utstyr". Metoden er omtalt i Ot. prp. nr. 60 (2004-2005) kapittel 8.5. I proposisjonen er det lagt til grunn at det er behov for lovhjemmel for bruk av metoden. Det er vel imidlertid ikke helt klart hva slags straffebud som krenkes, med mindre utstyret også brukes til å avlytte samtale, noe som rammes av strl. 1902 § 145 a / strl. 2005 § 205. Det er mulig at man har ansett oppfanging av mobilidentiteten som en del av "privat liv", jf. EMK 8, slik at lovhjemmel av den grunn er nødvendig. Man får jo også rede på den fysiske lokaliseringen til den som bærer telefonen på seg, noe som i hvert fall omfattes av EMK art. 8. Det er derfor mulig at bruk av slikt utstyr kan anses om en fredsforstyrrelse, jf. strl. 1902 § 390 a. Etter Rt. 1995 s. 1983 (Speil-dommen) er det neppe et krav at den personen som utsettes for "sporingen" blir klar over fredsforstyrrelsen. I "speildommen" fant nemlig Høyesterett at det var utvist uanstendig atferd ved "kikking", selv om den som var blitt observert ikke hadde lagt merke til det. I vilkåret om "samtykke" kunne det ikke innfortolkes et krav om at fornærmede faktisk hadde blitt klar over at vedkommende var observert og hadde en rett til å reservere seg mot "kikkingen" (se strl. 1902 § 201, tidligere § 212). Tilsvarende resonnement kan føres for bestemmelsen om fredsforstyrrelser.

Eksemplene viser at verktøyene ikke nødvendigvis er bundet til den ene eller andre representasjonsformen, tastetrykksregistratoren kan således være en fysisk innretning og et dataprogram. Det er derfor naturlig at bestemmelsen likestiller verktøy som har samme skadeevne, i forhold til befatningsformene. Den praktiske forskjellen som går ut på at piratdekoderkort og fysisk tastetrykksregistrator håndteres ved en fysisk handling, mens dataprogrammet håndteres ved hjelp av datamaskinen, er ikke rettslig relevant.[481] Det betyr at også denne bestemmelsen behandler data som "gjenstand", både som lagret og under overføring. Det er altså tydelig at data og fysiske ting er likestilte etter straffebudet.

10 Oppsummering av forholdet mellom data, informasjon og fysiske objekter

Analysen av forholdet mellom data og gjenstandsbegrepet var i utgangspunktet en jakt på rettslige fiksjoner. Jeg antok at fordi nettverksteknologien opphever forutsetningen om samtidighet mellom tid og sted, ville tradisjonelle strafferettslige konsepter blir satt på prøve. I den fysiske verden er vi vant til samtilstedeværelse. Ting som vi kan "kan ta og føle på" er fysisk sett på samme sted som oss selv. Motsatt aksepterer vi at ting som er andre steder enn oss selv, er utenfor rekkevidde.

Et kjennetegn på modernitet er at dette premisset endres.[482] Det har mange konsekvenser, for eksempel utviklingen av "risikosamfunnet" som kjennetegnes av at stadig flere fenomener *som er andre steder*, oppfattes å angå oss *her vi er*.[483] En annen konsekvens er at det oppstår et tomrom som før var dekket av fysisk samhandling. *Giddens* kaller det behovet som tomrommet skaper, for "trust".[484] "Trust" er en sosialt betinget forventning om oppfyllelse av en handling, om å bli møtte med en reaksjon m.v., når man selv har foretatt seg noe.[485] Der man tidligere kunne basere seg på fysisk samhandling må det kompenseres med *mekanismer*

[481] Det er bare skadeevnen som er relevant, jf. "at dataprogrammet eller innretningen må være «særlig egnet» som middel til å begå straffbare handlinger rettet mot data eller datasystemer … denne egenskapen må fremstå som programmets eller innretningens nest fremtredende …", se Ot.prp. nr. 22 (2008-2009) kapittel 2.8.3.8.
[482] Dette har *Giddens* gitt en kjent beskrivelse av i *Consequences of Modernity,* se *Giddens* (1990).
[483] Den skoledannende teorien om risikosamfunnet har vel først og fremst hatt den tyske samfunnsviteren *Ulrich Beck* i førersetet.
[484] *Giddens* (1990) s. 33: "Trust is related to absence in time and in space. There would be no need to trust anyone whose activities were continually visible and whose thought processes were transparent, or to trust any system whose workings were fully known and understood."
[485] *Giddens* (1990) s. 33-36.

som skaper "trust".[486] Elektronisk signatur er et aktuelt eksempel på en "trust"-mekanisme. Overført til strafferetten er poenget at gapet mellom tid og sted er en drivkraft for å utvikle *nye konsepter* som gjør at vi kan innrette oss *på samme måte som før*. I dette ligger en konservatisme som tilrettelegger for bruk av fiksjoner for å kompensere for forandring.

Nettverksteknologien gjør det mulig å utnytte ressurser som er et annet sted enn en selv. Det gir også mulighet for selv å ha et nærvær - være handlende - et annet sted enn man faktisk er.[487] Det har gitt store fordeler og betydd en sterk drivkraft for samfunnsmessig utvikling. Her tar jeg bare opp det negative, nemlig problemet med rettsstridig innhold i nettet.

Via nettverket kan vi sende skadelig dataprogram til en datamaskin som står på den andre siden av kloden, og den vil ha nådd destinasjonen i løpet av sekunder. Via nettverket kan vi se på overgrepsbilder uten å laste dem ned, og vi kan anskaffe vår egen samling ved kjøp i en kriminell nettbutikk eller bytte ved fildeling. Vi sprer og anskaffer data og databasert informasjon med "hele verden som arena" uten å gå utenfor vår egen stue. Våre egne data (ressurser) behøver vi heller ikke ha på datamaskinen hjemme. Vi kan ha dem plassert hos en nettvert i "internettskyen" uten at det endrer utnyttelsesmuligheten. Nettvertens server er vår egen virtuelle datamaskin. Innenfor denne virkeligheten skal strafferettslige konsepter som "produserer", "besitter", "anskaffer", "gjør tilgjengelig", "gjenstand/ting", "beslag" og "inndragning" fungere.

Jeg tenkte derfor at sjelden har forholdene ligget bedre til rette for å avdekke noen fiksjoner og vise hvordan ting "egentlig er". Jeg bruker da 'rettslig fiksjon' slik *Fuller* gjør, nemlig om et utsagn som man vet er feil, men som ikke er ment å føre noen bak lyset. Fiksjonen er ikke en løgn, ei heller et uttrykk for en feilslutning; den er ikke sann, men kan være hensiktsmessig fordi den kort oppsummerer essensen i det man ønsker å uttrykke, samtidig som man kan regne med at andre forstår uttrykksmåten.[488] Rettslige fiksjoner kan således være et nyttig

[486] *Giddens* (1990) bruker penger som eksempel. Moderniteten innebærer en konvertering fra verdi i gull til regulære banktransaksjoner, hvor verdien ikke ligger i pengerepresentativet, men i en garanti stilt av en tredjepart (sentralbanken). Tredjeparten fyller behovet for "trust".
[487] *Lyon* anser dette som en dikotomi mellom "presence" og "absence". Hans poeng er nærmest det motsatte av *Giddens,* nemlig at moderne teknologi *tilrettelegger for samtilstedeværelse* ("copresence") selv om kroppen er fraværende. Han kaller fenomenet "disappearing bodies", *Lyon* (2001) kapittel 1 s. 15 flg. Den utstrakte bruken av teknologi er i seg selv en egenskap ved overvåkingssamfunnet, og er ikke noe negativt i seg selv. Teknologiutviklingen innebærer at gamle forståelser av 'overvåking' (særlig 'panopticon') bør revurderes. Det er mer nærliggende at teknologien dekker moderne behov, og at man tenger ny konseptuell forståelse av fordeler og ulemper. Se *Lyon* (2001) kapittel 7 om nye retninger i overvåkingsteorien, s. 107 flg.
[488] *Fuller* (1967) s. 1.

redskap fordi vi, med *Fullers* ord, er tvunget til å håndtere nye problemer innenfor et eksisterende konseptuelt apparat, som naturlig nok, aldri kan være helt adekvat for fremtidige forhold. [489]

I forhold til de *strafferettslige* spørsmål jeg har behandlet, har det blitt avklart at nettverksteknologiens separering av *data* og *informasjon* har relevans, samtidig som *data* og *fysiske objekter* likebehandles selv om de er forskjellige typer "grunngoder" (*bits* v. atomer).

I forholdet mellom data og informasjon har jeg funnet én fiksjon, nemlig at man formulerer seg som om det er tilstrekkelig at befatningen med overgrepsbilder gjelder meningsinnholdet. Men det er ikke tilstrekkelig for straffeskyld, befatningen må gjelde dataene. Som tidligere nevnt skyldes nok uttrykksmåten at den har vært praktisk, og at den ikke var egnet til å villede før man fikk nettverksteknologien.[490] For befatning med skadelig dataprogram foreligger det ikke en tilsvarende fiksjon, fordi det er – når man tenker etter – helt klart at bestemmelsen mener "data" når det er tale om skadelig objektkode.

Dette bringer meg tilbake til begrunnelsen for å anvende et klart begrepsskille mellom 'data' og 'informasjon', jf. kapittel 2. Det er nødvendig fordi det er strafferettslig relevant, og bidrar til å avklare hva rettsspørsmålene gjelder. Innen personopplysningsretten har *Bygrave* stilt seg undrende til at man ikke har vært mer stringent i så henseende.[491] Innen strafferetten har man kanskje ikke hatt samme oppfordring til å være seg bevisst forholdet mellom 'data' og 'informasjon', fordi rettsområdet tradisjonelt har vært så fokusert mot vernet om liv, legeme og fysisk eiendom. Uansett er det hevet over tvil at hvorvidt man taler om 'data' eller 'informasjon' kan ha avgjørende strafferettslig betydning, og alt tyder på at betydningen er økende. Jeg er enig i *Bygraves* observasjon om at

> "legal rules are increasingly being formulated such that their scope does turn on the ambit of basic information concepts."[492]

[489] *Fuller* (1967) s. 65 sier: "We are forced to deal with new problems in terms of an existing conceptual apparatus which in the nature of things can never be entirely adequate for the future".
[490] Se kapittel 9.2.4.
[491] *Bygrave* (2006) s. 121.
[492] *Bygrave* (2006) s. 122.

Det er en effekt av at vi lever i "informasjonssamfunnet", en effekt som også har slått inn i strafferetten.[493] For de reglene avhandlingens analyse har vært innom, gjelder det ikke bare bestemmelser med praktisk anvendelse på nettet, som strl. §§ 201 og 311, men også bestemmelser med begrepene "gjenstand" og "ting". De kan omfatte data, men ikke informasjon. Det er utgangspunktet, men hvorvidt den enkelte regel omfatter data, må avgjøres ved en konkret fortolkning:

- Tyveri: Omfatter ikke data på grunn av vilkåret om besittelsesforrykkelse.

- Underslag: Omfatter data fordi nettverten har dataene i sin besittelse, og "tilegnelse" ikke krever besittelsesforrykkelse.

- Skadeverk: Omfatter data fordi de kan endres, slettes og gjøres utilgjengelige.

- Ulovlig bruk: Data omfattes, for eksempel utnyttelse av et kunderegister for utsendelse av spam.

- Overgrepsbilder: Gjelder hovedsakelig befatning med data. Tilfeller hvor befatning med informasjonen er tilstrekkelig for straffansvar, er spesialregulert.

- Skadelig dataprogram: Omfatter data, men *kan* også omfatte informasjon (kildekode). Det er upraktisk.

- Inndragning: Kan foretas i data, men informasjon kan ikke inndras.

- Beslag for å sikre et inndragningskrav: Kan tas i data, ikke i informasjon.

Avhandlingen har også avdekket at data er "gjenstand" på linje med fysiske objekter. Uttalelser om at data ikke er "gjenstand", er ikke en fiksjon etter den definisjonen jeg har brukt. Utsagnet er feil, men avgiver vet ikke at det er feil. Selv om utsagnet ikke er ment å føre noen bak lyset, blir resultatet feil, og representerer ikke en "forenklet" oppsummering av rettstilstanden. Situasjonen synes å ha sin årsak i altfor utilstrekkelige beskrivelser av data, og

[493] Se kapittel 8.2.

en viss glidning over i informasjon (i betydningen ”meningsinnhold”). Da må man kompensere med fiksjoner, som for eksempel å pretendere at data beskyttes gjennom læren om det funksjonelle gjenstandsbegrepet. I realiteten gis data et direkte strafferettslig vern.

Gjennomgående likestiller loven data med fysiske objekter, både slike som er lagret og som er under overføring, jf. ”anskaffer” og ”tilgjengeliggjør”, se også ”overfører … *informasjon*” i strl. 2005 § 206 om fare for driftshindring. Her menes *data* som overføres over nettverk fra en datamaskin til en annen. Den asymmetriske rettighetssituasjonen som er vanlig ved web 2.0, viser også at data behandles selvstendig. Straffelovens anvendelighet på web 2.0-situasjonen er ikke trukket i tvil.

Det foreligger altså likestilling mellom data og fysiske objekter, ikke mellom data og informasjon. Den vide rettslige teknologinøytraliteten gjelder mellom fenomener som har en ytre manifesterbar representasjon, ikke mellom kognitive prosesser og de nevnte objektene. Dette resultatet virker helt rimelig.

Rettslig etablering av data som selvstendig objekt leder til at det er langt lettere å forestille seg inndragning i nettet som strafferettslig konsept. Data er objekter som finnes naturlig i elektroniske nettverk, slik man naturlig finner biler på en vei og bagasje på et transportbånd. Da er det vel også slik at om samfunnet undergår en utvikling som kan anses dramatisk (”paradigmeskifte”), har strafferetten en tidsbestandighet også for å håndtere problemer avfødt av nettverksteknologien. *Eng* har i mer generell kontekst drøftet om jussen på linje med naturvitenskapen undergår ”paradigmeskifter”, og konstaterer at

> ”paradigme og paradigmeskifte anser vi lite fruktbare i forhold til rettsdogmatikken. Noe av rettsdogmatikkens egenart i vitenskapsteoretisk forstand ligger i at den i motsetning til en del andre fag og vitenskaper i *svært liten grad* undergår paradigmeskifter.”[494]

Denne observasjonen er også dekkende for analysene jeg har utført i forhold til data som strafferettslig objekt. Problemene har vist seg mer å ligge i uklar begrepsbruk og hvordan vi ”tenker på ting”, enn i jussen. Konklusjonen er at strafferetten konseptualiserer data som ”gjenstand” og ”ting” og det gir grunnlag for å drøfte muligheten for inndragning av data i nettet.

[494] *Eng* (2007) s. 545.

V Inndragning av dubletter

11 To tilnærminger til inndragning av dubletter

11.1 Problemstilling

I denne del V innledes drøftelsen av automatisert inndragning i nettet. Her behandles det materielle inndragningsgrunnlaget for dublettene. I del VI fullføres drøftelsen med å vurdere om retten til privatliv og ytringsfrihet setter grenser for automatisert inndragning, jf. EMK art. 8 og 10.

Problemstillingen er om det finnes rettsgrunnlag for at inndragningen av datafilen i straffesaken kan få rettsvirkning for dublettene, slik at også de anses for å være inndratt. Det er en forutsetning for automatisert fullbyrdelse av inndragningen i nettet. I kapittel 5.9 pekte jeg på muligheten for å beslutte inndragning av dublettene med hjemmel i strl. 2005 § 74 tredje ledd, dvs. uten at lovbryteren eller besitteren har kjent oppholdssted i Norge. Bestemmelsen forutsetter imidlertid at tingen er beslaglagt. Det følger av henvisningen "på de vilkår som er nevnt i annet ledd", og i annet ledd nevnes "beslaget".[495] Dublettene i nettet er rent fysisk ikke i beslaget. Men de har en kjent identitet som gjør at de kan gjenkjennes. Dublettene er bare gjentakelser av en opprinnelig instans – kildefilen – hvorav én er inndratt.

Jeg ser to mulige rettsgrunnlag etter gjeldende rett: Det ene er at dublettene anses som like eksemplarer i en "orden", hvor alle inndras under ett i henhold til en felles dataidentitet. I så fall er denne "ordenen" "tingen" som inndras, jf. strl. 2005 § 69. Det andre grunnlaget er at datafilen i beslaget og dublettene i nettet anses som utslag av ett og samme fenomen ("ting") som inndras, jf. strl. 2005 § 69. I begge tilfeller må fullbyrdingen i nettet skje med referanse til dataidentiteten, fordi det er denne som overføres fra RDB til filtrene i nettet.

Inndragningen fullbyrdes i nettet ved bruk av filterteknologi som får "input" i form av dataidentiteten til de inndratte dublettene. Dermed bringes instruksen til datasystemet ned på et helt konkret plan, slik: "Dubletter med dataidentitet "NN" skal blokkeres". Filterteknologien er en *mekanisme* for fullbyrding av inndragning ved blokkering av inndratte datafiler. Mekanismen oppdateres fortløpende med dataidentiteten til nye inndratte datafiler.

[495] *Matningsdal* (1987) s. 491 understreker at det må være foretatt et formelt gyldig beslag.

Jeg antar at den tekniske mekanismen må karakteriseres forskjellig i forhold til de to rettsgrunnlagene. Dersom inndragningen fullbyrdes mot dublettene som følge av at "ordenen" de tilhører er inndratt, fremstår mekanismen som et praktisk verktøy for å gjennomføre beslutningen. Hver blokkering er et tilfelle av fullbyrding overfor et selvstendig objekt.

Dersom inndragningen av dubletter fullbyrdes på grunnlag av at de er en del av samme fenomen som datafilen i straffesaken, synes mekanismen å være en direkte forlengelse av inndragningsbeslutningen. Med "input" om dataidentitetene integreres *subsumsjonen* i fullbyrdelsesmekanismen, som reagerer på utslag av fenomenet ved blokkering. I dette tilfellet kan man tale om rettslig programmering.

11.2 Betydningen av at inndragningen skjer automatisert

11.2.1 Internett som samfunnsområde

Inndragning av dubletter forutsetter at elektroniske nettverk som internett og mobile nettverk, anses som deler av samfunnet hvor politiet har kompetanse til å utføre sine oppgaver i likhet med andre samfunnsområder. Denne forutsetningen har ikke bestandig vært ukontroversiell, noe som gjenspeilte seg i en heftig debatt om internettets "natur" fra midten av 1990-tallet og inn på 2000-tallet.[496] Jeg anser en slik diskusjon for å være lite fruktbar. Det er ikke tvilsomt at aktiviteten i det elektroniske nettverket omfattes av rettsreglene, og oppfatninger om at internett skulle være "et annet sted" med egen jurisdiksjon (suverenitet), eventuelt helt være unndratt alminnelige lover og regler, må anses å være helt forlatt.[497] Et eksempel på at rettshåndhevende virksomhet faktisk utføres på nettet, er det såkalte "Kripos-filteret", hvor Kripos i et samarbeid med tjenesteyterne stenger nettsteder som tilgjengeliggjør overgrepsbilder.[498]

[496] Se de innledende kapitlene hos *Goldsmith* (2006). *Murray* (2007) vier store deler av boken sin til disse diskusjonene; *Lessig* ble berømt i første omgang for å ha påpekt at internett var "regulable" stikk i strid med det "cyberlibertarians" trodde, men ikke på grunn av lovgivers initiativ, men på grunn av at programvaren (teknologien) kom til å bestemme brukernes frihet ("code is law"), se *Lessig* (1999), som skilte mellom to typer "lov"; teknologiens lov skapt av IKT-industrien på den amerikanske vestkysten og formell lov skapt av lovgivende organer i Washington D.C. ved den amerikanske østkysten, derav uttrykkene "West Coast Code" og "East Coast Code". *Lessig* opprettholder synspunktene i *Lessig* (2006).

[497] Se for eksempel *Schellekens* (2006) s. 51 som analyserer "what holds off-line should also hold on-line" (se mitt kapittel 6.4.2). Han påpeker at det for eksempel kan innebære følgende påstand: at "the Internet is not beyond the law. In principle, the law is applicable in on-line situations". *Schellekens* kommentar er at denne posisjonen har "lost its function. Nobody seriously contends that the law is not applicable to on-line situations." (s. 56).

[498] Filteret er omtalt i kapittel 1.2 og 14.4.

Noe av kritikken mot å tenke på internett som et samfunnsområde, har rettet seg mot uheldige virkninger av å basere rettslige løsninger på metaforer fra den fysiske verden. *Lemley* har påpekt at "cyberspace" ikke er en god metafor siden internett ikke er et område i fysisk forstand, og at tatt på ordet er uttrykket latterlig ("faintly ludicrous") siden ingen person er inne i nettverket.

Men internett må anses som et samfunnsområde selv om det også er et elektronisk nettverk. Spørsmålet er om rettsregelen virker for den aktuelle aktiviteten på nettet. I noen tilfeller - *Lemley* har en rekke eksempler fra amerikansk rett - kan neppe rettslige konsepter som er utviklet for fysiske objekter, anvendes for handlinger på nettet. Kravet om besittelsesforrykkelse kan for eksempel ikke oppfylles sidene dataene kopieres og kildefilen blir liggende. Etter det tradisjonelle konseptet kan det altså ikke begås tyveri på nettet.[499]

Men det finnes også eksempler i motsatt retning, for eksempel at den tradisjonelle skadeverksbestemmelsen i strl. 1902 § 291 kan anvendes for å ramme DOS-angrep på internett.[500] Dessuten er en rekke bestemmelser utformet teknologinøytralt i vid forstand, samtidig som det er klart at de har sitt viktigste virkeområde på nettet. Det gjelder blant annet legaldefinisjonen av "offentlig handling" i strl. 2005 § 10 annet ledd. Definisjonen er todelt, hvor første del er beregnet på den fysiske verden, og den andre på den virtuelle. Bestemmelsen lyder som følger:

> "En handling er offentlig når den er foretatt i nærvær av et større antall personer, eller når den lett kunne iakttas og er iakttatt fra et offentlig sted. Består handlingen i fremsettelse av et budskap, er den også offentlig når budskapet er fremsatt på en måte som gjør det egnet til å nå et større antall personer".

"Egnet til å nå" i annet punktum tar sikte på at budskapet er lagt opp på et allment tilgjengelig nettsted. Av den medienøytrale utformingen fremgår det ikke at den også er ment for rettsstridige ytringer på nettet, men det sies i forarbeidene uten problematisering av om nettet er et "sted" hvor normen kan virke.[501]

[499] Det hindrer selvsagt ikke innføring av en bestemmelse om "datatyveri", jf. drøftelsen i kapittel 8.5.
[500] Se kapittel 7.6.3.
[501] Ifølge forarbeidene er definisjonen medienøytral, men det å fange opp ytringer på nettet er et viktig formål. Ot.prp. nr. 90 (2003-2004) kapittel 12.2.2 s. 163-4.

Foranledningen til strl. 2005 § 10 annet ledd annet punktum, var at legaldefinisjonen av offentlig handling i strl. 1902 § 7 nr. 2 har et krav om samtidighet, som ligger i vilkåret om at handlingen må skje i "overvær av et større antall personer". På nettet er dette et problem fordi webben utnyttes ved individuell nedlasting av innhold. I første omgang ledet problemet til en endring i strl. 1902 § 135 a, hvor man tilføyde "egnet til å nå" for å ramme de praktiske tilfellene at internett var brukt som medium for fremsettelse av diskriminerende og hatefulle ytringer.[502] Senere kom formuleringen inn i legaldefinisjonen i strl. 2005 § 10, noe som medfører at det er tilstrekkelig for å være en offentlig handling, at data er lastet opp til en nettside. Dette har virkning for alle ytringer (§ 10 bruker ordet "budskap") som straffeloven kobler til et vilkår om offentliggjøring.[503] Bestemmelsen er altså utformet på en måte som inkluderer internett i den alminnelige regelsfære, noe som ikke problematiseres i seg selv. Det samme gjelder strl. 2005 §§ 201 og 311, som har det mest praktiske virkeområdet på nettet. Også strl. 1902 § 201 a / strl. 2005 § 306 om "grooming" kan det være naturlig å nevne her. Lovgiver har ikke funnet det nødvendig å presisere at bestemmelsene også gjelder handlinger på nett, det følger av en naturlig fortolkning.

Det samme utgangspunktet må tas ved fortolkningen av inndragningsreglene. Tilnærmingen bør være at man vurderer om bestemmelsen er anvendelig *hensyn tatt til hvordan fenomenet arter seg på internett*. Det er slik man går frem ved fortolkningen av bestemmelsen om kontaktforbud i strl. 2005 § 57. Ifølge forarbeidene gjelder den ikke bare oppsøkende handlinger i fysisk forstand, men også forbud mot å oppsøke noen på nettet. I forarbeidene er det kalt "immaterielle steder", en språkbruk som ligger ganske nær "cyberspace".[504] I realiteten innebærer det et forbud om å kontakte en annen ved bruk av elektronisk kommunikasjon, direkte for eksempel ved oppringninger, og mer indirekte, for eksempel på en pratekanal eller i et sosialt forum på internett. For så vidt gjelder inndragning er det uansett ikke behov for å ty til metaforer fordi en datafil er en "ting". Da er inndragningsreglene direkte anvendelige, og man må bare finne ut hvordan de virker for dublettene på nettet. Det er et spørsmål om reglenes operasjonaliserbarhet på nettet.

[502] Se Ot.prp. nr. 33 (2004-2005) kapittel 17.1.6.2 s. 187, hvor det fremgår at formålet var å ramme den som fremsetter "en grovt krenkende ytring under slike forhold at den var *egnet til å nå et større antall personer*, selv om ytringen (tilfeldigvis) ikke ble oppfattet av andre. Bestemmelsen vil for eksempel kunne omfatte budskap som settes fram i radio, fjernsyn, over åpne internettsider og ved oppslag, uavhengig av om budskapet faktisk når et større antall personer." Endringslov nr. 33/2005, i kraft 1.1.2006.
[503] Se eksempler i kapittel 11.4.3.3.
[504] Ot.prp. nr. 90 (2003-2004) kapittel 24.4.3. s. 323-324 om strl. 2005 § 57, og s. 483 (om korresponderende endring i strl. 1902 § 33).

11.2.2 Automatisert vs. manuell metodebruk

Håndhevelse på nettet må nødvendigvis skje ved bruk av datateknologi, og dermed blir det et poeng nøyaktig å fastlegge hva som menes med at en metode er *automatisert*. Det er slik jeg har lagt til grunn at inndragning av dubletter praktisk sett må foregå. Er det tilstrekkelig at man utnytter en vertsmaskin for å være på nettet, eller er det noe annet som kjennetegner en automatisert metode?

For inngrep i nettet er det et viktig valg om den metoden som vurderes brukt baseres på at gjennomføringen skjer *automatisk*, eller om inngrepet skal skje *manuelt*, dvs. *vurderes i hvert enkelt tilfelle*. Det at noe utføres automatisk innebærer som *Seipel* skriver "… att det sker *utan mänskligt ingripande.*"[505] Automatisering er med andre ord databasert utføring av operasjoner uten utøvelse av skjønn.

Forutsetningen om *automatisert* inndragning begrunner hvorfor jeg kommer opp med de to rettsgrunnlagene for inndragning av dubletter som jeg har nevnt. Et sentralt poeng er at det ikke finnes noe manuelt alternativ til den automatiserte, så derfor kommer hjemmelsspørsmålet på spissen. Jeg skal gå noe nærmere inn på hva automatisering innebærer.

Ved automatisert inndragning er én inndragningsbeslutning tilstrekkelig, deretter gjennomføres inndragning automatisk for alle dublettene uten ytterligere vurdering. Når operasjonen gjelder identifisering av dubletter, må datamaskinen ha et sammenligningsgrunnlag for "matching". Sjekksum er det mest presise kriteriet for likhet, og kun i kraft av dette kriteriet kan det tales om "dubletter". Det åpner ikke for menneskelig vurdering, for hvorvidt en fil er en dublett kan bare avgjøres ved automatisert behandling. Allerede dette utelukker bruk av manuell metode.

Operasjonen som går ut på "matching" består i å kalkulere sjekksummen til filer i nettet og sammenligne med sjekksummene i filteret, som refererer seg til de "svartelistede" filene i RDB.[506] Inndragningen forutsetter således at den rettslige beslutningen er truffet i forkant, slik

[505] *Seipel* (2004) s. 44.
[506] Se kapittel 3.3.3.

at iverksettelsen kan skje fortløpende automatisk.[507] Den rettslige beslutningen er truffet i straffesaken ved inndragning av datafiler, jf. de regler som er gjennomgått i kapittel 5.

Automatisert inndragning utelukker ikke at politiet spaner og avdekker rettsstridig innhold i nettet. Det er *manuelle metoder* som forutsetter bruk av vurderinger, og ikke en automatisert arbeidsform. Det å utnytte datautstyr for å "surfe" på internett er ikke tilstrekkelig for å anse en metode for å være automatisert. Først når man har innrettet seg slik at datamaskinen utfører operasjonene uten ytterligere menneskelig involvering, kan metoden anses for å være automatisert.

Dersom politiet for eksempel oppsøker dertil egnede tjenester og får opp overgrepsbilder på skjermen, har man anvendt en manuell metode som gir dokumentasjon for kriminell virksomhet. Det kan gi grunnlag for å åpne etterforsking, jf. strpl. § 224 første ledd, som bestemmer at etterforsking foretas når det

> "som følge av anmeldelse eller andre omstendigheter er rimelig grunn til å undersøke om det foreligger straffbart forhold som forfølges av det offentlige."

I dette tilfellet kan alternativet "andre omstendigheter" begrunne iverksettelse av etterforsking. I løpet av strafforfølgningen kan det tas beslag og rettsstridige filer kan inndras slik det er redegjort for. På denne måten er det mulig å bygge opp RDB som i neste omgang kan brukes for automatisert inndragning.

Manuell spaning foregår på nivået for *meningsinnhold* hvor det må foretas vurderinger, mens automatisert inndragning skjer på *datanivået* ved at datamaskinen utfører operasjoner. Ved valg av tiltak mot rettsstridig materiale på nettet har det betydning at politispaning ikke kan antas å være like effektivt som automatisert inndragning. Ved automatisert inndragning kan det for eksempel blokkeres for rettsstridig materiale som forsøkes utvekslet ved fildeling.[508]

[507] Se kapittel 5.1 og henvisningen til *Staksrud* (2002) s. 72.
[508] I Belgia har rettighetshavere til digitaliserte musikkverk anvendt fremgangsmåten for å blokkere mot utveksling av piratvare på fildelingstjenester. I en avgjørelse fra "District Court of Brussels" av 28. juni 2007 ("SABAM") (jeg har bare avgjørelsen i engelsk oversettelse) ble fremgangsmåten prøvet i forhold til ehandelsdirektivets (direktiv 2000/31/EF) forbud mot å pålegge tjenesteyter en generell overvåkingsplikt, jf. direktivet artikkel 15 (smlg. ehl. § 19). Rettighetshaverne (SABAM) krevde bistand fra tilbyder (SA Scarlet) til å implementere filteret i nettet. SABAM hadde databasen med sjekksumdefinerte filer som inneholdt de musikkverk som de hadde rettighetene til, mens tilbyder skulle sette filtrene i nettet og oppdatere med sjekksummer overført fra SABAM. SABAM fikk medhold. Retten påpekte at "the blocking measure has a

Dette er man avskåret fra ved manuell metode. Det samme gjelder filtrering av skadelig dataprogram som skjer ved bruk av "antivirus"-filtre (også kalt "malware"-filtre), det kan ikke gjøres manuelt. Valg mellom automatiserte og manuelle metoder er derfor ikke valg mellom likeverdige alternativer, og det blir viktig å avklare om loven gir hjemmel for å anvende den mer effektive automatiserte håndhevelsesformen.

Forskjellen mellom metodene utfordrer en påstand som synes å ha vunnet alminnelig tilslutning. Den går ut på at de data som en datamaskin kan behandle, kan også et menneske behandle; forskjellen består bare i tiden som medgår til å utføre oppgaven. Med andre ord er manuell og maskinell håndtering teoretisk sett likeverdige alternativer (noe jeg nettopp har avvist). Dette synet ligger for eksempel til grunn for at *Udsen* behandler maskinlesbare signaler og tegn som mennesker kan forstå, som prinsipielt samme fenomen, dvs. som data.[509]

I forhold til den praktiske virkelighet som strafferettslige regler er ment å regulere, har en slik teoretisk tilnærming etter min mening liten verdi, og det må stilles spørsmål ved om den i det hele tatt er holdbar.[510]

Første innvending gjelder *tidsfaktoren.* Ved rettshåndhevelse gjelder en målsetting om å få løst et problem. Målsettingen er ikke å fjerne kriminaliteten totalt, men å bringe den ned på et akseptabelt nivå. Det er selvsagt ikke likegyldig hvilket *tidsperspektiv* som gjelder for å oppnå målsettingen, og siden tidsfaktoren er en meget reell begrensning for menneskelige prestasjoner, må automatisering tas i bruk. Man kan ta kodeknekking som eksempel. I et eksperiment utført av forskningsinstitusjonen EPFL i Sveits i 2007, tok det 400 datamaskiner 11 måneder på full tid å knekke en kode som tilsvarte sikkerheten til en 700 bit RSA krypteringsnøkkel.[511] I dag brukes 1024 bit RSA krypteringsnøkkel som sikkerhet ved vanlig kommersiell bruk av internett, og det er antatt å være umulig å knekke nøkkelen med "rå

purely technical and automatic character, as the intermediary has no active role in the filtering" (utskrift av rettsavgjørelsen s. 9). Å pålegge tilbyder medvirkning til filtrering av denne art ble ikke funnet å være i strid med direktivet art. 15.

[509] *Udsen* (2009) s. 35: "Al data, der behandles af en computer, kan teoretisk undergives tilsvarende behandling i den menneskelige hjerne […] Forskellen består i den hastighed, hvormed behandlingen sker." Se også avhandlingen kapittel 8.2.

[510] Man ser noe lignende i påstanden om at informasjon kan spres "i det uendelige". Det finnes en reell begrensning og det er antallet potensielle medier som informasjonen kan spres til. Antakelig er meningen at så lenge man har informasjonen og nye medier, foreligger *en mulighet for* informasjonsdeling. Det kan også være det negative, at informasjon ikke går til grunne uten at mediene går til grunne.

[511] Se artikkel på Wikipedia om "Key size" http://en.wikipedia.org/wiki/Key_size (besøkt 11.11.09), med henvisning til artikkel i PCWorld om eksperiment utført ved Ecole Polytechnique Federale Lausanne, Sveits, se http://www.pcworld.com/article/132184/researcher_rsa_1024bit_encryption_not_enough.html (besøkt 11.11.09).

kraft" ("brute force") i overskuelig fremtid. Da behøves i så fall ny teknologi.[512] Det sier seg selv at menneskelig innsats ikke er noe aktuelt alternativ her.[513]

For det annet kan neppe menneskelig innsats utføre *mange like operasjoner* med de samme *krav til presisjon*, som et datasystem kan. Mennesker kan se at bilder ser like ut, men har ikke gode kriterier for å avgjøre hva som er likt etter en konkret vurdering, og kan derfor ikke nødvendigvis repetere vurderingen med presisjon. Eksemplet illustrerer i realiteten forskjellen mellom å ha en regel som angir vurderingskriterier for menneskelig skjønn, og å foreta *en automatisert anvendelse av regelen på det konkrete tilfellet*. Det siste kan datamaskinen gjøre på grunnlag av sjekksumkriteriet, og da blir resultatet riktig hver gang. Datamaskinen kan således *integrere en rettslig subsumsjon* som går ut på at en bestemt datafil er rettsstridig og besluttet inndratt, og *repetere subsumsjonen* korrekt for dublettene hver gang.[514] Automatisert inndragning kan ses som en rettslig programmert funksjon av subsumsjonen i inndragningsbeslutningen (se kapittel 11.5.3).

For det tredje er *digitalisert innhold rent teknologiskapt*. Til tross for at innholdet er menneskelig konsumvare kan det ikke håndteres direkte av mennesker. Innhold på nettet kan nytes av mennesker på innholdsnivået, men bare datasystemene kan overføre og tilgjengeliggjøre innholdet. Følgelig kan bare datasystemene gjenkjenne noe som dubletter, og

[512] Og om ikke annet har formålet for lengst gjort knekkingen irrelevant. Etter så lang tid er krigen overstått (med tanke på bruk av krypterte meldinger i den forbindelse) og den krypterte forretningshemmeligheten for lengst blitt "common knowledge". Men at mennesker "kan utrette det utrolige" under ekstreme omstendigheter er (de)krypteringsinnsatsen under annen verdenskrig et godt eksempel på, noe *Singh* (2000) beskriver i kapittel 4 "Cracking the Enigma" i sin bok om kryperingens historie. Her kan man lese om polske og engelske (de)krypteringshelter som Marian Rejewski og Alan Turing.

[513] En annen sak er at et menneske kan avdekke svakheter ved å analysere algoritmen. Men i dette tilfellet gjaldt eksperimentet kodeknekking som går ut på å prøve forskjellige tegnkombinasjoner som potensielt kan være nøkkelen. Kodeknekking er *gjetting,* og må holdes atskilt fra et *analytisk* angrep som retter seg mot svakheter ved kryptoalgoritmen. Ideelt sett skal kryptoalgoritmen være kjent og tåle analyse for å etterprøve om den er tilstrekkelig robust. I NOU 2007:2 kapittel 3.4.7 beskriver Datakrimutvalget kodeknekking ved "brute force" som en mulig *strategi* for å gjette kryptonøkler. En annen strategi er "å basere søket etter korrekte nøkler på kjente ord og uttrykk", noe som kan gjøres ved "å prøve alle ord som finnes i en ordliste". Tidsbruken ved "brute force"-angrep på nøkkelen avhenger av lengden på nøkkelen: "Med et passord på fem bokstaver vil en vanlig datamaskin vanligvis finne det rette svaret i løpet av noen timer. Med et passord på åtte bokstaver kan det derimot ta tiltalls år, og i tilfeller med lengre nøkler kan tiden for å søke gjennom hele nøkkelrommet være lenger enn solsystemets levetid." (s. 27).

[514] Dette poenget er også fremhevet av *Schartum* (2002) som skriver om rettslige systemavgjørelser i datasystemer for e-forvaltning, som produserer massevedtak om skatt og trygd. På s. 120 skriver *Schartum* at: "Det er åpenbart en gevinst ved automatiseringen at lovanvendelsen kan bli riktigere enn før. Datamaskinprogrammet kan riktignok inneholde feil, men har koden først fått et korrekt rettslig innhold, blir alle avgjørelser korrekte. Det samme er det ikke realistisk å ha som mål når det er saksbehandlere som skal foreta saksbehandlingen … Fra et slikt ståsted kan automatisert anvendelse av lover og forskrifter … ses som både nødvendig og ønskelig."

overføre eller blokkere dem. Av de tre nevnte grunner er ikke påstanden om at mennesket kan behandle data slik som datamaskiner, holdbar i praktisk sammenheng.[515]

Det synes mer realistisk å si at mennesket *ikke* kan behandle data slik som datamaskinen. Det betyr at selv om politiet kan ta i bruk visse manuelt betonte metoder, kan ikke politiet utføre automatiserte prosesser. Manuell metodebruk kan av denne grunn ikke være et substitutt for automatisert inndragning. På den annen side er det mennesker som *bestemmer hva datamaskinen skal gjøre*. Mennesker er derfor *ansvarlige* for de operasjoner som datamaskinene utfører, og dette ansvaret gjelder uavhengig av om operasjonen kunne vært utført av et menneske eller ei.

Siden det ikke kan antas å finnes noe manuelt alternativ til automatisert inndragning, blir spørsmålet om *hjemmelen* for metoden desto viktigere. Dersom det foreligger hjemmel *de lege lata*, beror iverksettelse av automatisert inndragning bare på oppbygning av teknologi og infrastruktur. Hvis det ikke foreligger hjemmel kan ikke inndragning i nettet foretas, fordi *det finnes ikke noe adekvat manuelt alternativ.* I så fall har drøftelsen belyst behov for å vurdere å innføre slik hjemmel.

11.3 To rettslige tilnærmingsmåter til automatisert inndragning

11.3.1 Inndragningsbeslutningens objekt og rettsvirkninger

For å repetere fra kapittel 5.9, gjelder første punktet i inndragningsbeslutningen datafilene i beslaget. Det som skal drøftes er hva som er det materielle grunnlaget for det neste punktet i beslutningen, som retter seg mot ukjent eier eller besitter, jf. strl. 2005 § 74 tredje ledd. Først introduserer jeg to mulige rettsgrunnlag for deretter å foreta en grundigere behandling i kapittel 11.4 og 11. 5.

[515] Jeg tror jo ikke at dansk teori har ment at digitalisert innhold kan håndteres av mennesker direkte, fordi mennesker kan tolke data (i tradisjonell betydning). Men posisjonen om at data kan behandles av mennesker så vel som av datamaskiner, blir problematisk når drøftelsene gjelder digitalisert innhold og automatisering. Poenget er vel bare at en teoretisk posisjon kan være gyldig inntil et bestemt punkt, dvs. at man neppe kan operere med en allmenngyldig lære her, men må se på teorien i forhold til virkelighetens omskiftelighet. Mot min posisjon kan det for eksempel innvendes at informasjon tross alt *er* i nettverket, den er bare ikke presentert ennå. Da vil jeg si at det er korrekt, men at det står fast at informasjonen må behandles av et datasystem slik at informasjonshåndteringen skjer indirekte, og må gjennom et presentasjonsstadium før den blir interessant for mennesker. Det samme er tilfelle for tegn i en bok. En lukket bok kan eies, men ikke leses. Derfor står det fast at data kan sammenlignes med et fysisk medium.

11.3.2 Alternativ 1: Dublettene er eksemplarer i samme orden

Det første alternativet går ut på at "tingen", jf. strl. 2005 § 69, er den "orden" av dubletter som har dataidentitet "NN". Inndragningsgrunnlaget kan sammenlignes med inndragning av en rettsstridig utgave av en bok, og dermed av alle eksemplarene av utgaven. Etter dette synet er hver dublett et selvstendig objekt og den tekniske mekanismen i nettet er et praktisk verktøy for gjennomføring.

I teorien synes man å ha vært inne på denne inndragningsmuligheten for bøker, men jeg kan ikke se at den har vært benyttet i praksis.[516] Imidlertid er det etter spesialhjemmelen i strl. 1902 § 38 om inndragning av "trykt skrift", tilstrekkelig for inndragning at skriftet er av "forbrytersk innhold".[517] Dersom rettsstriden er fastslått for ett eksemplar må det nødvendigvis gjelde alle, og effektivitetshensyn tilsier at alle eksemplarene bør anses å være omfattet av inndragningen.

Fra et annet rettsområde kan nevnes systemet med tilbakekall av helsefarlige produkter m.v., i medhold av produktkontrolloven § 6 b.[518] Tilbakekall baserer seg på de negative egenskapene ved ett produkt, som gjør seg gjeldende for hele produktserien. Tilsvarende kan man tenke seg inndragning av bøker.

Regelen om inndragning av "trykt skrift" avløses av strl. 2005 § 76, jf. §§ 69 og 70. Bestemmelsene viderefører i hovedsak rettstilstanden i teknologinøytralisert form, med bruk av begrepene "ting" og "informasjonsbærer" (som er et underbegrep av "ting"). Etter straffeloven 2005 gjelder inndragningsadgangen medier generelt, både bøker og data.[519]

Problemstillingen er dermed om "ting" i strl. 2005 § 69 kan fortolkes slik at det er adgang til å inndra en orden av rettsstridige eksemplarer, uavhengig av om eksemplarene er tatt i beslag eller ei. Drøftelsen tar utgangspunkt i strl. 1902 § 38 fordi den gjelder inndragning av et medium ("trykt skrift"). Siden data og dubletter også er medier og straffeloven 2005 er teknologinøytral, er spørsmålet om rettstilstanden for trykt skrift er videreført med virkning for dublettene.

[516] *Matningsdal* (1987) har antydet muligheten for at strl. 1902 § 38 fjerde forutsetningsvis inneholder hjemmel for inndragning av eksemplarer utenom beslaget. Jeg har redegjort for dette i kapittel 11.4.3.4.
[517] Se kapittel 11.4.1.
[518] Lov nr. 79/1976.
[519] Se kapittel 5.4.1.

Ved inndragning av en "orden", er det behov for en entydig referanse. For bøker kan man tenke seg henvisning til tittel, utgave eller opplag. Bøker kan komme i en eller flere utgaver, og hver utgave trykkes i ett eller flere opplag. ISBN (Internasjonalt standard boknummer) er identifikasjon for én bestemt utgave av en bok. Er en publikasjon blitt endret, for eksempel ved oversettelse til et annet språk, nytt innhold (for eksempel fjerning av rettsstridige deler), nytt format, innordning i ny serie eller utgivelse på nytt forlag, skal den ha et nytt ISBN. [520] Selv om en bok er kommet i flere utgaver med forskjellig ISBN, kan den ha beholdt tittelen. Det åpner for at en bok med noen rettsstridige partier kan være skrevet om og utgitt på nytt i lovlig form. Tittelen er derfor ikke nødvendigvis en presis referanse til de rettsstridige eksemplarene som er i omløp, så tittel som inndragningsreferanse kan favne for vidt. Et "opplag" er bare betegnelsen på en serie eksemplarer, så det avgjørende i forhold til inndragningen må være *utgaven* med tilhørende ISBN.

Dubletter av overgrepsbilder og skadelig dataprogram som skapes av brukerens aktivitet på internett, kopieres ikke i noe spesielt antall. Det synes anstrengt å tale om "utgivelse" av slikt innhold. Parallellen til bøker er at det må tas utgangspunkt i den inndratte datafilen med tilhørende *dataidentitet*. Da kan man for eksempel bruke sjekksumkriteriet som nevnt i kapittel 3.3.3.

Jeg har ikke sett det som nærliggende at inndragningen av trykt skrift kan gjelde *verket* som sådan. Et slikt krav kan neppe anses å være hjemlet i straffelovens bestemmelser, som avgrenser begrepet "ting" mot immaterielle objekter av denne art.[521] Det samme må antas å

[520] ISBN ble innført i Norge i 1971. Opplysningene om ISBN er funnet på Nasjonalbibliotekets hjemmeside www.nb.no (besøkt 10.3.9).

[521] Se kapittel 7.2 og 7.3. Se også *Rognstad* (2009) s. 35-36 som skriver at "åndsverket vanskelig kan forstås som en fast definerbar størrelse eller en ikke fysisk gjenstand man råder over på samme måte som fysiske ting. Retten til å råde over *verket* er mer en hensiktsmessig uttrykksform for at man har vern mot at andre utnytter ens skapende virksomhet." På s. 35 og 75 gir han eksempler på at verket kan komme til uttrykk på forskjellig vis. I loven reflekteres muligheten for at verket kan representeres i forskjellige former, jf. åvl. § 2 første ledd, som bestemmer at eneretten til å råde over åndsverket blant annet omfatter retten til å fremstille eksemplar "i opprinnelig eller endret skikkelse, … i annen litteratur- eller kunstart eller i annen teknikk". Det betyr blant annet at eneretten ikke bare omfatter kopiering av identiske eksemplarer, men også reproduksjoner som ikke er identiske, se *Rognstad* (2009) s. 152. Verksidentiteten kan være i behold selv om det kommer i nye eller endrete versjoner. Dermed foreligger det en mulighet for at et verk kan representeres både i en lovlig og en ulovlig form. Det viser problemet med å betegne et *verk* som "forbrytersk" og da kan det ikke inndras, i hvert fall ikke med hjemmel i strl. 1902 § 38. Smlg. *Stuevold Lassen* (2009) s. 485-487, om *verksidentiteten*, hvor det fremgår at det konkrete uttrykket kan ta mange skikkelser. Han skriver også at "Ethvert spørsmål om en åndsproduksjonsrett er krenket, innebærer et *identitetsproblem.* Ophavsmannens enerett til å fremstille eksemplarer omfatter jo bare fremstilling av eksemplarer som kan formidle opplevelsen av *det verk han har skapt*. Læren om det immaterielle

være tilfelle for begrepet "trykt skrift" i strl. 1902 § 38, som tar sikte på det konkrete uttrykket, noe som både kan være utgaven og eksemplarene.[522] Et verk kan uttrykkes på forskjellig vis, og *verksidentiteten* kan være i behold selv om det konkrete uttrykket varierer noe. For eksempel kan et bokverk skrives om for å unngå rettsstrid, slik jeg alt har nevnt. Da blir det for vidtrekkende å inndra verket. Til slutt er det noe søkt å ta verksbegrepet som utgangspunkt for resonnement, i hvert fall når det er tale om å inndra overgrepsbilder. Retten til verket er en rett til vern om den skapende innsatsen, og nettopp dette vern har lovgiver besluttet *ikke* å yte overfor overgrepsbilder, jf. forbudet i strl. 2005 § 311. For skadelig dataprogram er ikke reguleringen like entydig. Det leder til de noe kompliserte inndragningsvurderingene som er omtalt i kapittel 5.7.

Uansett, av disse grunner konsentrerer jeg drøftelsen om inndragning av en "orden" av like eksemplarer. Jeg tar utgangspunkt i strl. 1902 § 38, og går over i videreføringen i de teknologinøytrale bestemmelsene i straffeloven 2005. Jeg legger til grunn at både en utgave identifisert ved ISBN, og en datafil identifisert ved sjekksum, er egnede betegnelser for den "orden" som eksemplarene tilhører.

11.3.3 Alternativ 2: Dublettene er én "ting"

Den andre tilnærmingsmåten går ut på inndragning av dublettene som ett fenomen. Datafilen i beslaget i straffesaken er utslag av et større fenomen som materialiserer seg flere steder. Den tekniske mekanismen er ikke bare et verktøy for gjennomføring av inndragning, men integrerer den konkrete rettsanvendelsen (subsumsjon), nemlig inndragning av datafil med et bestemt innhold.

Denne tilnærmingsmåten tar utgangspunkt i at teknologien innebærer noen egne premisser som antas å ha betydning for fortolkningen av "ting". Det tas hensyn til at dublettene skapes og kontrolleres av teknologien, og kun eksisterer på datanivået utenfor direkte menneskelig rekkevidde. Inndragningen kan følgelig fullbyrdes ved å programmere den tekniske

verket som rettens gjenstand har, med alle sine feil, den fordel at den setter nettopp dette sentrale problemet i fokus." (s. 487).

[522] Også etter åndsverkloven er inndragningsadgangen begrenset til å gjelde "eksemplar", jf. åvl. § 56. Her er inndragning et middel for å effektivisere vernet om verket på rettighetshaverens hånd. Inndragningen retter seg derfor nettopp mot eksemplarer som er fremstilt og spredt i strid med eneretten. I strafferettslig sammenheng er situasjonen motsatt, så man kunne tenkt seg å ramme det rettsstridige verket, ikke bare eksemplarene. Men av de grunner som er nevnt i brødteksten synes en slik tilnærming å ha lite for seg.

mekanismen med beslutningen. Fordi dublettene kan kontrolleres av teknologien, har de en egenskap som gjør dem spesielle som "ting", idet teknologien kan behandle "alle som én".

Dette er et teknologibetinget synspunkt, men likevel ikke begrenset til bestemte tekniske løsninger som anvendes her og nå. Det er bare teknologibetinget på den måten at det forutsetter anvendelse av datateknologi, med den iboende egenskapen som IKT har for å generere dubletter.[523] Innenfor den elektroniske konteksten er tilnærmingen både tids- og tjenesteuavhengig, med unntak for sanntidsoverføringer.

"Ting" er et teknologinøytralt begrep i vid forstand. Begrepet var opprinnelig knyttet til fysiske objekter og teorien har i den forbindelse fundert over spesielle tilfeller som inndragning av levende dyr og av ting som ikke kan forflyttes, som et hus.[524] I takt med samfunnsutviklingen og fokuset på økonomisk kriminalitet, har det skjedd en bevisstgjøring av nye sider av begrepet, blant annet at det omfatter bankkonti og innestående beløp som direkte skriver seg fra handlingen.[525] Utviklingen for enkle fordringer er et lignende eksempel vedrørende "gjenstand".[526] Teknologiutviklingen får nå frem ytterligere en dimensjon av begrepet "ting": At data omfattes er ikke tvilsomt, men spørsmålet er om begrepet rommer mer enn datafilen i beslaget, dvs. at "ting" har en dimensjon som omfatter dublettene, slik at datafilen i beslaget bare er en del av en større "ting".

De tidligere drøftelsene har gjennomgående vist at nettet representerer en virkelighet som fortolkningen av rettslige konsepter tar hensyn til *de lege lata*. Utgangspunktet for fortolkningen bør derfor være at begrepet "ting" kan tenkes å ha *et annet omfang og dybde* enn man er vant til ved anvendelse i den fysiske verden. Når dublettene anses som utslag av ett fenomen, er de ikke selvstendige eksemplarer, men utslag av et større fenomen som teknologien programmeres til å reagere på, i henhold til rettslig beslutning truffet i en ordinær inndragningsprosedyre. Fenomenet defineres ut fra teknologiens premisser, og speiler at håndhevelsen skjer på teknologiens premisser.

[523] Se kapittel 3.3.4.
[524] *Matningsdal* (1987) s. 242-243; *Dyrnes* (2004) s. 90. Se også omtale av det tingsrettslige tingsbegrepet som ligger til grunn for begrepet "ting" i inndragningsreglene, i kapittel 7.2.
[525] Se *Dyrnes* (2004) s. 176-177 om beslag i konto for å sikre krav på gjenstandsinndragning.
[526] Se kapittel 7.6.4.

Jeg skal bruke et eksempel med fysiske objekter for å vise hva jeg mener ("heroineksemplet"): Loven bestemmer at befatning med narkotika er straffbart og gjør narkotika til et ulovlig stoff. I en sak om befatning med heroin konstateres det ved fysiske undersøkelser at stoffet er heroin, og stoffet inndras. På markedet finnes det mer heroin av samme type, men inndragningen har ikke virkning for det andre heroinet. Loven åpner ikke for å treffe forhåndsbeslutning om inndragning av alt heroin av samme type, fordi de er konkrete partier stoff som uansett må undersøkes i hvert enkelt tilfelle. Da er ikke noe vunnet ved å ha truffet beslutning på forhånd. Derfor kan inndragning bare skje overfor ting som er beslaglagt, også når eieren eller besitteren er ukjent. Etter beslag kan tingen undersøkes og det kan konstateres at vilkårene for inngrepet er oppfylt. Dersom loven hadde åpnet for å forhåndsbeslutte inndragning av ting som ikke var tatt i beslag, ville man ikke oppnå mer enn det som alt følger av lovregelen, nemlig at heroin er ulovlig materiale og skal inndras.

Det jeg har beskrevet følger av skillene mellom regel, faktum og subsumsjon (rettsanvendelse). For *fysiske objekter* avhenger subsumsjonen av en konkret undersøkelse av faktum hver gang. I kontrast til dette kan det konstateres at datateknologien nettopp muliggjør *automatisering av den konkrete rettsanvendelsen*. På grunnlag av dataidentiteten kan beslutningen om å inndra en datafil gjøres automatisk gjeldende for alle dublettene. Den tekniske mekanismen speiler dublettene som fenomen og reagerer med blokkering hver gang den treffer en av dem.

I forbindelse med e-forvaltning kaller *Schartum* den tekniske mekanismen en "rettslig systemavgjørelse". Det er en beskrivelse av hva regelen går ut på som legges inn programmet til datasystemet. "Inputen" er konkrete saksopplysninger for eksempel om kjønn, inntekt, bosted osv. *Schartum* påpeker at rettslige systemavgjørelser i e-forvaltning muliggjør automatisk utføring av massevedtak vedrørende individuelle borgeres rettigheter og plikter (trygd, skatt). I en vurdering opp mot rettssikkerhetsidealene (effektivitet, rettsriktighet, likebehandling) konkluderer han med at slike beslutningssystemer er egnet til å fremme rettssikkerheten, forutsatt at den rettslige systemavgjørelsen holder god kvalitet.[527]

Med tanke på det foreliggende inndragningsgrunnlaget er det ikke helt treffende å kalle den tekniske mekanismen en "rettslig systemavgjørelse". Mekanismen inneholder ikke den

[527] *Schartum* (2002) s. 120. Se sitat fra dette stedet i kapittel 11.2.2.

generelle inndragnings*regelen* som i de systemer *Schartum* beskriver, men *subsumsjonen* som går ut på at "dubletter med identitet "NN" er inndratt". Mekanismen fungerer på et helt partikulært nivå i henhold til forhåndsbeslutning vedrørende individualiserte dubletter. "Ting" kan fortolkes ut fra teknologiens egne premisser, dvs. hvordan fenomenet arter seg gitt at det må håndheves ved bruk av teknologi. Da er det vesentlig at konsepter som *antall og enheter er irrelevant*, fordi teknologien blokkerer uansett hvor og når dubletten forekommer. Teknologien har ikke noe behov for å telle "eksemplarer", den bare reagerer på fenomenet i henhold til sjekksummen.

Jeg har ikke kunnet finne en brukbar parallell fra den fysiske verden, hvor noe som opptrer forskjellige steder til forskjellige tidspunkter, likevel skulle anses som ett og det samme. Men det er etter mitt syn mulig for data. En tenkelig parallell er dog en bakterie med stor utbredelse; bakterien er den samme overalt (smlg. dublettene er samme "ting") og må kontrolleres med samme medisin (smlg. filtrering av dublettene). Jeg skal ikke trekke rettslige slutninger av parallellen, men nevner den bare for å anskueliggjøre hva slags fenomen jeg har i tankene innenfor den elektroniske konteksten.

11.3.4 "Ting" vs. "eksemplar"

Hovedspørsmålet for begge alternativene er fortolkningen av "ting" i strl. 2005 § 69, enten om "tingen" er den sjekksumdefinerte "orden" av dubletter, eller om alle dublettene er ett og samme objekt. Begge drøftelsene kan innby til bruk av ordet "eksemplar". I det første tilfellet fordi ordet brukes i strl. 1902 § 38 fjerde ledd, og det er en vanlig betegnelse på de bøker m.v., som bestemmelsen gir hjemmel for å inndra. Strl. 1902 § 38 fjerde ledd sier således at reglene om inndragning av trykt skrift ikke gjelder for

> "*eksemplarer* som ikke er tilgjengelige for almennheten, og som befinner seg på et sted hvorfra de ikke tilsiktes videre utbredt." (min uth.).

Med tanke på det andre alternativet skyldes det at ordet "eksemplar" er lett å ty til når man snakker om mange like objekter, for eksempel et eksemplar av et planteslag eller som nevnt, av en bok. Men man bruker neppe ordet like naturlig om forekomsten av en bakterie, som jeg også har nevnt, så her tar tanken en annen vei, mer i retning av en forekomst eller en *tilstand*,

slik *Negroponte* beskriver data.[528] Det at data er en *tilstand* ligger også til grunn for at det blir mer data ved deling, noe som er en teknologibetinget egenskap.

I *strafferettslig* sammenheng har "eksemplar" liten betydning. I straffeloven 1902 forekommer det bare i § 38 fjerde ledd og i § 434 (som rammer den som unnlater å tilstille stedets politi et eksemplar av et offentlig utgitt blad, tidsskrift eller flyveblad). Straffeloven 2005 bruker ikke "eksemplar", heller ikke i inndragningsbestemmelsene, selv om de representerer en videreføring av reglene i straffeloven 1902. I straffeloven 2005 er "ting" hovedbegrepet i bestemmelsene om gjenstandsinndragning, med "informasjonsbærer" som underbegrep. Eventuell bruk av "eksemplar" uten henvisning til lovsted, er derfor bare en språklig vending som ikke i seg selv gir grunnlag for rettslige slutninger.

Innen *opphavsretten* derimot, er "eksemplar" et meget viktig rettslig begrep. Ifølge *Rognstad* har eneretten til

> "å fremstille eksemplar av verket […] alltid vært en helt grunnleggende del av opphavsmannens enerett, idet verksutnyttelsen for en stor del tradisjonelt sett har vært knyttet til eksemplarer."[529]

Bruken av "eksemplar" i strl. 1902 § 38 fjerde ledd må ses i sammenheng med at bestemmelsen primært retter seg mot litterære verk. "Eksemplar" er i den sammenheng en spesiell type "ting" av fysisk karakter. Forøvrig gjelder tolkingsspørsmålene "ting", og det er ikke gitt at man skal være bundet av forestillingen om et fysisk eksemplar når begrepets innhold skal fastlegges. Fortolkningen av "ting" bør skje i lys av at inndragningen skal effektivisere håndhevingen av straffebudet, jf. strl. 2005 § 69 tredje ledd. Det må også omfatte håndhevelsen på nettet.

11.4 Inndragning av dubletter som individuelle gjenstander

11.4.1 Oversikt over bestemmelsene om inndragning av "trykt skrift"

Problemstillingen er om dublettene kan inndras fordi de er like, omtrent som eksemplarer av en rettsstridig utgave. Resonnementet tar utgangspunkt i strl. 1902 § 38 om inndragning av "trykt skrift av forbrytersk innhold", jf. bestemmelsens første ledd. Bestemmelsen er sitert i

[528] Se hvordan *Negroponte* beskriver data i kapittel 3.3.1.
[529] *Rognstad* (2009) s. 151.

sin helhet i neste kapittel. Bestemmelsen avløses av straffeloven 2005 §§ 69 og 70, som jamføres med spesialregelen for inndragning av informasjonsbærer, jf. strl. 2005 § 76. Den sistnevnte bestemmelsen er ikke en selvstendig hjemmel for inndragning, men presiserer hvordan inndragning av informasjonsbærer skal gjennomføres når det er besluttet med hjemmel i en av de to andre bestemmelsene. Betydningen av de nye bestemmelsene behandles i kapittel 11.4.4.

Strl. 1902 § 38 inngår i et regelsett som er blitt kalt "presseretten".[530] Reglene gjelder betingelsene for pressefrihet, hvor ytringsfriheten avveies mot behovet for å beskytte offentlige interesser og private individer mot krenkelser forøvet i skriftlig form. Rettsområdet omfatter rettsregler av både offentlig- og privatrettslig karakter. Drøftelsen her angår det strafferettslige, hvor en hovedproblemstilling har vært hvordan man kan gjøre ansvar for krenkelser gjeldende til tross for at det ikke alltid er mulig å holde forfatteren (den originære ytrer) ansvarlig.[531] Her kommer blant annet reglene om redaktøransvar inn. Regler om ansvar anses ikke alene å være tilstrekkelig, og suppleres med regler om beslag og inndragning for å kunne gripe inn mot utbredelse av skriftet. Strl. 1902 § 38 er altså en inndragningsregel som effektiviserer ansvarsregler i "presseretten", og bidrar til å forebygge og begrense skade forøvet ved trykt skrift. Det kreves ikke at noen kan holdes strafferettslig ansvarlig; det forbryterske innhold er tilstrekkelig som inndragningsgrunnlag. Inndragningen kan også skje før skriftet er spredt blant publikum. Dette viser bestemmelsens preventive og effektiviserende formål.

Strl. 1902 § 38 første ledd bruker uttrykket "trykt skrift", og må derfor leses i sammenheng med legaldefinisjonen i strl. 1902 § 10 første ledd, som lyder slik:

> "Under trykt Skrift henregnes Skrift, Afbildning eller lignende, der mangfoldiggjøres ved Trykken eller paa anden kemisk eller mekanisk Maade."

[530] S.R.I. 1955 kapittel II s. 8 om betegnelsen "presserett", hvor det bl.a. står at i Norge blir "ordet «presserett» undertiden brukt i en omfattende betydning i de fremstillinger i faglitteraturen som behandler rettsregler av betydning for pressens virksomhet." Det sies videre at disse reglene er "til dels privatrettslige" og dels "offentligrettslige".

[531] I S.K.M. 1896 brukes uttrykket "Presseforbrydelser" (kapittel 32 s. 262). Problemet ble inngående behandlet i forbindelse med lovendring i 1958 som angikk ansvar for rettskrenkelser i trykt skrift, se S.R.I. 1955 og Ot.prp. nr. 5 (1958) (endringslov 12. desember 1958 nr. 1). I den forbindelse ble inndragningsregelen for trykt skrift flyttet fra strl. 1902 § 323 til § 38.

Som følge av legaldefinisjonens teknologispesifikke utforming har det oppstått problemer med anvendelsen av redaktøransvaret på internett, men det faller utenfor temaet her.[532]

Eksemplarer av trykt skrift er "ting" som også kan inndras etter de alminnelige bestemmelsene om gjenstandsinndragning, jf. strl. 1902 §§ 35 og 37 b. Siden prevensjon ved å foreta inngrep *før* krenkelse begås ved utbredelse av skriftet, er et hovedformål med strl. 1902 § 38, er den nært beslektet med strl. 1902 § 37 b om forebyggende inndragning.[533]

Straffeloven 1902 kapittel 43 om forseelser forøvet ved trykt skrift, inneholder et straffebud som rammer den som søker å utbre "et trykt skrift som er erklært beslaglagt eller inndratt", jf. strl. 1902 § 433. Dersom skriftet er inndratt, er det altså straffbart å utbre det, og hvis så skjer, "skal skriftet alltid inndras overensstemmende med reglene i § 38", jf. strl. 1902 § 435 første punktum. Straffetrusselen er tidsbegrenset, den avhenger av at inndragningen var erklært "for mindre enn 15 år siden". Begrensningen skyldes at utvikling i rettsoppfatningen kan lede til et endret syn på hva som er "forbrytersk innhold".[534] Disse reglene (strl. 1902 §§ 433 og 435), er ikke videreført i straffeloven 2005 fordi de alminnelige inndragningsbestemmelsene anses å være tilstrekkelige.[535]

Ordningen etter straffeloven 1902 er følgelig at det foreligger flere hjemler for å inndra eksemplarer av trykt skrift. Inndragning kan skje både etter strl. §§ 35 og 37 b, og etter § 38 (som kan brukes både før og etter utbredelse). Videre er det et lovbrudd å utbre et skrift som er inndratt for inntil 15 år siden (uavhengig av hjemmel), jf. strl. 1902 § 433. De eksemplarene som er omfattet av lovbruddet skal i så fall inndras etter strl. 1902 § 38, jf. pålegget i strl. 1902 § 435.

Systemet med *gjentatt inndragning* av et trykt skrift som alt er inndratt, utløser spørsmål om hva som menes med "trykt skrift" i strl. 1902 §§ 38, 433 og 435. Er det en henvisning til konkrete eksemplarer eller kan det også forstås å omfatte en utgave? Inndratte eksemplarer kan jo ikke inndras på nytt, men det kan være behov for å inndra nye eksemplarer av en

[532] Legaldefinisjonen har også betydning for reglene om redaktøransvar og andre forseelser i trykt skrift i strl. 1902 kapittel 43. Flere av bestemmelsene bruker uttrykket "blad eller tidsskrift", og ikke "trykt skrift", men det er å anse som klart en underkategori av det legaldefinerte begrepet. Se *Bing* (2008) kapittel 5.
[533] *Matningsdal* (1987) konkluderer på s. 306 med at det neppe kan påvises noe tilfelle hvor man ikke kunne oppnådd samme resultat ved bruk av strl. 1902 § 37 b, som etter § 38.
[534] *Matningsdal* (1987) s. 304-305.
[535] Ot.prp. nr. 90 (2003-2004) kapittel 26.6, se særlig kapittel 26.6.2 om kommisjonens forslag om å fjerne bestemmelsene og departementets tilslutning til dette i kapittel 26.6.4 (s. 349-350)

utgave som alt er inndratt. Med dette spørsmålet som en introduksjon til problemstillingen, drøfter jeg om "trykt skrift" kan forstås både som utgave og eksemplar.

11.4.2 Strl. 1902 § 38: Bestemmelsens innhold og struktur

Strl. 1902 § 38 er en nokså omfattende bestemmelse som lyder slik:

> "Et trykt skrift av forbrytersk innhold kan ved dom inndras uten hensyn til om noen straffes for skriftet eller selv om forfatteren på grunn av de i § 249 nr. 3 nevnte eller andre straffeutelukkende omstendigheter overhodet ikke kan straffes.
>
> Dommen skal betegne de deler av skriftet som begrunner inndragningen. Ved fullbyrdelsen av dommen skal de øvrige deler på vedkommendes forlangende og på hans bekostning om mulig utsondres og tilbakeleveres.
>
> Inndragningen kan også omfatte plater og former som er forferdiget til trykningen; den til trykningen benyttede sats skal på vedkommendes forlangende og på hans bekostning foranstaltes avlagt i stedet for å inndras.
>
> Foranstående bestemmelser får ikke anvendelse på eksemplarer som ikke er tilgjengelige for almenheten, og som befinner seg på sted hvorfra de ikke tilsiktes videre utbredt."

Ifølge bestemmelsens første ledd gjelder inndragningsadgangen "[e]t trykt skrift av forbrytersk innhold". Ifølge legaldefinisjonen i strl. 1902 § 10 som jeg siterte i forrige kapittel, er "trykt skrift" slikt som "mangfoldiggjøres ved Trykken". Bruk av begrepet "trykt skrift" markerer således inndragningsbestemmelsens sammenheng med ansvarsreguleringen for krenkelser i trykte massemedier.

Av "forbrytersk" følger det at innholdet må rammes av en bestemmelse som hører hjemme i kategorien forbrytelse (i motsetning til forseelse).[536] Praktiske eksempler på innhold som rammes som forbrytelser etter straffeloven 1902, er diskriminerende og hatefulle ytringer (§ 135 a), oppfordring til straffbar handling (§ 140), pornografi og overgrepsbilder (§§ 204 og 204a) og ærekrenkelser (§§ 246, 247). Offentlig meddelelse som krenker privatlivets fred, jf. strl. 1902 § 390, er en forseelse og omfattes ikke direkte av § 38. Men av § 390 tredje ledd følger det at dersom handlingen er "forøvet i trykt skrift, kan inndragning besluttes i samsvar med § 38."

[536] Skillet mellom forbrytelser og forseelser er ikke videreført i straffeloven 2005, se om begrunnelsen for dette i Ot.prp. nr. 90 (2003-2004) kapittel 4.1.3 s. 55 flg. Loven bruker i stedet uttrykket "en straffbar handling", se inndragningsreglene i strl. 2005 §§ 69 flg.

Avhandlingen har nevnt at også forbudet mot skadelig dataprogram kan overtres ved trykt skrift, fordi kildekoden uttrykkes skriftlig.[537] Kildekoden til et skadelig dataprogram kan derfor publiseres i en bok og etter omstendighetene inndras med hjemmel i strl. 1902 § 38.[538] Forbudet mot befatning med skadelig dataprogram er imidlertid nytt med strl. 2005 § 201, og holdes utenfor drøftelsen av strl. 1902 § 38.

I strl. 1902 § 38 tredje ledd *utvides* inndragningsadgangen utover "trykt skrift", til å omfatte "plater og former som er forferdiget i trykningen". Bestemmelsen skal hindre at effekten av inndragningen av skriftet omgås, ved at man fortsetter å trykke opp nye eksemplarer med rettsstridig innhold. Den teknologispesifikke bestemmelsen er lite aktuell i dag, på grunn av digitalisert trykketeknologi.[539]

I fjerde ledd derimot begrenses inndragningen. Det bestemmes nemlig at

> "Foranstående bestemmelser får ikke anvendelse på eksemplarer som ikke er tilgjengelige for almenheten, og som befinner seg på sted hvorfra de ikke tilsiktes videre utbredt".

Unntaket går tilbake til straffelovens tilblivelse. Det ble ikke gitt noen begrunnelse, annet enn at man viste til at det fantes et slikt unntak i "den tyske Presselov, § 27".[540] Inndragningsunntaket for eksemplarer i privat eie videreføres ikke i straffeloven 2005.[541]

Til slutt inneholder strl. 1902 § 38 annet ledd krav til at "[d]ommen skal betegne de deler av skriftet som begrunner inndragningen". Det åpnes også adgang for ved fullbyrdelsen å utsondre lovlige deler som tilbakeleveres den som må tåle inndragningen. Denne bestemmelsen er som vi har sett, videreført i noe endret form i strl. 2005 § 76 annet ledd.[542]

[537] Se kapittel 4.4.
[538] Se *Wagle* (1997) s. 533 flg., som har inntatt eksempel på en kildekode.
[539] *Bing* (2008) kapittel 5.
[540] S.K.M. 1896 s. 264: "Exemplarer i almindeligt privat Eie kan derimod ikke konfiskeres, selv ikke om de udlaanes eller overlades til Andre, naar dette dog ikke kan betegnes som en Tilgjængeliggjørelse for Almenheden og ikke heller Erhvervelsens Øiemed har været Videreoverdragelse."; se også Skeie (1946) s. 449.
[541] Ot.prp. nr. 90 (2003-2004) kapittel 26.6.4 s. 349-350. Se avhandlingen kapittel 11.4.4.
[542] Omtalt i kapittel 5.6.

11.4.3 Inndragning av utgave eller eksemplar

11.4.3.1 Problemstilling

Spørsmålet er om det er adgang til å inndra utgaven, eller om inndragningen må begrenses til de beslaglagte eksemplarene. Det avhenger av en fortolkning av strl. 1902 § 38. Bestemmelsen gir hjemmel for inndragning av "trykt skrift", og sier ikke noe om at det må være beslaglagt.[543] Spørsmålet har betydning for inndragning av eksemplarer som ikke er beslaglagt, og ikke er i privat eie (jf. strl. 1902 § 38 fjerde ledd). Det kan være eksemplarer hos forlag og distributører. Tidligere var bokomsetning gjerne begrenset til bokhandlerne, men foregår i dag også i andre butikker, for eksempel matvareforretninger, kiosker, multimediaforretninger m.v. I tillegg kommer salg via nettet. For en utgave som alt er vidt distribuert er det umulig, eller i hvert fall en urimelig ressurskrevende oppgave for politiet, å møte opp hvert sted og beslaglegge eksemplarene fysisk før de inndras. Det er langt mer hensiktsmessig å inndra utgaven med den følge at forlag og forhandlere mister retten til å trykke, distribuere og selge eksemplarene.

Det synes også å være lite hensiktsmessig med en ordning som krever at rettsstriden prøves for hvert eksemplar. Siden alle eksemplarer av en utgave er like, er alle rettsstridige dersom det er fastslått for ett av dem. Både rettstekniske og effektivitetshensyn tilsier at det bør være mulig å inndra utgaven.

11.4.3.2 Fortolkningsmomentene

Rent språklig synes "[e]t trykt skrift" både å kunne bety en utgave og eksemplarene av utgaven. Men i praksis har strl. 1902 § 38 første ledd bare blitt brukt på beslaglagte eksemplarer, og spørsmålet om utgaven som sådan kan inndras, er ikke prøvet av Høyesterett. Jeg har heller ikke funnet omtale av denne muligheten i bestemmelsens forarbeider. Men det finnes en tendens i rettspraksis til å formulere seg som om man mener utgaven

[543] Et uttrykkelig vilkår om at det som skal inndras først må være beslaglagt, synes bare å fremgå av strl. 1902 § 37 c, om inndragning av "beslaglagt ting" når eieren ikke er kjent eller ikke har kjent oppholdssted i riket. Det samme gjelder etter bestemmelsens annet ledd som regulerer inndragningsadgangen uten at noen er gjort til saksøkt. Tilsvarende regler er inntatt i strl. 2005 § 74, som jeg har vist til i kapittel 5.9. For så vidt gjelder inndragning i sak mot lovbryteren, gjelder det ikke noe uttrykkelig vilkår om at tingen må være beslaglagt, se strl. 1902 § 36, smlg. strl. 2005 § 71.

Videre fremmer inndragning av utgaven bestemmelsens formål mer effektivt enn inndragning av beslaglagte eksemplarer, jf. de hensyn jeg har nevnt over. Effektivitetshensynet går ikke på bekostning av privatlivets fred og den private ytringsfrihet i dette tilfellet, på grunn av unntaket i strl. 1902 § 38 fjerde ledd, som uansett hindrer at inndragning av utgaven rammer private eksemplarer.

Til sist gir en fortolkning av "trykt skrift" som åpner for å inndra utgaven, best sammenheng mellom reglene. Det er tale om forholdet mellom strl. 1902 § 38 første og fjerde ledd, og mellom strl. 1902 § 38 og bestemmelsene i straffeloven kapittel 43 som ble beskrevet tidligere. Jeg skal redegjøre for momentene i det følgende.

11.4.3.3 Strl. 1902 § 38 i forhold til relative og totale forbud mot ytringer

Inndragningsbestemmelsen har hatt sitt viktigste virkeområde for trykt skrift som rammes av *relative forbud*, som skiller mellom (offentlig) utbredelse og privat besittelse. Det gjelder for det første *pornografiforbudet* i strl. 1902 § 204. Opprinnelig var dette et forbud mot *utuktige skildringer*, jf. strl. 1902 § 211, som ble overført til § 204 i forbindelse med seksuallovbruddsreformen i 2000. Samtidig ble begrepet "utuktig" fjernet fordi "pornografisk" ble ansett som mer tidsmessig og dekkende for hva man ønsket å ramme.[544] Det finnes imidlertid tre Høyesterettsavgjørelser som berører spørsmålet om inndragning av utuktige skrifter, jf. strl. 1902 § 211, som jeg kommer inn på nedenfor.[545]

Videre er forbudet mot *diskriminerende og hatefulle ytringer*, jf. strl. 1902 § 135 a, basert på sondringen offentlig – privat. Forbudet rammer bare ytringer som fremsettes "offentlig", smlg. også forbudet mot *offentlig oppfordring til iverksettelse av en straffbar handling*, jf. strl. 1902 § 140, og forbudet mot *offentlig meddelelse som krenker privatlivets fred*, jf. strl. 1902 § 390.

[544] I 2005 ble forbudet mot overgrepsbilder skilt ut i en egen bestemmelse, som strl. 1902 § 204 a, jf. lovendring nr. 29/2005.
[545] Rt. 1958 s. 479 ("Sangen om den røde rubin"); Rt. 1959 s. 431 ("Sexus"); Rt. 1967 s. 1502 ("Uten en tråd").

Ærekrenkelsesreglene inneholder ikke noe vilkår om at ærekrenkelsen må være fremsatt offentlig, jf. strl. 1902 §§ 246 og 247, men besittelsen av slike skrifter er ikke rettsstridig, så også her gjør forbudet en reservasjon for befatning i den private sfære.

Dersom forholdet mellom strl. 1902 § 38 første og fjerde ledd fortolkes slik at første ledd gir hjemmel for inndragning av utgaven, mens fjerde ledd avgrenser inndragningen overfor eksemplarer som er i lovlig privat besittelse, korresponderer reglene langt på vei med den objektive rekkevidden til de nevnte straffebestemmelsene. Det synes også å være unntakets formål. Derved hindrer man at trykt skrift som det er lovlig å besitte, men som det er straffbart å utbre, omfattes av en inndragningsbeslutning som gjelder utgaven. Dette styrker at første ledd gir hjemmel for å inndra utgaven, fordi det ellers ikke er noe behov for unntaket i fjerde ledd.

Fordi inndragningsbestemmelsen i første rekke har et preventivt formål og søker å hindre spredning av skrifter som det vil være en forbrytelse å utbre, kunne man tenkt seg at inndragningsadgangen rakk videre enn strafferegelen. Risikoen for at eksemplarer i privat eie kan bli spredt offentlig tilsier at også de inndras. Det gir da loven også adgang til, men det må hjemles i strl. 1902 § 37 b om forebyggende inndragning.

Innføringen av *totalforbudet* mot overgrepsbilder i 1992, forstyrret forholdet mellom utformingen av inndragningsbestemmelsen og straffebudets objektive rekkevidde. For overgrepsbilder kan det ikke gjelde noe unntak for eksemplarer i privat eie. Forholdet til denne inndragningsregelen ble imidlertid ikke behandlet av lovgiver ved innføring av totalforbudet.[546]

Det må tilføyes at det ikke er tvilsomt at pornoblader som vesentlig består av bilder, er "trykt skrift", jf. strl. 1902 § 10, og kan inndras etter strl. 1902 § 38. Det følger av alternativet "Afbildning" i strl. 1902 10, og ifølge *Matningsdal* kreves det ikke:

> "… at bildet er ledsaget av noen tekst. Bestemmelsen gir dermed også hjemmel for å inndra et utuktig bilde eller et bilde som ved spredning vil krenke privatlivets fred."[547]

[546] Ot.prp. nr. 20 (1991-1992) kapittel 7 s. 53 flg. Besittelsesforbudet ble innført ved lov 22. mai 1992 nr. 49.
[547] *Matningsdal* (1987) s. 300.

På den ene siden inneholder loven dermed et forbud mot *privat besittelse* av trykt skrift med overgrepsbilder, og på den annen side en unntaksregel som sier at eksemplarer i privat eie ikke omfattes av inndragningen. Det harmonerer ikke.

Det er heller ikke slik at strl. 1902 § 38 gir en "spesialordning" for fremstillinger i skjønnlitterær form, kontra "hardkokt" materiale som viser bilder av seksuelt misbruk av barn. Lovgiver har ikke lagt opp til spesialregulering for verk av typen "Lolita" (Vladimir Nabokov 1955).[548] Det fremgår av at den materielle straffebestemmelsen gjør unntak for kunstneriske verk, jf. strl. 1902 § 204a siste ledd, jf. strl. 1902 § 204 annet ledd annet punktum, som lyder:

> "Som pornografi regnes ikke kjønnslige skildringer som må anses forsvarlige ut fra et *kunstnerisk*, vitenskapelig, informativt eller lignende formål." (min. uth.).

Loven gir altså anvisning på en "enten-eller vurdering". Enten er verket omfattet av unntaket for kunstneriske verk, og da er det lovlig og kan ikke inndras. Men dersom innholdet først er bedømt som "forbrytersk" i henhold til totalforbudet, gjelder intet unntak, og da kan det inndras etter strl. 1902 § 38.[549]

Konklusjonen så langt er at det synes rimelig å fortolke strl. 1902 § 38 første, jf. fjerde ledd, slik at første ledd gir hjemmel for inndragning av utgaven som sådan, mens eksemplarer i privat eie ikke omfattes, jf. unntaket i fjerde ledd. Også inndragning av blader med overgrepsbilder må ved anvendelse av strl. 1902 § 38, begrenses til eksemplarer som er beslaglagt eller som finnes hos distributørene. Men her er man hjulpet ved å kunne anvende de mer omfattende reglene om gjenstandsinndragning i stedet, jf. strl. 1902 § 35. Det blir ikke tale om å anvende forebyggende inndragning, jf. strl. 1902 § 37 b, fordi selve besittelsen er straffbar så en straffbar handling er alt begått.

[548] Det er jo lite fantasifullt å bruke et forslitt eksempel som "Lolita". Fra nyere tid kan nevnes *Marques'*(2009) "Memorias de mis putas tristes" om det seksuelle forholdet mellom en 90 år gammel mann og 13 år gammel pike som må tjene penger for å forsørge familien sin. En eldre klassiker er *de Sades* "Justine", skrevet i løpet av to uker i 1787 mens forfatteren var fengslet i Bastillen (norsk utgave 1973).

[549] I Rt. 1958 s. 479 ("Sangen om den røde rubin") anførte forsvaret at strl. 1902 § 211 ikke kunne anvendes på skjønnlitterære verker, både på grunn av unntaket for kunstneriske verk og fordi bestemmelsen ikke hadde vært anvendt på 70 år (den gang), dvs. siden dommene mot Hans Jæger og Christian Krogh i 1880-årene. Høyesterett fant det imidlertid "klart" at anførselen ikke kunne godtas, det fulgte verken av lovens ordlyd eller mening (s. 482). Bestemmelsen kan følgelig også anvendes på skjønnlitterære verk. Tilsvarende synspunkt ble lagt til grunn i Rt. 1959 s. 431 på s. 438 men det må gis "rommelig målestokk" for skjønnet. Smlg. også Rt. 1967 s. 1502 ("Uten en tråd") på s. 1508. Denne rettstilstand er videreført i dagens pornografibestemmelser, dvs. strl. 1902 § 204 / strl. 2005 § 317.

Slik situasjonen er etter gjeldende rett, synes lovgiver å ha inntatt en skranke til vern om privatlivets fred i inndragningsreglene, jf. strl. 1902 § 38 fjerde ledd. Det er vel noe tvilsomt om det foreligger behov for en slik skranke her, siden den alt er etablert gjennom garantien i G § 102 om vern mot husinkvisisjoner, og vilkårene for bruk av tvangsmidler som ransaking og beslag. Det er heller ikke behov for unntaket av materielle grunner, fordi lovgiver har tatt stilling til straffetrusselens rekkevidde ved utforming av straffebestemmelsene. I forhold til inndragning av overgrepsbilder går unntaket dessuten for langt.

Jeg går nå over til å vurdere hva som kan utledes av teori og praksis om adgangen til å inndra utgaven med hjemmel i strl. 1902 § 38.

11.4.3.4 Teori og rettspraksis i tilknytning til strl. 1902 § 38

I teorien har *Matningsdal* antydet at strl. 1902 § 38 fjerde ledd forutsetningsvis kan anses å hjemle inndragning for mer enn de beslaglagte eksemplarer. Konklusjonen er likevel at bestemmelsen ikke kan regnes som noe annet enn

> "en materiell bestemmelse om hvem et krav kan rettes mot. Den er mao. ikke en prosessuell bestemmelse om hvem en inndragningsdom er bindende for. En motsatt tolking har heller ikke nevneverdig støtte i rettstekniske hensyn: Selv om en dom mot forlaget også kunne fullbyrdes hos bokhandlere, biblioteker osv., måtte de likevel ha krav på å få prøvd om deres eksemplar omfattes av unntaksbestemmelsen i fjerde ledd. Dermed ville man være like langt."[550]

Dette kan man si seg enig i for så vidt gjelder trykt skrift som er undergitt *relativt* forbud. Da må det i hvert tilfelle prøves om vilkårene for inndragning (dvs. om skriftet har vært eller tilsiktes tilgjengeliggjort slik at unntaket ikke kan gjøres gjeldende) foreligger. Men for trykt skrift som er undergitt *absolutt forbud* (totalforbud) slik som fremstillinger som nevnt i strl. 1902 § 204a, er det *intet å prøve* i den nye situasjonen. Eksemplarene bør derfor uten videre kunne inndras med henvisning til den opprinnelige beslutningen.

Matningsdal hadde imidlertid ikke foranledning til å drøfte dette, fordi besittelsesforbudet ble innført i 1992, og det var flere år etter at han skrev om inndragning (1987). Etter at besittelsen

[550] *Matningsdal* (1987) s. 303-304.

ble gjort straffbar, taler rettstekniske hensyn *med styrke for* å anse alle eksemplarene som inndratt uten behov for å prøve vilkårene på nytt. Hvis dette hadde vært situasjonen også i 1987, kan det ikke utelukkes at Matningsdal ville sett annerledes på spørsmålet.

Rettspraksis gir lite veiledning for å avklare de spørsmål som her behandles. I de få tilfeller man har forsøkt å foreta inndragning med hjemmel i strl. 1902 § 38 og som er brakt inn for Høyesterett, har temaet vært om et skjønnlitterært verk var i strid med strl. 1902 § 211 fordi det var "utuktig" og dermed av "forbrytersk innhold".

Den første saken gjaldt "Sangen om den røde rubin" av Agnar Mykle (Rt. 1958 s. 479). Tiltale var tatt ut mot forfatteren og mot administrerende direktør i forlaget. Påtalemyndigheten reiste også krav om inndragning av utbyttet og "om inndragning av boken og den sats som var brukt til trykningen", jf. strl. 1902 § 323 (som senere ble avløst av strl. 1902 § 38).[551] Det fremgår at boken var kommet ut i ca 35 000 eksemplarer og at den alt hadde blitt så vidt spredt at forhørsretten hadde avslått påtalemyndighetens begjæring om at "boken skulle beslaglegges", fordi det i lys av spredningen ikke ville være særlig betenkelig å avvente resultatet i straffesaken, som man "regnet med kunne bli fremmet nokså raskt".

Høyesteretts flertall (12) kom til at innholdet ikke var å regne som utuktig slik at resultatet måtte blir frifinnelse, og kravet om inndragning ble ikke tatt tilfølge. Mindretallet (3) sa for så vidt gjaldt inndragningskravet, at

> "« Sangen om den røde rubin » er et utuktig skrift og kan inndras etter straffeloven § 323. Og jeg er enig med byretten i at inndragning av boken bør finne sted".[552]

Selv om avgjørelsen ikke resulterte i inndragning, har den interesse via språket som føres om inndragningen. Gjennomgående brukes ordet "boken", og det oppstår en tvetydighet om hvorvidt det betyr *utgaven* eller *de beslaglagte eksemplarer*. Dommer Bahr som tilhørte mindretallet, treffer etter mitt syn best når han fastslår at "« Sangen om den røde rubin » er et utuktig skrift". Det er utvilsomt en vurdering som gjelder *utgaven*. Påtalemyndigheten hadde imidlertid bare krevet inndragning av de beslaglagte eksemplarer, og dermed var det disse

[551] Ved endringslov den 12. desember 1958 nr. 1, se også kapittel 11.4.1.
[552] I sammendraget står det at dommen ble avsagt "med 13 stemmer i plenum", men det fremgår av dommen selv at det var 15 voterende dommere som fordelte seg 12-3.

som dommer Bahr refererte til i sin neste setning hvor han nevner "boken". Sammenholdt med "trykt skrift" i inndragningsbestemmelsen, ser man at det godt kan bety utgaven.

De to neste sakene gjaldt "Sexus" av Henry Miller (Rt. 1959 s. 431) og "Uten en tråd" av Jens Bjørneboe (Rt. 1967 s. 1502). I begge sakene kom retten til at skriftene var utuktige og kunne inndras. Inndragningskravene var rettet mot bokhandleren ("Sexus") og mot forlaget ("Uten en tråd").[553] Og i begge sakene gjaldt inndragningen *de beslaglagte eksemplarer*.

Etter mitt syn kan ikke dommene tas til inntekt for at strl. 1902 § 38 bare hjemler inndragning av beslaglagte eksemplarer. Inndragningsbeslutningens rekkevidde har ikke vært tema i sakene, og når påtalemyndigheten nøyer seg med å kreve de beslaglagte eksemplarene inndratt, fremfor å kreve inndragning av utgave, blir resultatet slik som beskrevet.[554] Frem til 1999 var nemlig retten bundet av påtalemyndighetens påstand om inndragning. Domstolen kunne ikke idømme inndragning dersom det ikke var påstått, og ikke i større omfang enn påstått.[555] Jeg synes derfor at *Matningsdal* går noe langt når han skriver at den rettsoppfatning han har redegjort for "er tydeligvis også lagt til grunn i rettspraksis."[556] I de ovennevnte avgjørelsene som også Matningsdal viste til, ble ikke spørsmålet prøvet, så de verken støtter eller går imot hans syn.

Videre kan det konstateres at i rettsspråket er det vanlig å bruke ord som "boken" når man mener *utgaven* eller *alle eksemplarene* som et verk er trykket i. Av rettspraksis kan nevnes:

> Rt. 1981 s. 1305 (Løpeseddel): Saken gjaldt overtredelse av strl. 1902 § 135 a for ytringer fremsatt i "tre løpesedler". Det fremgår av dommen at "løpesedlene ble spredt i et samlet antall på ca 16.000 eksemplarer." "Løpeseddel" blir her brukt på samme måte som Høyesterett bruker "utuktig skrift" og "boken" i Rt. 1958 s. 479 ("Sangen om den røde rubin").

[553] Overfor Bjørneboe selv ble det krevd bøtestraff og inndragning av vinning som ble kalkulert til kr. 100.
[554] Dessuten ble ISBN innført først i 1971, mens de kontroversielle sakene er fra før den tid. Man har derfor kanskje savnet en entydig referanse for å inndra utgaven.
[555] Ved lovendring nr. 39/1999 ble strpl. § 38 endret slik at retten ikke er bundet av "tiltalen eller de påstander som er fremsatt" med hensyn til "straff og andre rettsfølger", noe som omfatter inndragning. Se strpl. § 38 annet ledd annet, jf. første punktum. Se også *Andenæs/Matningsdal/Rieber-Mohn* (2004) s. 513; smlg. *Andenæs/Myhrer* (2009) s. 838.
[556] *Matningsdal* (1987) s. 304. Uttalelsen står i direkte forlengelse av hans omtale av de rettstekniske hensyn som er sitert over.

LA-2008-87454 (Agder): Her refererte man til "boka": Saken gjaldt krav om oppreisningserstatning for krenkelse av privatlivets fred, for uttalelser om fraskilt ektefelle (saksøker) i en bok som forfatteren (saksøkte) selv kalte "lokalhistorisk". Forfatteren ble idømt erstatningsansvar og det ble nedlagt forbud mot "… å gi bort/selge eller på annen måte distribuere boka «Æ» uten etter samtykke fra A eller ved at omtalen av henne på sidene 117-122 og sidene 136-137 tas bort." Av dommen fremgår det klart at "boka" betyr alle de trykte eksemplarene som representerte utgaven.

RG 1967 s. 65 (Eidsivating): Saken gjaldt krav om midlertidig forføyning ved forbud mot "distribusjon og omsetning av Michael Grundt Spangs bok « Den ukjente morder»". Også dette gjaldt selvsagt alle eksemplarene og man kunne krevet forbud mot distribusjon av utgaven.

Rt. 1986 s. 267 ("Hær-Værk"): Saken gjaldt to vernepliktige som var domfelt for overtredelse av strl. 1902 § 134 tredje ledd, for å ha delt ut "eksemplarer av et blad med navnet « Hær-Verk » med innhold som tok sikte på å skape uvilje mot den militære tjenesten."[557] De beslaglagte eksemplarene ble inndratt. Denne avgjørelsen skiller seg ut fra de øvrige, fordi den er særlig presist formulert med hensyn til at det er tale om *eksemplarer* av en *publikasjon* (blad) med *tittel* ("Hær-Verk").

De beste grunner taler for å fortolke strl. 1902 § 38 første ledd slik at den hjemler adgang til å inndra utgaven. Både effektivitetshensyn og strukturen i lovbestemmelsen taler for det. Dersom inndragningen skal kunne forebygge skaden mer generelt, må kravet rettes mot utgaven, og eksemplarene omfattes som følge av det. Det gir også best begrunnelse for unntaket i fjerde ledd. Riktignok gir første ledd hjemmel for inndragning av eksemplarer utelukkende etter en innholdsmessig vurdering, men det fremstår som lite nærliggende at politiet skulle inndra private eksemplarer når besittelsen uansett er lovlig. Det er jo heller ikke adgang til å ransake med sikte på å foreta beslag for å sikre inndragningskravet, fordi det grunnleggende vilkåret om straffbart forhold ikke er oppfylt, jf. strpl. § 192 og G § 102 som forbyr "Hus-Inkvisitioner" uten i "kriminelle tilfelle".[558] En slik begrensning i

[557] Strl. 1902 § 134 tredje ledd setter straff for den som "offentlig søker at ophidse nogen som hører til den væbnede magt, til uvilje mot tjenesten eller til hat mot militære foresatte eller overordnede."
[558] G § 102 lyder: "Hus-Inkvisitioner maa ikke finde sted, uden i kriminelle Tilfælde."

inndragningsadgangen måtte derfor uansett innfortolkes. Strl. 1902 § 38 første ledd bør derfor fortolkes innskrenkende, og fjerde ledd gir dermed et naturlig begrunnet unntak for eksemplarer i lovlig privat besittelse, når utgaven er inndratt.

Da gjenstår spørsmålet om hvordan strl. 1902 § 435, jf. § 433, passer inn i dette bildet. Bestemmelsene skal løse problemet med eksemplarer som alt var brakt i handelen på inndragningstidspunktet, eller som trykkes opp etter at inndragningen ble "erklært".[559] Disse eksemplarene "skal… inndras", jf. strl. 1902 § 435. Det betyr at "trykt skrift" i strl. 1902 § 433 må forstås å bety *eksemplarer av en utgave som alt er inndratt.* Inndragningshjemmelen i strl. 1902 § 435 fremstår imidlertid som overflødig, annet enn at den avskjærer skjønnet med hensyn til om inndragning bør skje. Det må antas å ha sammenheng med at spørsmålet alt er vurdert i den tidligere saken.

Hovedkonklusjonen er at strl. 1902 § 38 "trykt skrift" må antas å gi hjemmel for å inndra utgaven. Så kan det reises spørsmål om hvorfor ikke dette har vært gjort i praksis. Bortsett fra de tre nevnte sakene fra 1950-og 60 tallet, har ikke strl. 1902 § 38 vært prøvd for Høyesterett, og ved søk på Lovdata har jeg ikke funnet underrettspraksis som inndrar trykt skrift. De tre nevnte Høyesterettsavgjørelsene gjelder pornografi (utuktighet) og om dette skriver *Andenæs/Andorsen* at det er:

> "i våre dager helst billedpornografi (i blader, film eller video) som det er aktuelt å aksjonere mot. Den verbale pornografi er kommet i bakgrunnen. De mest omstridte pornografisaker i vår historie har man imidlertid hatt i forbindelse med dristige seksualskildringer i litteraturen. Her er det hensynet til kunstens frihet som skaper motforestillinger. Den litterære verden har gjerne rykket ut til forsvar for forfatter og forlag og med latterliggjørelse av påtalemyndigheten. Det har også vært et dilemma for påtalemyndigheten i slike saker at en bok som blir beslaglagt som pornografi, får en effektiv gratisreklame. Etter noen saker i 1950- og 1960-årene har påtalemyndigheten resignert."[560]

Hvorvidt påtalemyndigheten kan sies å ha resignert i forhold til å aksjonere mot skjønnlitterære verk, er et poeng som i denne sammenheng ligger noe på siden. Det er vel heller slik at det i et demokratisk samfunn med stor grad av frihet for kunstneriske uttrykk, ikke er særlig nærliggende å gripe inn overfor slike verk, og dertil kommer at rekkevidden både av porno- og kunstbegrepet byr på tvil. Men man kunne tenkt seg at *alminnelig*

[559] Ot.prp. nr. 5 (1958) s. 27-29; Ot.prp. nr. 4 (1978-1979) s. 15-19.
[560] *Andenæs/Andorsen* (2008) s. 185-186.

bildepornografi hadde blitt rammet på denne måten fordi det da normalt er enklere å ta stilling til rettsstriden.[561]

Men fordi det minst har vært dobbel hjemmel for inndragning av trykt skrift, har praksis måttet velge mellom bestemmelsene. Ved gjennomgang av rettspraksis har jeg ikke kunnet finne avgjørelser med en prinsipiell begrunnelse for hvorfor man i det konkrete tilfellet har valgt å benytte strl. 1902 § 35 fremfor § 38. Men det lar seg konstatere at strl. 1902 § 38 bare har vært benyttet ved spørsmål om inndragning av skjønnlitterære verk, mens bestemmelsen om inndragning av "ting" er anvendt på materiale med ytringer som kan karakteriseres som regulær pornografi (bilder). I pornosaker kan det ha vært praktisk å hjemle inndragningen i strl. 1902 § 35, fordi beslaget ofte gjelder mer enn "trykt skrift", for eksempel også VHS-kassetter med rettsstridige filmer. Dermed kan samme bestemmelse anvendes for hele beslaget.[562]

Som et enslig tilfelle av bruk av strl. 1902 § 35 på trykt skrift utenfor pornografiområdet, har vi den nettopp nevnte saken "Hær-Verk" (Rt. 1986 s. 267). Eksemplarene av bladet som tok sikte på å skape uvilje blant rekruttene mot militærtjenesten, ble inndratt som "ting", jf. strl. 1902 § 35.

Når det gjelder *behovet* for inndragning av utgaven for så vidt gjelder pornoblader, må den imidlertid sies å være liten. Det er nemlig lite sannsynlig at en beslutning rettet mot utgaven vil bli utnyttet rent praktisk. For mye beror på tilfeldigheter når det er tale om fysiske eksemplarer som er vidt spredt og etter hvert går til grunne. Men her stiller det seg vesentlig annerledes med data, fordi *gjenbruksnytten* av inndragningsbeslutningen er stor i forhold til dublettene, dersom de inndratte filene legges i RDB og utnyttes i filtrene i nettet. Dette leder over i neste kapittel.

[561] Utviklingen i pornografibegrepet, også for bilder, medfører at det trekkes en romslig grense når bildene viser seksuell aktivitet mellom (forhåpentlig) samtykkende voksne. Illustrerende er Rt. 2005 s. 1628 (Frie Aktuell Rapport). Høyesterett bemerket at "rettslige standarder som grunnlag for straffereaksjoner er ikke uproblematisk på bakgrunn av de hensyn som ligger til grunn for lovkravet i Grunnloven § 96. Jeg er enig med lagmannsretten i at denne type straffebestemmelser må tolkes med varsomhet, og at det gjelder enn mer når det som her er spørsmål om en standard som viser til en bestemt oppfatning om seksualitet og moral." (avsn. 16). Frifinnelse for distribusjon av 13 000 pornoblader.

[562] Se følgende pornografisaker: Rt. 1979 s. 863 og Rt. 1979 s. 1418: Inndratt "magasiner og filmer", jf. strl. 1902 § 35; Rt. 1980 s. 1532: Inndratt bildemagasiner, filmer og videobånd, jf. strl. 1902 § 35; Rt. 1985 s. 569: Inndratt videokassetter, filmer og blader, jf. strl. 1902 § 34 flg.; Rt. 1987 s. 1194: Inndratt blader, videokassetter og filmer, jf. strl. 1902 § 35.

11.4.4 Straffeloven 2005 og koblingen til strl. 1902 § 38

Det er konkludert med at strl. 1902 § 38 om inndragning av trykt skrift må antas å gi hjemmel for å inndra utgaven med virkning for alle eksemplarene. I straffeloven 2005 er bestemmelsen ansett dekket av bestemmelsene om inndragning av "ting" og "informasjonsbærer", jf. §§ 69 og 70, jf. § 76. Spørsmålet er om disse bestemmelsene generaliserer adgangen til å inndra en bokutgave med virkning for eksemplarene, til data med virkning for dublettene.

Straffeloven 2005 viderefører ikke bare rettstilstanden etter straffeloven 1902, men gjør også en vesentlig endring ved å fjerne unntaket for private eksemplarer. I forarbeidene gis følgende begrunnelse for endringen:

> "Normalt er ikke innholdet av en informasjonsbærer straffbart i seg selv. For eksempel kreves det i straffeloven § 135 a at innholdet fremsettes offentlig. Unntaksvis er besittelse tilstrekkelig, se for eksempel § 204 første ledd bokstav d om barnepornografi. Da bør informasjonsbæreren etter departementets syn kunne inndras med hjemmel i utkastet § 69 uavhengig av om den er tilgjengelig for allmennheten eller ikke."[563]

Dermed har lovgiver positivt gitt uttrykk for at eksemplarer i privat eie kan inndras. For å oppfylle lovgiverviljen må inndragning kunne besluttes for utgaven (ISBN) eller en annen ordensbetegnelse som omfatter alle eksemplarene.[564] Dermed bringes inndragningen i pakt med straffebudenes rekkevidde. Dersom inndragningsadgangen anses å være begrenset til de beslaglagte eksemplarene er intet vunnet ved endringen.

Adgangen til å inndra en "orden" med hjemmel i "ting" kan neppe antas å være forbeholdt bøker, fordi vi jo har med en generell regel å gjøre. Også data er "ting" og "informasjonsbærer", og siden data kan identifiseres ved sjekksum synes inndragning av datafilen å kunne omfatte alle dublettene på grunnlag av *dataidentiteten.* Det ligner eksemplarene i en utgave identifisert ved ISBN.

Denne tilnærmingsmåten til inndragning av dubletter synes derfor å ha hjemmel i inndragningsreglene i straffeloven 2005.

[563] Ot.prp. nr. 90 (2003-2004) kapittel 26.6.4 s. 349-50. Sitatets referanse til "utkastet § 69" er blitt vedtatt som strl. 2005 § 69.
[564] Dersom det gjelder en tilsvarende identifikasjonsordning for utgivelser av musikk- og filmverk på CD og DVD, bør løsningen bli den samme.

Det kan likevel innvendes at løsningen bygger på en haltende analogi mellom eksemplarer av trykt skrift og dubletter som selvstendige "eksemplarer". Det er en tilnærming som avhandlingen alt har avvist ved fortolkningen av straffebudene og inndragningsreglene, så løsningen er heller ikke konsistent med prinsipper som tidligere er lagt til grunn. Det blir tydelig i forhold til fortolkningen av inndragningsgrunnlaget i strl. 2005 § 69 bokstav a "frembrakt ved", hvor det er lagt til grunn at dubletter i beslaget teller som én.[565] Analogien halter fordi at hvert enkelt eksemplar av en bok har verdi for innehaveren. Eksemplaret er varen. Dublettene derimot skapes av en rekke forskjellige grunner som har med databehandling og distribusjon av kommunikasjon i nettet å gjøre, så de representerer ikke nødvendigvis selvstendige objekter for en innehaver. Denne tilnærmingen har derfor ignorert egenskaper ved teknologien som tilsier at vurderingen av dubletter bør skje på selvstendige premisser.

Kritikken ligger i forlengelsen av det syn som er lagt til grunn ved inndragning av datafiler (i beslaget) som har vært tilgjengeliggjort i nettet. Konklusjonen var at de skulle inndras med hjemmel i strl. 2005 § 69 bokstav b ("gjenstand for"), fordi de hadde tilgjengeliggjort mer av seg selv.[566] Med andre ord at kildefilen og dublettene er utslag av samme fenomen.

Jeg har derfor reist en selvstendig diskusjon av om dublettene, ulikt eksemplarer av en bok, kan anses som utslag av ett og samme fenomen ("ting"), jf. drøftelsen i neste kapittel.

11.5 Dubletter som én "ting"

11.5.1 Det faktiske fenomen som fortolkningen gjelder

Spørsmålet er om datafiler med samme sjekksum kan anses som samme "ting", jf. inndragningsreglene i straffeloven 2005. For så vidt gjelder fysiske gjenstander er utgangspunktet at de inndras separat, med mindre det er naturlig å anvende mengdekriterier. Et kjennetegn på en fysisk gjenstand (A1) er at den kan *lokaliseres til et bestemt sted.* Selv om vi ser en annen lik gjenstand (A2) vet vi at den ikke er den samme, fordi den ikke er på nøyaktig samme sted som A1 (og vi vet hvor A1 er). Tilstedeværelse av ett fysisk objekt

[565] Se kapittel 5.3.2.2.
[566] Se kapittel 5.3.2.4.

ekskluderer samtilstedeværelse av et annet fysisk objekt, og på den annen side er vi ikke i tvil om at vi forholder oss til *to objekter* (A1 og A2).

Data oppfører seg annerledes enn fysiske objekter. De er som nevnt en tilstand, de er ikke-rivaliserende og kan skape mer av seg selv. Det å telle dubletter på samme måte som fysiske objekter gir derfor lite relevant informasjon om *forekomsten.* Forekomsten er ubestemt og mengden varierer hele tiden. En datafil kan isolert sett lokaliseres til ett bestemt sted i nettet, men mange kan utnytte den og laste ned en kopi (dublett). Som en del av funksjonaliteten skaper datateknologien mer av den samme filen og datafilen er kilde for et ubestemt antall dubletter.[567] *Lemley* er inne på dette poenget i sin kritikk av metaforer om internett, og viser til at

> ”While in the physical world I can occupy only one place at a time, on the Internet I – or at least my data – can be everywhere at once (and indeed it is often hard to avoid doing so).”[568]

I motsetning til fysiske objekter kan datafiler tilegnes av mange uten at den enes bruk går på bekostning av en annens. Denne ikke-rivaliserende egenskapen er velkjent for *informasjon*, se for eksempel *Lessig* som i sedvanlig poengtert stil konstaterer at *det blir ikke mindre av Einsteins relativitetsteori om noen bruker den.*[569] Også *Udsen* fremhever egenskapen. Han sier at informasjon ikke er undergitt ”knaphedens lov” og utdyper synspunktet slik:[570]

> ”Information indgår i en kommunikationsproces, der bevirker, at information kopieres. Denne proces kan principielt gentages i det uendelige, og information kan derfor overdrages i det uendelige. Sammenholdt med, at omkostningerne til kopieringen typisk er minimale set i relation til informationens værdi, bevirker dette, at information ikke er underlagt knaphedens lov.”[571]

Udsen følger opp med å påpeke at denne egenskapen ved informasjon er blitt særlig uttalt ”med udbredelsen af den digitale teknologi”, og at det ”har sat hele det ophavsretlige system

[567] Se kapittel 3.3.4.
[568] *Lemley* (2003) på s. 526.
[569] *Lessig* (2002) s. 21:”Einstein’s theory is fully nonrivalrous; […] If you use the theory of relativity, there is as much left over afterwards as there was before.” Tilsvarende bruker *Eide* (2001) *kunnskap* som eksempel på kollektivt gode, fordi ”den kan brukes ubegrenset uten å tæres”, se s. 65. Både *Lessig* og *Eide* bruker informasjon (kunnskap) i betydningen ”fleksibel og medieuavhengig”, jf. dansk teori, se *Udsen* (2009) s. 40: ”Inden for kategorien af fleksibel information består en væsentlig sondring mellem information, der behøver et fysisk medium, og information der kan lagres og overdrages uden et fysisk medium.” og han tilføyer at det ”er karakteristisk for den medieuafhængige information, at den ikke kan gives tilbage.”
[570] *Udsen* (2009) s. 37.
[571] *Udsen* (2009) s. 37.

under pres."[572] *Udsen* lar altså – slik jeg alt har forklart – informasjonsbegrepet omfatte databaserte signaler, og sitatene viser tydelig at det er *dataenes* kopieringsevne han mener at er sentralt.[573] Databasert informasjon og data behandles som samme fenomen i forhold til delingsspørsmålet (ikke-rivalisering). Det må anses som en realistisk beskrivelse av delingen i elektroniske nettverk.[574]

Så, for å trekke drøftelsen over til dublettene, kan det konstateres at datafilen kan deles og er etter deling intakt og kan fortsatt deles. Mottakerne har dubletter som også kan deles. Dermed ligger forholdene vel til rette for en eksponentiell delingstakt i nettet. Det å telle hver dublett som én synes lite relevant, fordi det er *samme fenomen som sprer seg utover i nettet*. Det elektroniske nettet opphever – som vi alt har vært inne på – forbindelsen mellom tid og sted og da blir en bestemt tallfesting lite meningsfylt. Dersom man ønsker tilgang på en spesiell type rettsstridig bilde, kan man søke på nettet ved bruk av mange forskjellige tjenester, hvor teknologien til slutt finner det for en. Hvor datafilen fysisk er lagret har ingen betydning. Filen kan være tilgjengeliggjort på flere forskjellige tjenester.

Den filen man anskaffer kan dessuten være et resultat av "databiter" som er hentet fra forskjellige kilder rent fysisk, men som er satt sammen til det endelige bildet / dataprogrammet.[575] Moderne fildelingstjenester får datamaskinen til hver deltaker som har en fil som etterspørres, til å samarbeide teknisk. Hver deltakers datamaskin bidrar med en liten del av filen. Til slutt settes alle delene sammen til én fullstendig dublett hos den som opprinnelig søkte etter filen. Dette skjer selvsagt fordi tjenesten selv utnytter dataidentiteter (hash teknologi). Søk etter filer transformeres til etterspørsel og samarbeid om utveksling av innhold med spesifikke dataidentiteter. Den tekniske effektiviteten har økt så sterkt at den som er i ferd med å skaffe seg filen på den beskrevne måten, selv omgående bidrar ved å dele av de "snuttene" som vedkommende har lastet ned, dvs. før dubletten er komplett. Dette er "torrent"-teknologi som skaper en "datasverm", hvor alle datamaskinene deler og laster ned på mest mulig effektiv måte. Det sørger for at belastningen i nettet blir jevnt fordelt og at

[572] *Udsen* (2009) s. 37.
[573] Se kapittel 8.2 om sammensmelting a informasjon og data i uttrykket "elektronisk informasjon".
[574] Se om *Udsens* posisjon som smelter sammen data og databasert informasjon i kapittel 8.2 og 11.2.2.
[575] Dette skjer for eksempel på fildeling, se nedenfor. Det har en parallell i sammensatt innhold på nettsteder, såkalt "mash up", som betyr at innholdet fysisk hentes fra forskjellige kilder. (wikipedia.org/wiki/Mashup_(digital)). Forsåvidt gjelder dublettene som skapes ved torrent-teknologi, kan det kalles "mash up" av innholdet i en enkelt fil.

utvekslingen av dubletter går raskt.[576] Det betyr at dubletter som anskaffes på en fildelingstjeneste kan være sammensatt fra forskjellige kilder. Likevel er de identiske dubletter. På fildelingstjenester utveksles ikke bare opphavsrettslig vernet materiale, herunder dataprogrammer, det brukes også for utveksling av overgrepsbilder.[577]

Dublettenes tids- og stedsuavhengighet gjør også at brukerens behov fylles ved at filen er tilgjengelig et eller annet sted i nettet. Brukeren behøver ikke ha den på sin egen datamaskin. Via nettverket og funksjoner på eget datautstyr, kan brukeren utnytte bilder og programmer der de finnes uten å ha materialet selv, slik man må for å kunne utnytte fysiske ressurser.

Fordi datafilene oppfører seg så annerledes enn fysiske objekter, kan man ikke uten videre anta at ”ting” skal forstås på samme måte for dublettene som for fysiske objekter. Utgangspunktet for fortolkningen bør være langt mer åpent, hvor man stiller spørsmålet: Hvordan bør ”ting” fortolkes i forhold til dubletter? Dette handler om å tillegge de faktiske omgivelsene rettslig relevans. I den fysiske verden aksepterer vi at en ting bare kan være ett sted av gangen, og tolker rettsregler i lys av denne virkelighetsforståelsen. Men på internett kan tingen være flere steder på samme tid. Det er jo ikke engang sikkert at vi kan bruke ordet ”sted” som en treffende metafor.[578] Mitt syn er at dublettene er en del av teknologien og bør vurderes ut fra de betingelser som skaper dem.

Gitt at dublettene forekommer i et *uspesifikt antall,* at de kan oppsøkes og utnyttes *uavhengig av lokalisering*, og at teknologien kan *identifisere og likebehandle* dem uansett hvor de forekommer, synes begrepet ”ting” å få en annen dimensjon enn når det anvendes på fysiske objekter. Jeg går nå over til å kartlegge om det finnes rettslige holdepunkter for en slik fortolkning av ”ting”, som går ut på at dublettene anses som samme fenomen, dvs. én ”ting”.

[576] VG Nett ”Slik fungerer teknologien bak Pirate bay” hvor det blant annet står: ”En av de store fordelene med bittorrent-teknologien er at maskinen som i utgangspunktet deler ut innholdet ikke behøver å sende et eksemplar til alle som vil ha. Den behøver i prinsippet bare å sende ut ett eksemplar av filen som skal deles, så vil filen sirkulere mellom datamaskinene på nettverket.” http://www.vg.no/pub/vgart.hbs?artid=572013 (besøkt 22.04.2009).
[577] Se omtale av Operasjon Enea, en politiaksjon i 2004 mot utveksling av overgrepsbilder på fildelingstjenesten Kazaa, som ved utnyttelse av sjekksumidentitet avdekket 12 000 saker på 48 timer, se *Sunde* (2006) s. 20 og 224.
[578] Se kapittel 11.2.1.

11.5.2 Telleproblemet i praksis

Dublettene har gjort seg gjeldende i rettspraksis om overgrepsbilder. I beregningen av antallet kan man se utviklingen av et nettoprinsipp, dvs. at dublettene telles som én, i stedet for at man teller på "vanlig" måte, ved å summere alle rettsstridige filer (bruttoprinsipp). Avgjørelsene er en kime til en rettslig forståelse av dublettene som én "ting".

I Rt. 2007 s. 422 uttalte Høyesterett at av:

> "de 10 beslaglagte videosnuttene var tre like, slik at det i realiteten er tale om 8 ulike filmer".

Og i to saker fra lagmannsrettene i Borgarting og Eidsivating opplyses det at

> "Forsvareren har hevdet at en stor del av bildene var duplikater, det vil si at de samme bilder/bildeserier forelå i flere kopier, og at antallet ulike bilder utgjorde 2-3000. Aktor har for lagmannsretten sagt seg enig i at det forelå en del duplikater, men ikke i det omfang forsvareren har hevdet. Lagmannsretten legger til grunn at det i de 7490 bildene inngår en del duplikater, men finner ikke at antallet har nevneverdig betydning for straffutmålingen." (LB-2006-656 (Borgarting)),

og at:

> "A hadde lagret i alt 75.378 bilder og 1.090 videosnutter av barn på sin PC. […] Flere av bildene var lagret dobbelt. Lagmannsretten legger til grunn at dette er korrigert ved fastsettelsen av ovennevnte antall, slik det fremgår av politirapporten av 13. oktober 2003 vedrørende kategorisering av bildene og filmene." (LE-2004-13795 (Eidsivating))

Formuleringene i lagmannsrettsavgjørelsene tyder på at det er dubletter i teknisk forstand (lik sjekksum) som har gitt grunnlag for nettosynspunktet, jf. "duplikater", "dubletter", "flere billedserier forelå i flere kopier" (Borgarting), og "bildene var lagret dobbelt" (Eidsivating).

Flere andre underrettsavgjørelser gir også uttrykk for en nettobetraktning:

RG 2006 s. 595 (Agder): Domfelte gjorde gjeldende at han hadde kopiert de lagrede overgrepsbildene fra sin gamle datamaskin til to andre maskiner, en ny bærbar og en ny stasjonær, og at det i all hovedsak var det samme materialet som befant seg på de tre stedene.

”Påtalemyndigheten har forut for ankeforhandlingen gjennomgått materialet på nytt. Den siste undersøkelsen er den grundigste *og er utført ved hjelp av dataverktøy.* … Den siste undersøkelsen ga som resultat at det av et totalt antall på 3 961 billedfiler med barnepornografisk innhold ble funnet ca 750 bilder som forekom to eller flere ganger. Av disse var det noen få filer som forekom 8-13 ganger. Antallet *forskjellige filer – unike bilder* – var 3.209”. (mine uth.).

LF-2005-116879 (Frostating): 562 bilder hvorav ”noen av bildene forekommer i to eller flere eksemplarer”.

LG-2005-83688 (Gulating): 3 432 bilder redusert til 3 100 bilder fordi samme bilde og grupper av bilder var lagret i forskjellige mapper.

LG-2003-4852 (Gulating): 371 bilder ”hvorav antydningsvis inntil 25 % kan være bilder som foreligger i ulike lagringsenheter”.

LH-2004-51077 (Hålogaland): To domfelte: A i besittelse av 898 bilder, og ”av det totale antallet er en del bilder med to eller flere ganger, men det dreier seg iallfall om mer enn 500 forskjellige bilder.” B i besittelse av minst 5 000 bilder. ”Også dette bildematerialet er med to eller flere ganger, men det er iallfall tale om ca 3 000 forskjellige bilder.”

LH-2006-27124 (Hålogaland): 37 000 bilder ”etter at duplikater er luket ut”.

TBERG-2007-70663 (Bergen tingrett): 218 735 bilder og 59 filmklipp ”beregnet av et dataprogram”.

Høyesterettsavgjørelsen fra 2007 nevner ikke hvilket kriterium som ble lagt til grunn ved bedømmelsen av at videoklippene var like. Det var 10 videoklipp, så det har vært mulig å spille dem av. Men siden hash program er et vanlig politiverktøy er det nærliggende at like sjekksummer er konstatert i dataanalysen under etterforskingen, og deretter lagt til grunn av retten. Dessuten er det vanskelig for retten å vite hva som er likt idet man avviker fra sjekksumkriteriet. Ved vurderingen av *meningsinnhold* kan det være holdbart å anse *betydningen* for å være lik, selv om innholdet objektivt sett er forskjellig, men da taler man ikke lenger om dubletter. Poenget lar seg illustrere ved noen eksempler:

- Det kan gis forskjellige meldinger om det samme: En epost med beskjeden "*Selskap X ASA offentliggjør sitt dårligste årsresultat på 5 år i morgen"*, er likeverdig med en som lyder *"I morgen offentliggjør selskap X ASA sitt dårligste årsresultat på 5 år",* og med en som lyder *"X ASA off.gj. dårligste års.res. p 5 år imrg."*. I en innsidesak hvor vurderingstemaet er om det er gitt "presise opplysninger […] som er egnet til å påvirke kursen […] merkbart", jf. vphl. § 3-2 (1), er de tre meldingene likeverdige, men i forhold til sjekksumkriteriet er de forskjellige (ikke dubletter).

- Et bilde endres i et redigeringsprogram ved at det beskjæres i kantene. Det opprinnelige og det beskårne bildet inneholder lik, men ikke identisk, informasjon, og bildene er ikke dubletter.

- Det tas flere bilder med kort mellomrom av en person, eller det gjøres flere opptak av et musikkverk. Innholdet er likt, men de er ikke dubletter.

Når man begir seg ut i vurderinger av likhet på grunnlag av meningsinnholdet, er det bestandig tale om et *fortolket innhold* som sjalter vekk irrelevans og søker mening. Etter hvert blir det vanskelig å trekke grensen for hva som er likt. Sjekksumkriteriet er et objektivt kriterium for likhet og det er sannsynlig at dette er brukt i de nevnte sakene. Det betyr at dublettene er rettslig relevante. Dubletter gir ikke mer materiale, de er ett og det samme. I saker om overgrepsbilder må det foreligge et objektivt kriterium for likhet, ellers bryter tellemetoden sammen. Det tas jo ofte hele serier med bilder av det samme offeret, og bildene må innholdsmessig sies å være like. Men det leder ikke til at serien er ett bilde.

For så vidt gjelder skadelig dataprogram, er det bare sjekksummen som gir et godt kriterium. Av denne grunn anses et modifisert program som et nytt program.[579]

Rettsavgjørelsene begrunner ikke hvorfor dublettene skal telle som én ved beregningen av antallet. Alle er avsagt på et senere tidspunkt enn Rt. 2002 s. 1187, hvor Høyesterett i en sak om besittelse av 7 000 bilder og 191 videosnutter uttalte at det:

> "eksakte antall i en sak om et betydelig materiale, vil lett bero på tekniske forhold og kan […] ikke være så utslagsgivende" (på s. 1192).

[579] Se kapittel 5.3.2.2.

I henhold til denne uttalelsen er anvendelsen av nettoprinsippet i flere av de ovennevnte sakene, unødvendig nøyeregnende. Nettoprinsippet kan ikke anvendes utelukkende fordi det kommer lovbryteren til gode. Domfellelsen skal foregå på korrekt faktisk grunnlag, så antallet skal ikke nedjusteres uten forankring i et rettsgrunnlag. Heller ikke ved lite omfang kan det *eksakte* antallet antas å ha betydning. Det er jo ingen grunn til å legge vekt på om besittelsen gjelder 8 eller 10 videosnutter. Det har reelt sett ingen betydning. Beregningsmetoden som avgjørelsene gir uttrykk for, kan således skyldes en rettslig oppfatning om at dubletter én ting. Det har i så fall gode reelle grunner for seg, krenkelsen overfor barnet på bildet blir i hvert fall ikke større av at man *besitter* flere like bilder. Det samme gjelder skadelig dataprogram; *besittelsen* blir ikke mer alvorlig om man har flere filer med det samme programmet.

Ved kalkuleringen av omfanget synes anvendelse av en nettoberegning å gi det beste uttrykket for sakens faktum. Det er i samsvar med den fortolkning som har blitt lagt til grunn tidligere for produksjonsalternativet (”frembrakt ved”) i strl. 2005 § 69 første ledd bokstav a, sammenholdt med strl. 2005 §§ 201 og 311.[580] Det ble skilt mellom førstegangsproduksjon og kopiering, og konkludert med at bare førstegangs fremstilling kan anses som produksjon. Dubletter teller heller ikke med ved rekonstruksjon av filer. Denne løsningen kommer praktisk til uttrykk for inndragningssituasjonen ved at beslutningen bare teller med unike filer.[581]

Forekomsten av dubletter i beslaget kan imidlertid skyldes at lovbryteren har lastet ned bildet flere ganger fra internett. Det straffverdige består i *antallet anskaffelser*, og da bør antallet *markeringer av etterspørsel* etter overgrepsbildene telles. Man teller altså noe annet enn dublettene. Antallet anskaffelser kan det etter omstendighetene være mulig å avdekke ved analyse av tidsstempler i filsystemet, og av siktedes organisering av samlingen mer generelt.[582]

Hovedpoenget i den foreliggende sammenheng er at rettspraksis synes å legge til grunn at dubletter er ett fenomen, dog uten å ha bevisstgjort forskjellen mellom vurderinger av meningsinnholdet kontra vurderinger på grunnlag av dataidentiteten. Det er nok

[580] Se kapittel 5.3.2.2
[581] Se kapittel 5.5.
[582] En doktorgradsavhandling fra 2008 (NTNU) belyser hvordan tidsstempler i den databaserte informasjonen kan utnyttes som grunnlag for avdekking av faktum i straffesaker, se *Willassen* (2008).

dataidentiteten som reelt sett ligger til grunn for beregningene, men et klart standpunkt som viser at så er tilfelle, mangler. Men som kjent kan man ikke fastslå om filer er dubletter ut fra en vurdering av meningsinnholdet. Det må gjøres av et hash program. Etter å ha kalkulert sjekksummen kan det vise seg at to like bilder virkelig er dubletter, men også at de *ikke* er det. Da skyldes det en forskjell i datainnholdet (antallet pixler) som ikke skapte noen synlig forandring i bildet.[583] I så fall har hash programmet talt filene som to forskjellige. Dette blir nok lagt til grunn av domstolene på grunn av det betydelige antall filer som sakene ofte involverer.

Men det er viktig å merke seg at grunnen til at hash teknologien er så nyttig, er den store forekomsten av dubletter. Det er stadig de samme bildene og programmene som verserer, og som derfor kan identifiseres. Jeg viser til kapittel 3.3.3 og 3.3.4 om dette. Over tid, og med tanke på hensynet til likebehandling, blir derfor en konsistent anvendelse av nettoprinsippet reelt sett riktig, mens man på den annen side teller med alle unike filer.

Tellemetoden anvendt i rettspraksis sier først og fremst noe om rettsoppfatningen av dubletter, nemlig at de er ett og samme fenomen. Hvorvidt det å telle antallet unike filer er hensiktsmessig for straffutmålingen i saker om overgrepsbilder er et annet spørsmål. Etter min mening burde tellingen i stedet konsentrere seg om antall anskaffelser og førstegangsdistribusjoner, antall ofre og overgrep. Men det hører hjemme i en annen diskusjon.

11.5.3 Koblingen mellom identitet og norm

11.5.3.1 Subsumsjonen integrert i teknologien

Jeg har forutsatt at nettet er en del av den alminnelige samfunnsarenaen hvor inndragning kan iverksettes. Siden dublettene unndrar seg direkte menneskelig befatning, må den rettslige beslutningen integreres i teknologien, noe som gjøres ved å oppdatere filtrene med sjekksummene til inndratte filer. Filterteknologien opererer på datanivået, programmert med

[583] Binærfiler med grafikk (bilde) inneholder mye mer informasjon enn mennesket kan oppfatte. "Informasjonsoverkapasiteten" kan blant annet utnyttes for å formidle informasjon på skjult måte ved *steganografi*. Steganografi utnytter "the least significant bit" i hver pixel, som tas ut og erstattes med fragmenter av den skjulte meldingen. Mottakeren kan åpne den skjulte informasjonen ved å bruke et "stega-program" med en dekodingsnøkkel, som trekker ut og sammenstiller det skjulte innholdet. Det menneskelige øye kan ikke oppfatte informasjon som er skjult på denne måten, men dersom to øyensynlig like filer har forskjellig sjekksum kan en årsak være at den ene utnyttes som bærer av en skjult melding.

”input” fra beslutningen om inndragning. Dermed er et normativt element lagt inn i teknologien. Den tekniske mekanismen integrerer faktahåndtering og norm. Enkelt sagt representerer sjekksummene i filtrene den rettslige subsumsjonen.

Det skjer således en *automatisering av subsumsjonen* som rammer alle instanser av en inndratt og identifisert fil. Det er på dette punktet en avgjørende forskjell fra heroinet i den fysiske verden, jf. ”heroineksemplet” i kapittel 11.3.3. For å illustrere med et eksempel, kan den tekniske mekanismen forstås som en hybrid av to velkjente politiverktøy, nemlig DNA-registeret (faktum: identitet) og narkotikalisten (normativitet). Mekanismen kobler faktum og norm med virkning for dublettene sett under ett.

11.5.3.2 RDB vs. DNA-registeret (faktum om identitet)

RDB er orientert mot gjenkjenning av datafiler, dvs. *identitet*, og har her fellestrekk med DNA-registeret. Det sentrale DNA-registeret ved Kripos er bygget opp av ”DNA-profiler”, og en DNA-profil er:

> ”en analyse av biologisk materiale for å fastslå en persons identitet. DNA-profilen uttrykkes ved en tallkombinasjon”, jf. påtaleinstruksen § 11a-1 annet ledd.

Den tallkombinasjonen som uttrykker DNA-profilen er en funksjon av det biologiske materialet som analyseres.[584] Siden DNAet er unikt for personen, gir biologisk materiale fra samme person samme DNA-profil uansett hvor man finner materialet. Det kan for eksempel være sikret på flere åsteder hvor lovbryteren har vært, og være tatt fra lovbryteren selv ved avgivelse av DNA-prøve, jf. strpl. § 158. Fordi DNA-profilen er unik, kan den brukes til ”å fastslå en persons identitet” som det står i påtaleinstruksen.[585] DNA-profilen av biologisk materiale funnet på et åsted (”spormateriale”), kan sammenholdes med DNA-profilene i registeret. ”Match” foreligger dersom tallkombinasjonene til spormaterialet og en registrert

[584] Se NOU 2005: 19 kapittel 3.1.4.2 på s. 17: ” Det samlede resultatet, en DNA-profil, består derfor av en tallrekke samt angivelse av kjønn. Dette er et resultatformat som er enkelt å håndtere mht. databaser.”
[585] Hvorvidt personen er kjent for politiet er en annen sak. DNA-registeret er todelt, slik at identitets- og etterforskingsregisteret inneholder DNA-profiler til kjente personer, mens sporregisteret inneholder DNA-profil til ukjente personer.

DNA-profil er like.[586] Hvis man kjenner identiteten til personen med DNA-profilen, kobler "matchen" vedkommende til åstedet.

Bruk av DNA-profil er *biometri*, dvs. en metode basert på måling av biologiske mønstre som brukes til "verifikasjon av identitet".[587] Utnyttelse av *biometri i datasystemer* er et felt i rask fremvekst.[588] Jeg tenker for eksempel på datasystemer som baserer seg på innsamling av fingeravtrykk eller irismønster, som grunnlag for gjenkjenning av person. Slike systemer er basert på at den personlige egenskapen er unik for personen. DNA-registeret atskiller seg fra helautomatiserte biometriske systemer, fordi det *i hvert tilfelle er nødvendig med laboratorieundersøkelse* av det biologiske materialet ("DNA-analyse") for å bestemme DNA-profilen.[589] DNA-registeret kan ikke "mates" direkte med det biologiske materialet, slik man kan med et helautomatisert biometrisk system som for eksempel gjenkjenner fingeravtrykk som legges mot en "leser".[590]

Sjekksummen til en dublett kan sammenlignes med den tallkombinasjonen som uttrykker DNA-profilen. Sjekksummen er hash programmets uttrykk for filens dataverdi. På samme måte som en DNA-profil identifiserer en person, identifiserer sjekksummen en datafil. *Identifikasjonsformålet* realisert ved "matching" er derfor felles for de to teknologiene.[591]

[586] Se NOU 2005:19 kapittel 3.1.4.2 på s. 17: "DNA fra spormateriale og personer analyseres i to separate prosesser, og sammenligning av profiler kan først skje etter resultatbehandlingen. Det kalles en « match » når to profiler som sammenlignes, for eksempel en sporprofil og en identitetsprofil, er identiske."
[587] Ofte brukes "autentisering" om dette, men "verifikasjon av identitet" ble anbefalt brukt i *Biometriutredningen* (2008), fordi "det angir mer eksplisitt et meningsinnhold, og er trolig noe lettere å forstå", kapittel 2.2 s. 9.
[588] Jf. uttrykket "Biometric technologies" som er "automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic", se *Wayman* (2005) s. 1.
[589] Det er en analyse som hos oss utføres av Rettsmedisinsk institutt. NOU 2005: 19 kapittel 3.1.8 s. 19. Se om fremgangsmåten ved analysen i kapittel 3.1.4.1 s. 17.
[590] Systemet har forhåndslagret et "mønster" ("template") av fingeravtrykket, og fingeravtrykket måles mot dette mønsteret. Fingeravtrykket som sådan er altså ikke registrert i systemet for gjenkjenning av fingeravtrykk. Det er derimot tilfelle for Kripos sitt fingeravtrykksregister. Registrering og bruk av den personlige egenskapen omfattes av personopplysningsloven, og Personvernnemnda har behandlet flere saker om bruk av biometri for å verifisere identitet, se PVN-2006-07 (Tysvær kommune); PVN-2006-05 (Oxigeno Fitness); PVN-2006-09 (Oslo Trimsenter); PVN-2006-10 (Esso Norge) og PVN-2006-11 (Rema 1000). Avgjørelsene gjelder pol. § 12 som lyder: "Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering". Ifølge forarbeidene er "biometriske data" slike "entydige identifikasjonsmidler", se Ot.prp. nr. 92 (1998-1999) s. 114.
[591] Hva som er identifikasjon og hva som er verifikasjon av identitet, er også en egen diskusjon. Det er vel mest korrekt å si at "matchingen" verifiserer identiteten til en fil, men da er den også identifisert på filtreringspunktet i nettet. Jeg synes ikke bruken av "identifikasjon" skaper noen problemer her, fordi det er avklart at systemet ikke kan brukes uten "matchingrunnlag", dvs. filene i RDB. Dette er hva jeg kaller en "lukket" metode, kontra en metode som foretar en informasjonsfangst ut fra åpne kriterier ("åpen" metode), se kapittel 14.3.

Men RDB er et mer *definitivt* verktøy enn DNA-registeret, fordi alt innhold i RDB er å anse som kjent uansett hvor det befinner seg. Bruk av sjekksummen i nettet innebærer derfor gjenkjenning av en ting hvor *alle relevante karakteristika* allerede er kjent. Ut fra formålet med RDB består disse karakteristika av at datafilen er rettsstridig, jf. strl. 2005 §§ 201 eller 311, og at dette er fastslått ved rettslig prøving med den følge at filen er besluttet inndratt.

Dessuten er RDB *integrert i et helautomatisert system*. Når en datafil er besluttet lagt i RDB, kan inngrepet i nettet skje automatisk fordi filtrene oppdateres med den nye sjekksummen. I dette henseende har RDB mer til felles med et helautomatisert biometrisk system, enn med DNA-registeret, hvor ”matching” krever en manuelt utført DNA-analyse.

I forhold til ”heroineksemplet” ser man at håndtering av de faktiske instanser av dubletter kan skje automatisert (uten manuell kontroll), fordi de på forhånd er entydig identifisert. I motsetning til i den fysiske verden er det både mulig og hensiktsmessig at beslutningen om inndragning har virkning for dublettene, selv om de avdekkes i ettertid. Virkningen følger imidlertid ikke av ”matchingen”, men av at dataidentiteten er inndratt, se neste kapittel.

11.5.3.3 RDB vs. narkotikalisten (subsumsjonen inn i teknologien)

Datafilene er rettslig vurdert og kjent rettsstridige i henhold til regler som etablerer et totalforbud (i hvert fall for tilgjengeliggjøring i nettet).[592] Den rettslige klassifikasjonen gjelder derfor også alle dublettene. RDB fungerer dermed også *normativt* og har fellestrekk med narkotikalisten.

Befatning med narkotika er straffbart, jf. strl. 2005 § 231, men straffebudet regner ikke opp hva som anses som narkotika. I stedet henviser bestemmelsen til

> ”stoff som etter regler med hjemmel i legemiddelloven § 22 er å anse som narkotika.”[593]

Med hjemmel i legemiddelloven § 22 er det gitt forskrift om narkotika, som inneholder den såkalte narkotikalisten.[594] Ifølge narkotikaforskriften § 2, regnes stoffer, droger og preparater som er oppført i listen, som narkotika. Listen omfatter stoffer m.v., som er omfattet av

[592] Se om betydningen av filtrenes plassering, jf. en vurdering i forhold til EMK art. 8, i kapittel 13.
[593] Smlg. strl. 1902 § 162: ”stoff som etter regler med hjemmel i lov er ansett som narkotika”.
[594] Forskrift om narkotika av 30. juni 1978 nr. 8.

internasjonale konvensjoner mot narkotika, foruten de som man fastsetter på nasjonalt grunnlag.[595] Systemet baserer seg på internasjonalt samarbeid, hvor man blir enige om hvilke stoffer som anses som narkotika.[596] Kompetansen til å gjennomføre beslutningene nasjonalt ved å foreta oppføringer i listen, er lagt til Statens legemiddelverk, jf. forskriften § 3.

Endringer i listens innhold endrer rekkevidden av narkotikaforbudet, uten at straffebudets ordlyd endres. Henvisningen til listen gir derfor straffebudet en innebygd fleksibilitet med høyt presisjonsnivå i beskrivelsen av hva som rammes.[597] På denne måten er også "narkotika" et elastisk begrep, men innholdet bestemmes av formelle beslutninger, jf. narkotikalisten, ikke av friere vurderinger slik som for "gjenstand/ting".[598] Narkotikalisten inneholder blant annet virkestoffer. Stoff som inneholder et virkestoff på listen er derfor å anse som narkotika uavhengig av hvilken form det har, for eksempel tablett, pulver eller væske. Som ledd i etterforskingen må det foretas en analyse for å fastslå hva slags narkotikum det er tale om.

Narkotikalisten er en *norm*, ikke et register for faktaopplysninger. Den fungerer imidlertid som et "verktøy", fordi oppføringene i listen gir en normativ spesifikasjon av *faktabetingelser* for "matching". Det som skal skje er *en ren sammenligning* mellom det som står på listen og det som er i stoffet. *Hvis* stoffet inneholder Gammahydroksybutyrat (GHB) *så* er det å anse som narkotika. Sammenligningen verifiserer lovbruddet. Det innbys ikke til rettslige vurderinger annet enn en ja/nei-konstatering i forhold til spørsmålet om stoffet inneholder virkestoffet. De rettslige vurderingene knytter seg vanligvis til andre aspekter ved handlingen,

[595] Khat er et stoff som Norge etter selvstendig beslutning har kriminalisert via oppføring på narkotikalisten, mens stoffet er tillatt i flere europeiske land. Se *Hauge* (1990) som kritiserer dette.
[596] Jf. den alminnelige narkotikakonvensjon av 1961 og konvensjonen om psykotrope stoffer av 1971.
[597] Tvil kan oppstå, slik Derivatdommen illustrerer (Rt. 2009 s. 780). Spørsmålet gjaldt om GBL var et derivat av GHB. GHB står på narkotikalisten, og forskriften omfatter også "salter og derivater" av de stoffer m.v, som er oppført på listen. Statens legemiddelverk hadde i brev og pressemelding lagt til grunn at GBL var et narkotisk stoff, men det var ikke oppført på narkotikalisten, bare på legemiddellisten. Da GBL ikke var å anse som et derivat av GHB var det ikke narkotika i straffebestemmelsens forstand, jf. hjemmelskravet i G § 96 og EMK art. 7. Men uklarheten knyttet seg altså til fortolkningen av "derivat", og berører ikke mitt poeng, nemlig at dersom stoffet er direkte oppført på listen, er det presist angitt hva som omfattes av straffebudet. Lovteknikken har vært kritisert for at forbudets eksakte rekkevidde ikke fremgår direkte av straffebudet selv. Som det fremgår i *Andenæs/Andorsen* (2008) på s. 243: "Listen føres à jour etter som nye stoffer som helsedirektøren mener bør behandles som narkotika, blir kjent […] Det blir derved legemiddelverket som bestemmer hvor langt lovens straffetrusler skal rekke". Og Derivatdommen viser at det ville vært bedre om GBL hadde vært oppført på listen, enn
å ty til andre kommunikasjonsmåter om hva man mente at var narkotika i lovens forstand. Inkludering av alle stoffene i *straffebestemmelsen* ville nok gjøre oppdateringsprosessen enda tyngre, fordi det er nødvendig med lovendring hver gang. Men mer vesentlig er det kanskje at listen er en tabell med stoffangivelser som fyller ca 8 utskriftsider, så straffebudet ville neppe vært mer *oversiktlig* om listen hadde blitt inntatt i bestemmelsen.
[598] Se kapittel 7 og 8.

typisk hvilket alternativ forholdet skal subsumeres under (for eksempel besittelse eller oppbevaring), graden av skyld hos de impliserte og utmåling av adekvat reaksjon.

Man kan riktignok si at det å foreta en rettslig subsumsjon bestandig er en ”matching” mellom norm og faktum, så hva er egentlig nytt med denne tilnærmingsmåten? Poenget er at det normative elementet er redusert til *ett spesifikt moment* av helt avgjørende betydning, men som innbyr til en enkel vurdering.

Hvis man tenker seg systemet overført til skadelig dataprogram og overgrepsbilder, kan *sjekksummene sammenlignes med stoffene på narkotikalisten.* På samme måte som tabletter med et virkestoff som nevnt i narkotikalisten regnes som narkotika, jf. strl. 2005 § 231, regnes datafiler med sjekksum som nevnt, som skadelig dataprogram eller overgrepsbilder, jf. strl. 2005 §§ 201 og 311. Sjekksumlisten gir en ubetinget og entydig spesifikasjon av de inndratte dublettene. På basis av internasjonal regelharmonisering for å ramme skadelig dataprogram og overgrepsbilder, kan det også lages en internasjonal sjekksumliste som brukes til å oppdatere den nasjonale RDB. En internasjonal sjekksumliste korresponderer funksjonelt med vedtakene i det internasjonale forumet som oppdaterer narkotikalisten. Spørsmålet er om den også har en normativ funksjon.

Det er en viktig *forskjell* mellom oppføringene i narkotikalisten og sjekksummene til inndratte filer. Selv om narkotikalisten gir en detaljert utpensling av straffenormen, opprettholdes skillet mellom norm og faktum. For å kunne verifisere en mistanke og fastlegge forholdets karakter, må det beslaglagte stoffet *analyseres,* smlg. det tidligere nevnte ”heroineksemplet”. Narkotikalistens oppføringer gir ingen gjenbruksmulighet av opplysningene om et beslag overfor nye beslag; hvert tilfelle må undersøkes for seg. I verktøyet for automatisert inndragning integreres derimot selve subsumsjonen, som gjelder for og anvendes automatisk på, alle dublettene uavhengig av antallet og hvor de forekommer. Dersom man først aksepterer at inndragningsreglenes begrep ”ting” omfatter alle dubletter som ett og det samme, får sjekksummene i RDB normativ virkning, ved at subsumsjonen integreres i nettet.

11.5.3.4 Konflikt med eiendomsrett eller jurisdiksjon?

Fremstillingen har vist at normen kan integreres i teknologien med fullstendig automatisert presisjon. Den tekniske mekanismen retter seg mot entydig identifiserte datafiler (smlg. DNA-

profil) som står på listen over rettslig vurderte filer som er besluttet inndratt (smlg. narkotikalisten). Sjekksummen forener identitet og normativitet med virkning for alle datafiler som bærer sjekksummen, noe som betyr at sjekksummen uttrykker "tingen".

Et spørsmål er om synspunktet leder til konflikt, f.eks. med hensyn til eiendomsrett eller jurisdiksjon. Det er jo slik at forskjellige personer kan erverve hvert sitt eksemplar av digitaliserte åndsverk, og da eier alle hver sin dublett. Bryter fortolkning av dublettene som én "ting" med dette? Og hva med jurisdiksjon; i Norge er overgrepsbilder definert ut fra at barnets alder er inntil 18 år, mens enkelte andre land anvender en grense ned til 14 år. Kan dubletter som er lovlige i andre land inndras som "ting" fordi de er ulovlige i Norge dersom "ting" omfatter alle dublettene?

For så vidt gjelder mulig konflikt med eierrådigheten til eksemplarer, må svaret ta utgangspunkt i at "ting" er et strafferettslig begrep og ikke nødvendigvis har samme betydning som "eksemplar" i opphavsretten. Her kan jeg vise til den tidligere drøftelsen hvor det er konstatert at eksemplarbegrepet tjener egne formål innen opphavsretten. Eksemplarbegrepet har derimot meget begrenset betydning innen strafferetten.[599]

Strafferettslig inndragning kjennetegnes av å ramme eiendomsretten. Det har ingen betydning at eiendomsretten er spredt på forskjellige hender dersom vilkårene for inndragning først er oppfylt. Det som *kunne* vært relevant, er at iverksettelsen berører andre individer enn parten i inndragningssaken. Det gis imidlertid hjemmel i strl. 2005 § 74 tredje ledd for å foreta inndragning uten at noen gjøres til saksøkt (smlg. strpl. § 214 b), så heller ikke det skaper et problem.

For så vidt gjelder jurisdiksjon må det tas utgangspunkt i at det fra norske myndigheter bare kan være tale om å implementere filtre i nettet ved pålegg overfor norske tilbydere. Dubletter som overføres via andre tilbyderes nett eller tjenester, faller utenfor norsk jurisdiksjon. Dermed er det ikke sagt at man skal avstå fra håndhevelse i norsk område i nettet. Også trafikk som sendes fra utlandet, og eventuelt var lovlig der (jf. 14 årsgrensen), og sendes til Norge, *er ulovlig her* (på grunn av 18 års grensen) og undergis norsk jurisdiksjon for så vidt

[599] Se kapittel 11.3.4.

gjelder gjennomføring av sanksjon. Norge har kompetanse til å foreta rettshåndhevelse over den del av problemet (”tingen”) som manifesterer seg på norsk territorium.

11.5.4 Konklusjon

Hovedkonklusjonen er at det finnes grunnlag for å fortolke ”ting” slik at dataidentiteten er objektet for inndragning. Inndragningsbeslutningen kan derfor utformes slik som beskrevet i kapittel 5.9, slik at inndragningen kan fullbyrdes i nettet.

VI Automatisert inndragning i nettet

12 Fullbyrdelse og menneskerettigheter

12.1 Innledning

Utgangspunktet er at det foreligger en rettskraftig inndragningsbeslutning som omfatter dubletter, og beslutningen er beordret fullbyrdet. Fullbyrdelsen skal skje ved automatisert blokkering av dublettene i filtrene i nettet. Spørsmålet er om retten til privatliv og ytringsfrihet setter skranker for automatisert inndragning, jf. EMK art. 8 og 10.[600]

Bestemmelsene beskriver det vernede godet slik:

EMK art. 8.1:

> ”Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse”.

EMK art. 10.1:

> ”Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Denne artikkel skal ikke hindre stater fra å krever lisensiering av kringkasting, fjernsyn eller kinoforetak.”

Ifølge EMK art. 1 plikter staten å sikre rettighetene for ”enhver innen sitt myndighetsområde”. Det kan imidlertid gjøres inngrep i rettighetene forutsatt at betingelsene i art. 8.2 og 10.2 overholdes. Disse delene av bestemmelsene lyder:

EMK art. 8.2:

> ”Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter eller friheter.”

[600] EMK er som nevnt gjennomført i norsk rett med forrang foran norsk formell lov, jf. mrl. §§ 2 og 3. Se kapittel 4.2 i forbindelse med begrepet ”ytring”.

EMK art. 10.2:

> ”Fordi utøvelsen av disse friheter medfører plikter og ansvar, kan den bli undergitt slike formregler, vilkår, innskrenkninger eller straffer som er foreskrevet ved lov og som er nødvendige i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, territoriale integritet eller offentlige trygghet, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, for å verne andres omdømme eller rettigheter, for å forebygge at fortrolige opplysninger blir røpet, eller for å bevare domstolenes autoritet og upartiskhet.”

Inngrepsvilkårene er nesten identiske etter de to bestemmelsene. Begge krever at inngrepet er foreskrevet ved lov og ”er nødvendig i et demokratisk samfunn” for å fremme et legitimt formål. Begge bestemmelsene angir det ”å forebygge uorden eller kriminalitet” som et legitimt formål. Selv om ordlyden sier ”forebygge”, omfattes også tiltak mot straffbare handlinger som alt er begått. Automatisert inndragning faller inn under dette alternativet, fordi effektivisering av straffebudet er begrunnelsen for tiltaket. ”Nødvendig i et demokratisk samfunn” betyr at det må foreligge et visst kvalifisert behov for inngrepet (”a pressing social need”), og at inngrepet må være proporsjonalt sett i forhold til det formål det skal tjene.

Staten har en skjønnsmargin med hensyn til valg av tiltak, men må kunne vise at det er relevant og adekvat i forhold til formålet (krav til egnethet). Den innledende passusen i EMK art. 10.2 synes å gi vid adgang for å foreta inngrep, bare de øvrige vilkår er oppfylt, men slik er bestemmelsen ikke fortolket i praksis fra EMD. Ytringsfrihet er en av de viktigste rettighetene i konvensjonen, og inngrep kan bare skje etter en streng vurdering.[601] Statens skjønnsmargin innebærer ikke frihet fra EMDs kontroll, som hevder sin kompetanse til å overprøve inngrepet i lys av hensynet til ytringsfriheten. Staten må vise at valget av inngrepet er gjort under hensyn til de standarder som er utviklet til vern om ytringsfriheten.[602]

12.2 Presisering av temaet for inngrepsvurderingen

Både EMK art. 8 og 10 verner retten til kommunikasjon. Mens EMK art. 10 verner ytringsfriheten, både retten til å ytre seg og til å skaffe seg informasjon, verner EMK art. 8 retten til uforstyrret fortrolig kommunikasjon med andre. Det følger av alternativet ”rett til

[601] I henhold til en veletablert rettspraksis anses ytringsfriheten som ”one of the essential foundations of a democratic society and one of the basic conditions for its progress and each individual’s self-fulfilment”, se *van Dijk* (2006) s. 774 hend henvisning til en lang rekke avgjørelser.
[602] *Van Dijk* (2006) s. 774-775.

respekt for sitt privatliv … og sin korrespondanse". Bestemmelsene har forskjellig dekningsområde selv om begge verner kommunikasjon. Det følger av at bestemmelsenes formål er forskjellige, noe det må tas hensyn til ved fortolkningen.[603]

EMK art. 8 verner om kommunikasjon som en del av utfoldelsen av privatlivet. Alternativet "korrespondanse" er en del av det videre konseptet "privat liv" og omfatter langt mer enn brevpost. Det omfatter også telefoni, og annen bruk av elektronisk kommunikasjon, såfremt kommunikasjonstjenesten er slik at det hersker en berettiget forventning om privatliv.[604] Vernet for kommunikasjonen etter EMK art. 8 tar således sikte på å beskytte mot forstyrrelser og innsyn utenfra.[605] Det blir reelt sett tale om et vern om sikker kommunikasjon, som beskytter mot kommunikasjonshindringer og avlytting.[606] Strl. 2005 § 205 som rammer krenkelser av retten til privat kommunikasjon, og ekomlovens regler om kommunikasjonsvern og taushetsplikt i §§ 2-7 og 2-9, er bestemmelser som bidrar til å effektivisere rettigheten i det norske rettssystemet.

Etter EMK art. 10 er det retten til å formidle ytringer av ethvert slag som står sentralt, dvs. at vernet gjelder *innholdet* mer enn kommunikasjonssituasjonen. Vernet omfatter også ytringer som er sjokkerende og støtende ("shock and offend").[607]

[603] *Van Dijk* (2006) ss. 789-90, sier at "in Article 8 the main point is the protection of the private character of the means of communication referred to, while in article 10 its character as a means of expressing an opinion and of providing and receiving information is at issue."
[604] *Klass* (1978) gjaldt kvaliteten på tysk overvåkingslovgivning, som blant annet ga tillatelse til hemmelig avlytting av telefonsamtaler. EMD fant at telefonsamtaler "are covered by the notions of "private life" and "correspondence"" i art. 8. (pkt. 41). Dette er lagt til grunn i en lang rekke avgjørelser senere, blant annet oppsummert i *Liberty* (2008) pkt. 56, med henvisning til *Weber og Saravia* (2006) pkt. 77 m.v.. Det er fastslått at art. 8 også omfatter telefonsamtaler tatt fra arbeidsplassen, se *Halford* (1997) (pkt. 44-46) "it is clear from its case-law that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence". Det må antas at vernet gjelder elektronisk kommunikasjon generelt, uavhengig av hva slags type kommunikasjonstjeneste som benyttes, såfremt den er av en slik art at det hersker en berettiget forventning om privat liv, smlg. *Harris* (2009) s. 381, som fremholder at det ikke gjelder samme forventning om privat liv ved radiokommunikasjon og en åpen telefax, som ved bruk av telefoni. Men det er i hvert fall fastslått at vernet gjelder også samtaler utført ved bruk av mobiltelefon, se *AEIHRE* (2007) pkt. 92, epost og bruk av internett, se *Copland* (2007). I *Copland* sa retten at det var "logisk" at epost var vernet i forlengelsen av vernet om telefoni (pkt. 41). Det samme gjaldt opplysninger om bruk av internett ("internet usage") (pkt. 42). Både innholdet i kommunikasjonen og opplysninger *om* kommunikasjonen omfattes av EMK art. 8, dvs. at trafikkdata og logger som kan belyse tid og sted for oppkobling, B-nummeret m.v., er omfattet av vernet, se *Malone* (1984) pkt. 83 flg., og *Copland* om internettlogger.
[605] *Harris* (2009) sier på s. 380 om alternativet "correspondence" at det omfatter "a right to uninterrupted and uncensored communications with others."
[606] *Harris* (2009) s. 381.
[607] *Harris* (2009) s. 381.

Spørsmålet er om filtreringen som skjer ved automatisert inndragning er et inngrep i rettighetene etter EMK art. 8 og 10, og i så fall om vilkårene for inngrep er oppfylt. Vurderingene må foretas i lys av hvordan filtreringen konkret skjer.

Et viktig poeng er at automatisert filtrering bare går ut på fullbyrding av inndragning. Det innebærer ikke oppsporing av person, det skjer presist og gir ikke overskuddsinformasjon. Med tanke på å sikre formålsbestemtheten, bør man se på muligheten for å ta i bruk personvernøkende teknologi som for eksempel bryter koblingen mellom filtrering og datapakkenes IP-adresse. Da gir ikke filtreringen spor tilbake til kilden og medfører at fullbyrdingen skjer på anonyme betingelser, dvs. overfor ukjent lovbryter eller besitter. I kapittel 5.9 har jeg lagt til grunn at strl. 2005 § 74 tredje ledd kan anvendes ved inndragning overfor ukjent part. At fullbyrdelsen i nettet bør skje på anonyme betingelser synes å være en naturlig konsekvens.

Den filtreringsmetoden jeg tenker at kan ligge til grunn for automatisert inndragning, foregår i to trinn. Første trinn (”trinn 1”) berører all trafikk som kommer i kontakt med filteret, og er selve sjekksumkontrollen. Spørsmål som må drøftes er om sjekksumkontroll i seg selv representerer et inngrep i retten til privatliv og korrespondanse etter EMK art. 8, og i ytringsfriheten etter EMK art. 10. Disse spørsmålene gjelder alle brukerne uavhengig av om de bruker nettet til lovlige eller ulovlige formål. I forhold til EMK art. 8 er spørsmålet om sjekksumkontrollen representerer *en form for innsyn*. I forhold til EMK art. 10 kan det oppstå spørsmål om tiltaket, fordi det er av generell karakter, kan ha *en kjølende effekt* på frimodigheten, og komme i konflikt med læren om ”chilling effect”.

Filtreringens annet trinn (”trinn 2”) er blokkeringen av de inndratte filene. Dette inngrepet berører bare de brukere som formidler ”svartelistet” materiale, og er derfor et målrettet tiltak. Jeg antar at problemstillingen i forhold til EMK art. 8 er om *retten til uhindret kommunikasjon* berøres, og i forhold til EMK art. 10, den materielle retten til *å formidle og anskaffe* ytringer/informasjon.

Før jeg kom frem til den ovennevnte problemformulering, var jeg inne på følgende resonnement: Det kan reises spørsmål om nøyaktig *hvilken handling* som skal vurderes opp imot konvensjonsrettighetene. *Isolert sett* er automatisert inndragning en helt presis fullbyrdelse av inndragningsbeslutningen; det er tale om å gjennomføre et inngrep som er

lovlig hjemlet og besluttet. Siden fullbyrdingen er helt presis, representerer den ikke et inngrep utover det som lovgiver alt har vedtatt og reiser derfor ikke nye spørsmål i forhold til EMK art. 8 og 10.

Automatisert inndragning representerer imidlertid en ny fullbyrdelsesmåte. Selve blokkeringen av tingliggjorte datafiler med kjent identitet er parallelt med destruksjon av fysiske objekter, for eksempel av inndratte spritflasker eller pornoblader. Men mye av problemstillingen består i å identifisere de "filtrerbare" områdene i nettet. Bruk av elektronisk kommunikasjon er nærmest per definisjon innenfor beskyttelsessfæren til EMK art. 8 og 10. Derfor er spørsmålet hvor langt inndragningshjemlene rekker med tanke på problemstillinger som kan oppstå i nettet.

Jeg har lagt opp til å foreta drøftelsene i denne rekkefølgen:

Først tar jeg opp hvor automatisert inndragning kan foregå og hvem som kan utføre det. Jeg forskutterer konklusjonen, som er at filtreringen må utføres av tilbyder på grunnlag av sjekksummer som mottas fra politiet (RDB). Men tilbyders filtrering kan tenkes å skje på forskjellige steder i kommunikasjonen. I kapittel 13 drøfter jeg først om EMK art. 8 setter grenser for *hvor* tilbyder kan filtrere. Jeg behandler spørsmålet i forhold til den dimensjonen av rettighetsvernet som gjelder *frihet fra innsyn*. Drøftelsen gjelder trinn 1, dvs. sjekksumkontrollen.

Blokkering som følge av filtrering representerer en kommunikasjonshindring som kan berøre vernet etter EMK art. 8 (retten til uhindret kommunikasjon) og ytringsfriheten i EMK art. 10. Inngrepets karakter bør vurderes i lys av hvor presist det treffer. Dette behandler jeg i kapittel 14 om "presisjonsproblemet". Presisjonsproblemet gjelder således karakteristikken av metodens trinn 2, dvs. når blokkering skjer.

I kapittel 15 behandler jeg filtrering som inngrep i ytringsfriheten, jf. EMK art. 10. Her reiser jeg spørsmålet om den generelle sjekksumkontrollen som utføres for all kommunikasjon som passerer filteret, kan komme i konflikt med doktrinen om "chilling effect". Dette gjelder altså om kontrollen på trinn 1 kan være et inngrep i ytringsfriheten.

I kapittel 16 går jeg konkret til verks med endelige vurderinger av automatisert inndragning av skadelig dataprogram og overgrepsbilder.

13 EMK art. 8 – retten til privat liv og korrespondanse

13.1 Mulige filtreringspunkter

Spørsmålet er hvor i nettet filtrering kan tenkes å foregå. Jeg har alt sagt at filtreringen bør utføres av tilbyder. Det er klart at politiet som vanlig internettbruker, er avhengig av bistand fra tilbyder for å gjennomføre filtrering. Men forholdene behøver jo ikke være slik. Myndighetene kan for eksempel pålegge tilbyderne å gi politiet tilgang som "superbruker" med direkte inngrepsadgang på nettet. Ikke bare politiske grunner taler mot å gjøre det; også årsaker på et teknisk plan med dertil hørende policyhensyn, forklarer hvorfor tilbyder blir en sentral aktør ved filtrering. Det viser at det står et *begrenset spekter metoder* til rådighet når inngrep skal skje innenfor summen av de krav og skranker som følger av legalitetsprinsippet og EMK art. 8.

I en artikkel i 2003 analyserte *Zittrain* hva som er tenkelige "kontrollpunkter" for filtrering (såkalte "internet points of control").[608] Han tok utgangspunkt i hvordan en elektronisk melding sendes over nettet fra avsender til mottaker og identifiserte 5 "punkter": Punkt 1 og 5 er kommunikasjonens *endepunkter*, dvs. avsenders og mottakers datamaskiner. Derimellom finner man avsenders og mottakers *internettilbydere* (avsenders tilbyder (punkt 2) og mottakers tilbyder (punkt 4)). I midten finner man "*internettskyen*" (punkt 3).

"Internettskyen" er det område hvor datapakkene rutes fritt etter prinsippene om "best effort" og "ende til ende".[609] Det sistnevnte prinsippet innebærer at det skal være minst mulig hindringer i nettet, fordi generelle barrierer potensielt hemmer all kommunikasjon.[610]

[608] *Zittrain* (2003).
[609] "Internettskyen" brukes her om det tekniske overføringsnivået, dvs. der hvor rutere skuffer datapakkene frem over nettet. Ordet har derfor en annen mening enn i kapittel 3.3.5, hvor det brukes om *tjenesteutviklingen* i "web 2.0" (såkalt "cloud computing").
[610] Ende-til ende-prinsippet ble i 1981 beskrevet av *Saltzer, Reed og Clark* i "End-to-end arguments in system design", *Saltzer* (1981). Prinsippet ble et grunnleggende hensyn for den tekniske internettutviklingen, som særlig IETF ("Internet Engineering Task Force") tok et ansvar for. Senere utførte *Kempf* en kjent analyse, publisert som RFC 3724 (*Kempf* (2004)). Analysen påviste at ende-til-ende prinsippet kun hadde var et teoretisk utgangspunkt for å styre pakkeflyten, og at det gjaldt mange modifikasjoner i prinsippet. IETF publiserer RFCs (Request for Comment), som er anbefalinger for internettløsninger. De utvikles i et uformelt samarbeid mellom frivillige

Internettdesignet tilsier at "internettskyen" skal være "dum" og ideelt sett bare utføre én oppgave, nemlig "skuffe" datapakkene frem til målet på mest mulig effektiv måte. Dersom en melding er stor, sørger teknologien (TCP/IP protokollen) for å dele den opp i flere pakker for "bitvis" forsendelse over nettet. Datapakkene kan rutes forskjellig vei før de settes sammen til den fullstendige meldingen hos adressaten. Dette designet og respekten for ende-til-ende-prinsippet tilsier at man lar "internettskyen" være i fred. Filtrering bør derfor skje hos sluttbruker (punkt 1 og 5), eventuelt hos tilbyder (punkt 2 og 4), men midt i nettet (punkt 3) er det vanskelig og generelt sett lite ønskelig.[611]

Formuleringen "midt i nettet" er kanskje litt misvisende. Snarere er det uttrykk for at nettet er lite egnet for å sette opp et "sentralt rettshåndhevelsesfilter". Man kan her se en mulig begrunnelse for at norske myndigheter stiller seg avvisende til filtrering på "nasjonalt nivå", som det står i siste delproposisjon til straffeloven 2005.[612] Det ville innebære store anstrengelser for å kontrollere et nett som ikke er designet med tanke på kontroll, og er et tiltak man forbinder med stater som tar lite hensyn til ytringsfrihet og demokratisk styresett.[613] Generelle myndighetsinitierte tiltak av denne art er også tatt i bruk i Europa, men da primært for å skaffe etterretningsinformasjon, ikke for å blokkere for ytringer. Da kalles metoden "signalspaning", men det er bare en annen måte å ta i bruk filterteknologi på. "FRA-loven" i Sverige er et eksempel på dette (se kapittel 14.4).

Filtrering hos *sluttbruker* byr også på problemer (punkt 1 og 5). For det første har designprinsippet om *nettnøytralitet* gjort nettet åpent for enhver som har utstyr som kan kommunisere med internett.[614] Brukerne trenger ikke tillatelse for å bruke nettet og kan koble

bidragsytere som koordineres av IETF. Hver RFC gis et eget nummer. RFC-databasen hos IETF er tilgjengelig her: http://www.rfc-editor.org/rfc.html. Se *Alvestrand* (2009) for en beskrivelse av IETFs rolle og utviklingen av RFCs.

[611] *Hannemyr* (2005) s. 21, siterer *John Gilmore* som har sagt at "Nettet betrakter sensur som en teknisk skade, og ruter rundt det".

[612] Ot.prp. nr. 22 (2008-2009) kapittel 2.18 s. 70. Se også avhandlingen kapittel 1.2, hvor jeg nevnte at departementet forholdt seg til en sondring mellom filtrering "på nasjonalt nivå" og "på tilbydernivå". Departementet sa at filtrering på nasjonalt nivå ikke under noen omstendighet var aktuelt i Norge. Med filtrering "på tilbydernivå" mente departementet "… at de enkelte internettleverandørene blir pålagt å filtrere bestemte internettsteder gjennom å blokkere tilgangen for norske brukere." Filtreringen jeg drøfter atskiller seg fra den som departementet nevner, ved at den retter seg mot datafiler, ikke mot "internettsteder".

[613] Se oversikt hos *Staksrud* (2002); og gjennomgående hos *Deibert* (2008).

[614] 'Nettnøytralitet' brukes på forskjellig vis, noe som fremgår av en rapport fra Post- og teletilsynet (*Post- og Teletilsynet* (2008)), allerede på s 5. I sin kjerne er det et prinsipp om 'ikke-diskriminering', men det er ulike oppfatninger om hva som skal sammenlignes (innhold, tjenester, tilgangsmuligheter) og hva som representerer diskriminering, for eksempel om det kan tas hensyn til prisen på en tjeneste. I brødteksten over og slik *Zittrain* (2003) og (2006a) bruker uttrykket, betyr det at nettet ikke diskriminerer ved endepunktene, dvs. at alle kan

seg opp hvor man vil. Det medfører at brukerne er vanskelige å kontrollere, med mindre de å pålegges filtrerings*plikt*. Den må i så fall effektiviseres ved at produsenter av programutrustning og kommunikasjonsutstyr pålegges å integrere myndighetenes filterteknologi i sine produkter. *Zittrain* har i flere arbeider drøftet muligheten for å innføre et offentlig pålegg om å integrere filterteknologi i produktene, for å få bukt med *skadelig dataprogram.* Han anfører en risikobetraktning: Utgangspunktet er at usikrede maskiner som infiseres av skadelig dataprogram, representerer kilder for viderespredning av materialet, noe som er til skade for alle og en trussel mot nettets funksjonsevne. Siden nettets åpne arkitektur tillater enhver å koble seg opp, må motstykket være – argumenterer han – at hver bruker kan forpliktes til å innrette seg slik at man ikke representerer en risiko for andre.[615] Dette gir grunnlag for å innføre pliktig bruk av filtrering.[616]

Risikosynspunktet er klart relevant for skadelig dataprogram som gjerne sprer seg uten at brukerne er klar over det. Overgrepsbilder derimot, blir ikke spredt uten aktiv innsats fra brukerne, og da synes forsettet (”den onde vilje”) uten videre å kunne begrunne filtreringsplikt for sluttbruker, om nødvendig ved å kreve at det foretas tilpasninger i teknologien som leveres fra produsent. Uansett er problemet hvordan filtrering hos sluttbruker praktisk sett kan gjøres med tilstrekkelig effektivt resultat. Det hefter også prinsipielle betenkeligheter ved å pålegge produsenter å tilpasse produkter med tanke på filtrering. Jeg avgrenser mot denne problemstillingen, som åpner for en rekke spørsmål på siden av avhandlingens tema. Men *Zittrains* analyse er viktig for avhandlingens tema, fordi den viser at

bruke nettet som ressurs og ”tumleplass” dersom man har egnet utstyr. Diskriminering, for eksempel ved å stille bestemte krav til sikkerhet for å få tilgang til nettet, kan bryte med prinsippet om nettnøytralitet.

[615] *Zittrain* er bekymret for at sikkerhetsproblemet vil lede til myndighetspålegg som styrer utforming av teknologien. Det kan gå på bekostning av den ”kollektive intelligensen”, dvs. kreativitet og mangfold som raskt gir store bidrag til samfunnet og til personlig utvikling. Han kaller det åpne nettets evne til å utløse felles innsats og kreatitvitet ”the generative net”, som han beskriver slik: ”a system’s capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences”. Motsatsen er teknologi som er ”strammet opp” / ”tøylet” (”harnessed” / ”tethered”)), med risiko for tap av de fordeler som åpen- og ubundethet gir. Se *Zittrain* (2006a), (2006b) og (2008a). Smlg. *Kempf* (2004) om risiko for “trust breakdown” og konsekvenser for arkitekturen (pkt. 3.1 og 4.1.2).

[616] I Norge ble dette synspunktet fremmet i NOU 2006: 6 *Når sikkerheten er viktigst.* Utvalget anbefalte at det utredes nærmere om ”alle, både privatpersoner og virksomheter, skal være pliktige til å benytte oppdatert sikkerhetsprogramvare når de kobler seg til Internett” (s. 108). Datakrimutvalget som vurderte spørsmål om kriminalisering, distanserte seg fra forslaget, fordi brukerne ”er i stor grad avhengig av profesjonelle tjenesteytere for å kunne sikre seg.” Datakrimutvalget var uenig i Sikkerhetsutvalgets utgangspunkt ”om at det påhviler et eget ansvar for den enkelte bruker med hensyn til dette problemet.” NOU 2007: 2 kapittel 4.5.1 s. 48. Datakrimutvalget har altså først og fremst sett håndtering av sikkerhetsproblemet som et ansvar for offentlige myndigheter og profesjonelle aktører. Etter dette synet skal ikke den enkelte bruker kunne komme i straffansvar for å ha forårsaket skade eller fare for skade på andre datasystemer, som følge av at man har unnlatt å sikre datasystemet sitt.

teknologien er slik innrettet at automatisert filtrering må gjennomføres via tilbyder, noe jeg drøfter i neste kapittel.

13.2 Tilbyder som filtreringspunkt

13.2.1 Innledning

Siden "internettskyen" og sluttbrukerne ekskluderes som mulige filtreringspunkter, må oppmerksomheten rettes mot tilbyder / tjenesteyter (jeg foretrekker uttrykket "tilbyder").[617] Tilbyderrollene nevnt i ehl. § 1 annet ledd bokstav b, utpeker seg som interessante for filtrering.[618] Ifølge bestemmelsen omfattes

> "å gi tilgang til, eller overføre informasjon over, et elektronisk kommunikasjonsnett, eller å være nettvert for data som leveres av tjenestemottakeren".[619]

Det gir følgende roller for tilbyder:

- å gi sluttbrukeren tilgang til internett (tilgangsleverandøren kalles ofte "ISP");
- å besørge overføring, herunder mellomlagring, av innhold som tjenesteyteren ønsker å anskaffe eller å tilgjengeliggjøre;
- å lagre data som brukeren ønsker å ha oppbevart på en annen datamaskin enn sin egen (web 2.0-situasjonen).[620]

Brukeren trenger tjenesten til en ISP for å få *tilgang* til nettet. I tillegg behøves tjenesten fra en tilbyder som besørger *overføring* og *mellomlagring* av data, slik at brukeren kan kommunisere med andre og utnytte tjenester på nettet. Og som nevnt i kapittel 3.3.5 kan det være praktisk for brukeren å betro sine data til en *nettvert* i "internettskyen". I alle disse tilfellene kontrollerer tilbyderen en tjeneste som er et aktuelt filtreringspunkt.

Spørsmålet er om områder i nettet er *filtrerbare* for tilbyder med det formål å utføre automatisert inndragning, uten at retten til "privatliv" og "korrespondanse" krenkes, jf. EMK

[617] Begrepsbruken går litt om hverandre, men ekomloven bruker "tilbyder" og ehandelsloven "tjenesteyter".
[618] Loven definerer en tilbyder (egentlig "tjenesteyter") som "en fysisk eller juridisk person som tilbyr en informasjonssamfunnstjeneste", jf. ehl. § 3 bokstav a. Begrepet "informasjonssamfunnstjeneste" er definert i lovens § 1 annet ledd bokstav a og b.
[619] Smlg. ekomloven § 1-5 nr. 14 som lyder: "Tilbyder: enhver fysisk eller juridisk person som tilbyr andre *tilgang* til elektronisk kommunikasjonsnett eller -tjeneste." (min uth.).
[620] Se omtale i kapittel 3.3.5.

art. 8. Det må avklares om filtreringen representerer et inngrep i den vernede rettigheten, jf. EMK art. 8.1, og i så fall, om inndragningsbeslutningen oppfyller lovskravet. Selve proporsjonalitetsvurderingen foretas i kapittel 16.

Det er hensiktsmessig å foreta en "grovsortering" av situasjonene; innholdet på brukerens egen datamaskin representerer ett ytterpunkt, mens innhold som er lagt tilgjengelig på nettsteder som er egnet til å nå et større antall personer, er et annet ytterpunkt. I tillegg har man en kategori "i midten" som jeg også behandler.

13.2.2 Filtreringsalternativene og forholdet til EMK art. 8

Det ene ytterpunktet er brukerens datamaskin. Det synes nemlig å gå et skjæringspunkt ved brukerens tilgang til nettet. Brukerens datamaskin står på utsiden av tilgangspunktet og er en privat eiendel, mens tilgangen til nettet er en tjeneste som ytes av ISPen.

Det faktiske utgangspunktet er at når man er koblet til nettet går kommunikasjonsstrømmene både ut av og *inn i* datamaskinen. Derfor er det mulig å tenke seg at ISPen filtrerer brukerens datamaskin mens vedkommende er pålogget. Men brukerens datamaskin er en privat eiendel som ligger utenfor ISPens tjeneste. En beslutning om å inndra datafiler i nettet, kan ikke forstås å gi hjemmel til å gå inn på brukernes datamaskiner for å foreta søk etter rettsstridig materiale som er lagret på maskinen. Skjult filtrering av innholdet foretatt av tilbyder, ville representere et datainnbrudd fordi vedkommende skaffet seg uberettiget tilgang til datamaskinen, jf. strl. 2005 § 204, som rammer den som

> "ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystemet eller del av det".

Inndragningsbeslutningen gir ikke hjemmel for å sette strl. 2005 § 204 tilside, så allerede av den grunn kan man se bort fra dette grunnlaget.[621] Dermed må den private datamaskinen anses å være utenfor ISPens filtreringssfære. Dette er samme resultat som følger av *Zittrains* analyse, nemlig at sluttbrukerne (punkt 1 og 5) ikke er egnede filtreringspunkter. *Zittrains*

[621] En rett til hemmelig ransaking løser ikke problemet. For det første er ransaking et tvangsmiddel som brukes på tidligere stadier i strafforfølgningen. Det er altså ikke en strafferettslig reaksjon. For det annet forutsetter ransaking et mistankegrunnlag, mens filtrering er et generelt tiltak, som kan berøre også den som ikke besitter rettsstridige datafiler.

teknisk baserte analyse *utelukker* ikke sluttbrukerens datamaskin som filtreringspunkt; analysen viser bare at filtrering som skal utføres av sluttbruker selv, neppe er en *hensiktsmessig eller effektiv* ordning. Men som det fremgår, er sluttbrukerens datamaskin heller ikke filtrerbart område for tilbyderen etter gjeldende rett.

Brukeren kan imidlertid velge å dele noe av innholdet på maskinen sin med andre, for eksempel på fildelingstjenester. Brukeren tar da først stilling til hvilket innhold på maskinen som skal tilbys, for så å åpne dette området i et program som tilgjengeliggjør innholdet på fildelingstjenesten. Deling kan også skje ved å bruke en del av maskinen som server for et nettsted, dvs. en lokalt opprettet web-side. Det representerer et samtykke til at omverdenen tilegner seg deler av innholdet på datamaskinen. De deler av innholdet som brukeren tilrettelegger for åpen deling med omverdenen er også rent faktisk filtrerbart for tilbyder.

Filtrering av innhold som er åpent tilgjengeliggjort representerer åpenbart ikke noe datainnbrudd. Spørsmålet er utelukkende om innholdet omfattes av "privatliv … og korrespondanse", jf. EMK art. 8.

Hvis det legges til grunn at innhold som på denne måten er åpent tilgjengeliggjort omfattes av vernet etter EMK art. 8, tilsier likhetshensyn at det bør gjelde alt materiale som er åpent tilgjengeliggjort på nettet, også slikt som er lagt ut på en upersonlig tjeneste som news. Lagringsstedet har ikke noen betydning for utvekslingen av materiale, som er formålet med tilgjengeliggjøringen. Det sentrale er at brukeren har valgt å utnytte teknologi som sørger for å tilgjengeliggjøre innholdet for alle. Når brukeren velger å eksponere sitt innhold må det anses å ha forlatt privatsfæren. EMK art. 8 gir riktignok en viss beskyttelse også i det offentlige rom, fordi retten til privat liv blant annet omfatter retten til å inngå og utvikle sosiale relasjoner i fred. Men tilgjengeliggjøringen har til formål å dele materiale, ikke å bygge spesielle sosiale relasjoner, så man kan ikke regne med å være fri fra innsyn fra utenforstående. Det hersker dermed ikke noen berettiget forventning om privatliv for den aktuelle handling.[622]

[622] I *P.G og J.H* (2001) pkt. 56 sier EMD at "There is … a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life", og i pkt. 57: "a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. Smlg. *Gillan og Quinton* (2010) pkt. 61, som viser til *P.G og J. H* (2001) pkt. 56-57 og til *Peck* (2003) pkt. 57-63 (kameraopptak i byrommet). *Gillan* gjaldt kvaliteten på britisk antiterrorlovgivning som ga adgang til å foreta ransaking av person på offentlig sted. Ransaking ble i praksis foretatt på grunnlag av "the "hunch" or "professional intuition" of the officer

Når innholdet eksponeres ligger det til fritt gjennomsyn. I forhold til praksis knyttet til EMK art. 8, synes det å være vesentlig at filtreringen *ikke involverer lagring* av informasjon om resultatet av filtreringen. Beskyttelse av privatlivet i det offentlige rom, omfatter nemlig at opplysninger om ens handlinger, som selv om de i seg selv ikke er hemmelige, blir lagret av myndighetene.[623] Materiale som er åpent tilgjengeliggjort må derfor kunne sjekksumfiltreres. De åpne områdene synes derfor ikke å falle inn under privat liv etter EMK art. 8. De kan heller ikke anses å være omfattet av korrespondansealternativet, nettopp fordi det ikke gjelder å bygge opp sosiale relasjoner, bare å dele innhold, og det i full åpenhet.

EMK art. 8 synes derfor ikke å representere noen skranke for filtrering av åpne nettsteder. Jeg tenker da på områder som er egnet til å nå et større antall personer, smlg. definisjonen av offentlig "budskap" i strl. 2005 § 10. Disse må anses å være både patruljer- og filtrerbare for politiet ved hjelp av tilbyder.[624] Konklusjonen blir dermed at filtrering på åpne nettsteder ikke utgjør noe inngrep i retten til privatliv og korrespondanse etter EMK art. 8.

I en mellomkategori har man data som overføres over brukerens tilgangspunkt til nettet, og data som er lagret hos nettvert uten å være tilgjengeliggjort for allmennheten. I det første tilfellet griper filtreringen inn i data under overføring. I det andre gjelder det filtrering av private tilgangskontrollerte brukerområder i nettet. Begge steder er filtrerbare for tilbyder som yter tjenesten, men de er ikke åpent tilgjengelige for omverdenen.

Elektronisk kommunikasjon er vernet etter strl. 2005 § 205 bokstav a-d, hvorav alternativene i bokstav a og b synes å være aktuelle. Strl. 2005 § 205 bokstav a rammer den som

> "uberettiget og ved bruk av teknisk hjelpemiddel hemmelig avlytter eller gjør hemmelig opptak av telefonsamtale eller annen kommunikasjon mellom andre…".

---

concerned" (pkt. 83) og loven var ikke tilstrekkelig klar og presis til å forebygge misbruk (pkt. 89). EMD konstaterte krenkelse av EMK art. 8.

[623] Den grunnleggende avgjørelsen om at lagring av personopplysninger hos myndighetene er et inngrep i EMK art. 8, er *Leander* (1987) som gjaldt lagring av slike opplysninger i den svenske sikkerhetstjenestens register. Den svenske lovgivningen oppfylte imidlertid vilkårene etter EMK art. 8.2, så det forelå ikke krenkelse. Lagring representerer et inngrep selv om opplysningene verken er hemmelige eller sensitive. Se *Rotaru* (2000) pkt. 43-44 og *Amann* (2000) pkt. 65 og 69. *Peck* (2003) gjaldt bruk av kameraopptak i byrommet. I pkt. 59 skiller EMD mellom filming som ikke lagres (ikke inngrep) og slike som lagres. *Peck* hadde imidlertid ikke klaget på filmingen og lagringen, bare på bruken, så lagringsspørsmålet ble ikke satt på spissen.

[624] Se om strl. 2005 § 10 i kapittel 4.2 og 11.2.1.

Forbudet effektiviserer den dimensjon av EMK art. 8 som gjelder retten til å kommunisere i fred for andre. Filtreringen gir imidlertid ikke noe *innsyn* i dataene i kommunikasjonsstrømmen, og kan ikke anses som avlytting. Filtreringen innebærer heller ikke kopiering. Dette forbudet er derfor neppe en skranke for filtrering.[625]

Strl. 2005 § 205 bokstav b rammer den som

> "uberettiget bryter en beskyttelse eller på annen uberettiget måte skaffer seg tilgang til informasjon som overføres ved elektroniske … hjelpemidler".

Bestemmelsen viderefører overføringsalternativet i strl. 1902 § 145 annet ledd.[626] Lagringsalternativet er videreført i strl. 2005 § 204 som er sitert tidligere. Mens datainnbruddsbestemmelsen gir vern mot uberettiget tilgang til "datasystem", gir strl. 2005 § 205 bokstav b vern mot uberettiget "tilgang til informasjon". Det er altså ikke full parallellitet mellom de vernede objekter. Datainnbruddsbestemmelsen gir utvilsomt vern mot datainnbrudd utenfra mot et tilgangskontrollert brukerområde i nettet. Derimot kan den ikke antas å gi vern mot tilbyders tilgang til brukerområdet. Tilbyder har rett til å drifte sin tjeneste og normalt er ikke noen del av systemet stengt for vedkommende[627] Sjekksumbasert filtrering gir ikke tilbyderen tilgang til innholdet som sådan, det legger bare grunnlaget for blokkering av materiale som er besluttet inndratt. Det må derfor antas at tilbyder kan filtrere uhindret av denne bestemmelsen.

Hvorvidt tilbyderen også kan filtrere innhold som overføres over brukerens tilgangspunkt til nettet, kommer an på om det innebærer at vedkommende uberettiget skaffer seg tilgang til "informasjon". "Informasjon" tar nok sikte på meningsinnholdet, ikke dataidentitetene.[628] Tilbyder filtrerer et punkt på sin egen tjeneste og foretar ikke noe innsyn. Følgelig slår ikke de grunner som ligger bak forbudet til, og vedkommende kan vanskelig sies å uberettiget ha skaffet seg tilgang til informasjon.

---

[625] Konklusjonen gjelder bare sjekksumbasert filtrering, fordi det som jeg kommer til i kapittel 14.3, er en "lukket" filtreringsmetode. Det betyr at den ikke gir noe informasjon utover den man hadde fra før. Jeg vil tro at filtreringsmetoder som er "åpne", kan støte an mot avlyttingsforbudet.
[626] Ot.prp. nr. 22 (2008-2009) kapittel 16.2.
[627] Datakrimutvalget skriver at: "Straffebudet om ulovlig tilgang er altså ikke ment å gjøre noen innskrenkning i systemadministrators adgang til å utøve sine oppgaver." NOU 2007: 2 kapittel 5.6.2 s. 80. Ot.prp. nr. 22 (2008-2009) kapittel 16.2 fremhever bare at tilgangen må være uberettiget.
[628] Ot.prp. nr. 22 (2008-2009) kapittel 16.2 s. 404: "Med informasjon menes all informasjon uavhengig av om den er umiddelbart tilgjengelig eller om den først er lesbar (gir mening) ved bruk av teknisk utstyr."

Hvis man går direkte på EMK art. 8, så er spørsmålet om filtreringen gir tilbyder informasjon om kommunikasjonen. Jeg har forutsatt at filtreringen utføres på en måte som sikrer anonymitet ved bruk av personvernøkende teknologi som bryter koblingen mellom filtreringen og IP-adressene. EMK art. 8 kan neppe antas å utgjøre noe hinder på dette stadium. Spørsmålet som må drøftes er om *blokkeringen* av de "svartelistede" datafilene er en kommunikasjonshindring som støter an mot de nevnte reglene, se nedenfor i kapittel 14.

13.2.3 Oppsummering av filtrering i trinn 1 og EMK art. 8

Som en oppsummering av drøftelsene i dette kapitlet, har jeg konkludert med at brukerens private datamaskin ikke er å anse som filtrerbart område. Filtrering her er i strid med forbudet mot datainnbrudd og inndragningsreglene gir ikke grunnlag for å trenge inn på maskinen. Unntak gjelder innhold på datamaskinen som brukeren åpent tilgjengeliggjør. Det må vurderes på samme vis som materiale på åpne upersonlige tjenester, og faller utenfor området for EMK art. 8. Inndragningsreglene gir således hjemmel for å filtrere disse områdene.

Brukerens tilgangspunkt til nettet og private brukerområder faller innenfor området for EMK art. 8. Men filtreringen representerer ikke noe inngrep i retten til "uforstyrret" kommunikasjon. Verken strl. 2005 §§ 204 eller 205 setter skranker for slik filtrering. Hjemmelsgrunnlaget i inndragningsreglene og -beslutningen, gir dermed adgang til sjekksumbasert filtrering under anonyme forhold.

14 Blokkering av datafilen: Presisjonsproblemet

14.1 Innledning

I det følgende drøfter jeg filtreringens trinn 2, som er blokkeringen av de "svartelistede" filene. Blokkering representerer en kommunikasjonshindring. For kommunikasjon som faller inn under vernet etter EMK art. 8, er blokkering klart et inngrep som må rettferdiggjøres etter vilkårene i art. 8.2. Etter de foregående drøftelsene gjelder dette kommunikasjonsstrømmen over brukerens tilgangspunkt til nettet og de private brukerområdene i nettet. På de åpne områdene er man utenfor vernet etter EMK art. 8. Blokkering av overgrepsbilder og skadelig

kildekode er imidlertid ytringer, noe som krever en rettferdiggjøring av inngrepet, jf. EMK art. 10.

Det er altså behov for å foreta vurderinger av om filtreringen er "nødvendig i et demokratisk samfunn" både etter EMK art. 8 og 10. Denne vurderingen behandler jeg i kapittel 16. For vurderingene er det viktig at filtreringen treffer presist. Det generelle utgangspunktet må jo være at jo mer presist metoden treffer, jo mindre betenkelig er det å ta den i bruk. Presisjon er et problem for mange filtreringsmetoder, og problemet er sammensatt. Selv om jeg har hevdet at automatisert filtrering treffer presist, er det elementer i dette som bør avklares for å få frem momenter til inngrepsvurderingen.

14.2 Over- og underdekning

Presisjonsproblemet gjelder hvorvidt filtreringen rammer mer eller mindre enn det som er formålet. Dersom det rammer mer enn formålet tilsier, foreligger *overdekning.* Filtrering som retter seg mot *nettadresser* eller baserer seg på *søkebegreper* medfører overdekning, mens filtrering som baserer seg på gjenkjenning av "svartelistede" filer, treffer helt presist fordi det retter seg *direkte mot de rettsstridige objektene.*

Dersom filtreringen rammer mindre enn det som er formålet, foreligger *underdekning.* Dette problemet er sammensatt. En årsak kan være at den tekniske løsningen ikke er gjort tilstrekkelig robust, slik at filteret ikke fanger opp alt som skal filtreres. For sjekksumbasert filtrering betyr det at "svartelistede" dubletter slipper gjennom filteret. Jeg ser ikke dette først og fremst som et rettslig problem. Dersom man bestemmer seg for å iverksette automatisert inndragning bør også tilstrekkelig robust teknologi tas i bruk, slik at det ikke kan reises spørsmål ved om metoden er egnet til å oppnå det mål som er satt. Målsettingen er å blokkere de "svartelistede" dublettene. Tilstrekkelig robusthet må derfor være et oppdrag til teknologene for å realisere automatisert inndragning, og jeg behandler ikke dette nærmere.

Det er også tenkelig at det kan skje *omgåelse* som svekker filtreringens effektivitet. Man kan tenke seg at kriminelle miljøer tar i bruk dataprogram som endrer sjekksummen til alle sine rettsstridige dubletter, slik at de blir ukjente (nye) filer som filteret ikke kan blokkere. Dette forebygges i første omgang av at dataidentiteten ikke er offentlig, den tas jo ikke med i

inndragningsbeslutningen.[629] Dersom sjekksummene i RDB skulle komme på avveie, må det ha skjedd en omfattende lekkasje fra politiets database. Uansett kan man ikke regne med at denne type omgåelse vil frata filtreringen mye av effekten. De kriminelle kontrollerer ikke filene på nettet, så filteret vil virke for alle dubletter som allerede var tilgjengeliggjort. Filene kan jo ikke tas tilbake av de som har sluppet dem ut. Filteret vil også virke overfor alle som har dubletter og tilgjengeliggjør dem uten å være klar over at filene tilbys i "ny" versjon.

Den omgåelsesmuligheten som tross alt finnes, viser bare at automatisert inndragning alene ikke er tilstrekkelig for å få bukt med et omfattende problem. Tiltaket er likevel velegnet for den delen av problemet som det får gjort noe med. At tiltaket skal fungere som en *fullstendig løsning,* dvs. ramme alle de filer som er vurdert som rettsstridige, kan ikke være et mål.[630] Kriminelle mottrekk er en del av det alminnelige "arms race" mellom rettshåndhevende myndigheter og kriminelle miljøer, som gjør seg gjeldende ved nær sagt all metodebruk.[631]

Ytterligere et underdekningsproblem er *tidsetterslepet* ved at filtreringen nødvendigvis henger etter sett i forhold til tilstrømningen av nytt rettsstridig materiale i nettet. Sjekksumbasert filtrering er en *reaktiv metode;* den retter seg mot dubletter med en kjent identitet, dvs. gjentakelsene i nettet. Metoden kan ikke forhindre førstegangsspredning fordi datafilen da er ukjent. Men den kan forhindre den vedvarende sirkuleringen av rettsstridig materiale. Tidsetterslepet er ikke et presisjonsproblem i forhold til de "svartelistede" filene, men i forhold til den totale mengden rettsstridig materiale på nettet, hvorav bare en del er identifisert og inndratt. Mer enn å reise et presisjonsproblem reiser det et *effektivitetsproblem* som kan gi grunn til å diskutere hvor velegnet automatisert inndragning er for formålet. En slik drøftelse bør ikke føres på generelt grunnlag, men i forhold til de forskjellige innholdstypene, dvs.

[629] Se kapittel 5.5.
[630] Av denne grunn er problemet med å opprette en *fullstendig* referanseliste ("comprehensive list") som påpekt av *Open Net Initiative,* noe forfeilet (se sitat i kapittel 14.3). Selv om det ikke er et realistisk mål, kan tiltaket være velegnet.
[631] *Goldsmith* (2006) redegjør for at rettshåndhevende tiltak på nettet faktisk virker, noe han dokumenterer med en rekke eksempler i boken. Han kommer ikke spesielt inn på sjekksumbasert filtrering, men omtaler andre filtreringsmetoder. Bokens gjennomgående poeng er oppsummert på s. 81, som følger: "Our discussion of the techniques of government control over the Internet is not meant to suggest that the techniques always work perfectly. They do not. Nor do we mean to suggest that government control over Internet activities will always be as successful as when these activities take place outside the Internet. They will not, as consumers of pornography, web gambling, and free digital music know. […] But as we have emphasized throughout this book, law has never been perfect. It succeeds by lowering the incidence of prohibited activities to an acceptable degree." *Goldsmith* konkluderer slik: "The interesting and difficult questions are how such new techniques of control will fare against new techniques of avoidance – and what the ultimate result of such arms races will be."

skadelig dataprogram og overgrepsbilder, hvor tilgangen på alternative tiltak også tas i betraktning.[632]

14.3 Ulike filtreringsmetoder

Filtrering som metode inneholder generelt sett to elementer, først et deteksjons- og så et aksjonselement.[633] Først skjer *deteksjon* i henhold til et bestemt kriterium, for eksempel sjekksum, nettadresse eller nøkkelord (trinn 1). Det resulterer i en "informasjonsfangst" som for automatisert inndragning er de "svartelistede" dublettene som treffer filteret. Deretter skjer *aksjon*, hvor man gjør noe med fangsten. For automatisert inndragning går det ut på å blokkere de nevnte dublettene (trinn 2). Dette skjer samtidig med fangsten, så derfor smelter de to stadiene praktisk sett sammen til ett og kan gjennomføres automatisk. For andre metoder kan fangsten ha andre formål. Aksjonen kan gå ut på blokkering av informasjon, men kan også gå ut på å utnytte informasjonen aktivt, for eksempel til etterretningsformål.

Automatisert inndragning ved sjekksumbasert filtrering av dubletter, retter seg mot datafiler hvor alle relevante karakteristika er kjent. Gjennom den rettslige behandlingen som har konstatert rettsstrid og besluttet inndragning, er fasen for rettslige vurderinger avsluttet. Fra det tidspunkt en fil er lagt i RDB, skjer fullbyrdingen i nettet automatisk. Formålet er oppnådd når blokkering har skjedd og det er intet mer å vurdere. Derfor anser jeg sjekksumbasert inndragning som en "lukket" metode.

Det jeg på den andre siden kaller en "åpen" filtreringsmetode, resulterer i en "informasjonsfangst" som må vurderes for å unngå feiltreff og overdekning. Feiltreff betyr at materialet er helt irrelevant, mens overdekningen går ut på at man fanger mer enn det som er relevant. En "åpen" filtreringsmetode kan ikke brukes på helautomatisk vis uten å medføre omfattende krenkelser av ytringsfriheten og retten til privat uhindret kommunikasjon. Kontroll med informasjonsfangsten gir *innsyn* i innholdet og representerer dermed inngrep i privatlivet, jf. EMK art. 8. Det gjelder selv om den endelige beslutningen går ut på at informasjonsfangsten ikke var relevant og skal slettes. Filtrering på grunnlag av nettadresser, nøkkelord eller søkebegreper som "svartelistes" kan anses som "åpne".

[632] Se kapittel 16.
[633] Smlg. trinn 1 og 2 ved automatisert inndragning, som forklart i kapittel 12.2.

De åpne metodene skiller seg vesentlig fra sjekksumbasert filtrering fordi de ikke retter seg presist mot det objektet som de er ment å fange opp. I tillegg er omgåelsesmulighetene store. Problemene skyldes ikke primært mangler ved oppdraget eller den tekniske presisjonen, men at filtreringen skjer på et for høyt generalitetsnivå til å unngå feiltreff.

Filtrering av *nettadresser,* enten det er IP-adresse eller domenenavn (for eksempel www.skurk.no), rammer alt innhold som tilbys fra nettadressen. Dersom man stenger IP-adressen til en server for å ramme den ulovlige gamblingtjenesten til en av brukerne, blokkeres ikke bare denne, men tilgangen til de andre tjenestene på serveren uten at det er noen grunn til å blokkere dem. Det kan sammenlignes med å blokkere hoveddøren til en boligblokk. Selv om formålet bare er å hindre én person å slippe ut eller inn, rammes alle beboerne.[634]

Filtrering av nettsteder innebærer også risiko for at det rettsstridige materiale ikke rammes i det hele tatt. Underdekningen kan skyldes at innholdet flyttes mellom nettsteder, at nettadresser bytter IP-adresser, og at vertsmaskiner skifter IP-adresse. Ifølge forskningsprosjektet *Open Net Initiative* er mobiliteten mellom nettadresser et stort problem for de nevnte filtreringsmetodene, og det opplyses at:

> ”not only does the huge number of Web sites make building a comprehensive list of prohibited content difficult, but as content moves and Web sites change their IP-addresses, keeping this list up-to-date requires a lot of effort. Moreover, if the operator of the site wishes to interfere with the blocking the site could be moved more rapidly than it would be otherwise”.[635]

Filtrering som opprettholdes under slike forhold treffer ikke nødvendigvis det materialet som er formålet, men kan ramme annet materiale som mer tilfeldig er havnet på en ”svartelistet”

[634] Se *Murdoch* (2008) s. 59: ”Blocking based solely on IP addresses will make all services on each blacklisted host inaccessible”. Smlg. *Sieber* (2008) s. 181.
[635] *Murdoch* (2008) s. 59. *Open Net Initiative* er et samarbeidsprosjekt mellom Universitetene i Toronto (Canada), Cambridge og Oxford (UK), og Harvard (USA). Prosjektets formål er beskrevet slik: “to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion.” Se http://opennet.net. Boken *Access Denied* (*Deibert* (2008)) er utgitt som ledd i prosjektsamarbeidet. Som nevnt i forrige kapittel anser jeg problemstillingen med å lage en ”comprehensive” referanseliste for å være noe forfeilet. Hva som er et tilstrekkelig omfang av referansedata, må vurderes i forhold til den enkelte metode i lys av formålet, for å kunne ta stilling til om den er egnet.

IP-adresse.[636] *Open Net Initiative* konkluderer derfor med at å bygge opp en referanseliste med treffsikre kriterier er

> "a considerable challenge and a common weakness in deployed systems".[637]

Filtrering på grunnlag av *nøkkelord og søkebegreper* kan rette seg mot egenskaper i elektronisk kommunikasjon under overføring, informasjon lagt ut på nettsteder og ord i nettadresser. Problemet med fremgangsmåten er velkjent, så ett eksempel antas å være tilstrekkelig: Et navn som Osama, kan angå en terrorist, men kan også være navnet til en norsk statsborgers fredelige slektning i Tyrkia. Kort sagt, man vet ikke om filtreringen gir relevante treff. Funnene må analyseres manuelt for å skille bort det som er irrelevant og kunne vurdere informasjonsfangstens kvalitet. Søkebegreper bør altså ikke brukes som grunnlag for helautomatisert filtrering.[638]

Siden de åpne filtreringsmetodene med nødvendighet rammer mer eller annet enn det man hadde til hensikt, kan spørre hvorfor man ikke anvender sjekksumfiltrering i stedet, som treffer så presist. Den avgjørende grunnen er at *innholdet som søkes filtrert ikke er kjent på forhånd*, i den presise tekniske forstand som sjekkumfiltreringen betinger. En ulovlig gamblingtjeneste har ikke en fast form som kan låses til en sjekksum.[639] Og dersom man ønsker å stenge nettsteder som formidler diskriminerende og hatefulle ytringer, er problemet at det *eksakte* innholdet ikke er kjent på forhånd. Rettshåndhevende myndigheter kan kjenne til det generelle politiske budskapet, men budskapet kommer ikke til uttrykk på samme vis hver gang. Og selv om en fil med en rettsstridig ytring sjekksumdefineres, er nytten liten fordi det er lite sannsynlig at man finner dubletter mange steder i nettet over tid. For avsender er det

[636] Telenor baserte seg på samme type beskrivelse av internett som *ONI* i sitatet over, i en sak som gjaldt hvorvidt Telenor ved midlertidig forføyning kunne pålegges å stenge tilgangen til tjenesten Pirate Bay. Lagmannsretten frifant Telenor siden det påberopte hovedkravet – at Telenor medvirket til ulovlig tilgjengeliggjøring av opphavsrettslig vernet materiale – ikke ble funnet å ha noe lovgrunnlag. Uten et hovedkrav som skal sikres, kan man heller ikke bruke midlertidig forføyning, Borgarting lagmannsretts kjennelse av 9. februar 2010 (saknr. 10-006542ASK-BORG/04). I kjennelsen s. 27, anfører Telenor at "Internett er svært dynamisk og desentralisert. Nettsider og nettsteder endres, etableres, nedlegges og lenkes kontinuerlig. Internettleverandører har ingen muligheter for å holde seg oppdatert på enhver slik endring, noe en blokkeringsplikt forutsetter".

[637] *Murdoch* (2008) s. 59.

[638] Fra databasert etterforsking (analyse av databeslag) er problemet velkjent. *Aquilina* (2008) s. 225 flg., utelukker ikke at "searching a hard drive for keywords can prove an effective way to locate traces of malware, provided the search is conducted intelligently …", men "generally [it] will result in a high number of false positives because the occurrence often are legitimate references to known malware in signature files."

[639] Muligheter finnes det likevel bestandig. For eksempel kan tjenestens logo hash kalkuleres, og så brukes som filtreringsgrunnlag.

enkelt å formulere seg annerledes samtidig som meningen beholdes, og da kan ikke budskapet gjenkjennes ved sjekksumkontroll. Dette er en stor begrensning for bruk av sjekksumkontroll, men til gjengjeld er presisjonen dens store styrke. Metoden for oppbygning av RDB gir dessuten sikkerhet for et materielt riktig resultat i nettet.

14.4 Tilfeller fra praksis

Filtrering på grunnlag av *datafilenes identitet* brukes for å filtrere *skadelig dataprogram*. Dette er velprøvd teknologi og har som nevnt inspirert avhandlingens tilnærming til automatisert inndragning.[640]

Samme metode er brukt av belgiske rettighetshavere til *digitalisert musikk*, for å blokkere for piratutveksling ved fildeling. Det fremgår av en belgisk avgjørelse fra 2007 (”SABAM”) som gjaldt hvorvidt en internettilbyder (ISP) kunne pålegges plikt til å medvirke til filtreringen.[641] ISPen anførte at en slik plikt var i strid med forbudet mot å pålegge tilbyder en generell overvåkingsplikt, jf. ehandelsdirektivet artikkel 15 (smlg. ehl. § 19).[642] Retten påpekte at

> ”the blocking measure has a purely technical and automatic character, as the intermediary has no active role in the filtering”[643]

Siden ISPen ikke hadde noen aktiv rolle og kun utførte tiltak av ”rent teknisk og automatisk karakter”, kom retten til at plikten ikke var i strid med overvåkingsforbudet. Ifølge rettsavgjørelsen hadde rettighetshaverne databasen med sjekksumdefinerte filer av musikkverk som de hadde rettighetene til, mens tilbyder skulle sette filtrene i nettet og oppdatere med sjekksummer overført fra rettighetshaver. Dette er samme opplegg som jeg har forutsatt for automatisert inndragning.

Jeg kjenner ikke til at sjekksumbasert filtrering har inngått i saksforholdet i saker vedrørende EMK. Men to avgjørelser mot Tyskland og Storbritannia nevner bruk av *søkebegreper* (”Suchbegriffe”, ”catch words”, ”keywords”) ved filtrering av internasjonal kommunikasjon,

[640] Se kapittel 1.1.
[641] Jeg kaller avgjørelsen ”SABAM”, som er navnet til rettighetshaver som ønsket filtrering. Avgjørelsen er avsagt av ”District Court of Brussels” den v 28. juni 2007 (sak 04/8975/A ”of the general roll”) (jeg har bare avgjørelsen i engelsk oversettelse).
[642] Ehandelsdirektivet er direktiv 2000/31/EF.
[643] Jf. utskrift av rettsavgjørelsen s. 9

for å ivareta nasjonal sikkerhet, nemlig *Weber og Saravia* (2006) og *Liberty* (2008).[644] Det var tale om filtrering som ledd i strategisk overvåking, for anskaffelse av informasjon til bruk i etterretning. Selve filtreringen skjedde fra kontrollpunkter på eget territorium mot elektronisk kommunikasjon som krysset landegrensen. Metoden representerer et inngrep i retten til privat liv og korrespondanse, jf. EMK art. 8.1, et inngrep som anses å gjelde alle borgerne.[645]

I *Weber og Saravia* (2006) fant man at metoden kunne godtas. Man holdt seg til avgjørelsen *Klass* (1978), som på strenge vilkår godtar metodebruken, til tross for at den anses som en trussel ("menace") mot demokratiet. Staten har en vid skjønnsmargin ved valg av metode når formålet er å ivareta nasjonal sikkerhet. Vilkår er at det foreligger klar hjemmel og god uavhengig kontroll både i for- og etterkant av metodebruken.

I *Liberty* (2008) ble metoden underkjent. Hjemmelen var ikke tilstrekkelig klar i sin avgrensning av hva det kunne søkes etter og hvordan informasjonen skulle behandles. Dermed risikerte man formålsforskyvning, manglende forutsigbarhet og sviktende demokratisk kontroll med metoden.

De krav som stilles av praksis knyttet til EMK art. 8, reiser et dilemma for myndighetene. Hensyn til transparens og demokratisk kontroll med metodebruken medfører behov for kontroll med søkebegrepene for å motvirke formålsforskyvning og misbruk. Men referanselisten kan ikke gjøres kjent for da kan filtreringen omgås. Avgjørelsene hindrer heller ikke hemmelighold av den konkrete referanselisten, nettopp fordi statens legitime

[644] I *Weber og Saravia* (2006) pkt. 32 gjaldt spørsmålet kvaliteten på tysk overvåkingslovgivning. Det fremgår myndighetne singlet ut kommunikasjon med potensiell sikkerhetsmessig interesse på grunnlag av søkebegreper. I saken mot Storbritannia, *Liberty* (2008) nevnes bruk av "searchterm" og "keyword" i pkt. 43 og 66. *Klass* (1978) er en lignende sak (tysk lovgivning), men her ikke søkebegreper nevnt, derimot at myndighetene kan avlytte kommunikasjonens innhold (pkt. 17).

[645] At inngrepet presumeres å ramme generelt vises i at klageretten tilkommer enhver. Begrunnelsen liggerr i inngrepets hemmelige karakter.Man ville i praksis bli avskåret fra å prøve om sikkerhetslovgivningen og praktiseringen av den, respekterte EMK art. 8, dersom det ble krevet at man først beviste at man faktisk hadde vært utsatt for overvåking. Se *Klass* (1978) pkt. 34-37. "The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (art. 8) could to a large extent be reduced to a nullity" (pkt. 36) og "The disputed legislation directly affects all users or potential users of the postal and telecommunication services … this menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 (art.8)" (pkt. 37); smlg. *Weber og Saravia* (2006) pkt. 78; *Liberty* (2008) pkt. 56; *AEIHRE* (2007) pkt. 69. AEIHRE gjaldt overvåking både mistankebasert og generelt til strategisk beskyttelse av rikets sikkerhet.Til tross for mistankekravet later det til at avlytting ble foretatt i så stor utstrekning at det ikke ble praktisert kontroll med at de formelle vilkårene var oppfylt.

interesse i å ivareta den nasjonale sikkerhet veier tungt. Men det må legges opp til uavhengig kontroll i henhold til presise kriterier nedfelt i lov.

Den såkalte "FRA"-loven som ble innført i Sverige i 2008, hjemler et lignende filtreringssystem som ble brukt av Tyskland og Storbritannia i henhold til de nevnte sakene. Loven gir adgang til filtrering (kalt "signalspaning") av elektronisk kommunikasjon som krysser Sveriges grense.[646] Også det internasjonale overvåkingssystemet Echelon er opplyst å basere seg på nøkkelord. Det fremgår av en rapport som ble utarbeidet for Europaparlamentet i 2001.[647] Systemet har tiltrukket seg en del oppmerksomhet og kritikk, men det foreligger få konkrete opplysninger om systemet.[648]

Sjekksummer som referansedata er ikke direkte sammenlignbare med søkebegreper brukt ved signalspaning. Sjekksummene retter seg ikke mot egenskaper ved innholdet; det kan fremstilles nye sjekksummer for de samme filene, for eksempel dersom politiet tar i bruk en ny algoritme.[649] Det er innholdet i filene, i form av bildene og de skadelige dataprogrammene som korresponderer med søkebegrepene. Siden innholdet er rettsstridig kan det selvsagt ikke tilgjengeliggjøres for allmennheten for å sikre åpenhet om filtreringsmetoden. Men straffebudene gir anvisning på hva som er rettsstridig innhold, jf. strl. 2005 §§ 210 og 311, så dermed er informasjonshensynet overfor borgerne ivaretatt.

Overført til automatisert inndragning innebærer det at dataidentitetene kan holdes hemmelige, og at man dermed ikke over tid bindes til å bruke en spesifikk teknologi for å gjennomføre filtreringen.

[646] Se *Klamberg* (2009) for en analyse av "FRA"-loven i forhold til EMK art. 8. "FRA-loven" er egentlig lov om signalspaning i elektronisk nettverk, som er en endringslov til flere svenske lover. Det finnes altså ikke formelt sett en "FRA-lov". Analysen skjer overfor all trafikk, men bare de kommunikasjoner som inneholder nøkkelordet representerer en "match", og kan gi grunnlag for mer målrettede tiltak. Analysen skjer imidlertid overfor en kopi av all kommunikasjon, som mellomlagres på såkalte "samverkanspunkter"; kommunikasjonen som sådan slipper uhindret igjennom.
[647] *Rapport om ECHELON* (2001) s. 34 pkt. 3.3.2 sier at "… no single telephone connection is monitored on a targeted basis. Instead, some or all of the communications transmitted via the satellite or cable in question are tapped and filtered by computers employing keywords …".
[648] Personvernkommisjonen nevner FRA-loven, Echelon og datalagringsdirektivet (direktiv 2006/24/EF) under ett, se NOU 2009: 1 kapittel 4.4.1 s. 42. Det vesentlige fellstrekket er at metodene har en generell, ikke mistankebasert, tilnærming. Enhver bruk av opplysningene krever etterkontroll med informasjonsfangstens kvalitet. Utkast til lov som gjennomfører datalagringsdirektivet i Norge, er skrivende stund sendt på høring, jf. høringsbrev datert 8. januar 2010.
[649] Se kapittel 5.5, jf. kapittel 3.3.3.

Til slutt kan Kripos-filteret nevnes. Filteret stenger domener (nettsteder) som tilbyr overgrepsbilder. Avdekking av nettsteder skjer på grunnlag av tips og følges opp med kontroll fra Kripos som påser at "svartelistingen" er korrekt. Blokkeringen utføres av tilbyder på grunnlag av en liste med domener som utarbeides av politiet. Metoden er basert på en samarbeidsavtale mellom politiet og internettbransjen, og er altså ikke hjemlet i en spesiell bestemmelse. Metoden har fått internasjonal oppslutning via Interpol og EU/Europol i det såkalte "Circamp-prosjektet".[650]

14.5 Oppsummering

Som en oppsummering på dette kapitlet kan det konstateres at sjekksumbasert filtrering resulterer i at filtreringen skjer med et materielt korrekt og helt presist resultat i forhold til inndragningsbeslutningen. Metoden gir ikke overskuddsinformasjon og hindrer ikke annen trafikk. I kraft av sin presisjon er metoden mindre inngripende enn søkemetoder som har vært godtatt i forhold til EMK art. 8 for å ivareta nasjonal sikkerhet. Gjennom straffebestemmelsene gis dessuten borgerne presis informasjon om hva slags innhold man kan regne med at blir inndratt i nettet, noe som ikke er tilfelle for de andre filtreringsmetodene som er godtatt i forhold til EMK.

Automatisert inndragning er imidlertid en reaksjon med et visst *tidsetterslep*, noe jeg antar at kan ha betydning for de rettslige vurderingene, med tanke på hvor egnet metoden er for å ha en effekt på problemene med overgrepsbilder og skadelig dataprogram (se kapittel 16).

Dessuten er filtreringens trinn 1 en generell metode, selv om blokkeringen skjer presist. Jeg synes det gir grunnlag for en diskusjon i forhold til doktrinen om "chilling effect", og tar opp spørsmålet i neste kapittel.

[650] *Interpol* (2009). "Circamp" står for "Cospol Internet Related Child Abuse Material Project", se www.circamp.eu. Norge er prosjektleder for en mer samlet internasjonal innsats for utvikling av varslings- og filtreringsmetoder mot overgrepsbilder på nettet.

15 En ”chilling effect” av filtrering?

15.1 Innledning

I forhold til EMK art. 10 er det en problemstilling om automatisert inndragning kan virke kjølende på ytringsfriheten generelt, dvs. ha en ”chilling effect”. Grunnen er at filtrene sjekksumkontrollerer alle filene som de kommer i kontakt med, også de med lovlige ytringer. Selv om bare de inndratte filene blokkeres, er det spørsmål om den generelle filtreringen, kan virke dempende på frimodigheten, for eksempel fordi man frykter represalier.

Personvernkommisjonen nevner faren for en kjølende effekt som et argument mot et annet tiltak av generell karakter, nemlig pliktig lagring av trafikkdata m.v., jf. datalagringsdirektivet.[651] Datalagring er et inngrep etter EMK art. 8, og Personvernkommisjonen uttaler at

> ”Verdien av lagring må nemlig også veies opp mot effekter på frimodighet. Dette gjelder selv om formelle friheter ikke berøres … Allerede vissheten av at noen *kan* lete seg fram til dine kontakter og dine bevegelser, både i det virkelige rommet og på Internett, kan være nok til å hemme borgere i utøvelsen av sine friheter til å samles, til å ytre seg og til å søke opplysninger.” [652]

Standardverk om EMK gir knapp omtale av ”chilling effect”.[653] Men det fremgår at det er et hensyn som inngår i proporsjonalitetsvurderingen, og kan lede til at inngrepet anses som uforholdsmessig inngripende. Hensynet kan også fungere som et pålegg om å velge det minst inngripende virkemidlet (”the least restrictive alternative”) dersom flere virkemidler står til rådighet, og begrenser da statens skjønnsmargin.

Etter å ha søkt på ”chilling effect” i HUDOC-databasen, og fått opp 60 avgjørelser, har jeg imidlertid ikke kunnet finne noen sammenlignbar sak. Jeg har altså ikke funnet noen avgjørelse hvor ”chilling effect”-hensynet har kommet opp i forbindelse med innføring av en metode av generell karakter, slik det her er tale om. Ved å følge Personvernkommisjonens syn kunne man for eksempel ha tenkt seg at det ble brukt i avgjørelsene *Klass* (1978)*, Weber og*

[651] Direktiv 2006/24/EF.
[652] NOU 2009: 1, vedlegg 1, s. 222. Her brukes ”effekter på frimodighet” om ”chilling effect”.
[653] Van Dijk (2006) s. 340 opplyser at hensynet springer ut av vurderingen ”nødvendig i et demokratisk samfunn”; *Harris* (2009) s. 455, understreker at doktrinens formål er å effektivisere vernet om ytringsfriheten; *Eggen* (2002) ss. 456 flg., nevner ”chilling effect” i en drøftelse av om tilbyderne kan ilegges ansvar for brukernes ytringer på nett (se også s. 469). Det er tema som faller utenfor avhandlingen min.

Saravia (2006) *og* *Liberty* (2008), men det er ikke tilfelle.[654] Disse sakene gjaldt spørsmål om inngrep i EMK art. 8, hvor den alvorlige innvendingen er at metoden kan representere en trussel mot fortrolig kommunikasjon, som er en grunnsten i et velfungerende demokrati. I saker om EMK art. 8 synes betenkelighetene å være knyttet til at myndighetene skaffer seg hemmelig *informasjonsoverlegenhet* om borgerne. Det utgjør en spesiell trussel ("menace") i form av ukontrollerbart maktmisbruk, og innebærer at loven må være særlig klar og presis med hensyn til formål, behandling og kontroll med informasjonsfangsten.[655]

Også "chilling effect" gjelder hensynet til demokratiet, men ikke i form av informasjonsoverlegenhet hos myndighetene. Trusselen er at det gripes inn vilkårlig eller for strengt overfor en ytring, slik at reaksjonen skremmer andre fra å ytre seg. Dermed hindres meningsbrytningen i samfunnet mer generelt. "Chilling effect" gjelder bare ytringsfriheten, jf. EMK art. 10. Også Personvernkommisjonen kan ha sett at hensynet til den "kjølende effekt" ikke kommer inn ved inngrep etter EMK art. 8, fordi det sies at "formelle friheter ikke er berørt", jf. sitatet over. Kommisjonen har med andre ord fremført et politisk hensyn.

15.2 Valg av det minst inngripende virkemidlet

Spørsmålet er om det finnes mindre inngripende virkemidler enn filtrering basert på gjenkjenning av filene, for å foreta automatisert inndragning.

I utgangspunktet er det vanskelig å se at det står et bredt spekter av virkemidler til rådighet. En mulig posisjon er å gi en ubeskåret mulighet for fremsettelse av alle ytringer (og annet innhold) for deretter å spore opp lovbryteren og holde vedkommende ansvarlig ("ansvarsprinsippet"). Da får man ikke grepet inn mot det innhold som vedkommende har benyttet anledningen til å tilgjengeliggjøre, men man kan håpe på en allmennpreventiv effekt av strafforfølgningen.

[654] Se om disse avgjørelsene i kapittel 14.4. Sakene omhandler overvåkingslovgivning, og gir enhver borger rett til å anlegge sak fordi man potensielt er krenket på grunn av tiltakets generelle karakter.
[655] *Klass* (1978) pkt. 41, *Weber og Saravia* (2006) pkt. 78 og *Liberty* (2008) pkt. 59 og 60; AEIHRE (2007) pkt. 75: "In view of *the risk of abuse intrinsic to any system of secret surveillance*, such measurements must be based on a law that is particularly precise…". AEIHRE gjaldt både mistankebasert og strategisk overvåking til beskyttelse av rikets sikkerhet. Både kvaliteten på lovgivningen og praktiseringen ble underkjent av EMD som stridende mot EMK art. 8.

Dette er en sterk posisjon for å verne fremsettelsen av helt nye ytringer, dvs. slike som ikke har vært fremsatt tidligere. Det tilrettelegger for internettbrukere som informasjons*produsenter*, dvs. brukere som bidrar til at nettet fungerer som en "markedsplass for ideer".[656] Men det er ikke situasjonen i forhold til inndragningsspørsmålet hvor problemet består i *gjentakelse* av gamle ytringer som er fastslått som rettsstridige. Bruk av ansvarsprinsippet av hensyn til ytringsfriheten er derfor ikke relevant her. Dessuten har ensidig satsing på straffansvar og inndragning av beslaglagt materiale vist seg ikke å være tilstrekkelig effektivt, opphopningen av rettsstridig innhold på nettet tatt i betraktning.

Det kan derfor neppe antas å foreligge noe valg mellom virkemidler dersom inndragningen skal fullbyrdes. Filtrering må tas i bruk, og da er sjekksumbasert filtrering det mest presise verktøyet. Spørsmålet er snarere om det foreligger *misbruksmuligheter* som gjør at det hefter for store betenkeligheter ved metoden. Det er nærliggende å tenke på muligheten for at teknologien brukes til å blokkere for annet innhold enn det som er inndratt, for eksempel politiske eller religiøse ytringer. Dessuten kan det kanskje tenkes at man bruker teknologien til å spore opp personer, noe som ligger utenfor inndragningsformålet.

15.3 Blokkering av annet innhold enn det som er inndratt

Utgangspunktet er at teknologien er blind for karakteren av det innhold som skal blokkeres. Fra et teknisk synspunkt er det derfor mulig å misbruke systemet til å blokkere for lovlige ytringer uten at systemet i seg selv gir noen indikasjon på det.

Metoden kan imidlertid ikke brukes til systematisk å blokkere for ytringer fra bestemte miljøer, siden den ikke kan brukes mot førstegangs tilgjengeliggjøring av ytringer. Om man ønsker å hindre ytringer fra bestemte miljøer, må nettsteder filtreres, som jeg har redegjort for tidligere.

Selve metoden for oppbygning av RDB, med rettslig kontroll i forkant av innlegging av innhold, gjør at faren for misbruk ikke er nærliggende. Det må også stilles klare krav til hvordan RDB sikres og vedlikeholdes, slik at man har visshet for at innholdet ikke manipuleres. Med disse forutsetningene på plass er ikke en teoretisk misbruksmulighet et vektig argument mot metoden.

[656] Se kapittel 3.3.4.

15.4 Oppsporing av person

Filteret skal fullbyrde inndragningsbeslutningen. Dersom det også brukes til å oppspore lovbrytere på nettet, brukes det til et annet formål enn inndragning. Dersom også dette formålet er gyldig besluttet av lovgiver som en funksjon i tillegg til inndragningen, representerer det ikke et misbruk. *Misbruk* foreligger dersom filteret brukes til oppsporing *til tross for* at formålet er begrenset til inndragning.

Filtrene som inngår i teknologien etableres og driftes av tilbyderne. Politiets befatning med systemet gjelder oppbygning av RDB, og derigjennom overføring av sjekksummer til filtrene. For å kunne bruke filtrene til å oppspore personer måtte tilbyderne pålegges en plikt til å rapportere om kilder på nettet til politiet. Dersom det ikke foreligger en lovpålagt plikt om å gjøre dette, forutsetter misbruket et samarbeid mellom politi og tilbyder, hvor sistnevnte ofrer sin markedsmessige troverdighet og interesser i å tilby en sikker tjeneste til sine brukere, for å assistere politiet. Selv om man aldri helt kan se bort fra faren for misbruk er det i hvert fall ikke rimelig å tro at dette representerer noen stor risiko. Og som nevnt bør bruk av personvernøkende teknologi som sikrer anonymitet kunne hindre misbruk.

Det andre alternativet er at lovgiver beslutter at filteret også skal brukes til å oppspore lovbrytere. Avhandlingen har hele tiden hatt inndragningsformålet for øye. Når spørsmålet om oppsporing av lovbrytere reises, er det fordi det ikke bør overses at teknologien kan gjøre det mulig. Det er ikke dermed sagt at det er ønskelig eller uten betenkeligheter. Spørsmålet her tar utelukkende opp om lovgiver har rettslig handlingsrom til å beslutte en slik formålsendring, dersom man kommer til at det er politisk ønskelig.

Ordingen innebærer at tilbyderne må pålegges rapporteringsplikt om bruken av tjenestene sine. Plikten må antas lett å komme i konflikt med forbudet mot å pålegge tilbyderne en generell overvåkingsplikt, jf. ehl. § 19, som lyder:

> ”Bestemmelsene i §§ 16-18 medfører ikke at tjenesteyterne har en generell plikt til å kontrollere eller overvåke den informasjonen som lagres eller overføres på oppfordring fra en tjenestemottaker, eller en generell plikt til å undersøke forhold som antyder ulovlig virksomhet”.

Henvisningen til "§§ 16-19" gjelder ansvarsreguleringen som skal sikre at tilbyderne skal kunne yte elektroniske kommunikasjonstjenester til sine brukere, uten å risikere ansvar for den måte tjenestemottakerne bruker tjenestene på. Overvåkingsbestemmelsen er innført på bakgrunn av art. 15 i ehandelsdirektivet. I direktivets fortale pkt. 47 står det at

> "Det er bare med hensyn til generelle forpliktelser medlemsstatene er forhindret fra å pålegge tjenesteyterne overvåkingsplikt. Dette omfatter ikke overvåkingsplikt i særskilte tilfeller, og berører ikke avgjørelser truffet av nasjonale myndigheter i samsvar med nasjonal lovgivning".

Det er altså ikke tale om et absolutt forbud mot at tilbyderne kan pålegges å gripe inn i kommunikasjonen, men nøyaktig hvilken adgang som foreligger, er noe usikkert. De norske forarbeidene er svært knappe, og det knytter seg ikke rettspraksis til bestemmelsen fra norske domstoler, eller fortolkningsavgjørelser fra ESA- eller EU-domstolene (pr. januar 2010).[657]

Det man nok må kunne legge til grunn er at det er i strid med overvåkingsforbudet å pålegge tilbyderne å foreta en utvelgelse av opplysninger som skal sendes politiet, for eksempel bare rapportere om kilder med mange treff i filtrene. Da stilles de i posisjon som kontrollør av innhold og brukere, og det har man via ansvarsreguleringen i direktivet ønsket å unngå. Ehandelslovgivningen er altså basert på et motsatt kontrollprinsipp enn hvitvaskingslovgivningen, som nettopp pålegger finansinstitusjonen å rapportere om mistenkelige transaksjoner.[658] Derimot kan det tenkes at rutinemessig overføring av rapporter om *samtlige* treff i filtrene kan være forenlig med ehl. § 19, fordi det ikke setter tilbyderne i en selvstendig rolle som kontrollør. Siden blokkeringen gjelder et klart definert utvalg filer kan det anses å falle innenfor overvåkingsadgangen som gjelder for "særskilte tilfeller", jf. pkt. 47 i direktivets fortale.[659] Dette kan gjøres som en kontinuerlig online funksjon mellom tilbyderne og politiet, og på den måten ville politiet få en meget stor mengde data for analyse.

[657] Overvåkingsforbudet er omtalt i Ot.prp. nr. 4 2003-2004) kapittel 4.7.
[658] Forskjellen mellom overvåkingsprinsippene har jeg tatt opp i en artikkel, se *Sunde* (2008) s. 462. Overvåkingsforpliktelsen som påhviler finansinstitusjonene går ut på at de skal ta i bruk elektroniske overvåkingssystemer som skal "muliggjøre oppdagelse av og rapportering av mistenkelige transaksjoner", jf. hvitvaskingsloven § 15. Plikten til å ta i bruk elektroniske overvåkingssystemer skal effektivisere rapporteringsplikten, og reglene er resultat av forpliktelser fra et utstrakt internasjonalt samarbeid.
[659] Smlg. Ot.prp. nr. 4 2003-2004) kapittel 4.7 s. 10. Her står det om forståelsen av fortalen pkt. 47: "Dette betyr at en tjenesteyter kan pålegges å overvåke en viss avgrenset trafikk på nettet, f.eks. en bestemt chatte-gruppe, så fremt det er i samsvar med norsk lov."

De nevnte data omfattes imidlertid også av tilbydernes taushetsplikt om bruken av ekomtjenester, jf. ekomloven § 2-9, og kan av den grunn ikke overføres på generelt grunnlag til politiet. Politiet har bare adgang til denne type opplysninger på mistankegrunnlag, jf. reglene om utleveringspålegg, jf. strpl. § 210 og kommunikasjonskontroll, jf. strpl. § 216 b. Norge er folkerettslig forpliktet til å respektere taushetsreglene for elektronisk kommunikasjon, som anses som en del av vernet om borgernes korrespondanse, jf. EMK art. 8. Dermed finnes det effektive lovmessige skranker som hindrer vedtakelse av en slik formålsendring.

15.5 ”Function creep” og ”slippery slope”

Noen vil også anføre at når omfattende tekniske installasjoner først er på plass, er formålsendring uunngåelig. Det følger av teknologiens egen ”tyngdelov”. Dette er et teknologideterministisk syn som gjerne karakteriserer formålsendring som ”function creep”. Det er nært beslektet med synspunktet om at utviklingen i bruk av overvåkingsteknologi leder til at man havner ut på det teknologiske skråplanet (”slippery slope”), hvor det uvegerlig innføres stadig mer invaderende tiltak fordi det er enkelt og effektivt.[660]

Drøftelsen har imidlertid vist at formålsendring for å bruke filteret til *å oppspore personer* ikke er nærliggende. Formålsendring er imidlertid tenkelig for så vidt gjelder *den type innhold* som skal inndras, dvs. at det kan utvides til annet materiale enn overgrepsbilder og skadelig dataprogram. Dersom de integritetskrenkende fotografiene som ble inndratt i Rt. 2000 s. 40, hadde vært spredt på nettet, kunne man tenke seg at filtrering ble iverksatt for å stanse en vedvarende krenkelse mot kvinnene.[661] Det samme gjelder nakenbilder som barn ubetenksomt

[660] Uttrykket ”function creep” ble lansert av Langdon Winner i 1977. Det gjelder formålsforskyving ved bruk av teknologi generelt. I forhold til overvåkingsteknologi betyr uttrykket at “once in place a surveillance technique such as digitized identification number will tend to expand to cover other purposes”, *Lyon* (2005) s. 111. “Function creep” er også omtalt som et trekk ved “overvåkingssamfunnet”, beskrevet i A Report on the Surveillance Society (2006), Public Discussion Document s. 11 og i hovedrapporten s. 9 pkt 5.3. (http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (26.11.09)) (*Wood* (2006)). Fenomenet er omtalt i Personvernkommisjonens rapport NOU 2009: 1 s. 43. Personvernkommisjonen bruker “function creep” om *risiko for formålsforskyvning*, slik at personopplysninger som er innsamlet for ett formål, risikeres brukt for et annet formål. *Yttri Dahl* (2009) påpeker på s. 85, at utrykket ikke nødvendigvis skal forstås i negativ betydning, men medgir at det i hvert fall har ”ambivalent implications”. Andre uttrykk i samme gate er ”control creep” og ”surveillance creep”, som *Yttri Dahl* mener er mer negative enn ”function creep”. Se også *Taipale* (2007) om ”slippery slope”-argumentet. *Taipales* poeng er imidlertid at tekniske tiltak kan utformes slik at de *både* ivaretar sikkerhetsformål og personvern, og at man for dette formål i større grad bør ta i bruk personvernøkende teknologi.

[661] Saken er omtalt i kapittel 5.4.2.

har lagt ut på nettet, både av seg selv og av venner, skjønt slike bilder er "fremstilling som seksualiserer barn" og derfor omfattet av strl. 2005 § 311 objektivt sett.

Formålsendringer vedrørende innholdets karakter forandrer ikke *verktøyets* karakter, noe som synes å være det vesentlige poenget. Endringen skjer ikke på bekostning av noen kontrollmuligheter, så det hefter ikke noe betenkelig ved dette. Og som nevnt er automatisert inndragning bare egnet for innhold som stadig verserer på nettet. Det begrenser anvendeligheten for mange typer innhold.

Konklusjonen er således at det ikke later til å foreligge alvorlige misbruksmuligheter som skulle virke dempende på ytringsfriheten.

16 Avsluttende vurdering

16.1 Innledning

I dette kapitlet gjennomgår jeg argumentene som er løftet frem i det foregående, i en avsluttende vurdering av automatisert inndragning av skadelig dataprogram og overgrepsbilder. Det er konstatert at filtreringen (trinn 1) verken er inngrep i retten til privatliv og korrespondanse, eller i ytringsfriheten. Blokkeringen (trinn 2) derimot, er et slikt inngrep når det foregår på private brukerområder og over tilgangspunktet til internett, samt at det kan være et inngrep i ytringsfriheten. Det siste forutsetter selvsagt at blokkeringen gjelder en ytring.

Jeg har lagt til grunn at inndragningsbeslutningen gir hjemmel for blokkeringen.[662] Hjemmelens rekkevidde må imidlertid avgrenses i samsvar med det materielle ansvarsgrunnlaget, se nedenfor. Videre er det spørsmål om inngrepet er "nødvendig i et demokratisk samfunn", dvs. krav til proporsjonalitet og formålsegnethet.

[662] Det betyr at strl. 2005 § 205 bokstav d, som rammer den som "hindrer eller forsinker adressatens mottak av en meddelelse" ikke er et hinder. I henhold til lex superior prinsippet er det avgjørende at det foreligger hjemmel i rettslige normer på samme eller trinnhøyere nivå, i dette tilfellet i inndragningsreglene.

16.2 Skadelig dataprogram

Skadelig objektkode er et større problem enn skadelig kildekode, så jeg behandler det først. Drøftelsene i kapittel 5 viste at man ikke generelt kan gå ut fra at privat befatning med skadelig dataprogram er straffbart. Hovedregelen synes snarere å være motsatt. Det utelukker automatisert inndragning over brukerens tilgangspunkt til nettet og på de private tilgangskontrollerte områdene i nettet.

Derimot er det ubetinget straffbart å tilgjengeliggjøre programmene på de åpne tjenestene i nettet. Dersom objektkoden først er "særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem", må det i hvert fall foreligge forsett om medvirkning til (forsøk på) en straffbar handling ved tilgjengeliggjøringen av programmet. Dermed er det subjektive overskuddet oppfylt.[663] På de åpne områdene på internett faller den skadelige objektkoden utenfor vernet både etter EMK art. 8 (ikke privat liv og korrespondanse) og EMK art. 10 (ikke ytring). Her synes det således ikke å foreligge noe rettslig hinder for automatisert inndragning. Men på samme tid synes det vanskelig å begrunne hvorfor metoden burde tas i bruk mot skadelig objektkode, hensyn tatt til at inngrepet har til formål å effektivisere straffebudet.

Det er nødvendig å gå tilbake til utgangspunktet, som er at inndragningsadgangen etter strl. 2005 § 69 er fakultativ, jf. "kan inndras" i første ledd. Ved vurderingen skal det

> "særlig legges vekt på om inndragning er påkrevd av hensyn til effektiv håndheving av straffebudet", jf. tredje ledd.

I kapittel 5.7 ble det konstatert at til tross for at ordlyden indikerer noe annet, foreligger det inndragnings*plikt* for skadelig dataprogram som "er frembrakt ved" eller "har vært brukt eller bestemt til bruk" ved en straffbar handling, jf. strl. 2005 § 69 bokstav a og c. Drøftelsen gjaldt imidlertid bare skadelige dataprogram som var tatt i beslag av politiet. Spørsmålet om det bør foretas automatisert inndragning av skadelig dataprogram i nettet, er i realiteten spørsmål om det bør treffes beslutning mot ukjent lovbryter eller besitter, jf. strl. 2005 § 74 tredje ledd, slik jeg har forklart i kapittel 5.9. Også i dette tilfellet må de materielle inndragningsvilkårene

[663] I kapittel 5 har jeg lagt til grunn at det subjektive overskuddet som utgangspunkt må være oppfylt for å foreta inndragning, til tross for unntaket i strl. 2005 § 69 første ledd annet punktum.

prøves, og det er inngrepets hensiktsmessighet sett i forhold til effektiviseringsformålet som er temaet, jf. strl. 2005 § 69 tredje ledd.

To forhold leder til at det må reises spørsmål ved om automatisert inndragning er egnet til å effektivisere straffebudet. Det ene er *tidsetterslepet* som jeg har redegjort for.[664] Skadelig objektkode spres raskt i nettet og mottiltak må umiddelbart settes inn for å begrense spredning og skadevirkninger. Den sjekksumbaserte filterteknologien er reaktiv. Den tiden det tar for ekspertene å isolere, analysere og sjekksumdefinere en ny type "malware" anses i seg selv for å være en så stor hemsko, at det arbeides med å finne løsninger av mer "proaktiv" karakter. Slike løsninger tilstreber å identifisere og blokkere skadelige dataprogram på et tidligere tidspunkt enn det som er mulig på basis av gjenkjenning av dataidentiteten. Automatisert inndragning etter at inndragningsbeslutningen er rettskraftig, og etter at en sak har vært etterforsket og iretteført, skjer så sent at da har datasikkerhetsbransjen for lengst har tatt seg av problemet.

Mot skadelig dataprogram eksisterer det også et *marked* for salg av sikkerhetsløsninger, som de fleste brukere av elektroniske kommunikasjonstjenester er villige til å betale for. Dermed finnes det økonomisk grunnlag for at sikkerhetsproblemene håndteres av kommersielle aktører. Den automatiserte inndragningen som skjer lang tid i etterkant er ikke et reelt bidrag til løsning av problemet, og kan ikke antas å ha allmennpreventiv effekt som reduserer interessen for materialet. Konklusjonen er derfor at automatisert inndragning i nettet neppe effektiviserer forbudet mot tilgjengeliggjøring av skadelig dataprogram, og da har man strengt tatt ikke hjemmel for reaksjonen.

I stedet må det satses på andre tiltak. Det ligger vel til rette for en rollefordeling mellom politiet og datasikkerhetsbransjen, hvor sistnevnte tar seg av filtreringen i nettet på avtalegrunnlag med brukerne slik som i dag, mens politiet begrenser seg til å inndra de beslaglagte dataene. Det kan lett tenkes behov for å inndra dataene selv om det ikke skal foretas automatisert inndragning, for eksempel dersom dataene er lagret på brukerområder i nettet.

[664] Se kapittel 14.2.

På bakgrunn av konklusjonen for skadelig objektkode tar jeg ikke opp spørsmålet om å foreta automatisert inndragning av skadelig kildekode.

16.3 Overgrepsbilder

Overgrepsbilder er ytringer. Filtrering både på åpne og lukkede områder, og på kommunikasjonsstrømmen over tilgangspunktet til nettet, faller inn under en eller begge bestemmelsene.

Forbudet mot ytringene er imidlertid lovhjemlet og formålet legitimt. Det hersker internasjonalt konsensus om behovet, og Norge er folkerettslig forpliktet til å ha denne type forbud.[665] De skal også håndheves på en effektiv måte som oppnår en allmennpreventiv effekt, noe som begrunner bruk av inndragning i tillegg til personlig straffansvar.[666] Jeg reiser derfor ikke spørsmålet om reglene er nødvendige i et demokratisk samfunn.[667] Drøftelsen gjelder bare om *håndhevelsesmetoden* i form av automatisert inndragning, er nødvendig i et demokratisk samfunn.

Behovet for tiltak som effektiviserer straffebudene, er selvfølgelig et viktig moment for proporsjonalitetsvurderingen. Håndhevelsen må nødvendigvis tilpasses problemets karakter, og når det manifesterer seg på nettet må håndhevelsen være rettet mot nettet. Både fortalen til tilleggsprotokollen til FNs barnekonvensjon av 25. mai 2000 og fortalen til europakonvensjonen 201 ETS, understreker den betydning nettverksteknologien har som drivkraft i markedet for overgrepsbilder, og dermed for etterspørsel av barn som kan misbrukes. Europakonvensjonen sier således:

[665] De internasjonale forpliktelsene er beskrevet i Ot.prp. nr. 37 (2004-2005) s. 4, og i Ot.prp. nr 22 (2008-2009) s. 264.
[666] Både datakrimkonvensjonen (185 ETS) art. 13, jf. art. 9 og den europeiske konvensjonen om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk art. 27, krever at befatning med overgrepsbilder kan straffes med "effektive, forholdsmessige og forebyggende straffereaksjoner". Smlg tilleggsprotokollen til FNs barnekonvensjon av 25. mai 2000, som i art. 3 nr. 3 krever at staten "sørger for at slike overtredelser kan straffes med passende straffereaksjoner som tar hensyn til handlingenes alvorlige karakter".
[667] *Eggen* (2002) s. 643 skriver at "Forbudet mot å motta barnepornografiske ytringer vil utvilsomt bli ansett som nødvendig i et demokratisk samfunn." Han viser til den brede internasjonale enigheten om behovet for et slikt forbud.

> ”Observing that the sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs)…”[668]

Det er verdt å merke seg at til tross for den internasjonale oppmerksomhet som dette problemet over lang tid har blitt til del, konstaterer begge konvensjonene at problemet med overgrepsbilder *øker.* Det viser at totalforbud i seg selv ikke er tilstrekkelig; det er behov for mer effektiv håndhevelse.

I og med at filtrering ikke er uten betenkeligheter, er første spørsmål om man har tilgang på andre tiltak som er mindre inngripende enn automatisert inndragning, (jf. doktrinen om at man skal velge ”the less restrictive alternative”). Det er en del av vurderingen av om inngrepet er *nødvendig* i et demokratisk samfunn.

For overgrepsbilder ligger situasjonen vesentlig annerledes an enn for skadelig dataprogram, for så vidt gjelder markedsmekanismen og betydningen av tidsetterslepet.

For det første finnes det *ikke noen markedsmekanisme* som gir grunnlag for å lage og selge filterløsninger til privat bruk. Datasikkerhetsbransjen har et marked for sine ”malware”-filtere fordi de fleste brukere ønsker sikre tjenester på nettet, og sikkerhet for at personlige data ikke kommer på avveie. Men når det gjelder overgrepsbilder er det slik at de som vil ha bildene vil ikke ha filter, og de andre trenger ikke filter.[669] Derfor er det behov for tiltak fra myndighetenes side.

Tidsetterslepet er ikke et motargument mot myndighetenes filtrering på nettet, slik som for skadelig dataprogram. Tilgjengeliggjøring av overgrepsbilder representerer en integritetskrenkelse overfor barnet på bildet så lenge bildet verserer på nettet. Automatisert inndragning reduserer omfanget av skaden og kan kanskje praktisk sett bringe den til opphør. Den krenkelsen som tilgjengeliggjøringen representerer for barna på bildet er flere ganger konstatert i rettspraksis, jf. Rt. 2002 s. 1187 m.v..[670] Dessuten er traumatiseringen som

[668] Smlg. fortalen til tilleggsprotokollen til barnekonvensjonen: ”… som er bekymret over at barnepornografi stadig blir mer tilgjengelig på Internett og annen ny teknologi…”
[669] Det er et visst filtermarked beregnet på foreldre som vil beskytte sine barn mot innhold på nettet, men det er nok forsvinnende lite sammenlignet med markedet for ”malware”-beskyttelse.
[670] Rt. 2009 s. 140. Domfelte hadde forledet mindreårige til å sende seksualiserte bilder av seg selv via msn. Retten uttalte: ”Den kontakten domfelte hadde med andre med interesse for barnepornografi, medførte en

fotograferingen medfører for fornærmede, vektlagt som straffutmålingsmoment og som grunnlag for erstatning. Selve avbildingen er således en krenkelse av barnets integritet, og behovet for å bringe integritetskrenkelsen til opphør taler med styrke for å ta i bruk automatisert filtrering

Det er ikke lett å finne likeverdige alternative tiltak. Filtrering av nettsteder som jeg har redegjort for tidligere, hindrer ikke at overgrepsbildene forsetter å versere i skjulte fora på nettet. Det kan direkte blokkering av filene ved automatisert inndragning hindre. Stengning av nettsteder kan lede til stor overdekning, i hvert fall dersom det medfører at man stenger en hel tjeneste, for eksempel en fildelingstjeneste. Da er filtrering av dubletter mer velegnet, fordi det lar en ellers lovlig tjenesten pågå; inndragningen blokkerer bare for overgrepsbildene.[671]

Siden denne type filtrering ikke har negative sideeffekter i form av overdekning, innsyn i innhold, overskuddsinformasjon eller en kjølende effekt på frimodigheten, *og* det foreligger et stort behov for tiltak, er det neppe tvilsomt at automatisert inndragning oppfyller de betingelser EMK stiller for at det kan anses nødvendig i et demokratisk samfunn.

Barn er borgere med selvstendig krav på vern etter EMK. De avbildete barna har følgelig en selvstendig rett til vern om sitt privatliv. Bildene som verserer på nettet representerer en vedvarende integritetskrenkelse for barna. Private individer er ikke i posisjon til å stanse integritetskrenkelsen, så spørsmålet som oppstår er om myndighetene ikke bare har *adgang*

---

betydelig risiko for *irreversibel spredning* av materialet over Internett" (avsn. 25), min uth. Rt. 2005 s. 919 besittelse og tilgjengeliggjøring av overgrepsbilder. I avsn. 13 viser retten uttrykkelig til beskrivelsene av skadevirkningene i Rt. 2002 s. 1187, som blant annet gjelder krenkelsen av barna på bildene. RG 2002 s. 1307: Dom for seksuelle overgrep og fotografering av to barnehjemsbarn fra Murmansk. Om fotograferingen og spredningen på internett er det uttalt: " Retten har også vektlagt at bildene av jentene ble lagt ut på Internett *og derfor i praksis umulig å slette.* Jentene har uttrykt bekymring om dette og er redde for at noen skal kunne finne bildene igjen" (min uth.). Rt. 1997 s. 1994 , dom for seksuelle overgrep og filming av 7 årig stedatter. Høyesterett kommenterte at "selv om videoen i dette tilfelle ble beslaglagt før den var blitt kopiert og distribuert, og fornærmede dermed ble spart for den fremtidige belastning ved usikkerheten rundt eksistensen av en slik film…" Se også Innst.O. nr. 66 (2004-2005) hvor justiskomiteen uttalte at overgrepsbilder på nettet "representerer en livsvarig krenkelse for ofrene ved at slikt materiale i prinsippet blir liggende på nettet for evig tid." (s. 3).

[671] *Zittrain* drøfter forskjellige risiki med filtreing og hvilke formål som kan legitimere tiltaket. Om filtrering av overgrepsbilder skriver han følgende: "The easiest, perhaps most uncontroversial case is the common abhorrence of child pornography. Most societies share the view that imagery of children under a certain age in a sexually compromising position is unlawful to produce, possess, or distribute. The issue in the context of child pornography is less whether the state has the right to assert control over such material, but rather the most effective means of combating the problem it represents, and the problems to which it leads, without undercutting rights guaranteed to citizens". *Zittrain* (2008b) s. 44. *Zittrains* drøftelse gjelder andre teknikker som jeg har gjennomgått i avhandlingen kapittel 14. Som jeg har konstatert skiller sjekksumbasert filtrering seg fra disse ved å være særlig presis. Metoden vil derfor kunne imøtekomme respekten for sivile rettigheter som *Zittrain* nevner.

rettslig sett, men også en *positiv forpliktelse* til å ta i bruk automatisert inndragning, for å bringe integritetskrenkelsen til opphør.

Myndighetene plikter å sikre at de konvensjonsbaserte rettighetene ytes et effektivt vern, slik at de representerer reelle goder for borgerne. EMD har slått fast at staten ikke bare har en plikt til selv å avstå fra å krenke rettighetene, den skal også sørge for at rettighetene ikke er "theoretical or illusory", men "practical and effective".[672] Dette ligger nedfelt i EMK art. 1 som pålegger staten "å sikre" rettighetene for sine borgere. Forpliktelsen er fremholdt i en rekke avgjørelser fra EMK, hvorav flere gjelder retten til privat liv etter EMK art. 8. Forpliktelsen går da ut på å gjøre noe aktivt for å sikre respekten for privat liv.[673]

EMK art. 8 "privat liv" omfatter vernet om borgerens identitet. Dersom man kan gjenkjennes på et bilde er identiteten berørt, og man er innenfor bestemmelsens beskyttelsessfære.[674] Barn på overgrepsbilder er derfor regulært omfattet av dette vernet. Det at identifikasjon av ofrene er et problem for politiet, er ikke relevant. Her er det tilstrekkelig at barnet kan gjenkjennes av andre som kjenner det. Barnet kan traumatiseres av frykten for å bli gjenkjent senere i livet, i den fornedrende situasjonen som vises på bildet.[675] Det hefter ikke feil ved det norske lovverket, siden det finnes hjemmel både for straff og inndragning. Spørsmålet er om bruk av automatisert inndragning er et tiltak som staten plikter å iverksette for å effektivisere barnas rett til privatliv. Det er således tale om en mulig plikt til å foreta en *faktisk handling*.

[672] *Von Hannover* (2004) pkt. 71.
[673] *Van Dijk* (2006) s. 739 flg., som viser til rettspraksis som konstaterer handlingsplikten for staten til å effektivisere den konvensjonsbaserte rettigheten. Jeg finner ikke grunn til å gå konkret inn på de enkelte avgjørelsene her.
[674] I *Von Hannover* (2004) som gjaldt avveiningen mellom personvern og ytringsfrihet i forbindelse med publiseringen av bilder fra privatsfæren til Caroline von Hannover (prinsesse "Caroline av Monaco") i et tysk ukeblad ("Bunte"), tok retten utgangspunkt i at "the concept of private life extends to aspects of personal identity, such as … a person's picture" (pkt. 50); smlg. *Schüssel* (2002) om en østerriksk politiker hvis portrettfotografi var blitt brukt av politiske motstandere i valgkamp. Bildet og bruken ble ansett å være omfattet av "private life" i EMK art. 8 (beslutningen s. 7 pkt. 2).
[675] Smlg. en uttalelse fra Personvernkommisjonen i relasjon til retten til eget bilde, jf. åvl. § 45c, hvor det sies at det "er en forutsetning at personen på bildet kan identifiseres, direkte eller indirekte, men ikke et krav om at allmennheten skal være i stand til å foreta identifikasjon", NOU 2009: 1 kapittel 7.2.7 s. 66. *Bing* (2008) s. 47 og 73, har tatt til orde for at den nevnte bestemmelsen, som er straffesanksjonert, jf. åvl. § 54 første ledd bokstav b, brukes i saker om tilgjengeliggjøring av overgrepsbilder. Formålet er å lette muligheten for å tilkjenne oppreisningserstatning for krenkelsen, jf. åvl. § 55. Etter ordlyden er det mulig, men formålet med åvl. § 45c er å regulere tilfeller hvor fotograferingen i utgangspunktet ikke er kontroversiell. Det er fotografens senere ønske om å publisere bildet som reiser personvernsspørsmål for den avbildete. For barna på overgrepsbilder er selve avbildningen en selvstendig krenkelse, og de har ingen samtykkekapasitet, så man er utenfor det området som åvl. § 45c er ment for. Det kan også ligge en utilsiktet legitimerende effekt i å pretendere at det kunne vært tale om å samtykke til publisering av slike bilder, slik forutsetningen etter åvl. § 45c tross alt er. Det synes å være en klarere løsning å holde seg til at det er rettsstrid fra begynnelse til slutt i enhver handling som har med fotografering og senere befatning med overgrepsbilder å gjøre.

Utgangspunktet er at EMD vektlegger at barn er sårbare individer som har et spesielt behov for effektiv ivaretakelse av sin rett til respekt for sin integritet. Retten til effektiv beskyttelse står spesielt sterkt når det som her, gjelder vern mot seksuelle overgrep. Det har ikke betydning at bildet i seg selv ikke er et seksuelt overgrep; avgjørende er at det står i direkte sammenheng med og stimulerer til slike overgrep. Dette følger av flere avgjørelser fra EMD.

Det kan tas utgangspunkt i *K.U.* (2008) hvor Finland ble dømt for krenkelse av EMK art. 8, fordi reglene om tilbydernes taushetsplikt var så strenge at de avskar muligheten for å holde en lovbryter ansvarlig. Den straffbare handlingen besto i å ha lagt en melding på internett i navnet til en 12 år gammel gutt, som fremstilte ham som tilgjengelig for seksuelle overgripere. Dette representerte en krenkelse av guttens personvern, jf. EMK art. 8.

Meldingen var (selvsagt) ikke et seksuelt overgrep, men EMD reagerte likevel med et utvetydig krav om aktivitet fra statens side for å sikre barn beskyttelse mot å bli et mål for tilnærmelser fra pedofile. EMD tok utgangspunkt i saken *X og Y* (1985) som gjaldt voldtekt av en psykisk handikappet pike. Nederland ble dømt for utilstrekkelig lovverk i forhold til å sikre fornærmede rettsapparatets assistanse. I *K.U.* (2008) pkt. 41 viser EMD til den nevnte avgjørelsen, og fastslår at saksforholdet (den uriktige meldingen på internett) gjaldt

> "… a matter of "private life", a concept which covers the physical and moral integrity of the person … The Court would like to highlight these particular aspects of the notion of private life, having regard to the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age."

Videre sa retten at saken ikke var triviell selv om den ikke gjaldt et så alvorlig forhold som en voldtekt, fordi

> "… [t]he act was criminal, involved a minor and made him a target for approaches by paedophiles…" (pkt. 46).

Rettens oppsummering av problemet er treffende også for markedet for overgrepsbilder, og saken er følgelig relevant i forhold til spørsmålet om det gjelder en positiv forpliktelse til å bringe den vedvarende integritetskrenkelsen av barna til opphør.

Nettopp det at krenkelsen gjelder barn, gjør at synspunktet om en positiv forpliktelse gjør seg særlig sterkt gjeldende. I *K.U.* (2008) sier EMD at

> "sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of active deterrence, from such grave types of interference with essential aspects of their private lives." (pkt. 46).

Det er ikke tilstrekkelig at lovverket kriminaliserer slike handlinger, også håndhevelsen må være effektiv. I *K.U.* (2008) sviktet staten fordi sporingsinformasjon ikke kunne utleveres fra tilbyder. Retten konstaterte da at

> "the existence of an offence has limited deterrent effects if there is no means to identify the actual offender and to bring him to justice." (pkt. 46).

Retten avviste at en kompensasjonsordning fra en tredjepart var tilstrekkelig. Tilsvarende er krav til effektivisering av barns vern mot seksuelle overgrep og muligheten for effektiv strafforfølgning, fremholdt i *M.C.* (2003) hvor retten dømte Bulgaria for sviktende etterforsking av voldtekt av en mindreårig.[676]

Siden inndragningens formål er å effektivisere straffebudet, og det praktisk sett er eneste mulighet for å stanse integritetskrenkelsen som bildene representerer, er utgangspunktet at staten plikter å utføre automatisert inndragning i nettet. Den positive forpliktelsen gjelder imidlertid ikke ubetinget. EMD har trukket opp flere prinsipper som modifiserer den:

For det første er det et ufravikelig krav at rettssikkerhetsgarantiene, og andre konvensjonsbaserte rettigheter respekteres.[677] Ved inndragning av bilder på nettet er det kravet til rettsriktighet og presisjon som er viktigst. Kravet til rettsriktighet (dvs. kravet til et materielt riktig resultat) oppfylles via inndragningsprosedyren som ligger til grunn for oppbygningen av RDB. Videre skjer blokkering presist på grunnlag av dataidentiteten. Automatisert inndragning oppfyller altså dette vilkåret.

[676] Det uttales at "…effective deterrence against grave acts such as rape, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions. Children and other vulnerable individuals, are entitled to effective protection…" (pkt. 150). Saken gjaldt en såkalt "date rape". Bulgaria ble dømt for å ha sviktet sin positive forpliktelse til å oppfylle offerets krav på respekt ved å gjennomføre en profesjonell etterforsking på effektiv måte.
[677] *K.U* (2008) pkt. 48.

Videre gjelder følgende tre retningslinjer for vurderingen: For det første må det foreligge slik kunnskap om problemet at det gir grunn til å reagere på det (hensynet til "the social context of the time"). For det annet anerkjenner EMD at det ikke er enkelt å utøve politivirksomhet i moderne samfunn ("the problem of policing modern societies"). Og til sist går man ikke så langt som til å pålegge staten en forpliktelse som er umulig eller urimelig byrdefull å oppfylle ("an impossible or disproportionate burden").[678]

Forbeholdet "the social context of the time" kan åpenbart ikke slå til i dette tilfellet. Problemet med overgrepsbilder er velkjent og har vært det lenge, så det finnes foranledning til å handle. Det er ikke tilstrekkelig med et velutviklet regelverk, også håndhevelsen må skje på en effektiv måte. Det følger også av utgangspunktet om at rettighetene ikke bare skal være flotte formuleringer på papiret, men en praktisk realitet for borgerne. I de tidligere drøftelsene har jeg kartlagt at de rettslige normene også gjelder på nettet, og dermed omfatter håndhevelsesforpliktelsen nettet.[679]

Men det er ikke enkelt å utøve politivirksomhet i moderne samfunn (jf. forbeholdet "the problem of policing modern societies"). Urbanisering, mobilitet og stor individuell frihet medfører at selv om det finnes indikasjoner på en fare, er det ikke nødvendigvis lett å vite om, når og hvordan den vil realisere seg i en straffbar handling. Derfor påhviler det for eksempel ikke staten en generell plikt til å holde "risikoelementer" under oppsikt hele tiden.[680] Hvor mye staten plikter å gjøre må vurderes konkret ut fra situasjonen, og myndighetene har også frihet til å foreta prioriteringer ut fra de ressurser som er stilt til rådighet for kriminalitetsbekjempelse.

Denne reservasjonen er interessant med tanke på automatisert filtrering. Etter en umiddelbar vurdering synes den å passe godt for internett, fordi dynamikken, tempoet og foranderligheten

[678] Disse forbeholdene gjentas i avgjørelsene om positiv forpliktelse, se bl.a. *Osman* (1998) pkt. 116; *K.U* (2008) pkt. 48.
[679] Se blant annet kapittel 11.2.
[680] Dette var et problem i *Osman* (1998) hvor en persons truende opptreden over tid til slutt endte med drap. EMD fastslo at som generell rettesnor for handlingsplikten er det "sufficient … to show that the authorities did not do all that could be reasonably expected of them…" (pkt. 116). Etter en konkret vurdering av forholdene i saken fant EMD at myndighetene ikke hadde krenket normen. At atferden skulle ende i drap var upåregnelig, og avverging ville i praksis ha krevd full overvåking av den nevnte personen, og det på et usikkert faktisk grunnlag med hensyn til gehalten i truslene.

gjerne er de egenskaper som trekkes frem ved beskrivelsen.[681] Det er en "sann" beskrivelse, men gir ikke nødvendigvis det fulle bildet. Spørsmålet er jo ikke hva som kjennetegner internett generelt, men *hva som kjennetegner problemet med overgrepsbilder spesielt*. Det kjennetegnes ved at man kjenner formatet (dataidentiteten) og vet hvordan de kan gjenkjennes og blokkeres. I motsetning til den uoversiktlighet som forbeholdet "the problem of policing modern societies" tar hensyn til, er overgrepsbildenes eksistens og identitet et *utpreget forutsigbart og standardisert problem*. De samme bildene verserer år etter år på nettet og kan blokkeres. De fanges derfor ikke opp av det nevnte forbeholdet.

Handlingsplikten går ikke så langt at staten kan pålegges tiltak som er umulige eller urimelig byrdefulle å oppfylle ("an impossible or disproportionate burden"). Hvorvidt filtreringen vil være uforholdsmessig kostbar kan bare en økonomisk undersøkelse besvare, så her foreligger det en usikkerhet som jeg ikke har kunnet avklare. Men det kan i hvert fall påpekes at automatisert inndragning i stor grad utnytter ressurser som *uansett går med* i etterforskingen og iretteføringen av en sak. Tiltaket representerer bare en begrenset merkostnad til filtre i nettet. Filterteknologien har lenge vært brukt i analyser av databeslag i saker om overgrepsbilder, så det handler bare om *å vri utnyttelsen av eksisterende ressurser* over på nettet i tillegg. Automatisert inndragning vil derfor i hovedsak innebære at ressurser som uansett medgår i straffesaksbehandlingen *utnyttes bedre* enn før.

Til sist er det klart at staten har rett til å utøve et selvstendig skjønn med hensyn til prioriteringer i kriminalitetsbekjempelsen innenfor de midler som kan avses til rettshåndhevende tiltak. Men påvisning av en felles europeisk oppfatning om tilnærmingen til et problem, kan innskrenke valgfriheten.[682] Det finnes imidlertid ikke europeisk konsensus om at nettopp automatisert inndragning bør brukes mot problemet. Det er internasjonalt konsensus om at problemet er omfattende og at det er viktig å ta i bruk effektive tiltak med allmennpreventiv virkning, men nøyaktig hvilke praktiske rettshåndhevende virkemidler som skal tas i bruk er ikke fastslått.[683]

[681] Se kapittel 14.3.
[682] *K.U.* (2008) pkt. 43; *M.C* (2003) pkt. 155; *Goodwin* (2002) pkt. 74.
[683] De aktuelle konvensjonene nevner imidlertid inndragning ("confiscation"), så det gir et utgangspunkt for vurdering. Se 201 ETS art. 27 nr. 3, tilleggsprotokollen til barnekonvensjonen art. 7.

Men for å oppsummere har avhandlingen vist at det er rettslig adgang til å foreta automatisert inndragning. Det er vanskelig å identifisere alternative effektive tiltak. Da er det ikke sikkert at det foreligger større valgfrihet og mye taler for at det foreligger en handlingsplikt.

Personlig strafforfølgning er ikke tilstrekkelig. Til tross for internasjonal nulltoleranse og forpliktelse til strafforfølgning for befatning med overgrepsbilder, pågår overgrepene og produksjonen. Strafforfølgningen har heller ingen effekt for det materiale som alt er tilgjengeliggjort på nettet. Filtrering av nettsteder dekker ikke det samme behovet. Det fanger ikke opp verserende bilder og utveksling i skjulte fora. Automatisert filtrering treffer mer presist og kan brukes på trafikk som filtrering av nettsteder ikke kan fange opp. I tilknytning til dette synes det relevant at EMD vektlegger betydningen av den trussel som moderne kommunikasjonsteknologi utgjør for personvernet. I *Von Hannover* (2004) ble det sagt slik:

> "increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and *reproduce* personal data." (min uth.)[684]

Uttalelsen refererer seg til nærgående paparazzi-fotografering av Caroline von Hannover (prinsesse "Caroline av Monaco"), som ble ansett å krenke hennes rett til å være i fred for innsyn og forstyrrelser. Bildene ble trykket i store opplag i tyske ukeblad. EMD bemerket teknologiens evne til å reprodusere ("reproduce") informasjonen. *Dubletter* viser mer enn noe annet teknologiens evne til reproduksjon, og gjør at synspunktet om behovet for økt aktivitet for å beskytte privatlivet, står spesielt sterkt.[685] På en eller annen måte må nettopp dette problemet håndteres.

Konklusjonen er dermed at med mindre myndighetene kan vise til iverksettelse av andre like effektive tiltak, foreligger det en positiv forpliktelse til å foreta automatisert inndragning.

[684] *Von Hannover* (2004) pkt. 70. Her vises det videre til *PG. og J.H* (2001) pkt. 57-60 ; *Amann* (2000) pkt. 65-67, sikkerhetstjenestens lagring av informasjon om en person var et inngrep, selv om informasjonen ikke var av sensitiv karakter; *Rotaru* (2000) pkt. 43-44, sikkerhetstjenestens lagring av informasjon om person var et inngrep, selv om informasjonen ikke var hemmelig; og *Peck* (2003) pkt. 59-63 og 78 (bruk av kameraovervåking fra offentlig sted).

[685] Smlg. *Times* (2009) hvor EMD fant at "the internet rule" var forenlig med EMK art. 10. Regelen medførte at skjedde en ny ærekrenkelse hver gang artiklene med det ærekrenkende innholdet ble lastet ned fra internettarkivene til avisen *Times.* Også dette gjelder *dubletter*. Avgjørelsen legger et ansvar på innehaveren av kildefilen for hver dublett som skapes ved nedlasting. Saken gjaldt krenkelse av EMK art. 10, ikke art. 8. Men temaet er relevant i saker hvor avveiningen går mellom art. 8 og 10, slik som i von Hannover. Og det har overføringsverdi til dublettene med overgrepsbilder, selv om slike saker ikke reiser spørsmål om hensynet til ytringsfriheten.

VII Oppsummering

Avhandlingens hovedspørsmål har vært fortolkningen av begrepet ”ting” i inndragningsreglene. Det har vært viktig å ta utgangspunkt i skillet mellom data og informasjon. Ved å analysere *hvilke kriterier* begrepet legger til grunn er det konstatert at *datafiler* kan inndras som selvstendige objekter. Det følger av at begrepet ”ting” forutsetter at objektet kan *spesifiseres og kontrolleres*. Videre er det konstatert at identiske datafiler (dubletter) kan inndras under ett med referanse til *dataidentiteten.* For at inndragningen skal får virkning for dubletter utenfor beslaget, må det besluttes med hjemmel i strl. 2005 § 74 tredje ledd, dvs. inndragning uten at noen er gjort til saksøkt. Avhandlingen har vist at nettet er en samfunnsarena for retthåndhevelse på linje med ”den fysiske verden”, slik at dagens håndhevelsesregler også gjelder for de straffbare handlingene på internett.

Analysen er ikke basert på analogier, men har påvist at datafiler, fysiske objekter og noen abstrakte goder som enkle fordringer og individuelle rettigheter, oppfyller lovens kriterier for å være gjenstand for inndragning.

Avhandlingens funn innebærer at påtalemyndigheten med hjemmel i dagens regler, kan begynne å kreve, og retten kan beslutte, inndragning av datafiler. Det bør gjøres for å legge grunnlaget for en størst mulig database med ”svartelistede” filer. Inndragningen innebærer ikke økt ressursbruk, fordi den baserer seg på analyser som uansett gjøres under etterforskingen for å beregne av lovbruddets omfang. Inndragning av datafiler fordrer derfor bare en *endring i praksis* med hensyn til utforming av inndragningsbeslutningen. På bakgrunn av konklusjonen i del VI kapittel 16.3 bør det denne praksisendring gjøres med en gang.

Videre har avhandlingen avdekket behov for å vurdere om det bør foretas noen endringer i inndragningsbestemmelsene. Jeg nøyer meg med en punktvis oppsummering:

- Uttrykket ”elektronisk lagret informasjon” brukes på forskjellig vis i strl. 2005 § 69 annet ledd og i strl. 2005 § 76 første ledd. I den førstnevnte bestemmelsen betyr uttrykket ’data’, i den andre betyr det ’meningsinnholdet i data’.

- Gjennomføring av inndragning i web 2.0-situasjonen stiller seg likt uansett om dataene er lagret på lovbryterens eget brukerområde i nettet, eller på en annens brukerområde eller tjeneste. I begge tilfeller må dataene slettes og/eller tilgang sperres med hjelp av tilbyder. Punktene i strl. 2005 § 76 tredje ledd kan derfor samordnes til én regel.

- Vilkåret "lagret" i "elektronisk lagret informasjon", jf. strl. 2005 § 69 annet ledd er unødvendig for data som er tatt i beslag, og kan hemme inndragning av dublettene i nettet. Det er vanskelig å se grunner for å beholde vilkåret.

Til slutt, og nærmest som en bivirkning, har avhandlingen påvist at rettssetningen om at det må utvises tilbakeholdenhet ved bruk av forebyggende inndragning, jf. strl. 2005 § 70, støter an mot forpliktelsen til å sikre retten til privatliv, jf. EMK art. 8. Bilder av personer som ufrivilling er blitt avbildet i krenkende positurer og som kan gjenkjennes på bildet, må inndras uavhengig av hvor nærliggende spredningsfaren er.

KILDEHENVISNINGER

LOVER

G	Norges Riges Grundlov av 17. mai 1814.
Ehandelsloven (ehl.)	Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester av 23. mai 2003 nr. 35.
Ekomloven	Lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83.
Esignaturloven	Lov om elektronisk signatur av 15. juni 2001 nr. 81.
Hvitvaskingsloven	Lov om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. av 20. juni 2003 nr. 41.
Kringkastingsloven	Lov om kringkasting av 4. desember 1992 nr. 127.
Legemiddelloven	Lov om legemidler m.v. av 4. desember 1992 nr. 132.
Markedsføringsloven (mfl.)	Lov om kontroll med markedsføring og avtalevilkår av 16. juni 1972 nr. 47.
Menneskerettsloven (mrl.)	Lov om styrking av menneskerettighetenes stilling i norsk rett av 21. mai 1999 nr. 30.
Personopplysningsloven (pol.)	Lov om behandling av personopplysninger av 14. april 2000 nr. 31.
Produktkontrolloven	Lov om kontroll med produkter og forbrukertjenester av 11. juni 1976 nr. 79.
Straffeloven 1902 (strl. 1902)	Almindelig borgerlig straffelov av 22. mai 1902 nr. 10.
Straffeloven 2005 (strl. 2005)	Lov om straff av 20. mai 2005 nr. 28.
Straffeprosessloven (strpl.)	Lov om rettergangsmåten i straffesaker (Straffeprosessloven) av. 22. mai 1981 nr. 25.
Verdipapirhandelloven (vphl.)	Lov om verdipapirhandel av 29. juni 2007 nr. 75.
Åndsverkloven (åvl.)	Lov om opphavsrett til åndsverk m.v. av 12. mai 1961 nr. 2.

FORSKRIFTER

Legemiddelforskriften	Forskrift om salg av legemidler til ikke-medisinsk bruk av 1. mars 1983 nr. 628.
Narkotikaforskriften	Forskrift om narkotika m.v. (Narkotikalisten) av 30. juni 1978 nr. 8
Påtaleinstruksen	Forskrift om ordningen av påtalemyndigheten av 28. juni 1985 nr. 1679

OFFENTLIGE DOKUMENT

Norske offentlige utredninger – NOU

NOU 1985: 31	*Datakriminalitet.*
NOU 1993: 3	*Strafferettslige regler i terroristbekjempelsen.*
NOU 1996: 21	*Mer effektiv inndragning av vinning.*
NOU 1997: 15	*Etterforskingsmetoder for bekjempelse av kriminalitet. Delinns. II.*
NOU 1999: 26	*Konvergens.*
NOU 1999: 27	*«Ytringsfrihed bør finde Sted». Forslag til ny Grunnlov § 100.*
NOU 2002: 4	*Ny straffelov.*
NOU 2003: 27	*Lovtiltak mot datakriminalitet. Delutredning I.*
NOU 2005: 19	*Lov om DNA-register til bruk i strafferettspleien.*
NOU 2006: 6	*Når sikkerheten er viktigst.*
NOU 2007: 2	*Lovtiltak mot datakriminalitet. Delutredning II.*
NOU 2009: 1	*Individ og integritet. Personvern i det digitale samfunnet.*
NOU 2009: 15	*Skjult informasjon – åpen kontroll.*

Odelstingsproposisjoner, innstillinger mv.

Ot.prp. nr. 5 (1958)	*Om endringer i den alminnelige borgerlige straffelov av 22. mai 1902 m.v.*
Ot.prp. nr. 26 (1959-1960)	*Om lov om opphavsrett til åndsverk..*
Ot.prp. nr. 4 (1978-1979)	*Om lov om endringer i straffeloven.*
Ot.prp. nr. 33 (1989-1990)	*Om lov om endringer i åndverksloven (endringslov).*
Ot.prp. nr. 20 (1991-1992)	*Om endringer i straffeloven og skadeserstatningsloven m.m (seksuelle overgrep mot barn).*
Ot.prp. nr. 8 (1998-1999)	*Om lov om endringer i straffeloven og straffeprosessloven mv (inndragning av utbytte).*
Ot.prp. nr. 92 (1998-1999)	*Om lov om behandling av personopplysninger (personopplysningsloven).*
Ot.prp. nr. 64 (1998-1999)	*Om lov om endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v).*
Ot.prp. nr. 28 (1999-2000)	*Om lov om endringer i straffeloven mv. (seksuallovbrudd).*
Ot.prp. nr. 58 (2002-2003)	*Elektronisk kommunikasjon (ekomloven).*
Ot.prp. nr. 4 (2003-2004)	*Om lov om endringer i lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven).*
Ot.prp. nr. 90 (2003-2004)	*Om lov om straff (straffeloven).*
Ot.prp. nr 33 (2004-2005)	*Om lov om forbud mot diskriminering på grunn av etnisitet, religion mv. (diskrimineringsloven).*
Ot.prp. nr. 37 (2004-2005)	*Om lov om endringar i straffelova (eige straffebod om kjønnslege skildringar som gjer bruk av barn).*

Ot.prp. nr. 40 (2004-2005) *Straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet).*

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

Ot.prp. nr. 60 (2004-2005) *Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet).*

Ot.prp. nr. 72 (2006-2007) *Om lov om endringer i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven).*

Ot.prp. nr. 22 (2008-2009). *Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon - sluttføring av spesiell del og tilpasning av annen lovgivning).*

Forhandlinger i Odelstinget (nr. 55) (1901-1902) 4. desember - Ang. straffeloven- §§ 4-6.

Indst. O. I – 1901 / 1902 *Indstilling fra justiskomiteen angaaende den kongelige proposition til en almindelig borgerlig straffelov.*

Innst. O. nr. 66 (2004-2005) *Innstilling fra justiskomiteen om lov om endringar i straffelova (eige straffebod om kjønnslege skildringar som gjer bruk av barn).*

Innst.S. nr. 223 (2003-2004) *Innstilling fra samferdselskomiteen om samtykke til godkjenning av EØS-komiteens beslutninger nr. 79/2003 og nr. 80/2003 av 20. juni 2003 og nr. 11/2004 av 6. februar 2004 om innlemmelse av direktiver på området for elektronisk kommunikasjon.*

S.K.M 1896 *Udkast til Almindelig borgerlig Straffelov for Kongeriget Norge. Udarbeidet af den ved kgl. Resolution 14de November 1885 nedsatte Kommission.* Kristiania, 1896.

S.R.I. 1955 *Innstilling fra Straffelovrådet om Ansvar for Rettskrenkelser i Trykt Skrift.* Oslo, september 1955.

St.meld. nr. 17 (2006-2007) *Eit informasjonssamfunn for alle.*

Utredninger og rapporter mv.

Biometriutredningen (2008)	*Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12.* Rapport 5. november 2008 til Justisdepartementet, fra Dag Wiese Schartum og Lee A. Bygrave.
Europarådet (2004)	Eurparådet *Organised Crime in Europe: the threat of cybercrime.* Situation Report 2004. Strasbourg, 2004.
Faremo-rapporten (2007)	*Forebygging av internettrelaterte overgrep mot barn.* Rapport 30. januar 2007 til Justisdepartementet fra Faremo-utvalget.
Rapport om ECHELON (2001)	Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098 (INI)). Europarlamentet, 11. juli 2001.
SOU 1992: 110	*Information och den nya InformationsTeknologin – straff- och processrättsliga frågor m.m.*
Wood (2006)	Wood, David Murakami and Kirstie Ball *A Report on the Surveillance Society. Public Discussion Document*. 2006.

KONVENSJONER OG DIREKTIVER MV.

Konvensjoner

185 ETS	Europarådets konvensjon om datakriminalitet av 23. november 2001 (Datakrimkonvensjonen).
201 ETS	Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk av 25. oktober 2007.

EMK	Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter. Roma, 4. november 1950.
Narkotikakonvensjonen	Den alminnelige narkotikakonvensjon av 1961.
Konv. om psykotrope stoffer	Konvensjonen om psykotrope stoffer av 1971.
SP	FNs konvensjon om sivile og politiske rettigheter av 16. desember 1966.

Valgfri tilleggsprotokoll til FNs barnekonvensjon, om salg av barn, barneprostitusjon og barnepornografi, 25. mai 2000.

Direktiver

Rettsakter som hører under den europeiske reguleringspakken for elektronisk kommunikasjon:

Rammedirektivet	direktiv 2002/21/EF
Tillatelsesdirektivet	direktiv 2002/20/EF
Tilgangsdirektivet	direktiv 2002/19/EF
USO-direktivet	direktiv 2002//22/EF
Frekvensvedtaket	direktiv 2002/676/EF
Kommunikasjonsverndirektivet	direktiv 2002/58/EF

Andre direktiver:

TV-direktivet	direktiv 1989/552/EØF, endret ved direktiv 1997/36/EF
Datalagringsdirektivet	direktiv 20006/24/EF
Ehandelsdirektivet	direktiv 2000/31/EF

Forklarende rapporter

Forklarende rapport til Datakrimkonvensjonen, 185 ETS. (http://conventions.coe.int/Treaty/en/Reports/Html/185.htm).

Forklarende rapport til Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk, 201 ETS. (http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm)

AVGJØRELSER

Avgjørelser fra Norges Høyesterett

Høyesteretts kjennelse av 29. september 1928 (utrykt, referert i Kjerschow 1930)

Rt. 1930 s. 1005 (Damluke)

Rt. 1953 s. 462

Rt. 1958 s. 479 (”Sangen om den røde rubin”)

Rt. 1959 s. 431 (”Sexus”)

Rt. 1966 s. 905

Rt. 1967 s. 1502 (”Uten en tråd”)

Rt. 1977 s. 513

Rt. 1979 s. 863

Rt. 1979 s. 1418

Rt. 1980 s. 1532

Rt. 1981 s. 1305 (Løpeseddel)

Rt. 1984 s. 1016 (”Snowwhite”)

Rt. 1985 s. 569

Rt. 1985 s. 1138

Rt. 1986 s. 267 (Hær-Værk)

Rt. 1986 s. 571

Rt. 1986 s. 1149

Rt. 1987 s. 49

Rt. 1987 s. 1194

Rt. 1989 s. 980

Rt. 1992 s. 790

Rt. 1992 s. 904

Rt. 1992 s. 928

Rt. 1992 s. 1219

Rt. 1994 s. 1610 (BetalTV)

Rt. 1995 s. 35 (Smartkort)

Rt. 1995 s. 867

Rt. 1995 s. 1583

Rt. 1995 s. 1872 (PINkode)

Rt. 1995 s. 1894

Rt. 1995 s. 1983 (Speildommen)

Rt. 1997 s. 27

Rt. 1997 s. 266

Rt. 1997 s. 470

Rt. 1997 s. 1760

Rt. 1997 s. 1994

Rt. 1998 s. 309

Rt. 1998 s. 2006

Rt. 1999 s. 1944

Rt. 2000 s. 40

Rt. 2000 s. 169

Rt. 2001 s. 1674

Rt. 2002 s. 133

Rt. 2002 s. 136

Rt. 2002 s. 1187

Rt. 2002 s. 1717 (Orderud)

Rt. 2003 s. 825 (Kvearner.com)

Rt. 2003 s. 1091

Rt. 2003 s. 1243

Rt. 2004 s. 215

Rt. 2004 s. 1580

Rt. 2004 s. 1619 (Bakdør)

Rt. 2005 s. 41 (Napster)

Rt. 2005 s. 919

Rt. 2005 s. 1058

Rt. 2005 s. 1365 (Finanger II)

Rt. 2005 s. 1628 (Frie Aktuell Rapport)

Rt. 2006 s. 813

Rt. 2007 s. 422

Rt. 2008 s. 1403 (Thailand)

Rt. 2008 s. 1582

Rt. 2009 s. 140

Rt. 2009 s. 780 (Derivat)

Rt. 2009 s. 1011 (”joyzone.no”)

Avgjørelser fra norske lagmannsretter

Publiserte

RG 1967 s. 65

RG 1998 s. 1155

RG 2002 s. 1307

RG 2003 s. 858

RG 2004 s. 215

RG 2004 s. 689

RG 2004 s. 929

RG 2005 s. 246

RG 2006 s. 595

RG 2007 s. 961

RG 2007 s. 1345 (MMS)

RG 2008 s. 1477 (epost)

Upubliserte

LA-2005-111640 Agder lagmannsretts dom av 14. november 2005.

LA-2008-87454 Agder lagmannsretts dom av 17. april 2009.

LB-2005-111057 Borgarting lagmannsretts dom av 5. mai 2005.

LB-2005-132404 Borgarting lagmannsretts dom av 21. september 2005.

LB-2006-656 Borgarting lagmannsretts kjennelse av 30. juni 2006.

LB-2006-31569 Borgarting lagmannsretts dom av 16. desember 2006.

LB-2006-51173 Borgarting lagmannsretts dom av 22. september 2006.

LB-2008-18408 Borgarting lagmannsretts dom av 23. oktober 2008.

LE-2002-242 Eidsivating lagmannsretts dom av 26. september 2002.

LE-2004-8204 Eidsivating lagmannsretts dom av 14. mai 2004.

LE-2004-13795 Eidsivating lagmannsretts dom av 8. september 2004.

LF-2005-116879 Frostating lagmannsretts kjennelse av 14. desember 2005.

LF-2006-159248 Frostating lagmannsretts dom av 22. februar 2006.

LG-2002-322 Gulating lagmannsretts dom 24. september 2002.

LG-2003-4852 Gulating lagmannsretts dom av 17. desember 2003.

LG-2005-83688 Gulating lagmannsretts dom av 5. desember 2005.

LG-2006-3339 Gulating lagmannsretts dom av 1. juni 2006.

LH-2004-51077 Hålogaland lagmannsretts dom av 21. oktober 2004.

LH-2006-27124 Hålogaland lagmannsretts dom av 11. mai 2006.

Borgarting lagmannsretts kjennelse av 9. februar 2010 (sak nr. 10-006542ASK-BORG/04).

Avgjørelser fra norske tingretter

Bergen tingretts dom av 19. september 2007 (TBERG-2007-70663).

Nedenes herredsretts dom av 1. juli 1998 (saknr. 98-00235).

Oslo tingretts dom av 10. mars 2005 (TOSLO-2004-84792).

Ringerike herredsretts dom av 13. desember 2001 (saknr. 01-00552 M).

Stavanger tingsretts dom av 19. august 2003 (02-634 M og 02-635 M).

Avgjørelser fra Personvernnenmda

PVN-2006-07 (Tysvær kommune)

PVN-2006-05 (Oxigeno Fitness)

PVN-2006-09 (Oslo Trimsenter)

PVN-2006-10 (Esso Norge)

PVN-2006-11 (Rema 1000)

Praksis fra den europeiske menneskerettighetsdomstol

AEIHRE (2007)	Association for Eurpoean Integration and Human Rights and Ekimdzhiev v. Bulgaria, dom 28. juni 2007
Amann	Amann v. Sveits, dom av 16. februar 2000
Copland (2007)	Copland v. Storbritannia, dom 3. april 2007
Gillan og Quinton (2010)	Gillan og Quinton v. Storbritannia, dom 12. januar 2010
Goodwin (2002)	Goodwin v. Storbritannia, dom 11. juli 2002
Halford (1997)	Halford v. Storbritannia, dom 25. juni 1997
K.U. (2008)	K.U. v. Finland, dom 2. desember 2008
Kudeshkina (2009)	Kudeshkina v. Russland, dom 26. februar 2009
Klass (1978)	Klass v. Tyskland, dom 6. september 1978
Malone (1984)	Malone v. Storbritannia, dom 2. august 1984

Leander (1987)	Leander v. Sverige, dom av 26. mars 1987
Liberty (2008)	Liberty v. Storbritannia, dom 1. juli 2008
M.C. (2003)	M.C. v. Bulgaria, dom 4. desember 2003
Osman (1998)	Osman v. Storbritannia, dom 28. oktober 1998
Peck (2003)	Peck v. Storbritannia, dom 28. januar 2003
P.G. og J.H. (2001)	P.G. og J.H. v. Storbritannia, dom 25. september 2001
Rotaru (2000)	Rotaru v. Romania, dom av 4. mai 2000
Schüssel (2002)	Schüssel v. Østerrike 42409/98, 21. februar 2002 EMK
Times (2009)	Times Newspapers Ltd. (Nos. 1 and 2) v. Storbritannia, dom 10. mars 2009
Von Hannover (2004)	Von Hannover v. Tyskland, dom 24. juni 2004
Weber og Saravia (2006)	Weber og Saravia v. Tyskland, beslutning av 29. juni 2006
X & Y (1985)	X & Y v. Nederland, EMD 26. mars 1985
Z (1988)	Z v. Østerrike, 13. april 1988. Avgjørelse av kommisjonen.

Andre utenlandske avgjørelser

”Pirate Bay”	Stockholm tingsrätts dom av 17. april 2009 (mål nr B 13301-06)
”SABAM”	Tingretten i Brussel, avgjørelse av 28. juni 2007 (sak nr. 04/8975/A)

LITTERATUR

Access Data (2006)	MD5 Collisions. White Paper. 2006. http://www.accessdata.com/media/en_US/print/papers/wp.MD5_Collisions.en_us.pdf (besøkt 15. desember 2008).
Adler (1995)	Adler, Michael *Cyberspace, General Searches, and Digital Contraband.* 105 Yale L.J. 1995-1996 s. 1093-1120.
Alvestrand (2009)	Alvestrand, Harald and Håkon Wium Lie *Development of Core Internet Standards: The Work of IETF and W3C.* Internet Governance. Infrastructure and Institutions. Lee A. Bygrave og Jon Bing (red.). 2009, s. 126-146.
Andenæs/Matningsdal/ Rieber-Mohn (2004)	Andenæs, Johs., Magnus Matningsdal og Georg Fredrik Rieber-Mohn *Alminnelig strafferett*. 5. utg. Oslo, 2004.
Andenæs/Fliflet (2006)	Andenæs, Johs. og Arne Fliflet *Statsforfatningen i Norge.* 10. utg. Oslo, 2006.
Andenæs/Andorsen (2008)	Andenæs, Johs. og Kjell V. Andorsen *Spesiell strafferett og formuesforbrytelsene.* Oslo, 2008.
Andenæs/Myhrer (2009)	Andenæs, Johs. og Tor-Geir Myhrer *Norsk straffeprosess.* 4. utg. Oslo, 2009.
Andersen (2003)	Andersen, Mads Bryde *Fragmenter af en informationsretlig grundregulering.* Festskrift til Mogens Koktvedgaard. København, 2003.
Andersen (2005)	Andersen, Mads Bryde *IT-retten.* 2. utg. København, 2005
Aquilina (2008)	Aquilina, James M., Eoghan Casey og Cameron H. Malin *Malware forensics.* Massachusetts, 2008.
Aschehoug (1995)	Henriksen, Petter … [et al.]. *Aschehoug og Gyldendals Store Norske Leksikon*. 3. utg. Oslo, 1995.
Barendt (2005)	Barendt, Eric *Freedom of Speech.* 2. utg. Oxford, 2005.
Benkler (2000)	Benkler, Yochai *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access.* 2000. 52 Fed. Comm. L.J. 561 (2000).
Berulfsen (1986)	Berulfsen, Bjarne og Dag Gundersen *Blå fremmedordbok.* 15.utg. Oslo, 1986.
Bing (1982)	Bing, Jon *Rettslige kommunikasjonsprosesser.* Oslo, 1982.
Bing (2008)	Bing, Jon *Ansvar for ytringer på nett.* Oslo, 2008.
Bjerke (2001)	Bjerke, Hans Kristian og Erik Keiserud *Straffeprosessloven med kommentarer*. 3. utg. Oslo, 2001.
Bygrave (2006)	Bygrave, Lee A. *The Meaning of «Data» and Similar Concepts.* Festskrift til Peter Seipel. Cecilia Magnusson, Peter Wahlgren (red.), Stockholm, 2006, s. 117-126.

Caloyannides (2004)	Caloyannides, Michael A. *Privacy Protection and Computer Forensics.* 2. utg. Boston, 2004.
Casey (2004)	Casey, Eoghan *Digital evidence and computer crime.* 2. utg. Amsterdam, 2004.
Castells (2000)	Castells, Manuel *The rise of the network society.* Singapore, 2000.
Deibert (2008)	Deibert, Ronald m.fl. (red.) *Access Denied.* Harvard, Mass., USA, 2008.
Dyrnes (2004)	Dyrnes, Anne-Mette *Inndragning: Hva må gjøres?* Oslo, 2004.
Eckhoff (2001)	Eckhoff, Torstein og Jan E. Helgesen *Rettskildelære.* 4. utg. Oslo, 2001.
Economist (2008)	*Let it rise. A special report on corporate IT.* October 25th 2008.
Eggen (2002)	Eggen, Kyrre *Ytringsfrihet.* Oslo, 2002.
Eide (2001)	Eide, Erling og Endre Stavang *Rettsøkonomi* Oslo, 2001.
Eng (2007)	Eng, Svein *Rettsfilosofi.* Oslo, 2007.
Eskeland (2006)	Eskeland, Ståle *Strafferett.* 2. utg. Oslo, 2006.
EØS-rett (2004)	EØS-rett. Frederik Sejersted m.fl. 2. utg. Oslo, 2004.
Falkanger (2007)	Falkanger, Thor og Aage Thor Falkanger *Tingsrett.* 6. utg. Oslo, 2007.
Frost (2002)	Frost, Kim *Informationsydelsen*. København, 2002.
Fuller (1967)	Fuller, Lon L. *Legal Fictions.* Stanford, USA, 1967.
Gaustad (2002)	Gaustad, Terje *The Problem of Excludability for Media and Entertainment Products in New Electronic Market Channels.* Electronic Markets Vol. 12 (4). 2002 s. 248-251.
Giddens (1990)	Giddens, Anthony *The consequences of Modernity.* Stanford, USA, 1990.
Goldsmith (2006)	Goldsmith, Jack and Tim Wu *Who controls the Internet?* Oxford, 2006.
Harris (2009)	Harris, David J., Colin Warbrick and M. O'Boyle *Law of the European Convention on Human Rights.* Oxford, 2009.
Hannemyr (2005)	Hannemyr, Gisle *Hva er internett.* Oslo, 2005.
Hauge (1990)	Hauge, Ragnar *Narkotika og delegasjon av lovgivningsmyndighet.* Lov og Rett 1990 s. 169-174.
Hov (2007)	Hov, Jo *Rettergang II*. Oslo, 2007.
Hubbard (2005)	Hubbard, Phillip A. *Making Sense of Search and Seizure Law* Durham, USA, 2005.
Interpol (2009)	Interpol, General Assembly *Combating sexual exploitation of children on the internet using all available technical solutions, including access-blocking by Interpol member countries* Report no. 10, 7. august 2009.
Irgens-Jensen (2008)	Irgens-Jensen, Harald *Bedriftens hemmelighet - og rettighet?* Oslo, 2008 Avhandling / Universitetet i Oslo. Institutt for privatrett).

Jacobsen (2008)	Jacobsen, Jørn RT *Fragment til forståing av den rettsstatlege strafferetten.* Bergen, 2008 (avhandling PhD/ Universitetet i Bergen).
Kalsnes (2009)	Kalsnes, Bente *Krigen mot kidsa.* Morgenbladet, 24. april 2009. http://www.morgenbladet.no/apps/pbcs.dll/article?AID=/20090424/OAKTUELT/200362984 (besøkt 17. august 2009)
Kempf (2004)	Kempf, J and R. Austein *The Rise of the Middle and the Future of End-to-End.* 2004. (RFC 3724).
Kerr (2006)	Kerr, Orin S. *Computer Crime Law.* American Casebook Series. 2006.
Kjerschow (1930)	Kjerschow, P. *Almindelig borgerlig straffelov av 22. mai 1902 og Lov om den almindelige borgerlige straffelovs ikrafttreden av 22. mai 1902.* Oslo, 1930.
Klang (2006)	Klang, Mathias *Disruptive Technology.* Göteborg, 2006. http://www.digital-rights.net/?page_id=1233.
Klamberg (2009)	Klamberg, Mark *FRA:s signalspaning ur ett rättsligt perspektiv.* Svensk Jurist Tidning (SvJT) nr. 4 /2009 s. 519 flg.
Knetzger (2008)	Knetzger, Michael og Jeremy Muraski *Investigating High-Tech Crime.* New Jersey, 2008.
Kolflaath (2004)	Kolflaath, Eivind *Språk og argumentasjon – med eksempler fra juss.* Bergen, 2004.
Koops (2006)	Koops, Bert-Jaap *Should ICT regulation be technology-neutral?* Starting Points for ICT Regulation. Bert-Jaap Koops m.fl. (red.), Haag, 2006, s. 77-108.
Kristensen (1996)	Kristensen, Terje *Datateknologi og kommunikasjon.* Oslo, 1996.
Lau Hansen (2001)	Lau Hansen, Jesper *Informationsmisbrug.* København, 2001.
Lemley (2003)	Lemley, Mark A. *Place and Cyberspace.* 91 Cal. L. Rev. 521. (2003).
Lessig (1999)	Lessig, Lawrence *Code and other laws of cyberspace.* New York, 1999.
Lessig (2002)	Lessig, Lawrence *The future of ideas*. New York, 2002.
Lessig (2006)	Lessig, Lawrence *Code version 2.0.* New York, 2006.
Lyon (2001)	Lyon, David *Surveillance society P*hiladelphia. USA (opptrykk, 2005).
Mestad (2009)	Mestad, Ola. *Rettens kilder og anvendelse.* Knophs oversikt over Norges rett. 13. utg. Oslo, 2009, s. 5-29.
Matningsdal (1987)	Matningsdal, Magnus *Inndragning.* Oslo, 1987.
Matningsdal (1995)	Matningsdal, Magnus og Anders Bratholm, *Straffeloven med kommentarer*. Anden del. Oslo, 1995.
Matningsdal (2003)	Matningsdal, Magnus og Anders Bratholm, *Straffeloven med kommentarer.* Første del. 2. utg. Oslo, 2003.
Murdoch (2008)	Murdoch, Steven J. and Ross Anderson *Tools and Technology of Internet Filtering.* Deibert (2008) s. 57-72.
Murray (2007)	Murray, Andrew D *The Regulation of Cyberspace* New York, USA, 2007.

Negroponte (1997)	Negroponte, Nicholas *Det digitale liv.* 2. utg. Århus, Danmark, 1997.
O'Reilly (2005)	O'Reilly, Tim *What is Web 2.0 – Design Patterns and Business models for the Next Generation of Software*. International Journal of Digital Economics 65. 2007, s. 17-37.
Ohm (2005)	Ohm, Paul *The Fourth Amendment Right to Delete* 119 Harvard Law Review Forum 10 (2005).
Post- og Teletilsynet (2008)	Post- og teletilsynet *Om nettnøytralitet.* Oslo, 5. mai 2008.
Riisnæs (2007)	Riisnæs, Rolf *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar*. Bergen, 2007.
Rognstad (2008)	Rognstad, Ole-Andreas *Opphavsrettens balanse. Avtale eller lovregler?* Festskrift til Marianne Levin. Stockholm, 2008, s. 521-545.
Rognstad (2009)	Rognstad, Ole-Andreas og Birger Stuevold Lassen *Opphavsrett*. Oslo, 2009.
Salgado (2005)	Salgado, Richard P. *Fourth Amendment Search and the Power of the Hash.* Harvard Law Review Forum. 2005, s. 38-46.
Saltzer (1981)	Saltzer, J.H., D.P. Reed and D.D. Clark End-*to-End arguments in System Design.* Boston, USA, 1981.
Schartum (2002)	Schartum, Dag Wiese *Fra rettsstat til rettsstatsautomat.* Digital makt: informasjons- og kommunikasjonsteknologiens betydning og muligheter. Tore Slaatta (red). Oslo, 2002, s. 118-135.
Schartum (2004)	Schartum, Dag Wiese og Lee A. Bygrave *Personvern i informasjonssamfunnet*. Bergen, 2004.
Schartum (2007)	Schartum, Dag Wiese *Elektronisk forvaltning og jus*. Elektronisk forvaltning i Norden. Dag Wiese Schartum (red.). 2007, s. 17-32.
Schellekens (2006)	Schellekens, M. *What Holds Off-Line, Also Holds On-Line?* Starting Points for ICT Regulation. Bert-Jaap Koops m.fl. (red.), Haag, 2006, s. 51-76.
Seipel (1977)	Seipel, Peter Computing Law. *Perspectives on a New Legal Discipline.* Stockholm, 1977.
Seipel (2004)	Seipel, Peter *Juridik och IT: Introduktion till rättsinformatiken.* 8. utg. Stockholm, 2004.
Sieber (1989)	Sieber, Ulrich *Informationsrecht und Recht der Informationstechnik – Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen.* Neue Juristische Wochenschrift (NJW), München, 1989, Heft 41, s. 2569 flg.
Sieber (2006)	Sieber, Ulrich *Cybercrime and Jurisdiction in Germany.* The Present Situation and the Need for New Solutions. Cybercrime and Jurisdiction. A Global Survey, s. 183-210. Bert-Jaap Koops og Susan W. Brenner (reds.) Haag, 2006.
Sieber (2008)	Sieber, Ulrich og Malaika Nolde *Sperrverfügungen im Internet (Entwurf (Version 0.9))*. Utredningen er utgitt som bok under samme tittel, Berlin (2008).
Singh (2000)	Simon Singh *The Code Book.* London, 2000.

Skeie (1946)	Skeie, Jon *Den norske strafferett.* 2. utg. Oslo, 1946.
Spannbrucker (2004)	Spannbrucker, Christian *Convention on Cybercrime (ETS 185) - Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht.* Regensburg, 2004 (avhandling /Universität Regensburg; der Juristischen Fakultät).
Staksrud (2002)	Staksrud, Elisabeth *Ytringsfrihet og sensur på Internett. Politisk regulering og kommersiell filtrering.* Digital makt. Informasjons- og kommunikasjonsteknologiens betydning og muligheter. Tore Slaatta (red.), Oslo 2002, s. 64-94.
Storsul (2008)	Storsul … [et al.] *Nye nettfenomener – Staten og delekulturen.* Oslo, 2008 (utgitt ved Institutt for Medier og Kommunikasjon ved Universitetet i http://www.itu.no/filearchive/NyeNettfenomener.pdf (besøkt 02. januar 2010).
Stuevold Lassen (2009)	Stuevold Lassen, Birger *Åndsretten.* Knophs oversikt over Norges rett. 13. utg. Oslo, 2009, s. 472 flg.
Sunde (2005)	Sunde, Inger Marie *Politi, pirateri og kodeknekking.* Tidsskrift for strafferett. 2/2005, s. 161-181.
Sunde (2006)	Sunde, Inger Marie *Lov og rett i cyberspace.* Bergen, 2006 (ØKOKRIMs skriftserie nr. 16).
Sunde (2008)	Sunde, Inger Marie *Beskyttelsen mot overvågning i den fysiske og elektroniske verden.* Det 38. nordiske juristmøte. København 2008. http://www.juraportal.dk/njm/495/
Taipale (2007)	Taipale, Kim A. *Why can't we all get along? Cybercrime – Digital cops in a Networked Environment.* Jack M Balkin m.fl. (red.) NYU Press, USA, 2007, s. 151-183.
Tapscott (2008)	Tapscott, Don and Anthony D. Williams *Wikinomics.* London, 2008.
Udsen (2009)	Udsen, Henrik *De informationsretlige grundsætninger.* København, 2009.
Vacca (2002)	Vacca, John R. *Computer forensics: computer crime scene investigation.* Massachusetts, USA, 2002.
Van Dijk (2006)	Van Dijk, Pieter … [et al]. *Theory and practice of the European Convention on Human Rights.* 4. utg. Oxford, 2006.
Wagle (1997)	Wagle, Anders Mediaas og Magnus Ødegaard jr. *Opphavsrett i en digital verden.* Oslo, 1997.
Walden (2007)	Walden, Ian *Computer Crimes and Digital Investigations.* Oxford, 2007.
Wall (2007)	Wall, David S. *Cybercrime: the transformation of crime in the information age.* Cambridge, 2007.
Wayman (2005)	Wayman, James … [et al.] *An Introduction to Biometric Authentication Systems.* Biometric Systems: Technology, Design and Performance Evaluation. London, 2005.
Wiener (1988)	Wiener, Norbert *The human use of human beings: Cybernetics and society.* Cambridge, 1988. Opptrykk fra utgave 1954. Første gang utgitt 1950.

Willassen (2008)	Willassen, Svein *Methods for Enhancement of Timestamp Evidence in Digital Investigations* (avhandling / Phd. NTNU 2008:19), Trondheim, 2008.
Yttri Dahl (2009)	Yttri Dahl, Johanne og Ann Rudinow Sætnan *«It all happened so slowly» - On controlling function creep in forensic DNA databases*. International Journal of Law, Crime and Justice nr. 37. 2009, s. 83-103.
Zittrain (2003)	Zittrain, Jonathan *Internet Points of Control.* Boston College Law Review, 2003 (44 B.C.L. Rev. 653).
Zittrain (2006a)	Zittrain, Jonathan *Without a Net*. Legal Affairs, 2006 (2006-FEB Legal Aff. 32).
Zittrain (2006b)	Zittrain, Jonathan *The Generative Internet.* Harvard Law Review, 2006 (119 Harv. L. Rev. 1974).
Zittrain (2008a)	Zittrain, Jonathan *The future of the Internet.* London, UK, 2008.
Zittrain (2008b)	Zittrain, Jonathan and John Palfrey *Internet Filtering: The Politics and Mechanisms of Control.* Access Denied. Deibert (2008) s. 29-56.

ANNET

Personlige meddelelser: Fagerland, Snorre. E-post. 16. mai 2007 (i arkiv hos meg).

Netthenvisninger:

Fra litteraturliste:

Access Data (2006): http://www.accessdata.com/media/en_US/print/papers/wp.MD5_Collisions.en_us.pdf

Kalsnes (2009): http://www.morgenbladet.no/apps/pbcs.dll/article?AID=/20090424/OAKTUELT/200362984

Klang (2006): http://www.digital-rights.net/?page_id=1233.

O'Reilly (2005): http://www.oreillynet.com/lpt/a/6228.

Saltzer (1981): http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.mss

Storsul (2008): http://www.itu.no/filearchive/NyeNettfenomener.pdf

Sunde (2008): http://www.juraportal.dk/njm/495/

Wikipedia:
Om kryptering og lengden på nøkkelen/betydningen for sikkerheten:
http://en.wikipedia.org/wiki/Key_size

Om hvordan tjenester på nettet sømløst kan smeltes sammen: http://en.wikipedia.org/wiki/Mashup_(digital)

Om hash teknologi: http://en.wikipedia.org/wiki/Cryptographic_hash_function (besøkt 21. oktober 2008)

Om krypteringsnøkler: http://en.wikipedia.org/wiki/Key_size (besøkt 11.11.09).

Om ormen Slammer: http://en.wikipedia.org/wiki/SQL_slammer_(computer_worm) (besøkt 31.3.2009)

Annet:
Om EUs Safer Internet program og tiltak mot overgrepsbilder på nett: www.circamp.eu.

Nasjonalbibliotekets hjemmeside www.nb.no (besøkt 10.3.9).

Om Open Net Initiative: http://opennet.net.

Om ord på nett: www.ordnett.no (besøkt 27.7.2009)

Teknologien bak Pirate Bay: http://www.vg.no/pub/vgart.hbs?artid=572013 (besøkt januar 2010)

Om kodeknekking: Artikkel i PC-world.
http://www.pcworld.com/article/132184/researcher_rsa_1024bit_encryption_not_enough.html

http://www.pcworld.com/article/132184/researcher_rsa_1024bit_encryption_not_enough.html (besøkt 11.11.09).

Om IPhone-ormen: http://www.sophos.com/blogs/gc/g/2009/11/08/iphone-worm-discovered (besøkt 16.11.09)

Overvåkingsrapporten bestilt av det britiske datatilsynet (Wood (2006))
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

En oversikt over Ulrich Siebers publikasjoner: http://www.mpicc.de/ww/en/pub/home/sieber/sieber_publ.htm

Forklarende rapporter til 185 og 201 ETS: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm,
http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm