Sitering av artikkelen i APA (6th):
Sunde, I. M. (2019). Datakrimretten i «fugleperspektiv». *Tidsskrift for strafferett, 19*(2), 129-147.

Datakrimretten i «fugleperspektiv»

Professor Inger Marie Sunde

Forfatterbeskrivelse

Inger Marie Sunde er professor i rettsvitenskap ved Politihøgskolen i Oslo og leder forskergruppen «Politiet i et digitalisert samfunn». Hun var sekretær og medlem av Datakrimutvalget I og II, har utgitt fagbøkene *Lov og rett i cyberspace* (2006) og *Datakriminalitet* (2016), og publisert artikler om datakriminalitet, politiets digitale metodebruk, personvern og overvåking.

ingsun@phs.no

Inger Marie Sunde

Politihøgskolen

Pb 2109 Vika. 0125 Oslo

Sammendrag

Artikkelen gir en oversikt over datakrimretten. Området anses å bestå av tema innen materiell strafferett, straffeprosess, politirett (forebyggende politiarbeid) og folkerett. Det foretas et tilbakeblikk på de lange linjer i datakrimretten. Deretter drøftes noen konsekvenser av at det savnes en underliggende filosofi som kunne bidra til å gi konsekvente rettslige løsninger på området. Også sammensmeltingen av konsepter som bærer de straffeprosessuelle tvangsmidlene, tas opp. Endelig reises noen spørsmål innen forebyggende politiarbeid på internett, et felt som hittil er lite utredet.

Nøkkelord: bevissikring, databedrageri, databevis, datakriminalitet, EUROPOL, nettovergrep, tvangsmidler

1. Innledning

Denne artikkelen behandler datakrimretten i et «fugleperspektiv». Formålet er å gi leseren oversikt over et felt som spenner over flere rettsdogmatiske områder. Fellesnevnerne er at de underliggende fenomenene involverer bruk av informasjons- og kommunikasjonsteknologi (IKT),[1] og at de gjelder kriminalitet eller kriminalitetsbekjempelse.

Slik jeg ser det, omfatter datakrimretten for det første tema innen materiell strafferett og straffeprosess for så vidt som de har en kobling til data. Med dette mener jeg at datateknologi må ha inngått som ledd i den straffbare handlingen, og at håndtering av databevis er et tema i

[1] Datakriminalitet betegnes derfor iblant som «IKT-kriminalitet», se f.eks. Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet (2015) – https://www.regjeringen.no/contentassets/8de0db6aff3e4dd79c92519057af690f/strategi_ikt-kriminalitet.pdf (besøkt 9. april 2019).

etterforskningen og den videre strafforfølgningen.[2] For det andre omfatter datakrimrett forebyggende politiarbeid på internett, et felt som hittil har fått liten akademisk oppmerksomhet. For det tredje omfattes folkerettslige problemstillinger drevet frem av internetteknologiens grenseløshet og andre globaliseringstrekk. Her gjelder hovedproblemstillingen hvor langt statens eget politi «kan gå» i cyberspace uten å krenke en annen stats suverenitet, et spørsmål som har relevans både for etterforsking og forebygging av kriminalitet. Hånd i hånd med dette går de internasjonale, formelle samarbeidsordningene for å oppnå tilgang til databevis som befinner seg utenfor den strafforfølgende statens geografiske grenser. Begrensningene og tregheten i de internasjonale, formelle prosedyrene er et bakteppe for problemstillingene rundt politiets internasjonale handlefrihet i cyberspace.[3] Samlet sett utgjør de nevnte områdene en funksjonell avgrensning av datakrimretten.[4]

2. Tilbakeblikk

2.1 Datakrimstrafferetten har vært prioritert

Materiell strafferett har vært datakrimrettens kjerneområde. I USA ble datakriminalitet fra 1960-tallet av ansett som «hvitsnippkriminalitet», en tankegang som ble reflektert i Norge da Økokrim i 1994 fikk nasjonalt ansvar for å bekjempe datakriminalitet. Man så det slik at datakriminalitet var «andre saker som naturlig faller inn under økonomisk kriminalitet», jf. påtaleinstruksen § 35-4 som angir Økokrims saklige kompetanse.[5] I 1994 var imidlertid datakriminalitet i ferd med å utvikle seg til langt mer enn økonomisk hvitsnippkriminalitet. Mer om dette nedenfor.

På 1960-tallet var ikke datamaskiner allemannseie. Datamaskiner var kostbare stormaskiner eid av foretak gjerne innen bank, finans og forsikring, og foretakets ansatte var de som hadde praktisk mulighet til å begå datakriminalitet. Det var gjerne tale om vinningsforbrytelser som databedrageri og økonomisk utroskap. Datamaskinene var ikke koblet i nettverk og kunne ikke angripes utenfra. Internett var bare på forstadiet, som et forskningsprosjekt i regi av det amerikanske militære forskningsinstituttet i samarbeid med noen utvalgte universiteter.

Sett med dagens øyne fremstår forholdene på 1960-tallet som nærmest uvirkelige. Vi kan vanskelig forestille oss en tilværelse uten datamaskin/smarttelefon og internett, og realiteten er at enhver har

[2] Spørsmål om bruk av datateknologi for å lette behandlingen av straffesaker, bruk av lyd- og videoopptak under hovedforhandlingen mv., har ikke vært vanlig å henregne til datakrimretten.
[3] Internasjonale samarbeidsprosedyrer i straffesaker er beskrevet i I. Bruce & G.S. Haugland, *Skjulte tvangsmidler*, Universitetsforlaget, Oslo, 2. utg. 2018, kapittel 5.
[4] P. Seipel *Juridik och IT – Introduktion till rättsinformatiken,* Nordstedts Juridik, Stockholm, 8. uppl. 2004, diskuterer fordeler og ulemper med en rettsdogmatisk, funksjonell eller praktisk inndeling av «IT-rätten», s. 194–195. Jeg mener at en funksjonell inndeling er mest hensiktsmessig for datakrimretten.
[5] Påtaleinstruksen er FOR-1985-06-28-1679. Ordningen opphørte i 2005 ved opprettelsen av «Nye Kripos» og det Nasjonale statsadvokatembetet for bekjempelse av organisert og annen alvorlig kriminalitet (NAST), jf. påtaleinstruksen § 38-1 (forskriftsendring FOR-2005-12-16-1573).

utstyr og praktisk mulighet til å kunne begå datakriminalitet. Mens datakriminaliteten på 1960-tallet bare gikk ut over foretaket (og dets kunder, men disse ble jo kompensert), kan dagens datakriminelle handlinger ha global rekkevidde. Merkelappen «datakriminalitet» kan dessuten settes på langt flere typer lovbrudd enn den gang, og lovbryterne er flere og mer forskjellige både hva gjelder motiv, alder og sosioøkonomisk bakgrunn. Datakriminalitet er blitt et svært utbredt fenomen, en trend som må forventes å vedvare som følge av den kontinuerlige digitaliseringen av samfunnet.

2.2. Utviklingsbølgene i datakrimstrafferetten

Sett over tid har datakrimretten vært drevet frem av praktiske problemstillinger som har måttet finne sin løsning. De skadelidende interessene har vært viktige drivkrefter i rettsutviklingen fordi man selvsagt har ønsket å beskytte disse, ikke bare gjennom tiltak som skal ivareta datasikkerhet mv., men også gjennom en bedre utbygd straffelovgivning. Hvilke interesser som har stått øverst på den lovgivningspolitiske dagsorden, har variert over tid.

Det sier seg selv at økonomiske interesser til enhver tid har vært et viktig legislativt hensyn, siden datautstyr er kostbart og tradisjonelt har vært brukt i virksomheter med økonomisk formål. Men også andre interesser spiller inn. Hvis vi flytter blikket til Europa, har utviklingen vært oppfattet som «bølger» hvor dominerende interesser fortløpende har avløst hverandre.[6] På 1970-tallet sto personvern i fokus, og konfidensialitetshensynet var fremtredende.[7] I 1979 ble derfor brevbruddsbestemmelsen i straffeloven 1902 (lov av 22. mai 1902 nr. 10, opphevet) § 145 supplert, blant annet for å ramme «uberettiget innkobling på telexnettet for å fange opp meldinger til andre, og det at man uberettiget gjør seg kjent med innholdet av lydbåndopptak eller opplysninger lagret ved hjelp av EDB».[8]

I neste «bølge» på 1980-tallet ble immaterialrettigheter og nærstående rettigheter satt på dagsordenen. Et stort marked for datamaskiner til bedrifter, og etter hvert også til hjemmebruk, var i ferd med å åpne seg, og sammen med dette et marked for standardpakker med programutrustning. Dataprogrammer kan kopieres, og piratkopiering ble etter hvert et betydelig bransjeproblem.[9] I Norge så vi i 1992 en innstramming i retten til å kopiere dataprogrammer til eget bruk, i åndsverkloven av 1961 (lov av 12. mai 1961 nr. 2, opphevet) og innføring av et straffesanksjonert forbud mot å omsette eller besitte i ervervsøyemed et hvilket som helst middel hvis «eneste formål»

[6] Bølgemetaforen ble brukt av den tyske professoren U. Sieber, en av arkitektene bak Europarådets datakrimkonvensjon som er nærmere omtalt i punkt 3. Se opprinnelig U. Sieber, «Legal aspects of computer-related crime in the information society», *COMCRIME study prepared for the European Commission*, 1998 (http://www.edc.uoc.gr/~panas/PATRA/sieber), og Sieber, «The threat of Cybercrime» i *Organised Crime in Europe: the threat of cybercrime,* Situation Report 2004, Europarådet, Strasbourg 2005, kapittel 3, s. 84–86.
[7] Sieber (2005), s. 84.
[8] Ot.prp. nr. 4 (1978–1979) s. 3. Endringen i § 145 skjedde ved lov av 16. februar 1979 nr. 2.
[9] Sieber (2005), s. 85.

er å gjøre det lettere ulovlig å fjerne eller omgå tekniske innretninger til beskyttelse av dataprogram (åndsverkloven 1961 § 54a).[10] Noe senere, i 1995, innførte man en særskilt straffebestemmelse mot uberettiget adgang til beskyttede TV- og radiosignaler, jf. straffeloven 1902 § 262 (straffeloven 2005 (lov 20. mai 2005 nr. 28) § 203).[11]

1990-tallets «bølge» gjaldt ulovlig innhold på internett. World Wide Web, som kom på begynnelsen av tiåret, brakte blant mye annet også med seg overgrepsbilder av barn, hatefulle ytringer og ulovlige gamblingtjenester.[12] På samme tid begynte erkjennelsen av at internettets åpenhet innebar en korresponderende sårbarhet, virkelig å synke inn, herunder farene forbundet med terrorisme og «cyberwarfare».[13] Oppmerksomheten ble dermed også rettet mot muligheten for å implementere datasikkerhetshensynene i straffelovgivningen. Datasikkerhetshensynene er hensynene til konfidensialitet, integritet og tilgjengelighet.[14] I Norge hadde man allerede i 1987 supplert straffeloven 1902 med noen datakrimbestemmelser av denne art.[15] Brevbruddsbestemmelsen hadde fått et nytt annet ledd som rammet beskyttelsesbrudd overfor data, både slike som var lagret og slike som var under overføring. I straffeloven 2005 er gjerningsbeskrivelsen fordelt på § 204 (innbrudd i datasystem) og § 205 bokstav b (ulovlig tilgang til elektronisk kommunikasjon). Datidens plassering i brevbruddsbestemmelsen satte konfidensialitetshensynet i forgrunnen, men ga nødvendigvis også et visst vern for integritet og tilgjengelighet. Konfidensialitetshensynet (vern mot uberettiget tilgang) er i realiteten et generelt skjermingshensyn som er grunnleggende for beskyttelse av datasystemers sikkerhet og funksjonalitet.[16] Videre innførte man en sabotasjebestemmelse (straffeloven 1902 § 151 b) som blant annet skulle verne slike datasystemer og databaser som var viktige for samfunnets infrastruktur (sml. straffeloven 2005 § 192), foruten en bestemmelse om databedrageri (straffeloven 1902 § 270(2) / straffeloven 2005 § 371 bokstav b). I 1987 valgte man *ikke* å supplere straffeloven med særskilte bestemmelser om dataskadeverk som spesielt kunne ivareta hensynene til integritet og tilgjengelighet. I stedet la man til grunn et funksjonelt gjenstandsbegrep som innebar

[10] Den nevnte bestemmelsen ble innført ved lov av 4. desember 1992 nr. 128. Foranledningen var gjennomføringen av EFs programvaredirektiv 91/250/EØF i norsk rett (Ot.prp. nr. 84 (1991–1992), Innst. O. nr. 6 (1992–1993)). Ved gjennomføringen av opphavsrettsdirektivet 2001/29/EF ble bestemmelsen omnummerert til § 53c, jf. lov av 17. juni 2005 nr. 97 (Ot.prp. nr. 46 (2004–2005), Innst. O. nr. 103 (2004–2005)). Åndsverkloven 1961 ble avløst av ny åndsverklov av 15. juni 2018 nr. 40 (åndsverkloven 2018), hvor bestemmelsen er videreført som § 101.
[11] Endringslov 7. april 1995 nr. 15. Ot.prp. nr. 4 (1994–1995) kap. 11, Innst. O. nr. 34 (1994–1995) kap. 10.
[12] Sieber (2005), s. 85.
[13] Sieber (2005), s. 85.
[14] Datasikkerhetshensynene er beskrevet i I.M. Sunde, *Datakriminalitet,* Fagbokforlaget, Bergen 2016, kapittel 2.3. Hensynene er reflektert i sikkerhetsloven av 1. juni 2018 nr. 24 § 5-2 bokstavene a–c og § 6-2 bokstavene b–d, politiregisterloven av 28. mai 2010 nr. 16 § 15, og i personopplysningsloven av 15. juni 2018 nr. 38 GDPR artikkel 32 bokstav b. Den sistnevnte bestemmelsen tilføyer også «robusthet» blant hensynene.
[15] Endringslov 12. juni 1987 nr. 54. NOU 1985: 31 *Datakriminalitet*, Ot.prp. nr. 35 (1986–1987), Innst. O. nr. 65 (1986–1987).
[16] Sunde (2016), s. 27.

at uberettiget endring eller sletting av data var å anse som skade på datasystemet. Datasystemet er «en gjenstand» beskyttet av skadeverksbestemmelsen (straffeloven 1902 § 291 / straffeloven 2005 § 351 første ledd), og dermed var man tilstrekkelig dekket opp i loven.[17]

Den siste «bølgen», som slo inn på 2000-tallet, bør heller karakteriseres som en «tsunami» på grunn av den akselererende digitaliseringen av samfunnet. Man innså nå at datamaskiner og datanettverk også brukes som verktøy til å begå *tradisjonell* kriminalitet som f.eks. omsetning av narkotika og våpen på internett, og hvitvasking av utbytte fra straffbare handlinger. Videre har seksuelle overgrep mot barn på internett, ofte ved direktesendt videooverføring *(live streaming)* blitt et stort samfunnsproblem, ikke bare i Norge, men globalt.[18] Også tilretteleggelse for å begå datakriminalitet ved programmering og spredning av skadelig dataprogram, og utleie av kriminelle online-tjenester f.eks. for å begå DDOS-angrep, ble løftet frem som en trussel. Straffebestemmelser som slår ned på dette, er inntatt i både straffeloven 2005 §§ 201, 203 første ledd og 370 og åndsverkloven 2018 § 99, jf. § 79. Endelig kan det nevnes at identitetskrenkelse ble ansett som et betydelig problem, og ledet til innføringen av § 190 a i straffeloven 1902, videreført i straffeloven 2005 § 202.[19]

Til forskjell fra politiet er de kriminelles virksomhet ikke bundet til nasjonalt territorium. Det asymmetriske forholdet mellom politi og lovbryter er sammen med *anonymitet* på internett (både for individer og transaksjoner) og *kryptering* som gjør det vanskelig å skaffe bevis, sterke drivere for utvikling av straffeprosessuelle løsninger for den digitale tidsalderen og å sørge for mer hensiktsmessige internasjonale samarbeidsformer. Dertil synes interessen for å avklare hvilke forebyggende tiltak politiet kan utføre på internett, å være økende. Disse områdene er et kriminalpolitisk minefelt hvor hensynene til personvern, ytrings- tros- og forsamlingsfrihet brytes mot behovet for en rimelig effektiv kriminalitetsbekjempelse. Kompleksiteten forsterkes av den betydelige usikkerheten som gjelder for praktiseringen av de folkerettslige suverenitets- og territorialprinsippene på internett. Rettsutviklingen på disse områdene har gått tregere enn for datakrimstrafferetten.

3. Internasjonalt samarbeid

På grunn av internetts åpne globale struktur ser man i mange land fordeler med å harmonisere straffelovgivningen (i vid forstand), og en rekke internasjonale instrumenter er utviklet for dette

[17] NOU 1985: 31, punkt 4.3.4, Ot.prp. nr. 35 (1986–1987) punkt 3.
[18] Kripos, *Seksuell utnyttelse av barn og unge over internett*. Rapport, mars 2019; Europol Internet Organised Crime Threat Assessment (iOCTA) 2018, Strasbourg, kapittel 5.
[19] Innført i straffeloven 1902 ved lov 10. desember 2010 nr. 73. Prop. 14 L. (2010–2011), Innst. 89 L (2010–2011).

formålet.[20] Viktigst er Europarådets datakrimkonvensjon fra 2001 (CETS 185), som for Norge trådte i kraft 1. oktober 2006. Konvensjonen er åpen for stater også utenfor Europa, og er per april 2019 ratifisert av 63 nasjoner, blant annet USA.[21] Konvensjonen tjener dessuten som modell for lignende regionale folkerettslige instrumenter. Konvensjonen angir minimumsforpliktelser og har tre hoveddeler. For det første har den en strafferettslig del som lister opp ni typer datakriminalitet konvensjonspartene må kriminalisere.[22] En jurisdiksjonsbestemmelse (artikkel 22) skal sørge for at handlinger som rammes av bestemmelsene på listen, skal anses straffbare uansett hvor de er begått. For det andre har den en straffeprosessuell del som skal sørge for at data kan sikres som bevis, og for det tredje en del om internasjonalt samarbeid. Tanken er at hvis alle land sørger for at lovverket gir hjemmel for å sikre data som bevis,[23] og de internasjonale samarbeidsavtalene forholder seg til de nevnte straffeprosessuelle metodene for slik bevissikring, bedres de rettslige rammevilkårene for internasjonalt samarbeid i strafforfølgningen av kriminalitet. I utgangspunktet tenkte man nok mest på å ramme datakriminalitet som nevnt i konvensjonen artikkel 2 til 10, men man hadde også tradisjonell kriminalitet for øye. Konvensjonen forplikter derfor partene også til å samarbeide om tilgang til databevis for enhver straffbar handling, se artikkel 14 bokstav c, sammenholdt med artikkel 25 og de øvrige bestemmelsene om internasjonalt gjensidig samarbeid. Hvert land skal dessuten utpeke et 24/7 kontaktpunkt for internasjonale henvendelser om bistand, en rolle som i Norge er tillagt Kripos. Verdt å nevne er at konvensjonen også har en bestemmelse som sier noe om hva nasjonalt politi kan gjøre internasjonalt på internett *uten* å gå veien om en formell samarbeidsprosedyre (artikkel 32).

4. Kulminasjon av datakrimretten

Med den siste «bølgen» kulminerte den datakrimrettslige agendaen. Den gjennomgående digitaliseringen gjelder alle samfunnsområder og angår alle rettsfelt. Per i dag utvikles derfor datakrimretten i tilknytning til avgrensede rettsspørsmål, ikke etter en bred programerklæring slik man så med datakrimkonvensjonen. For tiden synes adgangen til bevissikring i utlandet og tilhørende

[20] For en utførlig oversikt over relevante internasjonale instrumenter innen Europarådet, OECD, EU og FN vises det til S. Schjølberg, *Cyberkriminalitet*, Universitetsforlaget 2017, kapittel 3 og 4.
[21] Ratifikasjonsliste på Europarådets nettsted https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=afk4Jfwx (besøkt 9. april 2019).
[22] Lovbruddene er ulovlig tilgang til data (artikkel 2), ulovlig oppfanging av data (artikkel 3), inngrep i dataenes integritet (artikkel 4), inngrep i driften av et datasystem (artikkel 5), misbruk av innretninger og tilgangsdata (artikkel 6), datarelatert falsk (artikkel 7), datarelatert bedrageri (artikkel 8), straffbare handlinger knyttet til barnepornografi (artikkel 9) (merk at «barnepornografi» er ordet som er brukt i den norske oversettelsen av konvensjonen inntatt i NOU 2007: 2 på s. 185. Denne ordbruken er senere forlatt), og straffbare handlinger knyttet til krenkelse av opphavsrett og nærstående rettigheter (artikkel 10).
[23] Om bevissikring, se Maria Astrup Hjorts artikkel i dette nummer av TfS.

jurisdiksjonsspørsmål å stå i fokus, aktualisert av USAs Cloud Act og EUs E-Evidence-initiativ.[24] I Norge kom spørsmålet om ransakingsadgangen på utenlandsk server opp i HR-2019-610-A. Spørsmålet begrenset seg til å gjelde ransaking hvor tilgangen var oppnådd ved ordinær pålogging fra foretakets (datainnehaverens) lokaler i Norge. Høyesterett fant at dette ikke stred mot suvereniteten til landet hvor serveren som lagret dataene, var plassert.

Kjennelsen sier ikke hvordan det stiller seg med bruk av dataavlesing for å oppnå det samme. Dataavlesing kan gjennomføres ved regulær hacking, jf. straffeprosessloven (strpl.) § 216p første ledd annet punktum som sier at politiet kan «bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å gjennomføre avlesingen». Med dette mener loven andre fremgangsmåter enn pålogging, fremgangsmåter som kan være vanskeligere å kontrollere og som kan berøre flere enn den som dataavlesingen retter seg mot. Slike omstendigheter kan tenkes å innvirke på vurderingen av suverenitetsspørsmålet. Et annet spørsmål er hvordan det stiller seg med adgangen til å føre et bevis hvor innhentingen har brutt med det folkerettslige suverenitetsprinsippet. Utgangspunktet er at ulovlig innhentet bevis kan føres, jf. prinsippet om fri bevisførsel og hensynet til den materielle sannhet. Reglene om bevisavskjæring har først og fremst tiltaltes situasjon for øye, dvs. om innhenting krenker tiltaltes integritet, og dette er jo ikke tilfellet ved internasjonal ransaking som nevnt.

Teknologiutviklingen gir generelt nye muligheter for politiet og har derfor til dels blitt satt på dagsordenen uavhengig av datakrimfenomenene. Et eksempel er kommunikasjonskontroll som er regulert i straffeprosessloven kapittel 16 a. Fra 1970-tallet ble metoden tillatt brukt i stadig større utstrekning på grunn av utviklingen av narkotikakriminalitet og organisert kriminalitet. Grunnen til at metoden er inntatt i datakrimkonvensjonen (artikkel 20 og 21), er at den etter sin art retter seg mot innsamling av databevis (elektronisk kommunikasjon og metadata). Konvensjonen skal imidlertid bare sikre at konvensjonspartene har hjemmel for metodebruken og kan bistå hverandre med å utnytte den. Videre har teknologiprodusentenes integrering av krypteringsbeskyttelse på alminnelige kommunikasjonstjenester bidratt til å presse frem adgangen til å bruke dataavlesing, som nettopp nevnt. Metoden ble innført i juni 2016.[25] Metodene synes derfor å tvinge seg frem uavhengig av

[24] USAs «Cloud Act» (The Clarifying Lawful Overseas use of Data Act) er en endring i «The Stored Communication Act» fra 1986, i kraft 23. mars. 2018, jf. Publ.L. 115–141, pkt. 2.20 («the Consolidated Appropriation Act», 2018). EUs E-evidence-initiativ fra april 2018 gjelder et direktiv som skal pålegge ikke-europeiske tjenesteytere å oppnevne representanter i EU som kan utlevere data lagret utenfor EU til europeiske myndigheter i straffesaker. Kommisjonen og Rådet ser ut til å ha blitt enige, mens Parlamentet skal avklare sin posisjon. https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/ (besøkt 26. april 2019).

[25] Endringslov 17. juni 2016 nr. 54, NOU 2009: 15 *Skjult informasjon – åpen kontroll* (Metodekontrollutvalget) kapittel 23, Prop. 68 L (2015–2016), Innst. 343 L (2015–2016).

noen datakrimrettslig agenda. De skyldes samfunnsendringer som henger sammen med teknologiutviklingen.

På den kriminelle siden utpeker seksuelle overgrep mot barn på internett seg som et stort problemområde, uten at det behøver å henføres til det datakrimrettslige. Datakrimkonvensjonen pålegger riktignok å kriminalisere befatning med overgrepsbilder av barn i digital form (artikkel 9), noe man hadde registrert som et stort problem på 1990-tallet og som fortsatt er utbredt.[26] Men senere har teknologien, særlig internett og krypterte kommunikasjonsformer som Skype, medvirket til økt barnesexturisme og til at overgrep som tidligere ble begått fysisk slik som voldtekt, mange ganger begås over internett. De viktigste internasjonale instrumentene i så måte er nok FNs barnekonvensjon, og den valgfrie protokollen om salg av barn, barneprostitusjon og barnepornografi av 25. mai 2000, og Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk (CETS 201). Metoder som kan gi politiet mulighet for å komme i inngrep med nettrelaterte overgrep, krever imidlertid gode teknologiske ferdigheter og avansert utstyr, blant annet for å avdekke overgrepsfora på det mørke nettet, spore opp anonyme overgripere og foreta preventive inngrep, f.eks. ved å forstyrre fildeling av slike bilder og slå opp automatiske advarsler. Dermed har nettovergrep vært et prioritert område for Europols senter for datakriminalitet (EC3) (European Cybercrime Centre) helt siden senterets etablering i januar 2013.[27]

EC3-senterets prioriteringer etableres i samarbeid med Europol-medlemmene, og kan langt på vei forstås som en felles internasjonal trusselbeskrivelse av datakriminalitet, uten at man er så opptatt av om det dominerende aspektet er data eller karakteren av de skadelidende interessene. Disse interessene spenner dermed over et vidt spektrum, fra barns fysiske og psykiske integritet til økonomiske interesser og samfunnsinteressene i datasikkerhet og bekjempelse av hatkriminalitet og terrorisme. I henhold til EC3s trusselrapport for 2018 er følgende områder prioritert:[28]

1. «Cyber-dependent crime». Kategorien gjelder angrep på datasikkerheten og omfatter utvikling og spredning av skadelig dataprogram (strl. § 201), angrep på kritisk infrastruktur (strl. §§ 192 og 351, se også HR-2016-2333-U som gjaldt lammelse av sentrale samfunnsinstitusjoner, jf. strl. § 117).
2. «Child sexual exploitation online». Kategorien gjelder nettovergrep mot barn.[29]

[26] Kripos (2019). Punkt 6.7 nevner behovet for en samfunnsøkonomisk analyse av konsekvensene.
[27] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (besøkt 26. april 2019).
[28] Internet Organized Crime Threat Assessment (iOCTA) 2018, Europol, Strasbourg, file:///C:/Users/ingsun/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/iocta2018.pdf (besøkt 21. april 2019).
[29] For en gjennomgang av de relevante straffebestemmelsene for nettovergrep, se I.M. Sunde «Sweetie, et politibarn eller en politistyrke på internett» i I.M. Sunde & N. Sunde (red.): *Det digitale er et hurtigtog – vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi*, Bergen, Fagbokforlaget 2019.

3. «Payment fraud». Kategorien omfatter forskjellige bedrageriformer, dokumentfalsk og identitetskrenkelse.
4. «Online criminal markets». Kategorien gjelder fora på det mørke nettet for tradisjonell kriminell virksomhet.
5. «The convergence of cyber and terrorism». Kategorien gjelder bruk av internett for å begå terrorisme.

Hvert hovedområde følges opp med anbefaling om tiltak. Den tydelige inndelingen i hovedområder ble innført med iOCTA-rapporten for 2017, men har i realiteten ligget fast siden den første rapporten kom i 2014.[30]

5. Datakrimretten er et produkt av kasuistisk problemløsning

Som det har fremgått, er datakrimretten et produkt av kasuistisk problemløsning over tid. En rettsfilosofi basert på prinsipper som knytter an til særtrekk ved den gjennomgripende digitaliseringen, lar seg ikke påvise. Det eneste prinsippet som lar seg spore som et legislativt hensyn, er prinsippet om teknologinøytralitet. Nøyaktig hva prinsippet innebærer, er ikke klart, annet enn at man så vidt mulig har ønsket å unngå dataspesifikke regler.[31] Det skal sikre lik praktisering av loven uavhengig av om det er tale om fysiske handlinger eller handlinger på internett, samt sørge for at reglene er fleksible og holdbare over tid. Det kan konstateres at datakrimretten har vært nokså lukket overfor ekstern teori som f.eks. rettsinformatikken kunne ha bidratt med.[32]

I en datakrimrettens filosofi kunne de grunnleggende forholdene være karakteren av de faktiske fenomenene som gjør seg gjeldende på området, og interessene som knytter seg til disse. I tidligere arbeider har jeg vært opptatt av *fenomenene*, særlig data, informasjon og datasystem.[33] Etter hvert har jeg imidlertid kommet til at *forholdet mellom mennesket og datateknologien* burde tas opp først.

[30] iOCTA 2017 finnes her: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017. Rapporten for 2014 finnes her: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014. Alle trusselrapportene er lagt ut på dette nettstedet: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment#fndtn-tabs-0-bottom-2

[31] Ot.prp. nr. 22 (2008–2009) s. 21; «Infiltrasjon og provokasjon som etterforskingsmetode – vederlag til politiets kilder», Riksadvokatens rundskriv 2/2018 31. oktober 2018, punkt I; NOU 2016: 24 *Ny straffeprosesslov* (Straffeprosesslovutvalget) kapittel 6.2.3. I I.M. Sunde, *Automatisert inndragning*, doktoravhandling (ph.d.) nr. 37 ved Juridisk fakultet, Oslo 2010 (*Complex* nr. 3/2011 Unipub, Oslo), kapittel 6.4, påviser jeg at prinsippet er utlagt i forskjellig betydning innen strafferettens og straffeprosessretten. Se for øvrig Jul Fredrik Kaltenborns artikkel «Teknologinøytralitet og datasystem» i dette nummeret av TfS.

[32] Jeg tenker særlig på den nordiske rettsteoretiske innsatsen, hvor Senter for rettsinformatikk ved IfP, Juridisk fakultet i Oslo, har hatt en ledende rolle.

[33] Sunde (2006), kapittel 4; (2010) særlig kapittel 2; (2016) kapittel 2.

5.1 To konkurrerende grunnsyn

Samfunnsutviklingen går i retning av at det tekniske kommer inn som mellomlag ved sosial samhandling. Nettverksteknologien skaper distanse, noe vi erfarer ved netthandel og generelt ved bruk av betalingskort. Det tekniske trer også inn som et mellomlag ved borgerens kontakt med det offentlige. Der vi tidligere hadde kontakt med en saksbehandler, møtes vi nå av «Min side» på Altinn eller NAV. Karakteren av flere lovbrudd påvirkes av om handlingen anses å være begått overfor en maskin eller et menneske, men hva man står overfor, er ikke uten videre lett å avgjøre, og det kan herske ulike syn på om samhandlingen faktisk skjer med en person eller et datasystem.

En posisjon som kan kalles grunnsyn 1, er at det er uproblematisk å anse teknologien som hjelpemiddel til å gjennomføre en samhandling som ellers hadde vært utført personlig. Interaksjonen anses derfor som en sosial handling selv om den ikke skjer umiddelbart ansikt til ansikt med den andre. Tanken er at det en foretar seg, berører en person i den andre enden av den elektroniske overføringen (nettverket). Nettverksteknologien opphever derfor ikke handlingens sosiale aspekt.

En annen posisjon (grunnsyn 2) legger vekt på at samfunnsutviklingen går i retning av å utvikle stadig større og mer omfattende systemer, hvor det menneskelige innslaget er vesentlig redusert – kanskje bortfalt – og i hvert fall usynliggjort. Nettverksteknologien fjerner det sosiale innslaget i situasjoner man tidligere til daglig sto i, slik at det skjer en reell avpersonifisering. Siden det uansett ville være umulig å realisere dagens handlings- og transaksjonshyppighet bare med menneskelig innsats, har systemene (teknologien) overtatt som selvstendig aktører. Det er følgelig irrelevant om det finnes en person i den andre enden av nettverket.

Straffeloven synes å være bærer av begge grunnsynene, noe som lar seg spore i bestemmelsene om bedrageri, dokumentfalsk og identitetskrenkelse (de videre paragrafhenvisningene i dette punktet gjelder straffeloven 2005). Bestemmelsene brukes ofte i konkurrens. Loven gjennomfører likevel ikke grunnsynene konsekvent, noe som leder til anomali og uklarhet. Bestemmelsen om databedrageri (§ 371 bokstav b) kom som nevnt til i 1987 og ble ansett som nødvendig på grunn av vilkåret i den alminnelige bedrageribestemmelsen om at handlingen måtte forlede «noen», dvs. et menneske.[34] Databedrageribestemmelsen er derfor basert på grunnsyn nr. 2; det er datamaskinen som «lures». Hvis man derimot hadde basert seg på grunnsyn 1, ville datamaskinen vært et verktøy som gjennomfører den menneskelige samhandlingen, og den alminnelige bedrageribestemmelsen kunne vært tilstrekkelig. Resonnementet ville da vært at handlingen (lovbruddet) begås overfor mennesket som tilbyr hjelpemidlet.

[34] NOU 1985: 31 *Datakriminalitet*, s. 29; M. Matningsdal *Straffeloven,* kommentarutgave, Universitetsforlaget, Oslo 2017, s. 985 punkt 7.

Kortsvindel er et praktisk eksempel og er som nevnt prioritert av Europol.[35] Etter gjeldende rett anses betaling med stjålet eller ettergjort betalingskort som databedrageri.[36] Dette følger av grunnsyn 2, som utelukker at handlingen har et sosialt aspekt. Ordlyden i den alminnelige bedrageribestemmelsen sier imidlertid ikke at forledelsen må skje ansikt til ansikt med fornærmede. Etter grunnsyn 1 kunne bestemmelsen vært fortolket slik at forledelsen skjedde overfor de ansatte i kortselskapet som forledes til å foreta utbetaling til brukerstedet på uriktige premisser. Et uttrykk for dette synet finnes i Rt. 2009 s. 397 hvor det ble domfelt for kortsvindel. Ifølge tiltalen hadde domfelte medvirket til «å forlede […] ansatte i kredittkortselskapet Visa […] til å utbetale verdier […] idet han tillot at det ble benyttet falske kredittkort på stedets betalingsterminal […]» (dommen, avsnitt 4). Domfellelsen gjaldt imidlertid overtredelse av databedrageribestemmelsen, noe som ikke harmonerer med grunnlaget.

Ved bruk av kort som er stjålet eller ettergjort, trekkes beløpet på kontoen (eller fra kreditten) til en tredjepart som er offer for identitetskrenkelse, jf. § 202. Ifølge forarbeidene er bestemmelsen basert på grunnsyn 1, nemlig at den rettsstridige bruken av identiteten (i dette tilfellet betalingskortet) må ha skjedd overfor et menneske (dette er en annen person enn den som får sin identitet misbrukt).[37] Handlingen vil også innebære bruk av ettergjort eller falskt dokument, jf. § 361 bokstav b. Det strafferettslige dokumentbegrepet som fremgår av § 361 annet ledd, er basert på grunnsyn 1 fordi informasjonsbæreren etter sikker rett må gi uttrykk for en «menneskelig tanke» eller et «budskap».[38] Bare mennesker kan være mottakere av menneskelige budskap.

Spørsmålet er om det virkelig var behov for bestemmelsen om databedrageri når man ellers i datatekniske omgivelser klarer seg godt med andre bestemmelser som forholder seg til mennesker, slik som §§ 202 og 361? Rettstilstanden fremstår som en anomali fordi man for samme handling (dvs. at man uberettiget trekker betalingskortet) kan dømmes for databedrageri («påvirker en automatisert databehandling»), dokumentfalsk (formidling av et menneskelig budskap) og identitetskrenkelse («opptrer» overfor et annet menneske). Det kan likevel være at grunnsyn 2 må anses som mest realistisk, men da burde man også forlate læren om at dokumentfalsk går ut på formidling av et menneskelig budskap, og at identitetskrenkelse kun kan begås gjennom en handling som utspiller seg overfor et annet menneske.[39] Etter strl. § 361 annet ledd er innholdskravet til et

[35] «Payment fraud» skiller mellom bedrageri hvor kortet er til stede, og bedrageri basert kun på bruk av betalingsopplysningene («card-not-present fraud»), iOCTA (2018) kapittel 6.
[36] Matningsdal (2017) s. 985 punkt 8.1.
[37] Ot.prp. nr. 22 (2008–2009) s. 45.
[38] Matningsdal (2017), s. 951, punkt 16.1.
[39] Bestemmelsen om identitetskrenkelse ivaretar flere forskjellige interesser, blant annet personvernet til den hvis identitet krenkes, og datasikkerhet ved netthandel. Blandingen har ledet til en vanskelig tilgjengelig bestemmelse. Se for nærmere behandling Sunde (2016), kapittel 8.

strafferettslig dokument at det må gjelde «et rettsforhold eller ellers [egne] seg som bevis for et rettsforhold». Den som bruker betalingsopplysninger som ikke tilhører en selv, pretenderer å ha disposisjonsrett over bestemte penger, altså å ha en rettighet. Dette oppfyller dokumentvilkåret, men behøver ikke utlegges som om et menneske må kunne lese innholdet i magnetstripen. Lignende situasjoner kan oppstå i andre sammenhenger, f.eks. ved bruk av stjålet boardingkort hvor QR- eller strekkoden inneholder den relevante informasjonen.

Den alminnelige bedrageribestemmelsen og bestemmelsen om databedrageri har så lite til felles at det kunne vært hensiktsmessig heller å regulere forbrytelsene i separate paragrafer. Alminnelig bedrageri skjer i en synkron situasjon hvor den som forledes, forholder seg til lovbryteren. Databedrageri kan involvere personer i enden av nettverksforbindelsen, men kun som en perifer tredjepart som står utenfor situasjonen som utløser kortbruken. Bruk av stjålet kort i butikk kan derfor bringe uklarhet med hensyn til om det er personen i kassen som er fornærmet (alminnelig bedrageri), eller om fornærmede er personer i kortselskapet (alminnelig bedrageri etter grunnsyn 1, men databedrageri etter grunnsyn 2), eller om det bare er datasystemet til kortselskapet (grunnsyn 2).[40] Uklarheten kan også ha betydning for forsettet, dvs. hvilke fakta lovbryteren må ha vært klar over da han brukte kortet. Under bevisførselen i hovedforhandlingen kan det bli klart at det er tale om databedrageri i stedet for alminnelig bedrageri som tiltalen gjelder (eller vice versa). Dermed oppstår spørsmålet om adgangen til å endre subsumsjonen, jf. strpl. § 38.[41] Hvis det ikke er adgang til dette og resultatet er frifinnelse, må dommen antas å sperre for ny sak med tiltale for databedrageri siden denne måtte bygge på det samme faktum som tiltalen i den frifinnende dom, jf. EMK protokoll 7 artikkel 4.[42] I så fall bør muligheten for å ta ut subsidiær tiltale og dermed dekke begge muligheter vurderes, og slik unngå å bli sperret av forbudet mot dobbeltforfølgning.

Både strafferettslig og prosessuelt tilstreber loven en individualisering av forholdet, noe vi blant annet ser i læren om konkurrens og om hva som er «samme forhold», jf. strpl. § 38. Dette taler for å løse opp betalingssituasjonen i flere bestanddeler slik at interessene til kortselskapet og brukerstedet (nettbutikken / den fysiske butikken) behandles separat. En uberettiget anskaffelse av en vare kan bedømmes som tyveri overfor butikken, jf. § 321, og som (data)bedrageri overfor kortselskapet. Men dersom anskaffelsen gjelder *en tjeneste*, er ikke tyveribestemmelsen anvendelig. Med tanke på tjenesteyterens (butikkens) situasjon synes det her å være et rettslig tomrom.

[40] Bedrageriformene er behandlet i Sunde (2016) kapittel 7.
[41] Straffeprosessloven er lov av 22. mai 1981 nr. 25.
[42] M. Holmboe & H.-P. Jahre, «Dobbeltstraff er ikke enkelt – gjentatt strafforfølgning etter Den europeiske menneskerettskonvensjon protokoll 7 artikkel 4 – en oppdatering», *Lov og Rett* 4/2011, s. 191–212.

5.2 Fenomenforståelse

Når det gjelder *fenomenene*, er spørsmålet om data burde regnes som et formuesgode, en sentral problemstilling. Eiendomsrett oppstår blant annet når man har skapt eller mottatt en ting, og til daglig skaper og mottar vi en betydelig mengde data. Konkret erfares dette når vi mottar varsel om at lagringsplassen er oppbrukt, f.eks. på ferier når vi tar mange bilder. Da smarttelefonen var ny, var lagringsplassen tom. Som følge av data vi har skapt eller fått, er lagringsplassen fullt utnyttet. Dataene må forvaltes, f.eks. ved selektiv sletting eller overføring til et annet lagringsmedium, f.eks. en skytjeneste. Denne forvaltningen vil vi gjerne forestå selv. Selv om bildene har lav kvalitet sett fra et profesjonelt ståsted, kan de ha stor personlig verdi, og datatap kan oppleves som en ulykke. Etter alminnelige eiendomsrettslige synspunkter burde data man har skapt eller mottatt, anses som et formuesgode og nyte det alminnelige vern som straffeloven gir formuesgoder, så langt som disse bestemmelsene passer for data. Skadeverksbestemmelsen (§ 351) annet ledd tyder på at lovgiver har tenkt slik, fordi den straffer den som skader «andres data». Forarbeidene tyder imidlertid på at bestemmelsen ble ansett som nødvendig nettopp fordi data *ikke* regnes som «gjenstand».[43] Dette legislative standpunktet bryter imidlertid med det tidligere omtalte prinsippet om teknologinøytralitet. Gjenstandsbegrepet brukes ellers i bestemmelsene som verner formuesgoder, blant annet i skadeverksbestemmelsen første ledd og i § 324 om underslag.

Borgerne er i økende grad avhengig av tjenester for datalagring, og mens de personvernrettslige aspektene ved dette lenge har fått stor oppmerksomhet, sist ved GDPR, har man i liten grad vært opptatt av å verne data som formuesgode. Hvordan stiller det seg da om en tilbyder av lagringsplass (skytjeneste) uberettiget kopierer data som er betrodd ham? En utro tjener hos tjenesteyteren kan nok staffes for utroskap mot arbeidsgiveren, jf. Rt. 1992 s. 1463 (Vekterdommen), men hvordan ivaretas interessene til datainnehaveren? Etter ordlyden er underslagsbestemmelsen anvendelig, men ordet «gjenstand» skal altså ifølge forarbeidene tolkes innskrenkende og utelate data. Straffeloven § 204 (innbrudd i datasystem) må selvsagt vurderes, men denne strekker ikke til dersom tilgangen som sådan ikke var uberettiget. Uansett er det *datatilegnelsen* som er det vesentlige ved krenkelsen, og denne er bare et straffutmålingsmoment i forhold til § 204. Andre bestemmelser til vern om informasjon kommer bare til anvendelse dersom datainnholdet er av kvalifisert art, f.eks. at det oppfyller krav til å være en bedriftshemmelighet, jf. § 208. En annen mulighet er å anse

[43] Forståelsen er i hvert fall nærliggende, selv om bemerkningene om annet ledd direkte synes å være foranlediget av at bestemmelsen om urettmessig bruk av bedriftshemmeligheter ble flyttet, se Ot.prp. nr. 22 (2008–2009) s. 304, spalte 1 nederst og øverst spalte 2. Om gjenstandsbegrepet slås det bare fast at gjeldende rett (før straffeloven 2005) var at data ikke var å regne som gjenstand (s. 303). Rettstilstanden skulle videreføres uten realitetsendringer (s. 303), uten nærmere vurderinger.

kopieringen som en fredsforstyrrelse, jf. § 266, men denne løsningen må sies å være usikker.[44] Når det gjelder de økonomiske interessene som knytter seg til data – nærmere bestemt «den digitale økonomien» – synes immaterialrettighetene å ha vært dominerende. Men disse gjelder dataenes innhold og er ikke utformet for å ivareta den alminnelige borgers behov for vern av sine digitale objekter. Sterke reelle hensyn taler derfor etter mitt syn for å se bort fra forarbeidene og anse den uberettigete tilegnelsen som underslag.

Et annet spørsmål gjelder forståelsen av skadeverksbestemmelsen i forhold til data og datasystem. Etter § 351 første ledd straffes den som skader en «gjenstand som tilhører en annen». Et datasystem kan settes ut av drift eller bli feilfungerende som følge av uberettigete endringer i programutrustningen. Programutrustningen er strengt tatt bare data, noe som omfattes av ordlyden i annet ledd, jf. «andres data» som tidligere nevnt. Etter det såkalte funksjonelle gjenstandsbegrepet som ifølge forarbeidene opprettholdes for den nye straffeloven, er uberettiget endring av data å regne som skade på datasystemet.[45] Spørsmålet blir da hva som er restområdet for annet ledd. Den naturlige antakelse er at data skal ha en egenbeskyttelse som formuesgode. Læren om det funksjonelle gjenstandsbegrepet gjelder i så fall ikke fullt ut. Sondringen mellom første og annet ledd-tilfellene ville imidlertid vært unødvendig dersom man hadde lagt til grunn at et datasystem er én formuesgjenstand, og at data man har rådighet over, er en annen formuesgjenstand. Begge tilfellene ville falt under første ledd, og annet ledd kunne vært fjernet. Loven ville sett enklere ut og vært lettere å praktisere.[46]

Etter tilsvarende tankegang kunne man – slik jeg tidligere har tatt til orde for – også regulere inndragning av ulovlig innhold på internett.[47] Ved å tilordne det ulovlige datamaterialet unik identitet som kan gjenkjennes uansett hvor det forekommer, kan filtrering utføres. Ordningen vil ikke medføre en fullstendig blokkering av det ulovlige materialet, men kunne redusere tilgjengeligheten vesentlig. I tillegg kunne systemet reguleres på tydelig vis slik at man sikret seg notoritet og kontrollerbarhet i samsvar med rettsstatlige verdier. I dag skjer regulert filtrering så vidt vites bare for å ivareta opphavsrettslige interesser i medhold av åndsverkloven 2018 § 88 flg. Et tilsvarende system er ikke innført f.eks. for å hindre tilgang til overgrepsbilder av barn. Tiltakene er først og fremst iverksatt av politiet i forebyggende øyemed, uten formell regulering i lov og tilhørende kontrollordninger.[48]

[44] Løsningen ville imidlertid harmonere med det jeg anfører om statusen til data i forbindelse med beslag, se punkt 6.
[45] NOU 1985: 31 *Datakriminalitet*, s. 10; Ot.prp. nr. 22 (2008–2009) s. 303, dog uten nærmere vurderinger.
[46] Bestemmelsene om skadeverk, driftshindring og sabotasje er nærmere behandlet i Sunde (2016) kap. 6.
[47] Sunde (2010).
[48] Noen slike tekniske inngrep i den elektroniske kommunikasjonen er omtalt i Kripos (2019) kap. 7.3.

6. Nytenkning om de straffeprosessuelle tvangsmidlene?

På det straffeprosessuelle området er det særlig tvangsmidlene som berøres av teknologiutviklingen. Straffeprosesslovutvalget har som nevnt basert seg på prinsippet om teknologinøytralitet og verken foreslått endringer eller nye løsninger foranlediget av teknologiutviklingen. Det skal sies at tvangsmidlene ikke veide tyngst i utvalgets mandat, fordi de alt hadde blitt utredet.[49] Senere har regjeringen varslet nedsettelse av et nytt offentlig utvalg for å evaluere dagens politimetoder.[50]

Jeg skal her bare reise ett poeng, og det gjelder at for databevis er de metodiske skillene mellom ransaking og beslag på den ene siden og kommunikasjonsavlytting på den andre i ferd med å brytes ned.[51] Hybriden dataavlesing føyer seg inn i problemstillingen. Hvis konseptene i realiteten smelter sammen, er det spørsmål om de i større grad burde reguleres under ett, i stedet for i en rekke forskjellige bestemmelser som det er vanskelig å få oversikt over. Spesifikt for databeslag synes det derimot å være behov for *flere* regler enn i dag.

Disse tankene har gjenklang hos den nederlandske jussprofessoren Bert-Jaap Koops som skriver at såkalte grensemarkerende konsepter representerer en viktig utfordring for loven i konfrontasjon med ny teknologi.[52] Koops tar for seg kroppen («body») og privat sted («private space») som grensemarkører for den private sfæren, mens jeg har fokusert på konseptene som ligger til grunn for tvangsmidlene. Koops viser at i møte med teknologien kan de tradisjonelle oppfatningene om hva som konstituerer – og hva som kan krenke – kropp og privat sted, bli utdaterte. Dermed risikerer det rettslige rammeverket for vern av menneskelig integritet og privatliv å kollapse.

Spørsmålet er altså om teknologiutviklingen tilsier at det tenkes nytt ved reguleringen av tvangsmidlene. Et klargjørende grep kunne være å regulere ransaking og beslag rettet mot data separat fra den tilsvarende tvangsmiddelbruken i fysiske omgivelser. Den gang ransaking og beslag kun rettet seg mot fysiske rom og objekter, var ransaking en fredsforstyrrelse. Beslag av fysiske objekter var i første rekke et inngrep i eiendomsretten. Ransaking av elektroniske (virtuelle) rom og beslag i data synes derimot i første rekke å innebære inngrep i kommunikasjon og uforstyrret

[49] Dette følger av punkt 5 i Straffeprosesslovutvalgets mandat, NOU 2016: 24 s. 95.
[50] Dette ble varslet i Jeløya-plattformen, 14. januar 2018, punkt 4, og på nytt i Granavolden-plattformen 17. januar 2019, punkt 4.
[51] Dette bygger videre på mitt kapittel «Straffeprosessuelle metoder rettet mot elektroniske bevis» i *Rettssikker radikaler – Festskrift til Ståle Eskeland 70 år*, Cappelen Damm Akademisk 2015, s. 266–283.
[52] B.-J. Koops, «On legal boundaries, technologies, and collapsing dimensions of privacy», *3 Politica e Societá* (2), 2014, s. 247–264. Temaet er fulgt opp i B.-J. Koops & Masa Galic, «Conceptualising space and place. Lessons from geography for the debate on privacy in public», i T. Timan, B.C. Newell & B.-J. Koops (eds.) *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar), s. 19–46, 2017. Det er ikke vist til Koops' artikkel fra 2014 i mitt arbeid fra 2015, fordi jeg først ble oppmerksom på den senere.

utvikling av sosiale relasjoner. De tilsvarer dermed inngrepet ved kommunikasjonsavlytting og har lite til felles med inngrep overfor fysiske objekter.

Her foreligger det også et merkelig paradoks fordi man i straffeprosessuell sammenheng har lagt til grunn at data kan anses som «ting», jf. strpl. § 203 om beslag, og derfor inntatt motsatt posisjon av strafferetten, jf. det som er sagt i punkt 5.2. Men til forskjell fra det som er tilfellet i strafferetten, er det for tvangsmiddelbruken mye som tyder på at data nettopp burde behandles annerledes enn fysiske objekter. De legislative posisjonene burde derfor vært omvendt.

Etter mitt syn bør ikke skillelinjene for digital tvangsmiddelbruk gå etter om objektet er lagret eller under overføring, men etter om metoden er skjult eller ei. Denne grensedragningen har betydning for den som utsettes for inngrepet, for tilliten til politiet og rettsapparatet, for kontrollproblemer og de rettssikkerhetsgarantier som må kreves av metoden.

For databeslag burde imidlertid reguleringen bli tydeligere. Høyesterett har i en rekke saker måttet tolke ransakings- og beslagsreglene, noe som sier sitt om behovet. Bakgrunnen er at politiet sikrer mer data enn det er adgang til etter reglene om beslagsforbud, relevanskrav og forholdsmessighetsvurderinger. Men det er flere grunner til at databeslag ofte blir svært omfattende. For det første er den kriminaltekniske metoden innrettet på å unngå at dataene endres (integritetshensynet), noe som har ledet til at alle data på hvert lagringsmedium kopieres.[53] Hvis man likevel skulle foreta et utvalg av data, er denne vurderingen ofte umulig å gjennomføre mens ransakingen pågår, fordi datamengdene er så store. Også derfor kopieres alt, eller i hvert fall mye.[54]

Hvis politiet også i fremtiden er henvist til å bruke verktøy og prosedyrer som resulterer i sikring av omfattende datamengder, bør loven stille tydelige krav til den etterfølgende behandlingen av data. Dataene vil nødvendigvis inneholde mye overskuddsinformasjon, og regler for håndtering av denne burde oppstilles. Loven burde også gi regler for adgangen til å gå utenfor det forhold siktelsen gjelder, ved analysen av beslaget. Per i dag er det bare forholdsmessighetsvurderinger som eventuelt kan begrense dette. Ytterligere burde loven oppstille klare dokumentasjonskrav når det gjelder fremgangsmåten for analysen. Dokumentasjonskravet burde ikke bare omfatte hvilke søk politiet har gjort i materialet, men også hvilke deler av materialet som politiet beviselig *ikke* har søkt i. Dette bør i hvert fall gjelde dersom det er grunner til å nekte innsyn i hele databeslaget, slik man f.eks. så i Rt. 2011 s. 1188 (hensyn til personvernet til utenforstående tredjepersoner og generelle taushetshensyn). Tiltalte skal ha samme tilgang til dokumentene som påtalemyndigheten, og dersom

[53] Om den rettstekniske fremgangsmåten for sikring av databevis vises det til A. Flaglien, «The Digital Forensic Process» i A. Årnes (red.), *Digital Forensics,* John Wiley & Sons, UK 2018, kapittel 2, s. 13–49.
[54] Jeg har beskrevet politiets problemer med relevansvurderingen ved databeslag i «Databevis», i R. Aarli, M.A. Hedlund og S.E Jebens (red.), *Bevis i straffesaker – utvalgte emner,* kapittel 17, s. 599–633.

påtalemyndigheten ønsker å begrense innsynet under henvisning til at den selv ikke har sett på det hele, bør dette dokumenteres. Endelig bør det innføres etterkontroll med overholdelse av vilkårene. Per i dag utføres etterkontroll av Kommunikasjonskontrollutvalget for kommunikasjonskontroll for skjulte metoder. Utfordringene skapt av datautviklingen gir imidlertid behov også for å kontrollere åpne metoder som beslag, dersom det innføres begrensninger på politiets håndtering av de store datamengdene som sikres.

Slike regler vil selvsagt kreve utstyr, prosedyrer og ressurser til politiet for å kunne overholdes, men de er nødvendige for å ivareta tiltaltes prosessuelle rettigheter, av hensyn til reglene om beslagsforbud, og generelt for å profesjonalisere håndteringen av databevis.

7. Avslutning

Artikkelens formål var som nevnt å gi en oversikt over datakrimretten. Et felt som ikke er beskrevet, gjelder politiets forebyggende arbeid på internett. Området har hittil påkalt liten rettslig interesse, men min spådom er at dette fort kan bli det mest brennbare, blant annet i jurisdiksjonsdiskusjonen, hvor omdreiningspunktet hittil har vært etterforskingsadgangen. For hvem skal bestemme at politiet skal kunne heve pekefingeren på bestemte kanaler på internett? Ved juletider 2018 skjedde et tragisk drap i Sandnes. Det viste seg at drapsmannen hadde luftet planene sine på en pratekanal på 4chan, hvor handlingen til dels hadde blitt heiet frem av de andre deltakerne.[55] I ettertid oppsto det spørsmål om muligheten til å gripe inn og avverge handlingen. På 4chan er imidlertid deltakerne anonyme, snakker engelsk, og deres nasjonalitet er ukjent. Flere tusen pratekanaler kan være aktive på samme tid. Hvordan skulle norsk politi kunne vite om samtalen? Og om man visste, hvordan skulle man kunne vite at planlegningen gjaldt et drap i Norge? Har ethvert lands politi adgang til å overvåke slike pratekanaler? Burde de ha det? Og hvordan burde advarsler og avvergende inngrep arte seg? Videre er det spørsmål om hvem som skal drive forebyggende arbeid på det vi oppfatter som norske hjemmesider i sosiale medier som ofte eies av utenlandske foretak. Kunne vi for eksempel tenke oss at amerikansk eller kinesisk politi begynte å legge ut formaninger på norske Facebook-sider? Er det i det hele tatt relevant å snakke om «norske sider» når tjenestene ytes av utenlandske foretak? Kort sagt er det viktig å avklare etter hvilke «områdeprinsipper» norsk politi kan drive forebyggende arbeid. Disse spørsmålene er meg bekjent foreløpig ikke tydelig tatt opp og behandlet, men her ligger åpenbart mange interessante spørsmål, også av rettslig art.

[55] Se eksempelvis Aftenposten 25. desember 2018 (https://www.aftenposten.no/norge/i/4d4prR/--Hvis-dette-er-ekte_-har-vi-drevet-en-mann-til-drap) og VG 27. desember 2018, https://www.vg.no/nyheter/innenriks/i/xRB6OQ/forsker-om-posting-paa-nettforum-foer-sandnes-drapet-hvis-ikke-du-gjoer-det-mister-du-all-respekt (begge besøkt 22. april 2019).