Automatisert rettshåndhevelse på nettet

Av Inger-Marie Sunde

Summary

What is the meaning of the proposition that the law applies to the Internet? The current article examines this proposition in relation to criminal law and to the widespread problems of malware and sexual abuse material of children (child pornography). These problems bear the marks of perpetuity and gross worldwide accumulation due to the computer's capacity for making duplicate files. There is a gap between the aims of the proposition and its current enforcement. If judicial enforcement of criminal law is limited to personal sanctions, e.g., imprisonment or a fine, then digital contraband falls outside the enforceable scope of the law. Given that criminal law already allows the application of sanctions to objects, for instance by confiscation of assets and contraband, one may envisage the application of these confiscation rules to illegal computer files, thus treating them as objects within the meaning of the law. The rules of confiscation thereby provide a legal basis for the filtering of illegal content on the Internet. This means that the criminal law can be enforced with practical effect to digital contraband within the ordinary framework of judicial review and fair trial. The filters required for enforcement can be implemented by national internet service providers. Furthermore, records containing the identity of each confiscated duplicate file can be swiftly shared between law enforcement agencies internationally, and deployed in national filters based on harmonized rules of criminal law. The end result is an enhanced and internationally concerted effort to discontinue gross violations of the privacy of victims displayed on sexually illicit material. This enforcement approach would be less effective against malware, however, due to the extensive time required for investigation and prosecution. In conclusion, application of the rules of confiscation with a view to subsequent international cooperation against digital contraband exploits the benefits of a harmonized criminal law without jeopardizing the fundamental rights of the individual.[*]

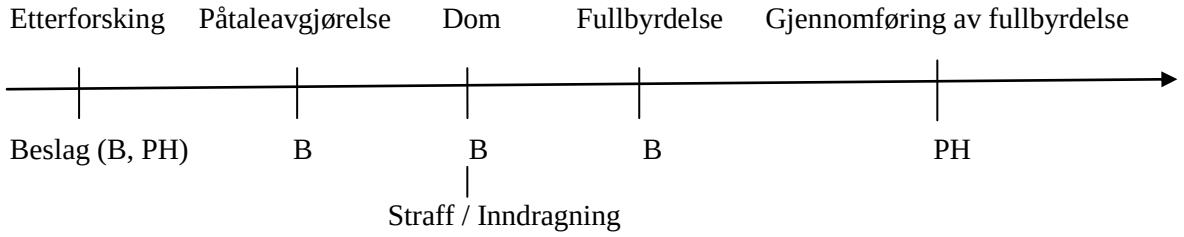
1. Tema

Det hersker bred enighet om at loven gjelder på internett, men hva betyr det egentlig? Jeg skal ikke undersøke påstanden i sin fulle bredde, men nøye meg med å se på rettshåndhevelse overfor noen straffbare handlinger som medfører rettsstridig innhold på internett. Spørsmålet er om påstanden om at loven gjelder på nettet innebærer at loven kan *håndheves* på nettet i en *praktisk operasjonaliserbar* forstand. Og kan i så fall inndragningsreglene gi hjemmel for de rettshåndhevende tiltak?

Rettshåndhevelse i form av inngrep i borgernes rettssfære krever hjemmel i lov og må skje i betryggende former for å ivareta rettssikkerheten.[1] Rettshåndhevelse er en normativt styrt prosess som går i faser. Den innledes med etterforsking, det tas beslag, treffes påtaleavgjørelse, avsies dom og beordres fullbyrdelse. Deretter iverksettes praktiske tiltak som å få domfelte inn på soning og å

[*]Title in English: Confiscation of duplicate files on the Internet

innkreve bøter. Også andre reaksjoner kan være på tale og jeg kommer her til temaet for artikkelen, nemlig destruksjon av objekter som er inndratt (konfiskert).
Vi kan forholde oss til følgende hendelser på en tidslinje, hvor 'B' betyr Beslutning og 'PH' betyr Praktisk Handling:



Inndragning er en strafferettslig reaksjon.[2] Det er reglene om inndragning av objekter som er relevante. I norsk rett er hjemmelen straffeloven 1902 § 35, som gjelder "inndragning" av "ting". I dansk rett er hjemmelen straffeloven § 75 stk.2, som gjelder "konfiskation" av "genstande". I svensk rett er hjemmelen BrB 36 kap. 2 § om "förverkande" av "egendom".

For så vidt gjelder kriminalitetsformene avgrenser jeg til befatning med skadelig dataprogram ("malware") og overgrepsbilder (jeg unngår betegnelsen "barnepornografi", fordi "pornografi" ikke beskriver det alvorlige overgrepet mot barnets integritet som fotografering og spredning på nettet innebærer). Analysen er også relevant for pirateri av digitaliserte åndsverk på nettet, men av plasshensyn har jeg avgrenset mot dette problemet.

I henhold til internasjonale instrumenter skal befatning med slikt materiale undergis omfattende kriminalisering ved at produksjon (fremstilling), anskaffelse, besittelse og spredning gjøres straffbart. Det kan vises til Europarådets konvensjoner av 2001 ETS nr. 185 (datakrim) og 2007 CETS nr. 201 (om beskyttelse av barn mot seksuell utnyttelse og overgrep). Datakrimkonvensjonen artikkel 6 nr. 1 a (i) og b, gjelder befatning med skadelig dataprogram og artikkel 9 overgrepsbilder. CETS 201 artikkel 20 gjelder overgrepsbilder. Dette gjelder også tilleggsprotokollen av 25. mai 2000 til FNs barnekonvensjon, artikkel 3 bokstav c. Videre foreligger to rammebeslutninger fra EU om angrep mot informasjonssystemer av 24. februar 2005, og mot overgrepsbilder m.v. av 22. desember 2003.

Det er adgang til å reservere seg mot befatningsforbudet for skadelig dataprogram, jf. artikkel 6 nr. 3, jf. nr. 1 a (i) og artikkel 42. Norge har benyttet reservasjonsadgangen, men den kan på sikt trekkes fordi straffeloven 2005 § 201 gjennomfører kriminaliseringsforpliktelsen fullt ut. Straffeloven 2005 antas å tre i kraft rundt 2015. Etter straffeloven 2005 § 201 rammes fremstilling, anskaffelse, besittelse og tilgjengeliggjøring av skadelig dataprogram når det skjer med forsett om å begå en straffbar handling. Danmark har verken en selvstendig bestemmelse om befatningsforbud, eller noen reservasjon mot datakrimkonvensjonen artikkel 6 a (i) og b. Det må bety at reglene om forsøk og medvirkning til datainnbrudd og hindring av bruk av datasystem, anses å oppfylle den folkerettslige forpliktelsen.[3] Sverige undertegnet datakrimkonvensjonen i 2001, men har ennå ikke ratifisert og behøver ikke følge konvensjonens forpliktelser.
Under enhver omstendighet har alle de tre landene straffesanksjonerte forbud mot datainnbrudd, angrep på tilgjengeligheten til datasystem, og mot uberettiget endring, sletting og undertrykkelse av data, jf. norsk straffelov 1902 §§ 145 annet ledd og § 291; dansk straffelov §§ 263 stk. 2 og 293 stk. 2; og i Sverige: BrB 4 kap. 9 c §. Ved disse bestemmelsene, eventuelt supplert med reglene om forsøk og medvirkning, kan spredning av skadelig dataprogram rammes.

Reservasjonsadgangen vedrørende overgrepsbilder er snevrere, og globalt kan man i hvert fall legge til grunn at stater har kriminalisert spredning av overgrepsbilder med barn inntil 14 år. I de skandinaviske land er fotografering, spredning og besittelse av overgrepsbilder straffbart. Det samme

gjelder anskaffelse mot vederlag. Det følger av norsk straffelov 1902 § 204a (og straffeloven 2005 § 311); dansk straffelov §§ 230 og 235 og i Sverige av BrB 16 kap. 10 a §. Av de nevnte bestemmelsene følger det også at man legger til grunn en aldersangivelse inntil 18 år med hensyn til hvem som anses som barn.

Det er *spredningen* og den forutgående *besittelsen* av skadelig dataprogram og overgrepsbilder, som er av interesse for artikkelens tema.

Inndragning er et virkemiddel for å effektivisere håndheving av straffebudene. Gjennom inndragning fratas lovbryteren eiendeler som utgjør utbyttet av den straffbare handling, eller ting / gjenstander som på annet vis er relatert til lovbruddet. Utbyttealternativet anses ikke å være relevant for materialet det her er tale om. Materialet kan sammenlignes med narkotika, dvs. at det er uten lovlig omsetningsverdi (”kontrabande”). Siden materialet består av datafiler kan det kalles ”digital kontrabande”.

Adgangen til å inndra objekter bestemmes av forholdet mellom det spesifikke objektet og den straffbare handlingen. Generelt baserer reglene seg på en tredeling. De gjelder objekter (”ting” / ”genstande” / ”egendom”) som (i) har vært brukt eller ment å brukes for å begå en straffbar handling *(instrumentum sceleris)*; (ii) er produkt av en straffbar handling *(productum sceleris);* og (iii) som har vært involvert i en straffbar handling *(corpus delicti).*[4]

Alle de tre kategoriene omfattes av de skandinaviske internrettslige inndragningsreglene som er nevnt over. Jeg går ikke inn på de konkrete bestemmelsene som sådan, som kan tenkes å ha noe ulikt innhold og rekkevidde. I Sverige er man skeptisk i det hele tatt til å anse data som et objekt. Dette er uttrykt i forbindelse med beslag, jf. RB 27 kap. 1 §, som bruker ordet ”föremål” til forskjell fra förverkandebestemmelsen som bruker ”egendom”, jf. BrB 36 kap. 2 §.

Lindberg (2009) s. 388-389 skriver at ”Det är inte heller möjligt att ta något immaterielt i beslag. Det är därför omdiskuterat i vilken utsträckning reglerna om beslag kan tillämpas på information som endast finns i elektronisk form utan att ha lagrats på en fysisk databärare.” Jeg tror noe av denne usikkerheten kan tilskrives at man i svensk straffeprosessrett ikke har skilt klart mellom data og informasjon. Se Sunde (2011) s. 175 med kritikk av SOU 1992:110 kap. 4.6.2. Utredningen av 1992 regnes som foreldet (Lindberg (2009) s. 539), men det synes fortsatt å være behov for en strafferettslig og prosessuell avklaring av forholdet mellom data og informasjon, se Ds 2005: 6 *Brott och brottsutredning i IT-miljö*, s. 99: ”Datorbehandlingsbara uppgifter räknas [som immateriell egendom]” som ikke kan være gjenstand for skadeverk. Dataene har bare indirekte vern gjennom beskyttelsen mot datainnbrudd (s. 215) og BrB4 kap. 9 c §. Sitatet nevner ”uppgifter”, dvs. det som på norsk kalles ”opplysninger”. Begrepet ’uppgift’ antas å være snevrere enn ’informasjon’, dvs. at det kan finnes databasert informasjon som ikke er ”uppgift”. Underholdningsfilm på skjermen kan være et eksempel. Sitatet tar heller ikke stilling til om data som medium (informasjonsbærer) kan ha et selvstendig strafferettslig vern, uavhengig av hvilken type informasjon de bærer.

I norsk rett synes man å være mer åpen for at data er et objekt i seg selv, således kan data tas i beslag som ”ting”, jf. straffeprosessloven § 203.[5] Og i den norske straffeloven av 2005 bestemmes det uttrykkelig at data anses som ”ting” i inndragningsreglenes forstand, jf. § 69, som sier at som ting regnes også ”rettigheter, fordringer og *elektronisk lagret informasjon*” (min uth.). Formuleringen anses som en direkte videreføring av gjeldende rett etter straffeloven 1902.[6] Loven gir således hjemmel for inndragning av data *de lege lata.*

Denne artikkelens formål er å vurdere om reglene om inndragning / konfiskation / förverkande rent konseptuelt kan danne rettslig grunnlag for destruksjon av datafiler ved filtrering, blokkering og eventuelt sletting. Behovet for enkelte lovtilpasninger kan vurderes i lys av de linjer som her trekkes opp. Slik jeg ser det er dette et spørsmål om gjeldende inndragningsregler kan operasjonaliseres slik at de kan håndheves med praktisk og konkret effekt for datafiler med ulovlig innhold på internett.

Jeg tar utgangspunkt i *gjeldende* regler. Karakteristisk for en rettsregel er at den gjelder generelt og over tid. Om det enn kan synes trivielt bør det fastslås at nye fenomener som lovgiver ikke tenkte på da bestemmelsene ble vedtatt, kan være dekket av *regelen* som *bestemmelsen* gir opphav til. Utgangspunktet bør derfor være at håndtering av fenomener forårsaket av ny teknologi ikke nødvendigvis krever nye regler.[7] Fordelen er at de nettopp er gjeldende og uten videre kan tas i bruk. Lovgiver har selvfølgelig frihet til å vedta et nytt sett bestemmelser for det formål jeg beskriver, men hvis eksisterende regler i hovedsak er dekkende er en slik lovgivningsinnsats unødvendig.

2. Kriminalitetsproblemet: Dubletter[8]

Da internett ble tatt i allmenn bruk på 1990-tallet, berømmet man nettets evne til å gi informasjonsmakt til den individuelle bruker. Borgerens situasjon endret seg fra en ensidig posisjon som informasjons*konsument*, til en tosidig posisjon som innebar at man også var informasjons*produsent.* Og på toppen av det hele fikk borgeren et personlig verktøy for å *distribuere sin informasjon til sluttbrukere verden over*. Internett lot til å realisere den gamle visjonen om borgernes likeverdige deltakelse i samfunnsdebatten. Internett skapte en genuin markedsplass for ideer, og tilrettela for demokratiutvikling, rettferdighet, likhet og personlig autonomi.

Men la oss reflektere over ordet ”produsere” og relatere det til den digitale teknologiens fremtredende evne til å lage kopier. En kopi er lik originalen. Digitale kopier er ikke bare like, de er *identiske* med kildefilen. Derfor kalles de ”dubletter” (på engelsk: ”duplicates” / ”duplicate files”). Hver enkelt dublett er en representasjon av kildefilen. Nye dubletter kan kopieres av dubletten og de nye generasjoner dubletter er også lik kildefilen. Under slike tekniske forhold gir begrepet ”originalfil” sjelden mening; kanskje må uttrykket reserveres for den filen som ble fremstilt aller først, for eksempel ved digital fotografering eller ved programmering.[9]

Det definerende kriterium for dubletter er at de har samme *hash verdi* eller *sjekksum* (jeg foretrekker ordet ”sjekksum”). Sjekksummen bestemmes av et hashprogram. Hvorvidt filene er dubletter kan bare kontrolleres ved å sende filene gjennom hash programet. Dataprogrammet regner ut og sammenligner sjekksummene for å se om de er identiske. Innholdet i to filer kan se likt ut for det menneskelige øye. Likevel kan filene ha forskjellig sjekksum. Sjekksummen er en funksjon av filens bitverdi. En forskjell i bitverdi gir ikke nødvendigvis en synlig forskjell, men gir ulik sjekksum. I et slikt tilfelle er *informasjonen* slik den presenteres, identisk, men filene er *ikke* dubletter. Begrepet ’identisk’ har således forskjellig betydning for informasjon og data. For informasjon avgjør menneskelig vurdering hva som er identisk (eller likt), mens for data bestemmes identitet av tekniske kriterier.[10]

Dubletter er et meget utbredt fenomen som spiller en viktig rolle i data- og nettverksteknologien. I et praktisk brukerperspektiv lar det seg illustrere med noen eksempler:

Når jeg sender en e-post beholder jeg kildefilen i ”sendt boksen” mens adressaten mottar en dublett. Tilsvarende, når jeg sender en melding til en news-gruppe beholder jeg kildefilen mens et ubegrenset antall dubletter distribueres gjennom Usenet over hele verden. Når jeg skriver ut en word-fil, lagrer jeg kildefilen og sender en dublett til skriveren (printeren). Når jeg laster ned informasjon fra webben mottar jeg en dublett fra en kildefil som ligger på en proxy server i nærheten, mens den opprinnelige filen er lagret på en server mye lengre unna. Fildelingstjenester (”P2P” / ”torrent” teknologi) bruker referanselister med sjekksummene til filene som tilbys fra deltakerne på tjenesten. Listen sørger for at brukernes datamaskiner kan lokalisere og kopiere de filer man søker. Tjenesten sørger også for at datamaskinene samarbeider om å lage nye dubletter ved å laste ned *bits* av den filen man søker fra alle de datamaskinene som har den. Og samtidig som man laster ned kan datamaskinen *tilby bits* av den samme filen. På denne måten skjer fremstillingen av dubletter - som fildeling i realiteten er - enda raskere.

Teknologiens evne til å lage dubletter bidrar til rask og effektiv dataflyt. Baksiden av medaljen er at dubletter også utbres i form av skadelig dataprogram og overgrepsbilder. Kriminologen David S. Wall har treffende karakterisert problemet som *"the globalized aggregate volume"*.[11] Med dette mener han at det ikke er det individuelle tilfelle, men den oppsamlede mengden materiale, som kjennetegner problemet. Og problemet er varig. Uten sletting eller lignende tiltak utbres dubletter fra stadig nye kilder og akkumuleres i stadig større mengde, noe som leder til varig krenkelse av rettslig vernede interesser.

Skadelig dataprogram spres med eksponentielt økende takt fordi hver dublett kopieres til nye vertsmaskiner i nettet, som igjen lager et ubegrenset antall nye dubletter som spres til andre maskiner osv. Over flere tiår har datasikkerhetsbransjen brukt hash teknologi i filtre som identifiserer og blokkerer skadelig dataprogram i form av dubletter. Jeg kaller det "antivirus teknologi" for å anskueliggjøre hva jeg mener, uten noen pretensjon om at betegnelsen er teknisk korrekt. Imidlertid, slik filtrering er et av flere tiltak for å begrense problemet.

Den kontinuerlige fremstillingen av dubletter medfører også at overgrepsbilder akkumuleres på nettet til tross for mange initiativ for å hindre det. På internasjonalt nivå uttrykkes bekymring over at nettverksteknologien leder til en forverring av problemet. De Jeg vil her trekke frem noen sitater fra internasjonale instrumenter. Fortalen i Europarådets konvensjon av 2007 om beskyttelse av barn mot seksuell utnyttelse og overgrep (CETS nr. 201) sier følgende:

"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), and that preventing and combating such sexual exploitation and sexual abuse of children require international co-operation".

I fortalen til tilleggsprotokollen til FNs barnekonvensjon, om salg av barn, barneprostitusjon og barnepornografi, av 25. mai 2000, uttrykkes det at man er

"… bekymret over at barnepornografi stadig blir mer tilgjengelig på Internett og annen ny teknologi, og [henvisning til konklusjonen i Wien-konferansen 1999] ber om en kriminalisering i hele verden av produksjon, distribusjon, eksport, overføring, import, forsettlig besittelse og annonsering av barnepornografi, og som understreker betydningen av et tettere samarbeid og partnerskap mellom regjeringene og Internett-industrien".

I den forklarende rapporten til Europarådets datakrimkonvensjon punkt 93, står det at

"it is widely believed that such material [overgrepsbilder] 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".

Sitatene gjelder nettverksteknologiens betydning for seksuelle overgrep mot barn. Av det som har fremgått forstår man at overgrepsbildene spiller en sentral rolle som årsak til det globale problemet. Overgrepsbildene fyller en funksjon i forhold til å stimulere potensielle overgripere til faktisk å begå seksuelle overgrep mot barn (andre barn enn det på bildet). Dertil utløser konsumpsjon av bilder etterspørsel etter nye bilder, noe som medfører stadig nye seksuelle overgrep mot barn begått av produsentene av overgrepsbilder.[12] Selv om sitatene ikke uttrykkelig nevner dublettene krever det bare et minimum av teknisk innsikt å forstå at den globale tilgjengeliggjøringen ikke bare skyldes tilførsel av nytt materiale fra forskjellige produsenter/overgripere, men også av den akkumulerte mengden overgrepsbilder.

Siden teknologien er "blind" for innholdets karakter, skulle man tro at velkjent "antivirus teknologi" også kan blokkere overgrepsbilder. I den digitale verden er data simpelthen data, og identitet bestemmes i henhold til tekniske kriterier.

Hvordan man skal designe et filter som kan fange opp slike tunge audiovisuelle filer som overgrepsbilder kan utgjøre (i motsetning til mindre programfiler med "datavirus") kan være et teknisk problem. Likeledes kan det være spørsmål om hvem skal betale for utviklingen av filterteknologien og for driften av filtrene. Men likevel, det er et faktum at teknologien finnes og kan brukes for å filtrere overgrepsbilder foruten skadelig dataprogram. Tekniske og økonomiske problemer kan løses. Det grunnleggende poenget er at *egenskapen av å være dublett* som gjør hash teknologien så nyttig og anvendelig, er den samme uansett hva innholdet består i.[13]

Gitt det store omfanget av automatisk genererte dubletter er det naturlig å reise spørsmålet om man i en normativ kontekst bør skille mellom "produksjon" og "reproduksjon". Med 'produksjon' forstår jeg en handling som skaper ny informasjon til sluttbrukerne, eller fremstiller nytt dataprogram til vertsmaskinene. 'Reproduksjon' er fremstilling av dubletter som et resultat av at *allerede eksisterende datafiler* "flyttes rundt" på datalagringsmedier eller sendes over nettverksforbindelser til andre lagringssteder / adressater. Reproduksjon er en teknisk integrert del av distribusjonsprosessen i et nettverk.[14] Effektiv distribusjon er viktig for å realisere verdiene opprinnelig assosiert med internett, men det betyr ikke at enhver sluttbruker som sender data til nettet bidrar med ny informasjon. Tvert imot består en stor andel av den tilgjengelige informasjon av dubletter, dvs. informasjon som var tilgjengelig fra før.

Reproduksjon fører til at rettsstridig innhold begynner "å leve sitt eget liv" på nettet uavhengig av hva lovbryteren videre foretar seg. Når innholdet først er spredt har lovbryteren tapt kontrollen, og om han angrer seg kan han ikke ta materialet tilbake. Det viderekopieres uten ytterligere handling fra den opprinnelige lovbryterens side. Bildet er en krenkelse av den psykiske integriteten og æren til barnet på bildet. Dublettene leder til at krenkelsen vedvarer.. For overgrepsbilder har norsk Høyesterett brukt karakteristikken *"livsvarig krenkelse"* av barnet på bildet, og uttalt at *"man må regne med at risikoen for at andre kommer over bildene vil være en betydelig tilleggsbelastning senere i livet for den det gjelder"* (Rt. 2002 s. 1187, s. 1192).

Men - som man forstår - ved rettshåndhevelse som tar i bruk teknologi beregnet på dubletter, kan innholdsproblemet begrenses. Inndragning / konfiskation / förverkande som fullbyrdes ved bruk av slik teknologi synes å være en mulig vei å gå.

3. Inndragning med virkning i den fysiske og digitale dimensjon

For analysens formål kan verden inndeles i to dimensjoner, nemlig den fysiske og den digitale. Individet utgjør forbindelsesleddet, så man kan si at gjennom det menneskelige grensesnittet smelter de to dimensjonene sammen til ett hele.

Et objekt som de to dimensjonene har felles er datafilen. I den fysiske "offline" dimensjonen lokaliseres datafilen på fysiske lagringsmedier. I den digitale "online" dimensjonen kan datafilen lagres og overføres over medier som er utenfor brukerens fysiske rekkevidde. Det betyr at datafilen kan "flyte" i et miljø spesielt laget for den. "Cloud computing" gjør skillet mellom data som er lagret og som overføres uklart. Det er mer realistisk å anse data for å være i konstant flyt. Det grafiske brukergrensesnittet på skjermen skaper inntrykk av at data er lagret på fast plasserte steder, mens de rent faktisk er i stadig flyt på grunn av tjenesteyternes kontinuerlige anstrengelser for å utnytte lagringsplass og båndbredde best mulig. Sluttbrukeren merker det ikke og kan stole på dataenes tilgjengelighet uavhengig av hvorfra de rent faktisk behandles og overføres.

"Cloud computing" innebærer at brukernes data og programutrustning først og fremst finnes på servere drevet av profesjonelle tilbydere. Eksempler er Google, iCloud (Apple) og Dropbox. Cloud computing har snudd situasjonen på hodet i den forstand at mens programutrustning og data tidligere primært ble lagret lokalt på sluttbrukerens personlige datamaskin, lagres de nå primært på serverne i "internettskyen". Det primære bevissikringsstedet er således de nevnte servere, ikke lokalt datautstyr. På grunn av dataflyten oppstår det som Spoenle (2010) kaller "loss of location". Han skriver at tjenesteyterne bruker "servers in different countries to store their user's data, which is being moved around constantly to minimize costs and maximize availability".

Og selv om datafilene som er lagret hos tjenesteyter er kontinuerlig tilgjengelige for sluttbruker, er datafilenes "exact location at a certain point of time practically indeterminable".[15]

Prinsipielt sett har rettslige beslutninger virkning overalt innen en jurisdiksjon. Med dette mener jeg at beslutningen kan fullbyrdes overalt bare det gjøres mot riktig part og gjelder riktig objekt. Det er derfor ikke noe i veien for å tenke seg at objekter kan inndras i den digitale dimensjonen likeså vel som i den fysiske. Dersom en datafil er konfiskerbar i den fysiske dimensjonen er den følgelig også konfiskerbar i den digitale. Spørsmålet gjelder lovens operasjonalisering i den digitale dimensjonen, dvs. om det på internett finnes en ekvivalent til fysisk berøvelse og destruksjon av det inndratte objekt.

4. Automatisert inndragning

Med henvisning til illustrasjonen i kapittel 1 minner jeg om at 'inndragning' betegnelser en *rettslig* beslutning med et bestemt innhold. Når dommen er rettskraftig beordres fullbyrdelse, hvoretter politiet gjennomfører permanent berøvelse ved salg eller destruksjon av objektet. For skadelig dataprogram og overgrepsbilder er det bare aktuelt å destruere, eller å gjøre materialet ubrukelig, siden det ikke har noen lovlig omsetningsverdi. Ellers er hovedregelen som kjent at inndratte objekter skal selges til fordel for statskassen.

Gjennomføring av inndragning i den digitale dimensjon må praktisk sett skje ved hindringer i dataflyten. Det kan gjøres ved bruk av filtre som gjenkjenner, blokkerer og kanskje også sletter dublettene basert på opplysning om sjekkummen.

For å kunne representere dette siste trinnet i en rettshåndhevende prosess må filtrene driftes på basis av rettslige instrukser. Driften omfatter oppdatering med sjekksummene til inndratte filer. Inndragning besluttes vanligvis av retten etter bevisførsel i hovedforhandling. Denne prosessen kan anvendes på datafiler på samme vis som andre objekter, og dermed ivaretas alminnelige sikkerhetsgarantier mot misbruk og vilkårlighet. Dette er ikke minst viktig fordi inndragning av dubletter har virkning for andre enn parten i straffesaken, dvs. individer som ikke har blitt hørt under saken (se umiddelbart nedenfor).

Fullbyrdelsesordre må gis som en instruks til filteret, dvs. at "dublett med sjekksum X skal filtreres". Praktisk sett kan det skje ved at sjekksummen legges i en referansedatabase som brukes for automatisk oppdatering av filtrene. Gjennom den automatiserte prosessen mottar filtrene informasjon om sjekksummene til dublettene som skal filtreres. Blokkering (eventuelt sletting) skjer deretter automatisk. Jeg kaller gjennomføringen av inndragningen i nettet for "automatisert inndragning" (automatisert konfiskation / automatisert förverkande).

I det følgende skal jeg vise hvordan gjeldende regler relaterer seg til denne prosedyren. For å konkretisere har jeg brukt et eksempel som involverer overgrepsbilder. Videre har jeg delt sakens faser i to, basert på hva som er velkjent og hva som er nytt. Del 1 beskriver dagens alminnelige rutine. Utgangspunktet er altså etterforsking og påtalearbeid i velkjent form. Del 2 representerer noe nytt i forlengelsen av vanlig praksis.

Del 1: I forbindelse med etterforsking av en straffbar handling beslaglegges datautstyr. Datainnholdet analyseres av politiet, og politiet finner 32 000 filer med overgrepsbilder av barn. Siden politiet alt har en referansedatabase som internt arbeidsverktøy, med kjente filer og sjekksum, ble 27 000 av filene gjenkjent ved automatisk match.[16] Det manuelle analysearbeidet kunne derfor reduseres til de uidentifiserte filene, hvorav 5 000 viste seg å være overgrepsbilder.

Med tanke på fremtidige saker oppdaterer politiet referansedatabasen med de 5 000 nye filene og sjekksum. Til slutt lager etterforskeren en analyserapport som spesifiserer de rettsstridige filene med referanse til filnavn, lagringsmedium og hvor i filsystemet de ble funnet. De 32 000 filene representerer et *netto*antall fordi dubletter bare telles én gang. Dette er i samsvar med vanlig praksis, se for eksempel Rt. 2007 s. 422. Her sa Høyesterett at *"av de 10 beslaglagte videosnuttene var tre like,*

slik at det i realiteten er tale om 8 ulike filmer".[17] Analyserapporten legges inn i sakens dokumenter og er gjenstand for innsyn og kontradiksjon før og under hovedforhandling.

Rapporten danner grunnlag for de poster i tiltalen som gjelder befatning med rettsstridig materiale, og for inndragningskravet.

Deretter følger hovedforhandling hvor tiltalte domfelles og idømmes straff. I tillegg inneholder dommen tre punkter som gjelder inndragning:

(i) Det fysiske datautstyret inndras siden det har tjent som verktøy for å utføre lovbruddet.

Del 2:

(ii) De 32 000 filene som er lagret på det inndratte utstyret inndras også, som ting som har tjent eller vært ment som verktøy for å begå den straffbare handling (kildefilen for ulovlig spredning); eller ting som har vært involvert i en straffbar handling (anskaffelse og besittelse); eller ting som er produktet av den straffbare handling (fotografering av seksuelle overgrep (originalfil)). Dommen kan spesifisere de inndratte filene med henvisning til analyserapporten som har vært gjenstand for bevisførsel.[18] Denne henvisningsformen gir en entydig og presis angivelse av de inndratte filene.

(iii) Inndragning av *dublettene* på internett av de filer som er nevnt i (ii). Til forskjell fra inndragningsobjektene i punkt (ii), knytter ikke de inndratte dublettene seg til noe spesifikt lagringsmedium. Forbindelsen mellom de inndratte datafilene i punkt (ii) og dublettene i (iii) er identiteten (sjekksummen) som er lik. Ved inndragning av dublettene på internett får inndragningsbeslutningen rettsvirkning ikke bare mot domfelte (jf. (ii)), men også mot tredjeparter (ukjent eier eller besitter). I norsk rett er hjemmelen straffeloven 1902 § 37 c annet ledd (straffeloven 2005 § 74 tredje ledd).

Lovens adgang til inndragning mot ukjent tredjeperson eller person som ikke er representert i inndragningssaken, har blant annet til formål å håndtere illegale objekter, som for eksempel narkotika som er sluppet langs grensen for å bli plukket opp og smuglet inn på det illegale markedet.[19] Rettsstridige dubletter på internett ("in the wild") kan sammenlignes med narkotika i forhold til inndragningsbehovet. Grunnene for å inndra dem er de samme. Forbudet effektiviseres gjennom å berøve lovbryteren fordelen av de ulovlige objektene, og hindre skadevirkningene av at objektene distribueres til det illegale markedet.

Norsk praksis går ut på å destruere kontrabande før inndragningsbeslutning foreligger for å slippe langvarig oppbevaring av gods som uansett skal destrueres. Denne praksis anses ikke å ha hjemmel i dagens regler. Men siden fremgangsmåten er effektiv og resultatet ønskelig, er det vedtatt hjemmel som delegerer inndragningskompetanse til påtalemyndigheten i slike tilfelle, jf. ny bestemmelse i straffeprosessloven § 214 b, som skal tre i kraft samtidig med straffeloven 2005. I forarbeidene nevnes "barnepornografisk materiale" ved siden av "narkotika" som eksempel på materiale som kan inndras i medhold av bestemmelsen (Ot.prp. nr. 90 (2003-2004) s. 359 og 492).

For å kunne oppdatere filtrene i nettet er det som nevnt behov for en referansedatabase (RDB). Den må etableres og driftes *under rettslig kontroll*. Den kan således høre under domstolene som beslutter inndragningen, eller under påtalemyndigheten som beordrer fullbyrdelsen. RDB er et verktøy for å gjennomføre inndragning innen nasjonal jurisdiksjon. Den kan også brukes i internasjonalt samarbeid forutsatt at den designes med dette i tankene (se kapittel 7).

Kvaliteten på RDB må innfri rettssikkerhetskrav. Siden innholdet er kommet til etter ivaretakelse av grunnleggende regler om kontradiksjon og rettslig overprøving, er filenes rettsstridige karakter verifisert. Og siden filtreringen retter seg spesifikt mot individualiserte dubletter, foreligger det ikke noe problem med overfiltrering (falske positive). Filtreringen begrenser seg imidlertid bare til

kjente dubletter og har derfor ingen effekt overfor nytt materiale som tilføres i nettet. Dessuten foreligger det her som ellers, en risiko for omgåelse.. Det består i at kriminelle innehavere av overgrepsbilder endrer bitverdien uten å endre bildenes karakter av å være overgrepsbilder. De bare endrer datafilens tekniske identitet. Filen vil dermed være ukjent for inndragningsfiltrene. Men slik omgåelse har ikke effekt for de dubletter som alt verserer i nettet, disse er jo utenfor de kriminelles påvirkningsmulighet. Dessuten kan politiet utøve mottiltak, for eksempel ved å bruke samme "bitchanger" program for å skaffe seg identiteten til de endrete filene. Problemet er altså bare en del av det alminnelige "arms race" mellom politi og røver.
I henhold til internasjonal rettslig harmonisering er spredning av skadelig dataprogram og overgrepsbilder en straffbar handling. Dubletter som flyter i nettet er den rettsstridige konsekvens av straffbare handlinger. Dette gjelder enhver dublett som gjenkjennes av et filter. Filen har blitt rettslig inndratt og beslutningen er beordret fullbyrdet. Det subjektive straffbarhetsvilkåret lar seg ikke kontrollere, men i hvert fall etter norsk rett representerer det heller ikke noe bevistema, fordi konstatering av et lovbrudd i objektiv forstand er tilstrekkelig for inndragning, jf. straffeloven 1902 § 35 første ledd siste setning (straffeloven 2005 § 69 første ledd siste setning).[20] Det er også nokså selvsagt at ulovlig materiale – kontrabande – ikke kan ignoreres av rettshåndhevende myndigheter på grunn av problemer med å bevise det subjektive straffbarhetsvilkåret (forsett/uppsåt). Det ville stride mot den alminnelige rettsfølelse.

Forutsatt at datafiler kan inndras synes det å være rettslig grunnlag for inndragning av dubletter i nettet. Adgangen til å beslutte inndragning av dubletter synes ikke å avhenge av at den tekniske infrastruktur alt er på plass. Situasjonen kan sammenlignes med å idømme fengsel vel vitende om at det kan ta meget lang tid før domfelte får sone. For å håndheve forbudet mot overgrepsbilder mer effektivt bør rettssystemet inndra dubletter uten påvente av innføring av filtrene. Jo større sjekksumgrunnlag, jo mer effektiv inndragning når infrastrukturen til slutt foreligger. Inndragning innebærer dessuten mer effektiv utnyttelse av etterforskingsressurser som uansett medgår til oppklaring av saken og representerer ikke noen merbelastning på systemet.

5. Kopiering og blokkering vs. Forflytning og berøvelse

Et problem som loven har strevet med siden digital teknologi ble vanlig er hvordan kopiering bør bedømmes. Betyr det at data ikke kan stjeles? Er inndragning /konfiskation /förverkande rettshåndhevende motstykker til tyveri, slik at hvis data ikke kan stjeles så kan de heller ikke inndras? Er man henvist til rettslig beskyttelse og sanksjon ved hjelp av opphavsrettslovgivningen, spesialregler om vern av stats- og bedriftshemmeligheter, personopplysninger, taushetsregler m.v.? Dette problemet er så sammensatt at jeg deler drøftelsen inn i underpunkter.

5.1 Data vs. Informasjon

En del av problemet gjelder skillet mellom *data og informasjon*, noe som kan illustreres med et eksempel: Jeg sender et brev til en venn. Brevet blir stjålet og ødelagt. Når jeg forstår at brevet ikke har nådd frem til min venn kan jeg ringe henne og fortelle det jeg har på hjertet over telefonen, eller jeg kan sørge for at vi møtes, og jeg kan også sende et nytt brev. Slik kan den samme *informasjonen* bli overført igjen og igjen, på mange måter. Men det gjelder ikke brevet, fordi denne *tingen* har gått til grunne. I dataverdenen kan vi tenke på data som det fysiske brevet (informasjonsbæreren) og på informasjonen som en prosess mellom datamaskinen og sluttbrukeren.

Uttrykket "elektronisk informasjon" som man ofte støter på, er ikke helt klart. En betydning er at informasjonen kommer fra en datamaskin, men straks kan man spørre om uttrykket begrenser seg til å omfatte informasjonen slik den presenteres på skjermen, eller om det også omfatter informasjonen på en papirutskrift. Og hvordan skal man vurdere et dataprogram i maskinlesbar kode (objektkode)? Et

slikt program kan bare leses og brukes av datamaskiner, ikke av individer. Skal det anses som ”elektronisk informasjon”?
Bruk av klassiske begreper som ’data’ og ’informasjon’ i en kontekst bestående av datamaskiner og elektroniske nettverk, er en kilde til forvirring. Den klassiske forståelsen er at ’data’ er fakta, tegn og symboler som kan leses og forstås av mennesker. ’Informasjon’ er meningsinnholdet i dataene når de er fortolket av mennesker. Begrepene er adekvate i en verden av bøker hvor tegnene på hver side er data og meningen er informasjon. Karakteristisk for situasjonen er at data og informasjon presenteres *samtidig* (parallelt) til sluttbrukeren, dvs. når hun åpner boken.

I henhold til tradisjonell begrepsbruk er et dataprogram i objektkode verken data eller informasjon, fordi det ikke er beregnet på et individ som skal fortolke det. Programmet kan heller sammenlignes med en bilmotor eller et urverk. Begge kan dekonstrueres og undersøkes slik at man kan forstå hvordan de er bygd opp og fungerer. Tilsvarende kan et dataprogram være gjenstand for omvendt utvikling (”reverse engineering”). Dataprogrammet er likevel ikke ’data’ for i så tilfelle skulle også motoren og urverket vært data.

I datakonteksten bør ’data’ bety ’elektroniske data’. Bare datamaskiner kan behandle elektroniske data. Fra tid til annen hører man påstanden om at data prinsipielt sett kan behandles likt av datamaskiner og mennesker, forskjellen er bare den tid som medgår til operasjonen (tidsfaktoren).[21] Men denne påstanden er ikke fornuftig dersom man taler om *elektroniske data*. Individer kan ikke behandle elektroniske data direkte. Individer kan behandle *opplysninger* som bæres av de elektroniske dataene, men da må innholdet først *presenteres* for dem. Derfor er elektroniske data og informasjon sekvensielle begreper, som krever en overgang i form av presentasjon.

Problemene med skadelig dataprogram og overgrepsbilder materialiserer seg på forskjellige nivåer. *Datamaskiner* er mål for skadelig dataprogram og lovbruddet materialiserer seg på datanivået i nettverket. *Individer* er mål for overgrepsbilder fordi informasjonen representerer verdien. For individet er lovbruddet manifest når filen er åpnet og innholdet fremvist på skjermen. Likevel, begge lovbruddene forutsetter dataoverføring fordi elektroniske data bærer innholdet. I begge tilfeller er de rettsstridige filene (elektroniske data) digital kontrabande som må blokkeres på datanivået.

Den rettslige implikasjonen er at *datafilen* er målet for rettshåndhevelsen. Datafilen kan identifiseres og kontrolleres ved filtrering og blokkering, og kan derfor anses som et konfiskerbart objekt. Det rettslige problemet går tilbake til det opprinnelige spørsmålet, nemlig om inndragning krever fysisk berøvelse av objektet, dvs. forflytning eller besittelsesforrykkelse. Problemstillingen innebærer at man både må ta stilling til om data er et objekt i inndragningsreglenes forstand og om data kan rammes på en inndragningsrelevant måte.

5.2 Data som strafferettslig objekt

Inndragning og beslag bør ses i sammenheng fordi de representerer samme type inngrep av henholdsvis permanent og midlertidig karakter. Jeg har dessuten forutsatt at dublettene først er beslaglagt via beslaget i kildefilene, jf. prosedyren beskrevet i kapittel 4. Etter mitt syn bør kildefil og dublett anses som en og samme ting på grunn av at teknologien ikke gjør forskjell. Normen bør gjenspeile realiteten. Et beslag i kildefilen gjelder også dublettene i den forstand at inndragningsreglenes vilkår om at objektet må være tatt i beslag for å kunne inndras, er oppfylt. Forutsetningen om beslag følger av straffeloven 1902 § 37 c, annet, jf. første ledd, som nevner ”beslaglagt ting”.

Beslag og inndragning kan anses som rettshåndhevende motstykker, ikke bare til tyveri, men også til underslag og skadeverk. Begge regelsett (straffe- og sanksjonsnorm) gjelder objekter, altså ”ting”, ”gjenstander” og ”föremål” som historisk sett var fysiske objekter. De normative begrepene gjaldt noe som kunne stjeles eller konfiskeres, dvs. at de kunne utpekes og tas vekk fra innehaverens besittelse. For eksempel det at de fysiske objektene grunnleggende sett besto av atomer var åpenbart

ikke rettslig relevant. Det må dermed antas at også objekter som består av *noe annet enn atomer*, men som kan *identifiseres og tas ut av eierens praktiske rådighetssfære* kan være rettslig relevante for nevnte straffe- og sanksjonsnormer.

Selv om tyveri og konfiskasjon kan sies å være rettslige motstykker, er de ikke like. Normene forutsetter at handlingen retter seg mot et objekt, men anvendelsesområdet avgrenses ulikt. Mat kan for eksempel være gjenstand for tyveri, men kan ikke senere inndras fordi det naturlig går til grunne. Tyveri kan omfatte tapping både av vann og strøm, men siden slike ressurser løpende forbrukes kan de ikke senere inndras.

I en bredt anlagt drøftelse i "Automatisert inndragning" (Sunde 2011) kapittel 6-10, har jeg påvist at det rettslig relevante kriterium i norsk strafferett er at objektetkan spesifiseres, kvantifiseres og kontrolleres. For øvrig er inndragning avhengig av om objektet består på inndragningstidspunktet. Kriteriene for å være et stjelbart objekt er oppfylt både for kubikkmeter vann og strøm per kilowatt time. Karakteren av godets grunnleggende bestanddeler er rettslig irrelevant, for eksempel er verken rennende vann i naturen eller naturlig energi (som er iboende i alle ting) å anse som slike objekter. Årsaken er at de rettslige begrepene "ting" og "gjenstand" refererer seg til fenomener som er brakt under menneskelig kontroll i en form som tilfredsstiller kriteriene. Det er *formen*, ikke de grunnleggende bestanddeler, som bestemmer om det foreligger en "ting" eller "gjenstand" i rettslig forstand.

Økonomiske krav som ikke er bundet til dokumenter (enkle fordringer) kan ikke stjeles, men kan underslås. Et eksempel er kontohaveren som hever et beløp han vet at er feilaktig innbetalt til konto. Tilsvarende kan enkle fordringer inndras.[22] Dette følger direkte av inndragningsbestemmelsens ordlyd, jf. "som ting regnes også rettigheter, fordringer [og elektronisk lagret informasjon]", jf. straffeloven 1902 § 35 [og straffeloven 2005 § 69].

Det er ikke nødvendig, og ville også bære galt av sted, å foreta en kobling til tyverinormen for å fastslå dette. Det samme gjelder rett til et domenenavn og retten til en brukerkonto som er benyttet til å begå straffbare handlinger. Slike rettigheter kan inndras.[23] Eksemplene viser at de rettslige begrepene "ting" / "genstand" ikke er bundet til fysiske objekter bestående av atomer, men gjelder fenomener som kan individualiseres, spesifiseres og kontrolleres. Man kan ikke slutte noe om rekkevidden av inndragningsnormen ut fra tyveribestemmelsens vilkår om besittelsesforrykkelse.
Det har derfor neppe relevans for vurderingen av om data er "ting" eller "gjenstand", at data består av *bits*. Avgjørende er at datafilene kan individualiseres, spesifiseres og kontrolleres. Det er disse egenskapene som gjør at de for eksempel lar seg beskrive i politiets analyserapport som nevnt i kapittel 4, og som gjør at de kan individualiseres og identifiseres i RDBen med effekt for filtre i nettet. *Informasjon* derimot kan klarligvis *ikke* inndras. Denne prosessen fra presentasjonen på skjermen til den menneskelige sluttbruker kan det ikke gripes direkte inn i.

5.3 Borttakelse – destruksjon – filtrering – sletting

Det gjenstående problemet er om inndragning krever at objektet borttas? Som nevnt er det rettslige utgangspunktet at kildefilen er beslaglagt og brakt under politiets kontroll. Drøftelsen gjelder dublettene i nettet.

Siden data består av *bits* kan de ikke forflyttes, i hvert fall ikke i en og samme handling. Men hvorfor skulle man kreve at borttakelse skjer i en og samme handling? I den digitale dimensjonen kan resultatet (besittelsesforrykkelse) oppnås ved kopiering og sletting, dvs. en to stegs handling. Da oppnås den digitale ekvivalenten til fysisk borttakelse. En påstand om at fysisk borttakelse bare består av én handling er dessuten en fiksjon. Hvordan man ser det avhenger av beskrivelsen. Borttakelse krever først at noen tar på objektet (= en handling) og løfter og tar det med seg (= minst en handling til). Tatt i betraktning at det ikke er noen forskjell på kildefilen og dubletten, burde ikke fremgangsmåten for besittelsesforrykkelsen være rettslig relevant. Loven vektlegger at *innehaveren*

taper rådighet og at staten *overtar kontrollen* over objektet. Dette oppfylles i den digitale dimensjonen ved fremgangsmåten som er beskrevet.
For øvrig er borttakelse (besittelsesforrykkelse) bare nødvendig ved inndragning av løsøre som skal selges til fordel for statskassen. Illegale objekter (kontrabande) må destrueres. Datafiler som er lagret på inndratt datautstyr kan enkelt destrueres, og derved fullbyrdes inndragning i fullstendig gjennomført form. Destruksjon korresponderer strafferettslig med *skadeverk*, som dermed blir et mer nærliggende motstykke til inndragning enn tyveri. I datadimensjonen kan skadeverk ta form av sletting av datafiler. Dermed synes det også naturlig at inndragning kan fullbyrdes i datadimensjonen på samme vis.

Hvorvidt dublettene i nettet kan slettes beror på tekniske forhold. Det er imidlertid klart at de kan undertrykkes med den følge at verdien forsvinner fordi materialet ikke kan brukes til bytte og salg, eller til å forårsake skade på datamaskiner. Også slik blokkering / undertrykking er strafferettslig sett å anses som skadeverk i form av angrep på tilgjengeligheten. Eksemplene viser at fullbyrdelse av inndragning kan ta forskjellig form. Det kan være overtakelse av kontroll over objekter med tanke på destruksjon, eller det kan være salg. For så vidt gjelder rettigheter, må inndragning fullbyrdes ved notifikasjon til skyldner, registerfører eller tjenesteyter.

Avgjørende for om fremgangsmåten er tilfredsstillende må være hvorvidt fullbyrdingsmåten effektiviserer hensynet bak straffebudet. Som det har fremgått oppnås dette formålet ved å ramme datafilenes tilgjengelighet. For digital kontrabande er det følgelig tale om undertrykkelse eller destruksjon. Dette rammer tilgjengeligheten for dem som etterspør materialet, sml. narkotika som ikke kommer frem til markedet. Og det reduserer verdien av materialet for innehaveren, fordi verdien vesentlig, dog ikke utelukkende, består i spredningsmuligheten.

Således antas det at også dette er en relevant form for fullbyrding av inndragning. Dermed er konklusjonen at inndragning kan operasjonaliseres med praktisk effekt i den digitale dimensjonen.

6. Normativ handling i den digitale verden

Referansedatabasen (RDB) er interessant fordi den representerer en sammensmelting av faktum og norm. RDB har egenskaper som kan sammenlignes med et DNA-register, noe som gjelder *faktum.* DNA-registeret skal bidra til å avklare faktaspørsmålet vedrørende lovbryterens identitet, noe som kan oppnås ved match av DNA-profiler. Tilsvarende inneholder RDB de rettsstridige dublettene, hver enkelt med unik identitet i form av sjekksum. I tillegg kan RDB anses å ha en *normativ* funksjon, som kan illustreres ved en sammenligning med narkotikalisten. Stoffene på listen er per definisjon ulovlige. Tilsvarende er dublettene i RDB per definisjon ulovlige, noe som er statuert ved rettslig prøving.

Vi ser nå at *fortolkningen av rettsregelen kan inkorporeres i nettverksteknologien* gjennom RDBen. For eksempel representerer de 32 000 filene som tidligere er nevnt, 32 000 nyanser av rettsregelen. Digital teknologi kan integrere subsumsjonen med virkning over tid for et uspesifisert antall instanser av dubletter. I datadimensjonen på datanivået hvor sjekkumfiltrering foregår, *oppheves distinksjonen mellom faktum og norm*.

Dette er vesensforskjellig fra forholdene i den fysiske dimensjonen. Selv om en rettregel er klar, for eksempel hva gjelder illegaliteten av narkotika, er ikke erfaring fra en narkotikasak rettslig overførbar til en ny sak med samme type stoff. I hver sak må etterforskningen undersøke om stoffet virkelig er narkotika. Man kan ikke nøye seg med en henvisning til at den forrige saken også gjaldt narkotika. I datadimensjonen kan alle dubletter behandles likt over tid ved automatiserte prosesser som er programmert i henhold til en rettslig beslutning, *én gang*.

7. Omgåelse og internasjonalt samarbeid

Filtreringen av dublettene som er fritt tilgjengelige på internett må utføres av tjenesteyterne. Myndighetenes kompetanse til å pålegge filtreringsplikt begrenser seg til tjenesteytere på eget

territorium. Siden filtreringen kun er av teknisk og automatisk karakter reiser den neppe noe spørsmål i forhold til det generelle overvåkingsforbudet i e-handelsdirektivet slik det er implementert i nasjonal rett.

Spørsmålet er om automatisert inndragning / konfiskation / förverkande – dvs. filtrering – bør gjøres. Lovens ordlyd gir en adgang, ikke en plikt til å inndra. En plikt til å inndra kan imidlertid innfortolkes forsåvidt gjelder (digital) kontrabande, allerede fordi et annet resultat er støtende.[24] Her skal jeg imidlertid se på momenter som inngår i vurderingen av om inndragning *bør* skje. Da skal det skal det særlig legges vekt på om inndragningen effektiviserer formålet bak straffebudet. Relevante hensyn synes å være omgåelsesmuligheten, ressursbruk, tilgangen på alternative tiltak, og tidsmomentet.

Et problem som *ikke* er relevant, gjelder tilførselen av *nytt ulovlig materiale* til nettet. Det kan ikke inndras ved sjekksumfiltrering fordi det først må beslaglegges, inndras osv., slik som beskrevet i kapittel 4. Dette er imidlertid ikke noe argument mot inndragning av det materiale som alt er beslaglagt og sjekksumidentifisert. Det finnes ikke noe vidundermiddel mot noen kriminalitetsform, og ulovlig materiale i nettet representerer ikke noe unntakstilfelle.

Det synes heller ikke som inndragningen kan omgås i et omfang som rammer effektiviteten, Hensynet særlig fordi omgåelse ikke kan ramme filer som alt er sluppet i nettet og politiet kan anvende mottiltak (se kapittel 4). Derimot bør det effektiviserende potensialet i internasjonalt samarbeid tas i betraktning. Ved utveksling av rettslig verifiserte sjekksummer kan innholdet i RDBene raskt økes. Selv om de nasjonale regler ikke er identiske, kan inndragning i hvert fall effektivisere håndhevelsen av det internasjonale normative minimum, dvs. utbredelse av overgrepsbiler med barn som er inntil 14 år gamle. Nasjonalt kan man i tillegg filtrere overgrepsbilder med eldre barn.

Et vesentlig hensyn for iverksettelse av filtrering, er at automatisert inndragning bedre utnytter de ressurser som alt medgår ved dagens arbeidsmetoder. Utferdigelsen av analyserapporten nevnt i kapittel 4, har vært vanlig rutine i etterforskingen i mer enn et tiår. Straffesaken skal gå sin gang uansett. Inkludering av inndragningskravet innebærer ikke noe merarbeid. Automatisert inndragning betyr at dagens rutinearbeid får effekt i den digitale dimensjonen. Det gir mer effektiv bruk av politiets ressurser, noe som i seg selv bidrar til å holde det kriminelle problemet nede.

Ved vurderingen av *alternative metoder* og *tidsmomentet*, er det nødvendig å skille mellom skadelig dataprogram og overgrepsbilder. For skadelig dataprogram er automatisert inndragning altfor sendrektig til å kunne effektivisere forbudet. Selv om filtreringen skjer automatisk skjer iverksettelse først etter tidkrevende etterforsking og rettslig behandling. Datasikkerheten krever umiddelbar respons mot nye skadelige dataprogram. Behovet for raske tiltak basert på spesiell datasikkerhetskompetanse har etablert et kommersielt marked for filtrering (”antivirus teknologi”), hvor tilbydere av ekomtjenester og sluttbrukere gladelig betaler for sikkerhet. Automatisert inndragning kan derfor ikke begrunnes ut fra effektiviseringshensyn (det forhindrer selvsagt ikke at fysisk beslaglagt skadelig dataprogram inndras i selve straffesaken).

Situasjonen er annerledes for overgrepsbilder. Her finnes ikke et effektivt kommersielt marked for filtre, siden at verken de som vil ha eller de som ikke vil ha materialet, vil betale for filtre. Her er behovet for rettshåndhevende tiltak klart tilstede. Eksisterende filtre (som Kriposfilteret) er ikke tilstrekkelig effektive fordi de ikke retter seg direkte mot de rettsstridige filene. Tidsmomentet har dessuten ikke samme betydning for overgrepsbilder som for skadelig dataprogram. Som nevnt i kapittel 2 representerer bildene en livsvarig integritetskrenkelse overfor barna på bildet. Denne krenkelsen plikter staten å bringe til opphør, dog uten å tilsidesette grunnleggende rettigheter og rettssikkerhetsgarantier. Automatisert inndragning respekterer disse kriteriene og effektiviserer vernet om barnas rett til privat liv, herunder retten til respekt for sin personlige integritet, jf EMK artikkel 8.1.

Problemet med overgrepsbilder er velkjent og representerer et meget grovt overgrep mot barns integritet. Dublettene medfører at problemet har en standardisert form som kan møtes med standardiserte metoder. Velkjent teknologi kan tas i bruk og, som alt påpekt, de ressurser som uansett medgår i kriminalitetsbekjempelsen vil utnyttes bedre. Dermed faller statens unnskyldningsgrunner for ikke *aktivt* å sikre rettighetene til barna på bildet, noe som ytterligere taler for å iverksette automatisert inndragning mot dette problemet.

8. Avsluttende bemerkninger

Artikkelen har vist at gjeldende rettsregler gir grunnlag for automatisert inndragning / konfiskation / förverkande. Det viktige er at *konseptet* finnes i dagens regler. Det kan kanskje være behov for enkelte lovtilpasninger, men antakelig er dette en lovgivningsoppgave av mindre omfang. Av avgjørende betydning er det at lovgiver og rettsanvender tar stilling til hva som menes med at loven gjelder på internett. Herunder bør man frigjøre seg fra analogier med fenomener i den fysiske dimensjonen og la loven virke direkte på den digitale dimensjonens realitet.

Litteratur:

Holmquist (2009) Holmquist, Lena m.fl. *Brottsbalken – En kommentar* Studentutgave 6. Stockholm. 2009.

Høgberg / Kinander (2011) Høgberg, Alf Petter og Kinander, Morten *Det formelle legalitetsprinsippet og rettskildelæren* TfR 1/2011 s. 15-55.

Lindberg (2009) Lindberg, Gunnel Straffprocessuella tvångsmedel Stockholm. 2009.

Mason (2010) Mason, Stephen (ed.) *Electronic Evidence* Reed Elsevier (UK) Ltd. 2010.

Matningsdal (1987) Matningsdal, Magnus *Inndragning* Universitetsforlaget. 1987.

Spoenle (201) Spoenle, Jan *Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?* Council of Europe, Project on cybercrime, Discussion paper, 31. august 2010. www.coe.int/cybercrime.

Stub (2011) Stub, Marius *Tilsynsforvaltningens kontrollvirksomhet* Phd.-avhandling nr. 41, juridisk fakultet, Universitetet i Oslo, 2011.

Sunde (2006) Sunde, Inger Marie *Lov og rett i cyberspace. Fagbokforlaget. Bergen. 2006.*

Sunde (2011) Sunde, Inger Marie *Automatisert inndragning* Complex nr. 3/2011. Senter for rettsinformatikk/Unipub. Oslo. 2011. Phd.-avhandling nr. 37, juridisk fakultet, Universitetet i Oslo, 2010.

Udsen (2009) Udsen, Henrik *De informationsretlige grundsætninger* København. 2009. Doktorgrad ved Det Juridiske Fakultet ved Københavns Universitet 2009.

Wall (2007) Wall, David S. *Cybercrime – The Transformation of Crime in the Information Age* Cambridge. UK2007

[1] Jeg viser til en materiell forståelse av legalitetsprinsippet som omfatter inngrep både i form av rettslige beslutninger og faktiske handlinger. Forståelsen har lang tradisjon i norsk rett, se Høgberg / Kinander (2011). Av

nyere norsk teori kan det også vises til Stub (2011) som drøfter legalitetsprinsippet i relasjon til beslag som rettslig beslutning og faktisk handling, s. 44-50.

[2] Etter norsk rett er inndragning en strafferettslig reaksjon. I svensk rett kalles det en "särskild rättsverkan av brott", se BrB 1 kap. 8 § og Holmquist (2009) s. 1:41. I dansk rett står bestemmelsene om konfiskation i straffeloven kapittel 9 om "Andre retsfølger af den strafbare handling".

[3] Jeg viser til reservasjonslisten på Europarådets hjemmeside (Treaty Office), besøkt 4. juli 2011. Spesialreglene i dansk straffelov om befatning med "kode eller andet adgangsmiddel", jf. §§ 263 a og 301 a omfatter i hvert fall ikke skadelig dataprogram. Sml. norsk straffelov 1902 § 145 b.

[4] Se Matningsdal (1987) kap. 11.1-11.3 om denne tredelingen.

[5] Rt. 1992 s. 904 og Sunde (2011) kap. 7.4.2 s. 152.

[6] Ot.prp. nr. 90 (2003-2004) s. 347.

[7] Sunde (2011) s. 120 flg. om overveielser i norsk rett om behovet for nye regler om datakriminalitet.

[8] Dette kapitlet er en konsentert versjon av Sunde (2011) kapittel 3.

[9] Mason (2010) skriver at "This crucial distinction [between the original and its copies] becomes problematic in the electronic medium, where not only copy and original are indistinguishable, but the very act of working on 'a' document will automatically and routinely without knowledge of the author create numerous copies on the computer…" (s. 27), se også Ch. 4 "Authenticating digital data" s. 83 flg.

[10] Sunde (2011) kap. 11.5.2 s. 237 gir noen eksempler på hvordan informasjon i teknisk forskjellige filer kan vurderes å være likt, for eksempel forskjellige meldinger som formidler samme innsideinformasjon, et overgrepsbilde som er endret i photoshop, og en fotoserie av samme objekt.

[11] Wall (2007) s. 19.

[12] Se mer om disse sammenhengene i Sunde (2006) kap. 8.

[13] Se Sunde (2011) kap. 3.3.3 s. 43 flg., om anvendelser av hash teknologi.

[14] Reproduksjonens betydning for e-handelstjenester er så viktig at den er beskyttet etter ansvarsfrihetsreglene i e-handelsdirektivet artikkel 13 om "caching", sml. e-handelsloven (lov 35/2003) § 16 annet ledd og § 17.

[15] Spoenle (2010), s. 5. Se også Sunde (2011) om betydningen av asymmetriske rettighetsforhold mellom tjenesteyterens fysiske bærer og sluttbrukerens data for spørsmålet om data er å anse som et selvstendig objekt strafferettslig sett (kap. 3.3.5 med videre henvsininger). Se også kritikk av sondringen mellom "lagret" og "under overføring" (blant annet kap. 6.1 s. 115-117).

[16] For eksempel disponerer KRIPOS i Norge en slik database.

[17] Se gjennomgang av norsk praksis i Sunde (2011) kap. 11.5.2.

[18] Denne spesifikasjonsteknikken har vært benyttet i sak om inndragning av stort parti pornografiske blader, se Rt. 1980 s. 1532 som gjaldt inndragning av utuktige skrifter med en anslått totalvekt på "vel 16 tonn". Tingretten inndro 97 000 pornoblader, 18 000 filmer og 20 videobånd og viste til beslagsrapporten. Fremgangsmåten ble opprettholdt av Høyesterett.

[19] Et annet formål er å ramme kriminelle som befinner seg utenfor rekkevidde av nasjonal rettshåndhevelse. Det kan for eksempel gjelde inndragning overfor "off shore" selskap som eier tråler og utstyr som benyttes til ulovlig fiske i nasjonalt farvann (miljøkriminalitet). Da kan det kostbare fiskeutstyret inndras.

[20] Se også Ot.prp. nr. 90 (2003-2004) s. 342.

[21] Se for eksempel Udsen (2009) s. 35.

[22] Rt. 2003 s. 1243 og Rt. 2008 s. 1582. Se omtale i Sunde (2011) kap. 7.6.4 s. 165 flg.

[23] Rt. 2009 s. 1011 ("Joyzone"). Beslag tatt i domenenavn for å sikre et senere inndragningskrav.

[24] Se Sunde (2011) som drøfter pliktspørsmålet i forhold til fysisk beslaglagte data i kap. 5.7. s. 104 flg.