«Effektiv, tillitvekkende og rettssikker behandling av databevis»

-

En straffeprosessuell utredning om ransaking, sikring og beslag i data

Avgitt til Justis- og beredskapsdepartementet

18. juni 2021

Inger Marie Sunde
Professor, Politihøgskolen

Effektiv, rettssikker og tillitvekkende behandling av databevis

Innhold

Effektiv, rettssikker og tillitvekkende behandling av databevis

1. Sammendrag

Utredningen behandler de rettslige spørsmålene i del III-VII. Som bakgrunn for utredningens analyser og forslag beskriver Del II *Praktisk bevishåndtering* utfordringer, dilemmaer og fremgangsmåter ved sikring og analyse av databevis i etterforskingen. Det er innhentet opplysninger fra dataetterforskere ved enheter for Digitalt PolitiArbeid (DPA) (kapittel 4). I tillegg beskrives metodikken for behandling av databevis (kapittel 5).

Den påfølgende rettslige analysen innledes med en presentasjon av lovtekniske overveielser (kapittel 6) og menneskerettslige utgangspunkter (kapittel 7).

Utredningen skiller mellom to faser i ransakingsprosessen. Del IV *Fase én – ransaking og sikring av data* presenterer gjeldende rett for ransaking og beslag i data (kapittel 8). Deretter drøftes det rettslige grunnlaget for ransaking av en databærer, og noen lovendringer for å klargjøre dette foreslås (kapittel 9). Det skilles mellom undersøkelser (ransaking) av originale data, og data som sikres for å være gjenstand for søk i etterkant. Ransaking av originale data foreslås tydeligere regulert (kapittel 10). Videre foreslås det en ny straffeprosessuell bestemmelse om sikring av data (kapittel 11). Endelig behandles hemmelig ransaking av databærer. Hjemmelsgrunnlaget foreslås endret slik at hemmelig ransaking av databærer omfattes av bestemmelsene om dataavlesing i strpl. §§ 216 o og p, i stedet for som i dag, av strpl. § 200 a (kapittel 12). Etterkontroll av KK-utvalget anses å være nødvendig uansett hvordan man ser på hjemmelsspørsmålet.

Del V *Fase to – ransaking og beslag av sikrede data* reiser spørsmål rundt rettssikkerheten og de rettslige rammene for ransaking og beslag i sikrede data. Flere av dagens problemer bør avklares gjennom retningslinjer for denne fasen, noe som gis i utkastet til forskrift om databevis (kapittel 14). Videre behandles innsynsretten i sikrede data, og en forskriftsbestemmelse om at siktede/forsvareren rutinemessig skal gis kopi av dataene som er sikret hos siktede (kapittel 15).

Del VI *Beslagsfrie data* drøfter fremgangsmåten for behandling av beslagsfrie data. Temaet inneholder sterke interessemotsetninger og løsninger avhenger også av tilgjengelig teknologi. For så vidt gjelder det siste har det vært vanskelig å avklare hva som er teknisk *umulig* og hva som er teknisk *mulig*, men så komplisert og tidkrevende at det *ikke er praktisk mulig* innen rammene av en etterforsking. Forhåpningen er at innspill i høringsrunden vil oppklare dette. Utredningen fremmer alternative forslag. Hovedforslaget er basert på prinsippene om at de sikrede dataene bør holdes intakt; tingrettens oppgave bør begrenses til det tingretten har forutsetninger for å gjøre; forsvarerens bistand til tingretten med å identifisere taushetspliktig

materiale må ikke medføre at taushetspliktige opplysninger tilflyter påtalemyndigheten; og, påtalemyndighetens primærkompetanse til å søke etter og beslaglegge bevis, bør så langt som mulig opprettholdes (kapittel 17). Alternativet antas å være å legge hele ordningen inn under domstolsapparatet (kapittel 18).

Del VI *Diverse spørsmål* inneholder noen avsluttende spørsmål som gjelder proporsjonalitetsvilkåret, heving av beslag og lagring av sikrede data. Endelig foreslås opprettelse av et nasjonalt tverrfaglig organ som kan følge den rettslige, teknologiske og etiske utviklingen nasjonalt og internasjonalt (kapittel 20).

Utredningens forslag til lovendringer og retningslinjer fremmes i del VIII. Retningslinjene fremgår av det utredningen har kalt «Databevisforskriften».

Del I: Introduksjon

Justis- og beredskapsdepartementet har gitt slikt mandat for utredning av den straffeprosessuelle ordningen for ransaking og beslag i databevis:

1. Mandat

1. Bakgrunn

Databevis er i dag en svært vanlig del av bevistilbudet i straffesaker. Bevisene sikres og beslaglegges med hjemmel i straffeprosessloven kapittel 15 om ransaking og kapittel 16 om beslag. Siden straffeprosessloven ble vedtatt, har det skjedd en betydelig teknologisk utvikling som gjør det mulig å innhente store informasjonsmengder lagret på blant annet harddisker, minnepinner, SIM-kort og telefoner. Gjeldende regelverk er skrevet med sikte på beslag av mer tradisjonelle realbevis og er ikke tilpasset muligheten for beslag av store mengder digitalt lagret materiale. Dette har skapt en rekke praktiske og rettslige utfordringer, og Høyesterett har ved flere anledninger gitt uttrykk for at det er behov for en nærmere lov- eller forskriftsregulering av databeslag, jf. blant annet HR-2017-111-A og HR-2018-699-A.

Straffeprosessutvalget har omtalt noen av utfordringene knyttet til håndteringen av databeslag i NOU 2016: 24 Ny straffeprosesslov punkt 14.8.1 til 14.8.3. Utvalget tar i liten grad stilling til hvordan disse utfordringene skal håndteres, men foreslår å åpne for forskriftsregulering av fremgangsmåten ved behandlingen av databeslag, jf. utkast til ny straffeprosesslov § 19-9. Utredningen har vært på høring med frist 6. juni 2017. Under høringen tok flere høringsinstanser til orde for en fullstendig gjennomgang av regelverket knyttet til beslag.

2. Nærmere om oppdraget

På et overordnet nivå skal utredningen belyse temaet databeslag eller elektronisk beslag i straffesaker. Utreder skal identifisere de særskilte problemstillingene databeslag reiser, vurdere om det er behov for lovendringer, samt komme med konkrete forslag til lovendringer. Hovedmålsettingen med utredningen er å gjøre beslagsreglene bedre tilpasset moderne informasjonsteknologi, og dermed også å effektivisere prosessen knyttet til håndtering av databeslag.

Utreder skal blant annet se nærmere på hvordan databeslag skal håndteres når hele eller deler av materialet som vurderes beslaglagt, er eller kan være underlagt beslagsforbud. Utreder bør i den sammenheng vurdere om det er grunn til å endre reglene om beslag i andre ting som kan være underlagt beslagsforbud, slik som papirdokumenter, lydopptak, telefonlogger mv.

Videre bør utreder vurdere om det gjeldende beslagsbegrepet er treffende for databeslag. I den forbindelse bør utreder gå nærmere inn på grensedragningen mellom ransaking og beslag i data. Som et bakteppe for drøftelsene bør utreder også gi en beskrivelse av de tekniske fremgangsmåtene som benyttes ved databeslag, og redegjøre for hvilke overordnede hensyn som begrunner valget av teknisk fremgangsmåte.

Problemstillingene skal drøftes i lys av grunnleggende straffeprosessuelle prinsipper som kontradiksjon, partslikhet og proporsjonalitet. Videre må forslagene være i samsvar med de menneskerettslige krav som følger av blant annet Grunnloven og Den europeiske menneskerettskonvensjonen, herunder bør forholdet til EMK artikkel 6 og artikkel 8 vurderes særskilt. Der det er hensiktsmessig bør utreder se hen til reglene om bevissikring etter tvisteloven og andre lover som inneholder slike bestemmelser, og om nødvendig vurdere endringer også i disse regelsettene. Utreder skal også – der det synes hensiktsmessig – se hen til hvordan problemstillinger knyttet til databeslag håndteres i andre jurisdiksjoner. Forslagene skal utarbeides på grunnlag av en overordnet målsetting om effektiv, rettsikker og tillitvekkende behandling av straffesaker.

3. Utredningsoppdraget for øvrig

Utredningen skal inneholde lovforslag med merknader i tråd med konklusjonene i vurderingen av behovet for lovendringer. Det skal så vidt mulig redegjøres for økonomiske, administrative og andre vesentlige konsekveser av forslaget.

Lovforslaget skal utarbeides i samsvar med retningslinjene i Justisdepartementets veileder Lovteknikk og lovforberedelse (2000).

Utredningen skal utformes slik at den kan sendes på høring uten ytterligere utredning av departementet.

Utrederen skal avgi sin utredning innen 1. november 2020.

I forståelse med departementet ble fristen utsatt til sommmeren 2021.

2. Utredningens tilnærming

2.1 En bred gjennomgang

Mandatet ber utreder om å «identifisere de særskilte problemstillingene databeslag reiser». Utredningen er lagt opp slik at den først beskriver praktisk bevishåndtering og tilhørende metodikk. Dette er holdt opp mot gjeldende regelverk, rettspraksis og praksis fra Den europeiske menneskerettighetsdomstolen (EMD). Forskning på dataetterforsking *(«digital*

forensic science») er trukket inn i fremstillingen. Noen aspekter av bevissikringen har det vært vanskelig å få full klarhet i. Forhåpentlig kan innspill i høringsrunden avbøte dette.

Spørsmål om ransaking og beslag i data ble for første gang reist for Høyesterett i 2011 (Rt. 2011 s. 296), og senest i desember 2020 avsa Den europeiske menneskerettighetsdomstol (EMD) dom mot Norge i en slik sak *(Saber)*.[1] De fleste avgjørelsene gjelder fremgangsmåten for beskyttelse av beslagsfrie advokatbetroelser, jf. straffeprosessloven («strpl.») § 204, jf. § 205 tredje ledd.[2]

Problemene med praktiseringen av beslagsforbudet skyldes omstendigheter som gjør seg gjeldende allerede når dataene sikres, uavhengig av om deler av dataene er beslagsfrie eller ei. Ransakings- og beslagsbestemmelsenes generelle egnethet for data bør derfor undersøkes før problemene med beslagsforbudet behandles. Utredningen foretar således en bred gjennomgang av regelverket, noe det fra flere hold har vært oppfordret til.[3] Fremgangsmåten ved beslagsforbud er et delspørsmål i denne helheten.

2.2 Data(bevis) er ikke et stabilt fenomen

Det må erkjennes at data og databevis ikke er stabile fenomener, slik som f.eks. fingeravtrykk og DNA-spor. Disse bevistypene er stabile i den forstand at det ikke er noen forskjell mellom fingeravtrykk og DNA-materiale avsatt i 1921 og i 2021. På grunn av teknologiutviklingen kan mer og sikrere informasjon hentes ut fra slike spor enn tidligere, men spormaterialet er det samme.

Slik er det ikke for data som stadig kommer i nye formater, på nye plattformer, og benyttes og beskyttes på nye måter. Det kan ikke tas for gitt at den størrelsen som man i en spesiell kontekst kalte «databevis», er lik en størrelse som i en annen kontekst kalles «databevis». Teknologiutviklingen endrer databeviset. En konsekvens er at dataverktøyene og den tekniske infrastrukturen man trenger for å kunne sikre og behandle dem, stadig må videreutvikles og/eller erstattes. I tillegg må nye fremgangsmåter hele tiden utprøves.

Dynamikken og databevisets egenart har konsekvenser for flere aspekter av det som til sammen skaper et effektivt og rettssikkert straffeprosessuelt system. Helt åpenbart har det betydning for

[1] *Saber mot Norge*. Dom 17. desember 2020. Saknr. 459/18.
[2] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven).
[3] Slik mandatet punkt 1.

det løpende kompetanse- og teknologibehovet. Det har også betydning for de praktiske mulighetene til å etterleve prosessuelle krav, som for eksempel å slette beslagsfrie opplysninger.

Dette har noen implikasjoner *de lege ferenda*.

Tekniske fagmiljøer utvikler teknologi for et globalt marked uten insentiver til å ta hensyn til nasjonale straffeprosessuelle krav, og det kan reises spørsmål om loven bør etablere et nasjonalt press for å utvikle dataverktøy som er bedre tilpasset prosesslovgivningen. Motargumentet er at står man for hardt på denne linjen risikerer man å innføre bestemmelser som ikke lar seg etterleve, og lykkes heller ikke med å løse dagens problemer. Rettslige insentiver for å få tilgang på bedre tilpassede verktøy bør heller skapes gjennom offentlige innkjøpsordninger.[4] Konsekvensen for moderniseringen av straffeprosesslovgivningen er at den må skje i lys av teknologien slik vi kjenner den i dag. Teknologien setter derfor i en viss utstrekning premisser for utformingen av loven.

Dette er ikke prinsipielt nytt, siden også gjeldende bestemmelser reflekterer bestemte teknologiske forutsetninger, f.eks. ved å tilrettelegge for sikringsformer som lar seg utføre i fysiske rom for fysiske objekter. Ransakingsbestemmelsens formulering «bolig, rom eller oppbevaringssted» tar åpenbart sikte på fysiske forhold, og det er kun ad tolkingsvei at også datamaskiner anses som «oppbevaringssted» (strpl. § 192).[5] Begrepet «ting» tok opprinnelig sikte på fysiske objekter (strpl. § 192 «ting som kan beslaglegges eller som det kan tas heftelse i»; strpl. § 203 «ting som antas å ha betydning som bevis»),[6] men tolkes slik at data omfattes.[7] I bunn og grunn er kriteriene for å være «ting», at det er tale om et påviselig stabilt fenomen som kan identifiseres og beskrives blant annet gjennom kvantifisering.[8]

Bestemmelsene om kommunikasjonskontroll i straffeprosessloven kapittel 16 a, er et annet eksempel på at teknologien setter premisser for lovgivningen. De forholder seg til at elektronisk kommunikasjon er data under overføring, og åpner ikke for å sikre kommunikasjon som er lagret, f.eks. meldinger i form av chat, sms eller epost. I så fall må man ty til ransaking og beslag, eller dataavlesing. Innføring av en ny kategori, f.eks. «data som ikke er under overføring» – dersom det er behov for det, vil derfor ikke være et tradisjonsbrudd prinsipielt sett. Det kan være aktuelt for data som er under behandling, dvs. i en dynamisk tilstand, uten at

[4] Riksrevisjonen (2021) kritiserer at det ikke har blitt etablert, jf. punkt 2.1.3.
[5] Se utredningen punkt 8.2.1.
[6] Se Inger Marie Sunde (2010) kapittel 7.2.
[7] Se utredningen punkt 8.2.2.
[8] Sunde, *ibid.*

man vil si at de er under overføring mellom forskjellige kommunikasjonsanlegg. I praksis sikres data som nevnt med hjemmel i bestemmelsene om ransaking og beslag, og dataavlesing.

Et annet spørsmål er hvordan man bør forholde seg til at teknologiutviklingen nok ikke kommer til å stoppe opp eller gå saktere enn i dag, heller tvert imot. Nye bestemmelser kan vise seg å bli uegnede og utdaterte etter relativt kort tid, selv om de utformes generelt og teknologinøytralt. Det er i det hele tatt vanskelig å utvikle et regelverk som fullt ut og på lengre sikt, ivaretar bredden og kompleksiteten i problemstillingene som følger med databevis. Etablering av en ordning eller et organ som jevnlig sørger for å avstemme regelverk og praktiske rettssikkerhetsmekanismer mot teknologiutviklingen bør derfor vurderes.[9]

Hensyn til forutsigbarhet og å kunne innrette seg, kan komme i konflikt med utviklingsbehovene, men ikke nødvendigvis. Det vesentlige er at systemet hele tiden inngir begrunnet tillit til at de grunnleggende hensynene til materiell sannhet, personvern og rettferdig rettergang respekteres, og at prosessordningen er rimelig effektiv. Utredningen holder alle disse perspektivene fremme.

2.3 Avgrensning

Mandatet gjelder beslag i databevis, dvs. elektronisk informasjon lokalisert i datasystemer. I følge grunnbestemmelsen om beslag (strpl. § 203), kan beslag ikke bare tas i ting som antas å ha betydning som bevis, men også i ting som antas å kunne inndras eller kreves utlevert av fornærmede. Inndragnings- og utleveringsformålene omfattes ikke av mandatet. Det synes heller ikke å være nødvendig å komme inn på dem i behandlingen av spørsmål som gjelder sikring og behandling av databevis. Det betyr ikke at behandlingen av datautstyret er irrelevant for bevisspørsmålene, f.eks. kan det være nødvendig med midlertidig beslag i en bærbar datamaskin eller smarttelefon for å sikre det elektroniske innholdet. Datautstyrets *indirekte* betydning for sikring av databevis, blir derfor behandlet.

Beslag i datautstyr kan være nødvendig for å sikre andre bevis enn databevis, f.eks. fingeravtrykk eller DNA-materiale. Også dette faller utenfor utredningen.

Utredningen drøfter ikke spørsmål som gjelder bevissikring på tvers av landegrenser, dvs. internasjonalt rettslig samarbeid i strafforfølgningen eller spørsmål om jurisdiksjon.

[9] Se kapittel 20.

2.4 Opplegget

Neste kapittel (kapittel 3) er det siste i introduksjonsdelen. Kapitlet gir en innledende oversikt over regelverket for ransaking og beslag i databevis, og beskriver de teknologiskapte omgivelsene som regelverket forholder seg til. I tillegg radegjøres det for noen internasjonale impulser.

Del II *Praktisk bevishåndtering* beskriver utfordringer, dilemmaer og fremgangsmåter ved sikring og analyse av databevis i etterforskingen. For å belyse den praktiske behandlingen (kapittel 4) er det innhentet opplysninger fra dataetterforskere ved enheter for Digitalt PolitiArbeid (DPA). Dataetterforskerne besitter spesiell datakompetanse, og har som hovedoppgave å tilveiebringe databevis. Deretter beskrives metodikken for behandling av databevis (dataetterforskingsprosessen) (kapittel 5).

De rettslige spørsmålene behandles i del III-VII. Analysen følger et vanlig opplegg med konkretisering av reguleringsbehovet, beskrivelse av gjeldende rett og de menneskerettslige rammene. Del III *Ransaking, sikring og beslag – Rettslige utgangspunkter* er en innledning til de påfølgende delene, og presenterer lovtekniske overveielser (kapittel 6) og menneskrettslige utgangspunkter (kapittel 7).

Utredningen skiller mellom to faser i ransakingsprosessen. Del IV *Fase én – ransaking og sikring av data* presenterer gjeldende rett for ransaking og beslag i data (kapittel 8). Deretter følger en drøftelse av det rettslige grunnlaget for ransaking av en databære (kapittel 9). Videre følger en drøftelse av undersøkelser (ransaking) av originale data. Slike undersøkelser som nevnt reiser egne spørsmål noe som gir grunn til å vurdere tydeligere regulering (kapittel 10). Neste kapittel behandler rettsgrunnlaget for sikring av data (kapittel 11). Endelig behandles hemmelig ransaking av databærer. Temaet ligger muligens i mandatets ytterkant, men henger nøye sammen med de øvrige spørsmålene. Dagens regulering kan neppe heller anses å være klar og tilstrekkelig rettssikker. Det har således vært naturlig å ta opp disse spørsmålene (kapittel 12).

Del V *Fase to – ransaking og beslag av sikrede data* reiser spørsmål rundt rettssikkerheten og de rettslige rammene for ransaking og beslag i sikrede data. Dette er spørsmål som har blitt belyst i forskning de senere år, og har gitt foranledning til kritikk. Muligheten for å styrke etterforskingskvaliteten gjennom tydeligere retningslinjer, bør derfor vurderes (kapittel 14). Videre behandles innsynsretten i sikrede data (kapittel 15).

Del VI *Beslagsfrie data* drøfter fremgangsmåten for behandling av beslagfrie data. Temaet inneholder sterke interessemotsetninger og løsninger avhenger også av tilgjengelig teknologi. For så vidt gjelder det siste har det vært vanskelig å avklare hva som er teknisk *umulig* og hva som er teknisk *mulig*, men så komplisert og tidkrevende at det *ikke er praktisk mulig* innen rammene av en etterforsking. Forhåpningen er at innspill i høringsrunden vil oppklare dette.

I del VI *Diverse spørsmål* drøftes noen avsluttende spørsmål som gjelder proporsjonalitetsvilkåret, heving av beslag og lagring av sikrede data (kapittel 19). I tillegg vurderes behovet for et nasjonalt tverrfaglig organ som kan følge den rettslige, teknologiske og etiske utviklingen nasjonalt og internasjonalt (kapittel 20).

Utredningens forslag til lovendringer og retningslinjer fremmes i del VIII. Retningslinjene fremgår av det utredningen har kalt «Databevisforskriften».

Flere av høringsuttalelsene til Straffeprosessutvalgets utkast til ny straffeprosesslov inneholder til dels omfattende merknader om problemstillinger som gjelder databevis, særlig uttalelsene fra Advokatforeningen, Kripos, Oslo politidistrikt, Oslo statsadvokatembeter, Oslo tingrett, Riksadvokaten og Økokrim. Uttalelsene har gitt verdifulle bidrag til problemidentifikasjon og legislative hensyn.

Utreder har også mottatt materiale og prosessuelle endringsforslag fra forsvarersiden og påtalesiden, samt materiale knyttet til riksadvokatembetets arbeid med midlertidige retningslinjer for ransaking i data, våren 2021.

3. Eldre bestemmelser og nye fenomener

3.1 Rettslige utgangspunkter

Det straffeprosessuelle systemet legger bevisoppgavene til politiet og påtalemyndigheten. Beviskravet er strengt; for domfellelse må skyld være bevist utenfor enhver rimelig tvil.[10] Påtalemyndigheten har bevisbyrden og skal tilveiebringe bevisene.[11] Beviskravet slår inn

[10] Rt. 2008 s. 1659: «Norsk straffeprosess bygger på at all rimelig og forstandig tvil skal komme tiltalte til gode» (avsnitt 17).
[11] Se f.eks. HR-2018-1901-U «I vårt system er det primært politiet som bringer relevante bevis til saken» (avsnitt 21).

allerede på påtalestadiet, dvs. at adgangen til å ta ut tiltale er betinget av at påtalemyndigheten er «overbevist om siktedes skyld, og av den oppfatning at straffeskylden kan bevises i retten».[12]

Straffeprosessloven som «etterforskingslov» pålegger ikke siktede eller forsvareren oppgaver i forbindelse med bevissikringen.[13] Rettighetene begrenser seg til å kunne begjære rettergangsskritt til avkreftelse av mistanken (strpl. § 241), dokumentinnsyn (strpl. § 242), en rett til å uttale seg før retten oppnevner sakkyndige (strpl. § 141), til å la en privat sakkyndig delta i granskingen (strpl. § 154), og – etter at tiltalebeslutningen og påtalemyndighetens bevisoppgave er mottatt – adgang til å be om supplerende etterforskingsskritt (strpl. § 265 første ledd tredje punktum). Siktede / forsvareren står fritt i å fremskaffe og føre egne bevis.

Ransaking er «undersøkelser i etterforskingsøyemed av privat område uten eiers samtykke».[14] Beslag går ut på at politiet sikrer seg rådighet over en ting man har funnet.[15] Hjemmelsgrunnlaget er bestemmelsene i straffeprosessloven kapittel 15 og 16, hvor inngrepshjemlene i strpl. §§ 192-195 (ransaking) og 203 (beslag) gjelder «åpen» metodebruk, mens strpl. §§ 200 a og 208 a gir hjemmel for «hemmelig» ransaking og beslag. Ved åpen metodebruk skal den som utsettes for inngrepet underrettes senest samtidig med at det foretas, jf. strpl. § 200 første ledd (ransaking) og strpl. § 205 første ledd siste punktum (beslag), mens hemmelig ransaking og beslag skjer med utsatt eller helt unnlatt underretning til mistenkte, jf. strpl. §§ 200 a og 208 a. Adgangen til ransaking og beslag, både åpent og hemmelig, begrenses av regler om beslagsfrihet, jf. strpl. § 204, og generelle krav til nødvendighet og forholdsmessighet, jf. strpl. § 170 a. Vilkårene for hemmelig metodebruk er ellers vesentlig strengere enn for den som skjer åpent.

Etter gjeldende rett er bestemmelsene om ransaking og beslag anvendelige både på fysisk datautstyr og innholdet, dvs. dataene som sådan. Det kan ransakes og beslaglegges på stedet og over nett, f.eks. i bedrifters datanettverk og på skytjenester. Ransaking og beslag over nett har nært slektskap med kommunikasjonsavlytting og dataavlesing.

---

[12] Riksadvokaten (2018) pkt. 4.3.2. Skyldkravet og bevisbyrden er aspekter av uskyldspresumsjonen, jf. Grunnloven § 96 annet ledd «Enhver har rett til å bli ansett som uskyldig inntil skyld er bevist etter loven.» Se Asbjørn Strandbakken (2003) s. 590-591; Gert Johan Kjelby (2019) kapittel 4.2.

[13] Straffeprosessutvalget betegner straffeprosessloven som en «etterforskingslov», NOU 2016: 24, kapittel 3.1, s. 101, og kapittel 29.1.2, s. 539. Når det gjelder forsvarers oppgaver i forbindelse med bevissikring, ses det her bort fra oppgaver som «skyggeforsvarer» ved skjult metodebruk, jf. strpl. § 100 a.

[14] Ingvild Bruce & Geir Sunde Haugland (2018) s. 186.

[15] *Ibid.*, s. 159.

3.2 Begrepsbruk: Internett, sosiale medier, skytjenester mm.

Internett med forskjellige tjenester er opphav til en rekke problemstillinger om bevissikring. Behandling av de rettslige spørsmålene fordrer en felles forståelse av noen sentrale fenomener og tilhørende begreper.

3.2.1 Internett

Sosiale medier, nettsteder og skytjenester er internettbaserte tjenester. Ordet «internett» brukes ofte synonymt med innholdet på tjenesten, f.eks. at man «fant det på internett». Men «internett» kan også bety *den TCP/IP-baserte overføringsteknologien* som gjør det mulig å nå tjenestene. Da betyr «internett» et datanettverk basert på TCP/IP-protokollene. Forstått i denne meningen er «internett» et «elektronisk kommunikasjonsnett» som nevnt i ekomloven § 1-5 nr. 2,[16] og verken tjenestens eller innholdets karakter er relevant for begrepet. Utredningen bruker «internett» i den sistnevnte betydningen, altså om datanettverket internett.

3.2.2. Sosiale medier

Med «sosiale medier» menes tjenester tilgjengelige via internett, som tilrettelegger for fellesskap og samhandling basert på relasjoner eller interesser, f.eks. Snapchat, Instagram, YouTube, TikTok, Facebook, Pinterest, Twitter, chattekanaler, debattråder og diskusjonsfora.

3.2.3 Nettsted vs. virtuelle rom

«Nettsted» er en uspesifikk betegnelse som vel først og fremst betyr web-basert innhold på internett, men uttrykket formidler også forestillingen om en geografi (jf. «-sted»). Ethvert nettsted lokaliseres ved hjelp av sin adresse (URL),[17] som sammenkoblet med DNS-systemet[18] gjør det søkbart etter semantiske kriterier, f.eks. søk «Lovdata», så finner nettleseren (browseren) nettstedet via DNS-systemet som peker på webadressen (URL). «Nettsted» omfatter det meste som kan nås over internett, f.eks. hjemmesiden til en bedrift, en nettbutikk, informasjonssidene til offentlige organer og ideelle organisasjoner, nyhetstjenester, strømmetjenester, billett-tjenester, web-basert epost, osv., osv.

Det stedsforankrede geografibegrepet i den fysiske verden, sier lite om nettstedenes betydning for personene som bruker dem. I den fysiske verden forutsetter umiddelbar tilgang fysisk nærhet

---

[16] Lov av 4. juli 2003 nr. 83. Se også ekomloven § 2-16 om nettnøytralitet som sier at all «internettrafikk» skal behandles likt, dvs. alt innhold som overføres ved bruk av TCP/IP på infrastrukturen internett. Også wikipedia beskriver internett som en infrastruktur, https://en.wikipedia.org/wiki/Internet (besøkt 22. februar 2021).
[17] Uniform Resource Locator.
[18] Domain Name Server (navnetjener).

til det man ønsker å ha tilgang til (objektet). Subjekt og objekt må befinne seg på samme sted. Slik er det ikke for nettstedene. Sett fra individets ståsted er de virtuelle rommene noe man hele tiden har, og tar med seg, uavhengig av hvor dataene som skaper det virtuelle rommet befinner seg, og for den del, uavhengig av hvor man selv befinner seg rent geografisk.[19] Vi lever derfor *«onlife»*, og i følge *Bert-Jaap Koops* er begrepet «rom» («space») mer relevant for brukeren enn «sted» («place»).[20] *Nina Sunde* påpeker at *onlife*-tilværelsen gjør individer kritisk avhengige av utstyr som sørger for internettilgang, typisk smarttelefon, noe som bør hensyntas i proporsjonalitetsvurderingen ved ransaking og beslag i smarttelefoner.[21]

3.2.4 Skytjeneste

«Skytjeneste» omfatter egentlig alle tjenester på internett, og har mer generell betydning enn «sosiale medier» og «nettsted». Uttrykket brukes hyppig om tjenester som behandler og oppbevarer brukerens data, dvs. at innehaverens data befinner seg et annet sted enn på innehaverens eget datautstyr. Dataene kan finnes på innehaverens datautstyr *i tillegg*, men ikke nødvendigvis, fordi bredbånd og annen kraftig teknologi reduserer lokaliseringens betydning for utnyttelse av dataene.[22] Innehaverens tilgang til egne data er med andre ord ikke betinget av at de er lagret på vedkommendes datamaskin. Skytjenester muliggjør lagring av større datamengder enn man kan lagre lokalt, og forenkler bruk og deling av data.

Dette har stor praktisk betydning for bevissikring i etterforsking, noe Økokrim påpeker i forbindelse med Straffeprosessutvalgets forslag til bestemmelser om ransaking:

> De foreslåtte reglene synes å forutsette at beslaglagte ting som sådan inneholder bevisene. I praksis kan det imidlertid være slik at beslaglagte ting (devices) ikke har selvstendig innhold, men peker på hvor innholdet befinner seg, for eksempel i andre databærere eller sky-tjenester.[23]

Smarttelefonen som kanskje er den vanligste datamaskinen vi benytter oss av, består av et håndsett med tilhørende integrert skytjeneste. Tjenesteyteren sørger for at innehaverens (brukerens) data løpende kopieres og lagres på skytjenesten. Dataene er tilgjengelige direkte

[19] Slik Thomas Hylland Eriksen (2021).
[20] Bert-Jaap Koops (2018) s. 614.
[21] Nina Sunde (2019a). Se nærmere om proporsjonalitetsvurderinger i utredningen punkt 19.1.
[22] I et informasjonssikkerhetsperspektiv er dataenes og tjenesteyterens lokalisering viktig, se *Nasjonal strategi for digital sikkerhet* som anser «Lange og uoversiktlige digitale verdikjeder, som spenner over flere sektorer og landegrenser» som «en kjerneutfordring» ved vurdering av digital sårbarhet (Justis- og beredskapsdepartementet & Forsvarsdepartementet, 2019), punkt 1.2, s. 6. Utredningen tar opp informasjonssikkerhet kun der det har betydning for behandlingen av databevis.
[23] Økokrim (2017) s. 20.

fra smarttelefonen.[24] Skytjenesten fungerer sømløst sammen med håndsettet. En forståelse av hva en smarttelefon er, må dermed nødvendigvis inkludere den tilhørende skytjenesten. Håndsettet er utstyrt med et minne som kan lagre betydelige datamengder. Dataene lagret i minnet og på skytjenesten, kan i stor utstrekning være dubletter.

3.2.5 Applikasjoner

I tillegg kommer alle appene (applikasjoner) til andre skytjenester, som også er tilgjengelige på smarttelefonen. En app er et dataprogram som gjerne ligger som et ikon på startskjermen, men det kan også være skjult. Den er en portal som skal gjøre det så enkelt som mulig for brukeren å utnytte tjenesten. Applikasjoner for mobiltelefoner ble vanlig ca 2010, og finnes for nær sagt enhver tenkelig internettjeneste, som dermed er tilgjengelig uavhengig av hvor man befinner seg.[25] Personlige apper kan gi tilgang til store mengder data som viser innehaverens bevegelser, private, halv-private og profesjonelle nettverk og aktiviteter. Smarttelefonen er dermed et viktig sporsted for politiet.

3.2.6 Flere tilganger til samme data

En skytjeneste kan gjerne også brukes uten å gå via appen, f.eks. med innlogging via tjenestens hjemmeside (nettsted), sml. for eksempel dokumenttjenesten Dropbox, Google epost eller en nettbankkonto, som er tilgjengelige både via mobilappen og tjenestens nettsted. De samme dataene kan således sikres fra forskjellige tilganger.

Flertilgangsmuligheten gir økt risiko for bevisforspillelse. Å frata siktede smarttelefonen er ikke ensbetydende med at siktede er fratatt muligheten for å bruke tjenesten og fjernslette data. Ifølge Økokrim må faren for bevisforspillelse derfor

> vurderes radikalt annerledes i dag enn for 20 år siden, da personlige møter og telefonsamtaler var de viktigste grunnlagene for å forspille bevis.[26]

Det underbygges med at

> Den teknologiske utviklingen har også gjort at stadig større deler av de elektroniske bevisene er lagret via sky-tjenester eller på annen måte er utfordrende å få oversikt over og ta beslag i. Tilsvarende er det enkelt for siktede å slette bevis forutsatt at man har tilgang til IKT-

[24] https://no.wikipedia.org/wiki/ICloud; https://support.samsungcloud.com/#/login (begge besøkt 22. februar 2021)
[25] Tjenester kan være begrenset til bestemte områder, ofte pga. klarering av immaterialrettigheter. Barrierer dannes på grunnlag av IP-adressen som indikerer den geografiske sonen man er i når man forsøker å koble til tjenesten («IP-geolokalisering»).
[26] Økokrim (2017) s. 20.

> tjenester/telefon. Det er også i mange tilfeller fare for at andre sletter viktige bevis på vegne av siktede dersom siktede får ha kontakt med andre, eller kan ha kontakt med omverdenen mer generelt. For eksempel kan man slette bevis eller forspille bevis på annen måte via offisielle nettsider hvis man har tilgang til internett, selv om man ikke har tilgang til egen smart-telefon.[27]

Bedrifter bruker skytjenester i utstrakt grad, eksempelvis som støtte for programvare, datalagring, eller følge opp funksjoner som ikke tilhører kjernevirksomheten, f.eks. lønn og regnskap. Bedriften eier og har tilgang til sine data, men betror dem til tjenestetilbyderen som har dataene lokalisert på sin infrastruktur. Til illustrasjon gjaldt Tidal-saken (HR-2019-610-A) blant annet

> «kildekoder» som under ransakingen – med bistand av den tekniske direktøren i Tidal – ble lastet ned fra en server i USA tilhørende Amazon Web Services.[28]

Her kan man gå ut fra at kildekodene tilhørte Tidal, men var lagret hos tjenestetilbyderen Amazon Web Services.

Videre gjaldt saken

> uttrekk fra den tekniske direktørens epostkonto hos Google. Dette materialet er lagret på servere i Nederland, Finland, Belgia og/eller Island. Det er ukjent i hvilket av disse landene materialet befinner seg.[29]

Dette gjaldt som det fremgår, ransaking av den tekniske direktørens epostkonto. Tjenestetilbyderen var Google. Om man kaller dette «nettsted» eller «skytjeneste» spiller ingen rolle i forhold til problemstillingene i denne utredningen.

3.2.7 De samme dataene flere steder

«Tingenes internett» *(Internet of Things (IoT))* forsterker kompleksiteten. «Tingenes internett» betegner at gjenstander har internettforbindelse. Formålet er å skape «smarte» hjem, biler og byer, og for den del, «smarte» individer. Utplasserte sensorer rapporterer hendelser til en digital sentral (datamaskin) som lagrer opplysningene og foretar seg noe på grunnlag av dem. Å kunne slå på panelovnen på hytta via en app, administrere hvem som skal få bruke en digital kodelås

[27] *Ibid.*
[28] HR-2019-610-A avsnitt 6.
[29] *Ibid.*, avsnitt 7.

på inngangsdøren, bruk av helse- og omsorgsteknologi (f.eks. måle blodsukkeret, få påminnelser om å ta medisin, slå av stekeovnen eller gå og legge seg) er noen eksempler.[30]

Med økende tilkobling av ting – inkludert sensorer festet på eller inkorporert i individer – øker antall digitale sporsteder. I tillegg til at man via forskjellige tilganger kan oppnå kontroll over de samme datene (jf. forrige punkt), kan de samme dataene finnes forskjellige steder, f.eks. *«on a cloud, in the device or in the smartphone linked with an application»*.[31] Via internett sammenkobles ulike sporsteder for den samme hendelsen, dvs. at sensoren/lagringsenheten i «tingen», appen på smarttelefonen, og skytjenesten som yter tjenesten, utveksler og synkroniserer informasjon. Aktivitet på disse tre stedene – av siktede eller av politiet i forbindelse med bevissikring – synkroniseres mot de andre sporstedene og kan påvirke de digitale sporene som er lagret der. *Servida & Casey* sier at

> Given the current challenges of the physical analysis of IoT devices, smartphone and cloud forensics are complementary. Indeed, most of the data will be sent to the cloud for easy retrieval from the smartphone applications/webpages, and most of that data will subsequently be synced to the mobile device.[32]

I klartekst betyr det at hvis politiets tilgang til data medfører endringer, vil disse kunne overføres og påvirke «de samme» dataene som finnes andre steder.

3.2.8 Oppsummering

Som en oppsummering har dette kapitlet pekt på:

- Smarttelefonen består av håndsett og integrert skytjeneste. Med alle sine apper er den en viktig beviskilde som gir mye informasjon om innehaveren, familieliv, og sosialt nettverk både privat og profesjonelt. Den gir også tilgang til innehaverens virtuelle rom.
- Sosiale medier omfatter per definisjon flere enn én person. Politiinngrep på sosiale medier berører bestandig flere enn siktede.
- Data lar seg vanskelig lokalisere presist, bortsett fra data på en fysisk databærer som politiet har rådighet over.
- På den ene siden kan de samme dataene finnes på forskjellige sporsikringssteder, og på den andre siden kan tilgang til data som tilsynelatende bare er lagret ett bestemt sted, oppnås fra forskjellige innganger. Sporsikringsmulighetene øker, men også risikoen for

[30] Noen strafferettslige implikasjoner av smartteknologien er behandlet av I.M. Sunde (2019a).
[31] Eléonore Ryser, Hannes Spichiger, Eoghan Casey (2020) s. 4.
[32] Fransesco Servida & Eoghan Casey (2019) s. 27.

> bevisforspillelse gjennom fjernsletting. Synkronisering mellom sporsteder kan medføre at politiet uforvarende endrer eller sletter spor.

3.3 Tilbakeblikk og utviklingstrekk

Som mandatet nevner er ikke dagens regler utformet med tanke på de utfordringer som har oppstått ved anvendelsen på data. Bortsett fra strpl. § 194 (razzia) kan bestemmelsenes ordlyd spores tilbake til straffeprosessloven 1887.[33] Komiteen som forberedte straffeprosessloven 1981, avga sin innstilling allerede i 1969,[34] og hadde ikke forutsetninger for å utrede problemstillinger som kom senere med datautviklingen.

3.3.1 Datautviklingens innflytelse på lovens ordlyd

For ransaking og beslag kan datautviklingens betydning spores bare i noen få tillegg i loven. Det første supplementet kom i 2005 da §§ 199 a og 215 a ble innført henholdsvis i kapittel 15 og 16, for å gjennomføre datakrimkonvensjonen (2001) i norsk rett.[35]

I henhold til strpl. § 199 a første ledd har politiet kompetanse til å pålegge

> enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet», slik at det kan ransakes.[36]

Bestemmelsen gjelder tilsvarende så langt den passer for gransking av «datasystem som er tatt i beslag» (fjerde ledd).[37] Innføringen er begrunnet i at passord og andre sperrer, inkludert kryptering, kan hindre muligheten for å ransake, eventuelt granske, datasystemer.

I henhold til strpl. § 215 a har påtalemyndigheten kompetanse til å gi pålegg om sikring av «elektronisk lagrede data som antas å ha betydning som bevis».[38] Behovet for sikringspålegg skyldes at data er flyktige og lett kan endres og slettes. Bevisforspillelsesfaren tilsier derfor at de bør kunne sikres raskt.[39] Sikringspålegg kan særlig være nyttig i internasjonalt samarbeid hvor politiet bistår utenlandsk politi i fremskaffelsen av bevis. Pålegg kan hindre at databevis

---

[33] Erik Keiserud m.fl. (2020) note 1 henholdsvis til §§ 192, 193, 195 og 203 (ss. 770, 774, 776 og 805). Razziabestemmelsen (§ 194) var ny i straffeprosessloven 1981, note 1 til § 194 (s. 775).
[34] NUT 1969:3 Innstilling om rettergangsmåten i straffesaker fra Straffeprosesslovkomiteen (Komiteen til revisjon av straffeprosessloven). Avgitt i juni 1969.
[35] Endringslov 8. april 2005 nr. 16; Ot.prp. nr. 40 (2004-2005); NOU 2003: 27 Lovtiltak mot datakriminalitet - delutredning I (Datakrimutvalget). Datakrimkonvensjonen er Europarådets konvensjon om datakriminalitet (ETS 185), 23. november 2001. Konvensjonen trådte i kraft for Norge 1. oktober 2006.
[36] Jf. datakrimkonvensjonen (2001) artikkel 19 nr. 4.
[37] Ved lovendring 21. juni 2017 nr. 92 fikk bestemmelsen også anvendelse på åpning av datasystem med biometrisk autentisering. Prop. 106 L (2016-2017).
[38] Jf. datakrimkonvensjonen (2001) artikkel 16 og 17.
[39] Den forklarende rapporten til datakrimkonvensjonen (2001), note 155.

forsvinner mens tidkrevende formelle bistandsprosedyrer gjennomføres. Bestemmelsen er mest praktisk når dataene besittes av tredjeparter som lojalt vil etterkomme utleveringspålegg, jf. strpl. § 210 flg.,[40] men kan etter omstendighetene også være aktuell sammen med beslag.

Det andre supplementet kom i 2012, da strpl. § 203 ble tilført et nytt annet ledd.[41] Her bestemmes det at ved anmodning fra fremmed stat om rettslig hjelp til utlevering av elektronisk lagrede data, gjelder § 216 a fjerde til sjette ledd tilsvarende. Tilføyelsen skjedde i forbindelse med gjennomføring av forpliktelser om internasjonalt rettslig samarbeid i kriminalitetsbekjempelsen, og letter den praktiske overføringen av dataene til myndighetene i den anmodende staten.[42]

3.3.2 En prinsipiell eller pragmatisk tilnærming til databevis?

Da den internasjonale interessen for databevis i kriminalitetsbekjempelsen i sin tid ble vekket var man særlig opptatt av databevisets egenart, sammenlignet med slike fysiske steder og gjenstander som bestemmelsene om ransaking og beslag tradisjonelt retter seg mot.[43] Siden data verken er flyttbare eller håndgripelige slik som fysiske objekter, var det tvilsomt om de kunne være gjenstand for beslag.[44] Norsk rettspraksis har imidlertid tatt en pragmatisk holdning og tolket «ting» i strpl. § 203 til å omfatte data.[45] Videre er strpl. § 192 ansett å hjemle ransaking etter bevis i datasystem, dvs. at datasystemer anses som «oppbevaringssted» i bestemmelsens forstand.[46]

Andre lands rett har hatt større problemer med å tillempe eldre bestemmelser på data.[47] For å lette det internasjonale samarbeidet i kriminalitetsbekjempelsen og effektivt kunne innhente og utveksle databevis, var det behov for å harmonisere metodereglene. Datakrimkonvensjonen artikkel 19 løste konseptualiseringsproblemet med de vide formuleringene «search or similarly access» / «ransake eller på annen måte få tilgang til» (artikkel 19 nr. 1) og «seize or similarly secure» / «beslaglegge eller på annen måte sikre» (artikkel 19 nr. 3). Formuleringene «på annen måte få tilgang til» og «sikre» åpner for utvikling av nye rettslige konsepter som ivaretar

[40] *Ibid.*
[41] Endringslov 22. juni 2012.
[42] Prop. 97 LS (2011-2012); Innst. 330 L (2011-2012).
[43] Den forklarende rapporten til datakrimkonvensjonen (2001), note 6, 184 og 187.
[44] *Ibid.*, note 184 og 187.
[45] Se utredningen punkt 8.2.2.
[46] Se utredningen punkt 8.2.1.
[47] Den forklarende rapporten til datakrimkonvensjonen (2001) note 184.

muligheten for sikring av databevis på linje med ransaking og beslag i fysiske objekter.[48] Men som nevnt, i norsk rett er de tradisjonelle bestemmelsene ansett å være anvendelige.

3.4 Internasjonal inspirasjon

Utredningen skal der det er hensiktsmessig se hen til «hvordan problemstillinger knyttet til databeslag håndteres i andre jurisdiksjoner».

3.4.1 Skandinavia

I Sverige la man i 2017 frem den offentlige utredningen «Beslag och husrannsakan – ett regelverk för dagens behov» (SOU 2017:100). Forslagene er foreløpig ikke gjennomført. Inntrykket er at hensynet til teknologinøytralitet har gått noe langt, slik at man i mindre grad har tatt hensyn til de særegne og utfordrende egenskapene ved databevis. Det tenkes særlig på kompleksiteten ved å analysere databeslag og det å skape en gjennomførbar prosedyre for å beskytte beslagsfrie data samtidig som påtalemyndigheten får tilgang på bevis. Det mest interessante forslaget gjelder en ny bestemmelse om kopiering som selvstendig tvangsmiddel, som *alternativ* til beslag. Det omfatter kopiering både av data og papirdokumenter.[49] Utredningen foreslår en lignende bestemmelse, avgrenset til data, se kapittel 11. Utredningens utgangspunkt er at kopieringen (sikringen) av data er et inngrep, men anses som et steg på veien til å finne bevis, og knyttes derfor til ransakingsbestemmelsen. Det er et annet utgangspunkt enn i den svenske utredningen.

I Danmark later det ikke til at man har spesielle bestemmelser for databevis. Det har man heller ikke på Island, noe utreder undersøkte fordi Island har hatt en omfattende sak for EMD hvor behandlingen av databevis hadde vært særlig krevende.[50] Saken stammet fra finanskrisen siste halvdel av 2010-tallet, hvor den islandske banken Kaupthing nesten gikk over ende. I straffesakene som fulgte var omfattende mengder databevis sentralt i bevistilbudet. Det har imidlertid ikke utløst noen lovgivningsaktivitet, selv om islandske kilder i påtalemyndigheten opplyser at datarelaterte bevisspørsmål stadig volder hodebry.

3.4.2 England

I England la man høsten 2020 frem rapporten «Search Warrants» som er en omfattende gjennomgang av reglene for ransaking og beslag, inkludert databeslag. Rapporten legger stor

[48] *Ibid.* note 184, og 191 (ransaking) og 197 (beslag).
[49] SOU 2017:100 kapittel 7.6.
[50] *Sigurdur Einarsson og andre mot Island.* Dom 4. juni 2019 (saknr. 39757/15). Saken er omtalt i utredningen kapittel 15.

vekt på at teknologiutviklingen har løpt fra lovverket, noe som har resultert i mangel på relevante prosessuelle garantier. Man er også bekymret for manglende proporsjonalitet i bevissikringen, gitt de store mengdene med irrelevante data som anskaffes med gjeldende sikringsmetoder. Rapporten opplyser at politiets praksiser varierer mye, noe som antas hovedsakelig å skyldes svakt regelverk. Samtidig erkjennes det at det ikke finnes enkle løsninger og at utviklingen kontinuerlig løper raskt avgårde. Rapporten foreslår derfor å opprette et nasjonalt tverrfaglig råd som kan evaluere tilstanden og adressere nye problemstillinger etter hvert som teknologien driver dem frem. En mulig viktig effekt antydes også å være at et slikt organ kan legge press på utviklere av dataverktøy, slik at teknologien i større grad enn i dag kan ivareta proporsjonalitet og rettssikkerhetshensyn.

Nedsettelse av et nasjonalt tverrfaglig organ ble foreslått av Økokrim i høringsuttalelsen til Straffeprosessutvalgets utredning og følges opp i utredningen kapittel 20.[51]

3.4.3 FORMOBILE

Det EU-finansierte FORMOBILE prosjektet forsker på teknologiske og rettslige sider av sikring og bruk av databevis fra smarttelefoner i straffesaker.[52] På nyåret 2021 kom prosjektets straffeprosessuelle rapport, som basert på en rekke landrapporter, foretar en sammenlignende analyse (heretter kalt FORMOBILE-rapporten).[53] Bekymring rettes særlig mot manglende kvalitet i lovverket, dvs. at eldre bestemmelser anvendes analogisk og er lite innrettet mot dagens utfordringer.[54] Det uttrykkes også bekymring for manglende proporsjonalitet i inngrepene, i og med at en smarttelefon gir adgang til så mye informasjon.

3.4.5 Betydningen for mulige endringer i norsk rett

Den internasjonale kilden som har hatt størst betydning for utredningens spørsmål er utvilsomt rettspraksis knyttet til den europeiske menneskerettighetskonvensjonen (EMK). Dette er det løpende gjort rede for.

Direkte å nyttiggjøre seg løsninger i nasjonale rettssystemer er vanskelig. I spørsmålene som utredningen behandler avhenger utformingen av lovverket av hvordan de teknologiskapte problemene oppfattes og beskrives. Her kan det være forskjeller. I tillegg, og kanskje viktigere, har det betydning i hvilken grad lovgiver velger å koble regler til teknologi. Dette har kanskje

---

[51] Økokrim (2017) s. 4, se også s. 19.
[52] FORMOBILE Project Page (formobile-project.eu) (besøkt 16. april 2021).
[53] Denitsa Kozhuharova, Pieter Gyffroy, Hristina Bogia, Snezhana Krumova (2021).
[54] *Ibid.*, punkt 2.1.

størst betydning for utformingen av rettssikkerhetsmekanismene. Det store spørsmålet er hvor langt man skal gå i å stole på tekniske systemer i forhold til manuell kontroll. Spørsmålet har stor betydning for notoritets- og dokumentasjonskrav, utførelsen av etterkontroll (f.eks. av KK-utvalget) og beskyttelsen av beslagsfrie data. Dette er rettspolitiske valg som det ikke er lett å gjøre gode sammenligninger med, fordi andre land kan ha andre tradisjonelle utgangspunkter, og andre rammebetingelser for å investere i og utvikle egnet teknologi.

Uansett, utredningen antas bare å være et første steg på veien i en mer fullstendig modernisering av straffeprosessloven, og forhåpentlig et konstruktivt bidrag i så måte.

Del II: Praktisk bevishåndtering

Mandatet ber utreder om

> en beskrivelse av de tekniske fremgangsmåtene som benyttes ved databeslag, og redegjøre for hvilke overordnete hensyn som begrunner valget av teknisk fremgangsmåte.[55]

Dette er besvart ved å innhente opplysninger om dagens praksis fra dataetterforskere ved enheter for Digitalt PolitiArbeid (DPA) (kapittel 4), og beskrive gjeldende metodikk for sikring og behandling av databevis (kapittel 5).

4. Dagens situasjon – opplysninger fra dataetterforskere

Digitalt PolitiArbeid (DPA) er organisert under felles enhet for etterretning og etterforsking, som en støttefunksjon som kan benyttes i alt politiarbeid. Funksjonen skal følgelig samhandle på tvers av politidistriktet. DPAens formål er å ivareta

> En bred og hensiktsmessig bruk av digital informasjon og elektroniske spor i politiarbeidet, herunder etterretning, operativt politiarbeid, forebygging, etterforsking og iretteføring.
>
> Gjennom utnyttelse av teknologi og elektroniske spor skal funksjonen sikre at flere straffesaker kan etterforskes raskt, og med god kvalitet i bevissikring, analyse og metodebruk.[56]

Å gi bistand til sikring og utnyttelse av databevis er en viktig del av DPAens oppdrag, jf. at blant hovedoppgavene inngår å

[55] Mandatet punkt 2.
[56] Politidirektoratet (2017) pkt. 3.2.26.1.

> bistå med sikring og tilrettelegging av digital informasjon, utføre de mest anvendte datatekniske undersøkelser av nettverksdata og digitale enheter som ikke krever spesielle, kostbare laboratoriefunksjoner.[57].

Fem dataetterforskere har bidratt enkeltvis, i møte, telefonsamtale og epostutveksling. Å få innhentet skriftlige redegjørelser fra dem viste seg å være vanskelig. De har imidlertid vært nokså samstemte.

4.1 Tekniske forhold

4.1.1 Store datamengder

Dataetterforskerne opplyser at datamengdene som de må håndtere ofte er svært store. Når datamengden øker blir alle prosessene mer tidkrevende og saksbehandlingstiden forlenges. Praktisk sett er det nær sagt umulig å utføre den konkrete relevansvurderingen på stedet. For å identifisere bevismateriale er det nødvendig å bruke automatiske søke- og filtreringsprogrammer. Dette må gjøres etterat dataene er sikret. Denne fremgangsmåten er den som best ivaretar bevisets integritet.

Dette kan suppleres med Kripos sitt innspill i høringsrunden til NOU 2016: 24 *Ny straffeprosesslov*, som understreket at de store informasjonsmengdene har gjort etterforskingsfasen mye mer kompleks enn før.[58]

4.1.2 Fragmentering – hva er et databevis

Flere av informantene mener at hva et databevis egentlig er, ikke er helt avklart. Et databevis kan bestå av fragmenter som tilsammen skaper en informasjonsenhet. Meningsbærende innhold som f.eks. en videosnutt, kan være oppdelt i fragmenter, og være lagret på steder som også lagrer andre informasjonsfragmenter. Alt innhold har underliggende (tilhørende) metadata, som lagres et annet sted enn innholdet de refererer seg til. Metadataene er nødvendige for å kunne si noe sikkert om innholdet, f.eks. om når det ble laget eller endret. Innhold og metadata må derfor sammenstilles for å gi helhetlig mening. Det skjer etter at dataene er sikret. Epost med vedlegg er et lignende eksempel. Eposten vil være ett sted og vedlegget et annet, og sammenstilling skjer etter at de er sikret.[59] Metadata kan dessuten være beviset i seg selv.

---

[57] *Ibid.*, pkt. 3.2.26.3.
[58] Kripos (2017) s. 6.
[59] For brukeren ser det likevel ut som om de er samme sted (i innboksen).

Fragmentering har kun å gjøre med *at ett og samme databevis* kan bestå av spredte bestanddeler. Sakens totale bevisbilde kan også være komplekst, men da er det tale om å se flere forskjellige bevis i sammenheng, også flere (fragmenterte) databevis.

På grunn av fragmenteringen ligner databevis lite på fysiske bevis. Uttrykk som brukes om fysiske objekter kan derfor være lite treffende, f.eks. er krav om å «hente ut» eller «tilbakelevere» databevis er vanskelige å etterkomme fordi man ikke har med kompakte fysiske enheter å gjøre. En fysisk gjenstand, f.eks. et papirdokument, kan «hentes ut» av et papirarkiv og beslaglegges uten at det går ut over de øvrige dokumentene eller arkivsystemet som sådan. Det er heller ikke nødvendig å beslaglegge hele arkivet hvis man bare er ute etter noen bestemte dokumenter.

Riktignok er det teknisk mulig å kopiere både datafiler og mapper enkeltvis. Ulempene er man taper konteksten som dataene lå i, og heller ikke vet om man har fått med alle relevante data. Datamengdenes størrelse kan dessuten gjøre det vanskelig der og da å avgjøre hvordan sikringen bør avgrenses, og da kopierer man heller alt.

Hvis «uthenting» skal brukes om databevis på en måte som ligner fysiske bevis, må det bety at dataene kopieres over til en ny databærer og slettes fra den opprinnelige kopien. Det vil imidlertid kunne endre databeviset og omkringliggende informasjonsenheter på uoversiktlige måter. Videre er det uklart hva som omfattes av «hente ut», er det innholdet *og* metadataene, eller bare innholdet? Uklarheten har betydning for hva som omfattes av sakens dokumenter og beslagsforbudets rekkevidde.

Å sette fragmenter sammen til ett databevis innebærer vurderinger, og kompleksiteten kan gjøre det nødvendig å ha ekspertise.[60] Det kan også være krevende å vurdere bevisets betydning og styrke. Analysejobben er i det hele tatt blitt veldig kompleks.

4.1.3 Kompleksitet og integrasjon: Hvor er dataene lokalisert?

At det digitale og det fysiske er så tett sammenvevd er kompliserende. Tidligere var den typiske bevissikringssituasjonen at data fantes lokalt på en datamaskin og kunne sikres ved å kopiere harddisken. Dette gjøres fortsatt når politiet får hånd om den fysiske databæreren. Adgangskontroll er imidlertid standardutrustning og beskytter smarttelefoner mot uberettiget tilgang. Beskyttelsen gjør det vanskelig for etterforskerne å sikre data fra håndsettet, men dette

[60] Sml. Kripos (2017) s. 39.

kan likevel utnyttes som utgangspunkt for å oppnå tilgang til dataene direkte fra skytjenestene som er knyttet til smarttelefonen. Integrasjonen mellom smarttelefonen og skytjenestene er så sømløs at man vanskelig kan si hvor dataene egentlig befinner seg.

I praksis blir det i mindre grad spørsmål om å finne ut hvor dataene befinner seg, men heller om å identifisere hvilke tjenester siktede bruker, og avklare hvilken fremgangsmåte som egner seg for å sikre dataene. Integrasjonen gjør det også merkelig å kreve «tilbakelevering» eller «sletting», hvis dataene uansett befinner seg i «skyen» og er tilgjengelige der.

Endelig påpekes det at etterforsking gir behov for å sikre data fra en rekke forskjellige medier, innretninger og skytjenester. Stadig flere elementer i omgivelsene kobles til internett og antallet digitale sporsteder øker. Den store bredden i innretninger og tjenester stiller store krav til innholdet i den digitale verktøykassen, etterforskernes kompetanse, rutiner og organisatorisk tilrettelegging av arbeidet. Her er det store mangler i praksis.

4.1.4 Dataene «låses ned» under ett

Forholdene nevnt i det foregående gjør det praktisk sett umulig å sikre databevis enkeltvis. Derfor sikres hele områder med data under ett, f.eks. alle data på en brukerkonto, på en harddisk, et minnekort, i en database osv.[61] Det kan sammenlignes med å kopiere et helt papirarkiv selv om man bare er ute etter noen få dokumenter.

Resultatet er at potensielle databevis bestående av innhold og metadata, «låses ned» i den store fragmenterte datamengden, sammen med data som er uten betydning for straffesaken og data som er beslagsfrie. De «låses ned» fordi kopien må behandles som originalbevis og holdes intakt.[62] Utreder får opplyst at det ikke lar seg gjøre å slette irrelevante/beslagsfrie data uten å forårsake endringer i de sikrede dataene som politiet kan ta i beslag. En av informantene beskriver det slik:

> Bevisverdien ligger i intakte speilfiler (uendret sjekksum). Hvis man skal slette et "dokument" må man individualisere og trekke ut alle informasjonselementene i speilfilen. Da ødelegges speilfilen og det blir vanskelig å gå god for ekthet av resten. Det er heller ikke så enkelt at et dokument tilsvarer en fil. Et dokument kan for eksempel være et vedlegg til en e-post som igjen oftest ligger i et e-

[61] Innholdet i skytjenester ligger i databaser. Informant B i telefonsamtale 22. januar 2021.
[62] Nærmere beskrevet i utredningen punkt 5.4.2.

> postarkiv (database-format). Selve e-postarkivet er en fil, men for å slette ett vedlegg må man individualisere alle e-postene, vedleggene, metadata osv osv og endre arkivet.[63]

Behovet for å kunne kontrollere databevisets ekthet innebærer at den opprinnelige kopien ikke bør røres. Dette skaper problemer for behandling av beslagsfritt materiale, og ved krav om tilbakelevering eller sletting av data.

4.1.5 Sikrede data skiller seg fra KK-data

Det følger av det foregående at behandling av sikrede data er mye mer komplisert enn behandling av KK-materiale (som også er data). Opptak av elektronisk kommunikasjon skiller mellom forskjellige samtaler, og dersom én ikke kan brukes, kan den slettes uten at de andre opptakene påvirkes. Som det er redegjort for stiller dette seg helt annerledes for sikrede data.[64] Hvordan en løsning for utskilling av beslagsfrie opplysninger som nevnt i HR-2017-111-A praktisk sett kan gjennomføres, er derfor uklart.

4.1.6 Lagring av data

Det hersker også stor usikkerhet rundt adgangen til å lagre de sikrede dataene. De sikrede dataene har jevnlig større omfang enn dataene som er gjort til del av sakens dokumenter, fordi de også omfatter irrelevante data, og iblant, beslagsfrie data. Det kan imidlertid være behov for å se gjennom de sikrede dataene på senere tidspunkt, f.eks. i forbindelse med gjenåpning av saken. Reguleringen av de sikrede dataene reiser derfor andre spørsmål enn de som gjelder dataene som inngår i sakens dokumenter. I følge Kripos er det «stort behov» for å få på plass en forskrift om lagring av bevis.[65]

4.2 Kultur, kompetanse og kvalitetssikring

En informant fremholdt med styrke at «det ikke er teknologien som er problemet, men hvordan vi forholder oss til den», og fulgte opp med at

> politietaten inkludert ledelsen på alle nivåer, forstår ikke kompleksiteten i det dataetterforskere må håndtere, eller hvordan ting henger sammen.[66]

Om ikke de andre informantene var like eksplisitte, har dette synet støtte. En viktig tilbakemelding er at etaten mangler nødvendig teknisk kompetanse for å løse oppgavene med

---

[63] Informant A i epost datert 21. januar 2021.
[64] Opplysninger fra politidistriktene i riksadvokatens materiale innhentet i forbindelse med utferdigelsen av de midlertidige retningslinjene for ransaking i data.
[65] Kripos (2017) s. 25.
[66] Informant B i telefonsamtale med utreder 22. januar 2021.

dataransaking og beslag på en god måte. Politiutdanning «med 30 studiepoeng i datateknikk i tillegg» dekker ikke kompetansebehovet.[67] Politiet har behov for flere sivilister med hovedutdanning i datateknikk. Å ha et solid teknisk faggrunnlag i utgangspunktet, anses som en forutsetning for å kunne henge med og løse nye utfordringer forårsaket av teknologiutviklingen.

Det opplyses at etterforskerne gjør godt arbeid innen de rammebetingelser de har. Det mangler imidlertid enhetlige prosedyrer for kvalitetssikring av arbeidsprosessene som inngår i behandlingen av databevis.[68] Dette kan lede til at bevis overses eller feiltolkes, og til svakheter og mangler i dokumentasjonen.

Informanten som fikk innlede dette punktet konkluderte med at «det mangler energi i etaten til å gå ordentlig inn i disse kompliserte problemstillingene».[69] Informanten oppfatter masteravhandlinger og forskning som belyser etatens utfordringer som en nødvendig og viktig drivkraft for forbedringer.

4.3 Teknologinøytral lovgivning

Informantene opplyser at på dette området er det er behov for mange flere tiltak enn lovendringer, men når det først er tale om rettslig regulering bør den gjøres «teknologinøytral», slik at håndteringen av databevis ikke bindes til spesifikk teknologi eller fremgangsmåte. Den hurtige tekniske utviklingen medfører stadige endringer i de praktiske fremgangsmåtene for å sikre databevis. Et regelverk som ikke tar hensyn til dette må antas raskt å bli utdatert.

5. Bevishåndteringsmetodikk: Dataetterforskingsprosessen

5.1 En generell metodikk

Politiets behandling av databevis følger den såkalte «dataetterforskingsprosessen». Prosessen er beskrevet i mange lærebøker om behandling av databevis.[70] I det følgende vises det primært til *Anders Flaglien,* «The Digital Forensic Process» (2018).[71] I tillegg har faglærere og forskere tilknyttet Politihøgskolens studium Nordic Computer Forensic Investigator (NCFI), bidratt.

---

[67] *Ibid.*
[68] Kripos (2017) har i tillegg påpekt behovet for ivaretakelse av informasjonssikkerhet «i alle ledd i straffesaksbehandlingen», s. 9. Og at det er behov for «i langt større grad [å] sørge for sikker oppbevaring av bevisene og god notoritet på oppbevaring og håndtering» (s. 24)
[69] Informant B, *ibid.* Torgeir Magnussen (2019) uttrykker tilsvarende synspunkter.
[70] Se f.eks. Stephen Mason & Daniel Seng (red.) (2017).
[71] Anders Flaglien (2018) i fagboken *Digital Forensics* André Årnes (red.) (2018). Boken brukes blant annet på masterstudiet Information Security ved NTNU, som er utviklet i samarbeid med Politihøgskolen.

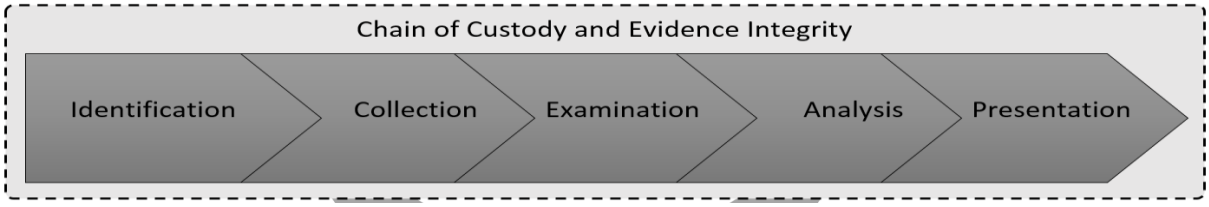
Dataetterforskingsprosessen er en generell metodikk for behandling av databevis uavhengig av sakstype. Verdien består først og fremst i at prinsippene og systematikken deles av det internasjonale fagmiljøet for digital rettsteknikk. Forskjellige ekspertfora beskriver prosessen med ulik detaljgrad, men hovedtrekkene er like.[72]

Det innarbeidete uttrykket «data*etterforskings*prosessen» er for snevert fordi det reserverer uttrykket for straffesaker. Derimot er det engelske uttrykket *«the digital forensic process»* dekkende.[73] Metodikkens generelle virkeområde innebærer at den gjelder for databevis uavhengig av om det er tale om etterforsking av en straffesak, eller andre saktyper.

Dataetterforskingsprosessen er også generell i den forstand at den gjelder for alle typer datamedier og -bevis, dvs. for sikring og behandling av data i form av tekst- og mediefiler, programfiler mv., fra så forskjellige enheter som bærbare datamaskiner, smarttelefoner og kroppsnære enheter (f.eks. treningsarmbånd og blodsukkermålere), så vel som datasystemer i bedrifter, i kjøretøy og skip, mv., og skytjenester. Metodikken må derfor tillempes konkrete forhold.[74]

Dataetterforskingsprosessen består av de fem fasene identifisering, sikring, klargjøring/tilrettelegging, analyse og presentasjon. Fasene inngår i en bevishåndteringskjede.

Figur 1: Dataetterforskingsprosessen



Flaglien (2018)

[72] N. Sunde (2019b) s. 59.
[73] «Forensic science» er vitenskapen om metoder for å sikre og behandle bevis på måter som ivaretar bevisets pålitelighet. Formålet er å kunne bruke beviset i en rettslig prosess, se William J. Tilstone m.fl. (2013), s. 3. N. Sunde (2019b) konstaterer at «forensics» savner et korresponderende ord på norsk, s. 62, note 44. Den engelske rapporten *Search Warrants* gir denne definisjonen av "digital forensics": *"the process by which electronic data is extracted from electronic devices and processed for the purpose of obtaining intelligence or for use in criminal proceedings"*, se UK Law Commission (2020) pkt. 14.97, s. 349.
[74] *Ibid.*, s. 14-15.

5.2 Integritetsprinsippet og forsvarlig bevisbehandling

Dataetterforskingsprosessen hviler på prinsipper om *bevisintegritet* og *sammenhengende bevishåndteringskjede* («evidence integrity» og «chain of custody»). Formålet er å sikre at bevishåndteringen er forsvarlig («forensically sound»).[75] *Forensic soundness* er et begrep som brukes i det internasjonale fagmiljøet for dataetterforsking, og ikke å anse som en rettslig standard.

Fagmiljøet har en løpende diskusjon om hvilke krav som realistisk bør stilles for å anse behandling av databevis å være forsvarlig. Integritetsprinsippet som sier at dataene skal sikres og bevares i sin opprinnelige form, lar seg nemlig vanskelig gjennomføre fullt ut i praksis.[76] I sikringsprosessen er visse mindre modifikasjoner visstnok uunngåelige, i hvert fall ved sikring av data fra aktive systemer.[77] En mer realistisk forståelse anses derfor å være at dataene skal holdes så intakte som omstendighetene gjør mulig.[78]

Det kritiske kriteriet er dermed *hvorvidt alt som er gjort med databeviset fremgår av dokumentasjonen*.[79] I følge en mye sitert oppfatning innebærer kravet til forsvarlig behandling at bevishåndteringsprosessen skal være transparent, og at dataene skal behandles på en måte som bevarer deres opprinnelige mening.[80] *Transparens* er således også et viktig prinsipp. Hvorvidt man vil anse det som et selvstendig prinsipp eller som et aspekt av prinsippet om sammenhengende bevishåndteringskjede (se nedenfor), kan være en smakssak.

5.3 Dokumentasjon og transparens – «presentasjonsfasen»

«Chain of custody» innebærer at bevishåndteringskjeden skal være ubrutt fra datamaterialet første gang tas hånd om, til siste gang det presenteres, f.eks. i en hovedforhandling eller ved en gjenopptakelsesbegjæring. Perioder hvor man ikke kan redegjøre for hvor beviset har vært oppbevart, hvem som har hatt ansvaret for eller håndtert det, skal ikke forekomme.[81] Dette stiller krav til praktisk bevishåndtering og oppbevaring, så vel som til dokumentasjonen.[82]

---

[75] André Årnes (2018) s. 6.
[76] *Ibid.*
[77] Sikring fra active systemer er beskrevet i pkt. 5.4.2.1. I relasjon til sikring fra aktive systemer skriver Flaglien, at *«data inevitably changes during acquisition"* og *"it is not just difficult but impossible to gather all the information from a computer system without changing its state"*, (2018) s. 30.
[78] Graeme Horsman (2020) s. 4; Årnes, s. 6.
[79] Se f.eks. Horsman (2020) som foreslår *"A practitioner should take all reasonable steps to preserve the integrity of any data/device(s) subject to investigation during the course of their examination"*, "Principle 5", s. 4.
[80] *«The application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law»*. Rodney McKemmish (2008).
[81] Flaglien (2018) s. 46.
[82] Årnes (2018) s. 6; Flaglien (2018) s. 23-24 og 45-47.

Presentasjonsfasen som er plassert til sist i Figur 1, gjelder dokumentasjonskravet. Ifølge *Flaglien* kulminerer bevishåndteringen med utferdigelsen av en sluttrapport som skal vise de funn som er gjort med «a sufficient level of certainty».[83] Rapporten skal også vise i hvilken kontekst funnene ble gjort, og hvilke valg man har gjort i hver fase.[84] Sluttrapporten er (data)etterforskerens grunnlag for å kunne uttale seg om funnene overfor påtalemyndigheten og retten, og hviler på dokumentasjonen som er utferdiget i de foregående fasene. I henhold til *chain of custody*-prinsippet skal dokumentasjonen som helhet gi grunnlag for å kunne kontrollere all håndtering av databevisene og overgangene mellom fasene («sporbarhet»).[85] Transparens er derfor som nevnt, et viktig prinsipp, og nøyaktig og hyppig dokumentasjon er da en forutsetning.

Flaglien konkretiserer dokumentasjonskravet dithen at dokumentasjonen skal gjøre det mulig å kontrollere bevisets integritet, og forklare hvordan man har kommet frem til datauttrekket som brukes i saken. Tidspunkter for håndtering av beviset og hvilke prosesser det har vært gjenstand for, er viktig informasjon. Tidsstempler bør bekrefte at integritetskontroll har vært gjennomført systematisk. Endringer i data som skjer i sikringsprosessen skal dokumenteres, og årsaken (feil, uhell) forklares, slik det følger av integritetsprinsippet. Endringens betydning for bevisverdien må også beskrives. Dette følger implisitt av forsvarlighetskravet, som sier at dataenes opprinnelige mening må kunne fastslås.[86] Hvem som har behandlet beviset (sporbarhet) skal også fremgå.[87]

Siden dokumentasjonskravet er en viktig rettssikkerhetsgaranti har det vært naturlig å nevne denne «fasen» først, men som man forstår er det ikke tale om en selvstendig fase, men om *et løpende dokumentasjonskrav* som gjelder for alle fasene fra begynnelse til slutt. Dokumentasjonen, i praksis politirapportene, legger premissene for hvordan databevis presenteres for bevisbedømmeren, dvs. påtalemyndigheten på påtalestadiet, retten under hovedforhandlingen, og siktede/forsvareren både under etterforskingen og iretteføringen.

Flere etterforskere kan stå bak politirapportene. Styringsdokumentet *Rammer og retningslinjer for etablering av nye politidistrikter* forutsetter at enhver tjenesteperson skal kunne utføre «enklere sikring og gjennomgang av digital informasjon».[88] Dataetterforskerne som har mer

[83] Flaglien (2018) s. 45.
[84] *Ibid.*, s. 45-47.
[85] *Id.*; sml. Jeff Hamm (2018) s. 149.
[86] Flaglien (2018) s. 22-24; McKemmish (2018).
[87] Årnes (2018) s. 6; Flaglien (2018) s. 23-24 og 45-47.
[88] Politidirektoratet (2017) kapittel 3.2.26.3 og -6.

datakompetanse, har først og fremst en bistandsfunksjon.[89] Ulike personer kan derfor utføre forskjellige deler av prosessen, og ofte produseres det flere rapporter, f.eks. én om (foreløpig) beslag i databærere, én om sikringen av dataene, én om klargjøringen og én om gjennomføring av analysen. I tillegg genererer mange av dataverktøyene logger over prosessene som har vært iverksatt. Disse kan supplere etterforskernes egne rapporter.

5.4 Identifiserings-, sikrings-, klargjørings- og analysefasene

5.4.1 Identifiseringsfasen

Identifiseringsfasen går ut på å avdekke mulige kilder for databevis. Generelt kan det være tale om å finne bærbare datamaskiner, smarttelefoner og forskjellige løse lagringsmedier mv. I tillegg vil man lete etter relevante områder på større systemer, f.eks. brukerkonti på skytjenester og andre typer nettsteder. I en bedrift kan det gjelde å identifisere hvilke datasystemer som er relevante, eventuelt hvilke deler av et datasystem som kan antas å være relevant, f.eks. om bevis må antas å finnes på produksjons- eller økonomisystemet, på en arbeidstakers dokumentområde eller på epost-serveren. Generelt vil man også være oppmerksom på opplysninger og utstyr for innlogging og dekryptering, f.eks. kodebrikker og nedskrevne passord.

5.4.2 Sikringsfasen

Sikringsfasen går ut på å skaffe seg kontroll over dataene på de identifiserte kildene. Sikringen skjer ved kopiering til politiets egen databærer. Kopien undergis en teknisk sikkerhetsprosedyre. Når den er gjennomført har man det som heretter kalles «sikringskopi».

Dataene anses ikke som sikret allerede som følge av at databærerne er tatt i besittelse, fordi det fremdeles finnes risiko for endring eller sletting, f.eks. ved fjernsletting, feilbehandling eller uhell. De originale dataene kan heller ikke umiddelbart analyseres, siden politiets undersøkelser av ubeskyttede data ville medføre endringer. Det kan riktignok være mulig å koble på en innretning for skriveblokkering slik at innsyn kan foretas uten at originaldataene endres.[90] Ofte er det imidlertid nødvendig først å fremstille en sikringskopi som deretter brukes som grunnlag for å finne frem til bevis.

Sikring forutsetter ikke nødvendigvis at de originale dataene tas ut av innehaverens besittelse. Årsaken er rimeligvis at dataene sikres ved kopiering, noe som gjør at innehaveren kan beholde besittelsen, eventuelt bare avstå dem i en kortere periode mens de sikres. Dessuten, selv om

[89] *Ibid*. Slik også innledningen til kapittel 4.
[90] N. Sunde (2019b) s. 71.

politiet tar med seg innehaverens datamaskiner, kan dataene også være lagret i skyen og da er det diskutabelt om man vil anse dem for å være borttatt.[91] Sikring av data skiller seg således fra fysiske objekter, hvor innehaverens rådighet nødvendigvis må opphøre når politiet overtar besittelsen. En fysisk parallell kan likevel være kopiering av dokumenter og la besitteren beholde originalene.

Det skjer hyppig at innehaveren beholder sine data etter at politiet har sikret dem, blant annet når det anses å være umulig eller uforholdsmessig inngripende å ta med seg datasystemet (f.eks. i en bedrift). Da må dataene kopieres på stedet. Originaldataene blir værende på systemet. Tilsvarende ved fjernsikring fra skytjenester. Med mindre innehaverens tilgang til datasystemet/tjenesten stenges etter at sikringen er foretatt, kan han/hun benytte, bearbeide og slette de originale dataene. Det er derfor påregnelig at kildedataenes tilstand endres etter sikringstidspunktet, og for data på aktive systemer vil dette bestandig være tilfelle, fordi aktiviteten fortløpende forårsaker endringer, om ikke annet så i logger og ved stadige oppdateringer. Det gjelder datasystemet i en bedrift, så vel som en påslått smarttelefon, og skytjenester. «Originaldata» må derfor forstås å *bety kildedataene i den tilstand de var på tidspunktet da de ble sikret*. Tidspunktet må selvsagt fremgå av dokumentasjonen. Implisitt følger det at politiets kopi er *den eneste representasjonen som finnes av originaldataene på et gitt tidspunkt.*[92]

5.4.2.1 Fremstilling av sikringskopien

Som det har fremgått kan data sikres etter at politiet først har tatt den fysiske databæreren i besittelse. Sikringen skjer da ved speilkopiering i politiets lokaler. Speilkopiering er kopiering på fysisk nivå og resulterer i en kopi som inneholder mengder av ustrukturerte data.[93] Alle data som fysisk befinner seg på originalbæreren, medtas, inklusive metadata og data som er slettet men ikke overskrevet (data i uallokerte områder). Kopien er en «speilkopi», dvs. en én-til-én kopi (1:1) av kildedataene. Speilkopiering utføres på et system som er avslått (kalles sikring *post mortem)*.[94]

[91] Se kapittel 3.2.
[92] Dog slik at hvis politiet har den originale databæreren i behold, kan ny sikringskopi lages fra denne.
[93] Casey (2011) s. 182-184; Hamm (2018), s. 149 og 152.
[94] Flaglien (2018) s. 22. Uttrykket brukes også i en litt annen betydning, for å skille bevissikring som skjer etter at en hendelse har inntruffet *(post mortem),* fra hendelseshåndtering mens den pågår (Årnes (2018) s. 5).

Speilkopiering kan anses som «dypsikring» fordi alle data medtas, inklusive underliggende metadata som er viktige for bevisverdien.[95]

Aktive filer og data i løpende prosesser må sikres med andre kopieringsteknikker. Sikring fra aktive systemer kalles *live* sikring. Dataene sikres på logisk nivå ved ordinær filkopiering («klipp og lim»), eller «datadump» (et uttrykk som visstnok brukes når data sikres fra datamaskinens minne (RAM – Random Access Memory), eller fra skjermen («skjermdump»)). *Live* sikring brukes f.eks. når data skal sikres fra stasjonære datasystemer i bedrifter, eller fra aktive datamaskiner som politiet har tatt i besittelse og som man ønsker å holde aktive for å unngå at adgangskontroll eller kryptering slår inn. *Live* sikring brukes også i datanettverk, og på skytjenester.[96]

Live sikring brukes derfor hyppig.[97]

Det *kan* også– etter det som har blitt opplyst[98] – speilkopieres fra et aktivt system, i så fall bare fra områder med lagret materiale som ikke er åpnet. Det er vanskelig å ha en formening om hvor praktisk dette er.

Ved *live* sikring er kopien en filkopi e.l., ikke en speilkopi. Sikringsformen medtar ikke uallokerte data. For utreder er det noe uklart i hvilken utstrekning autogenererte metadata som ikke er lagret sammen med innnholdsdataene, medtas. *Live* sikring er imidlertid ikke like «dyptpløyende» som speilkopiering og kan være å anse som «overflatesikring».

Siden speilkopiering medtar store mengder irrelevante data eksisterer det et «push» for utvikling av kopieringteknikker for *selektiv dypsikring,* dvs. fremgangsmåter som kopierer utvalgte deler av innholdet sammen med underliggende metadata. Så vidt forstås finnes slik teknologi for sikring *post mortem,* men ennå ikke som moden teknologi for aktive systemer (f.eks. skytjenester).[99]

---

[95] Se nærmere om metadata i punkt 5.5. Uten å gå for detaljert inn på tekniske forhold, kan det nevnes at «speilkopiering» iblant også brukes om andre svært grundige sikringsformer. Det har ikke noen betydning for denne utredningens problemstillinger. Se f.eks. Hamm (2018) s. 152.

[96] Se også Politidirektoratets (2010) beslagsrundskriv pkt. 3.3 tredje avsnitt, første punktum: *«I tillegg til lagrede data, kan e-spor også finnes i form av flyktige data i enhetens minne og datastrøm under kommunikasjon.»*

[97] Informant C i møte 19. september 2019. Dataetterforskingsprosessen har noen prioriteringsprinsipper for *live* sikring, f.eks. at de minst stabile sporene bør sikres først (*«order of volatility*»), og at de mest relevante data bør sikres før andre data (*«triage»)*, se Flaglien (2018) s. 30-31 og 36.

[98] *Ibid.*

[99] Dette utdypes i punkt 5.6.a.i, som redegjør for hvordan selektiv dypsikring kan brukes som teknikk for å skjerme taushetspliktige data fra beslagleggelse.

Speil- og filkopiering gir kopier som er identiske med kildedataene. Forskjellen består i hvilke kildedata de får fatt i, altså kopieringsgrunnlaget. En speilkopi er identisk med kildedataene i den form de eksisterer på databærerens fysiske nivå, men sikrer ikke data fra aktive filer og prosesser. Dette kan derimot oppnås ved filkopiering og «dumping» av data, men med disse teknikkene får man ikke fatt i data i uallokerte områder, og taper også metadata helt eller delvis.

Data kan også sikres fra databrikker (minnekort, chiper). Ekstrahering og sammenpusling av fragmenter krever spesialistkompetanse. Ekstrahering kan innebære at lagringsmediet må ødelegges. [100]

Den engelske rapporten *Search Warrants* skiller således mellom *physical, logical* og *specialist extraction of data.*[101]

5.4.2.2 Sikringskopien er et «øyeblikksbilde»

Et viktig poeng som utredningen alt har vært inne på, er at uavhengig av kopieringsteknikk *representerer den første kopien (speil- /filkopi / ekstraherte data) kildedataene på et gitt tidspunkt.* Den gir altså et «øyeblikksbilde».[102] Med mindre innehaveren har en sikkerhetskopi fra samme tidspunkt, vil politiets kopi være *den eneste representasjonen som finnes av de originale dataene.*[103]

Av hensyn til bevisverdien bør kopiens ekthet verifiseres. Den undergis derfor en teknisk prosess som dokumenterer hvor dataene stammer fra (autentisitet), og at de er intakte. Prosessen tildeler kopien en sikkerhetssignatur (sjekksum).[104] Man har dermed fremstilt en «sikringskopi». Sikringskopiens sikkerhetssignatur endres hvis innholdet endres. En uendret signatur er bekreftelsen på at sikringskopien er intakt. Som nevnt anbefaler Flaglien systematisk gjennomføring av integritetskontroll i hele prosessen, og at det dokumenteres med tidsstempler.[105]

---

[100] *Mobile and Embedded Forensics* er dekket av Jens-Petter Sandvik (2018). «Chip off» er såkalt «ødeleggende» bevissikring, se https://www.nist.gov/system/files/documents/2020/08/21/CFTT%20-%202019.pdf.
[101] UK Law Commission (2020), pkt. 14.105.
[102] Uttrykket brukes i sammenligningen av ransaking og dataavlesing i lovproposisjonen om skjulte tvangsmidler (Prop. 68 L (2015-2016)) pkt. 14.8.2 s. 262. Bevissikring ved ransaking skjer i et øyeblikk, mens dataavlesing foregår over tid.
[103] Dette gjelder med forbehold om at politiet ikke har databærerne i sin besittelse, men det er uansett ikke å regne som en sikker oppbevaringsmåte over tid. Dataene må uansett kopieres til et lagringsmedium som politiet fullt ut råder over.
[104] Casey (2011) s. 481. Flaglien (2018) pkt. 2.3.5.
[105] Utredningen punkt 5.3.

Hvis sikringskopien er en speilkopi av kildedataene og politiet har databærerne i behold, kan ektheten verifiseres ved at kildedataene gjennomgår samme prosess. Kildedataenes og sikringskopiens sikkerhetssignatur sammenlignes, og dersom de er identiske er sikringskopien en tro kopi av kildedataene.

For data som er sikret fra et aktivt system lar det seg ikke gjøre å fremstille en sikkerhetssignatur som er identisk med kildedataenes, fordi aktiviteten uunngåelig medfører endringer som vil gi dataene på kildesystemet en annen signatur enn sikringskopiens. Aktive kildedata kan heller ikke undergis den tekniske prosessen som resulterer i en sikkerhetssignatur. Ut fra bevissikringshensyn er det beste som kan gjøres, umiddelbart å la kopien gjennomgå sikkerhetsprosedyren. Det gir en sikkerhetssignatur nær i tid med sikringen, og utgjør den første referansen i bevishåndteringskjeden. Dermed kan det på et senere tidspunkt kontrolleres om sikringskopien har vært uforandret siden politiet sikret den.[106]

Samme prosedyre bør gjelde for data som politiet mottar fra eksterne, f.eks. trafikkdata fra teleoperatør. Politiet har ikke kontroll med at datafilen som mottas representerer originaldataene, men en sikkerhetssignatur vil kunne bevise at den opprinnelige filen har vært uforandret siden politiet mottok den.

Sikringskopiens verdi avhenger av at den holdes intakt.[107] Den behandles følgelig som originalbevis og legges til oppbevaring hos politiet. Betydningen understrekes av at man – som alt forklart – ikke kan regne med å ha de opprinnelige kildedataene tilgjengelig i ettertid. Sikkerhetssignaturen tilordnet sikringskopien «låser ned» dataene. Databevisene *og alle de øvrige dataene*, hva enten de er irrelevante eller beslagsfrie, «låses ned» under ett.

Søk etter databevis gjøres derfor ikke på sikringskopien, men på en *speilkopi* av denne som kan kalles «arbeidskopi».[108] I praksis kan det være tale om at sikringskopiens innhold legges over på politiets beslagsnett, teknisk skjermet mot endringer. Politidistriktenes tekniske løsninger/infrastruktur er ikke like, så det er mulig at begge løsninger brukes. Integritetsprinsippet tilsier imidlertid at etterforskeren som utfører analysen bare gis lesetilgang til de sikrede dataene.

[106] Informant C i møte med meg 19. september 2019.
[107] Se punkt 4.1.4 og sitatet fra informant A.
[108] Hamm (2018) pkt. 5.2.1.

Data som har bevisverdi kan kopieres fra beslagsnettet/arbeidskopien til en ny databærer, som legges i saken. Dataene «hentes» imidlertid ikke «ut» i den forstand at de fjernes fra sikringskopien/beslagsnettet/arbeidskopien, på grunn av endringene som da ville forårsakes. Det er derfor ikke uten videre mulig å utskille databevis fra irrelevante og beslagsfrie data.

Som det har fremgått er sikringskopien garantisten for at databevis kan påstås å være ekte. Det er viktig å unngå at den utsettes for endringer, eller i verste fall går helt tapt, f.eks. som følge av datakræsj. Derfor bør det tas enda en speilkopi av sikringskopien, dvs. en ordinær sikkerhetskopi *(«back up»)*, som verifiseres mot sikringskopien. Prosedyren følger av Politidirektoratets beslagsrundskriv som sier at

> det må tas back-up som oppbevares like lenge som speilkopien/filkopien. Back-up lagres på separat lokasjon. (RPOD-2010-7, pkt. 3.3 annet avsnitt).

5.4.2.3 Andre tiltak i sikringsfasen

For å hindre bevisforspillelse kan det være ønskelig å stenge innehaveren ute fra systemet / brukerkontoen. På grunn av flertilgangsmuligheten kan dette være vanskelig, men dersom det ligger til rette for det, er noen muligheter å endre passordet eller be tjenesteyter om å stenge tilgangen. Dette antas å kunne gjøres i medhold av beslagsbestemmelsene, dvs. enten ved at politiet foretar beslag gjennom å endre passord, eller gi pålegg om beslag til tjenestyter.

De fysiske databærerne har betydning for hvordan politiet går frem i sikringen av dataene.[109] I følge *Bjerknes & Fahsing*

> vil det alltid være et tema om beslaget [de fysiske objektene] er blitt utsatt for en behandling som kan ha påvirket innholdet av de elektroniske sporene.[110]

Det kan f.eks. være viktig å holde liv i en smarttelefon for å hindre at data går tapt, noe som tilsier at man sørger for strømtilførsel. Beslaglagte databærere bør legges i spesielle poser for å hindre at elektriske spenninger ødelegger innholdet, og settes i flymodus for å skjerme dem mot GPS-oppdateringer.[111] Av dokumentasjonsprinsippet følger det at objektene skal merkes. Merkingen av sikringskopien skal angi hvilken databærer, datasystem, brukerområde eller skytjeneste den er sikret fra, og dermed vise sammenhengen mellom kildedataene og

[109] Det minnes om at utredningen har avgrenset mot beslag i datautstyr for andre formål enn å sikre databevis, se punkt 2.3.
[110] Ole Thomas Bjerknes & Ivar Fahsing (2018) s. 251.
[111] *Ibid.*, s. 251; Flaglien (2018) s. 23; Sandvik (2018) s. 212-214.

sikringskopien. Det skaper visshet for at databevisene som etter hvert identifiseres, er autentiske.

Krav til håndtering av objektene og til merking, følger av strpl. § 207 og påtaleinstruksen § 9-5. I tillegg sier Politidirektoratets beslagsrundskriv følgende:[112]

> Ved beslag av hardware, skal alle beslaglagte enheter gis eget beslagsnummer. Merking av beslaget må foretas slik at beslaget ikke blir skadet. Beslaget bør merkes slik at alt kan monteres igjen på samme måte som før beslag ble foretatt. Ledninger som tas ut fra utstyr må også merkes. Beslaget må transporteres i adekvat emballasje.
>
> Også den kopierte informasjonen gis eget beslagsnummer, og dette må lett kunne knyttes til merkingen av gjenstandene i hardwarebeslaget og opplysninger i beslagsrapporten.

5.4.3 Klargjøringsfasen

Klargjøringen går ut på

> å trekke ut og gjøre [den sikrede informasjonen] tilgjengelig, slik at det blir mulig å vurdere om informasjonen har verdi som bevis i straffesaken.[113]

Sikring ved speilkopiering gir ustrukturerte rådata som må bearbeides for å bli forståelige.[114] Sikring ved filkopiering kan nok gi lesbare data, men problemer både med mengde og struktur gjør at de må tilrettelegges for etterforskeren som skal lete etter bevis.[115] I Rt. 2013 s. 968 var klargjøringen Økokrims begrunnelse for et forslag om at tingretten kunne la en medarbeider fra Økokrim tilrettelegge for utsorteringen av beslagsfritt materiale:

> Det er uvisst hvordan siktedes pc'er er organisert. Det antas at det vil være nødvendig med bruk av spesielle dataverktøy og bistand fra datakyndig i gjennomgangen av datamaterialet (…) slik at man kan skaffe en oversikt over hva materialet består i og hvordan en gjennomgang kan gjennomføres på mest mulig effektiv og målrettet måte.[116]

---

[112] Politidirektoratet (2010) RPOD-2010-7, pkt. 3.3 femte og sjette avsnitt.
[113] Flaglien (2018) kap. 2.4.
[114] I følge Flaglien kan rådata anses som *«a 'black box' of unstructured binary data»* (2018), s. 34.
[115] «Klargjøring» brukes om figurens fase «Examination», som på norsk betyr «undersøkelse». «Klargjøring», eventuelt «tilrettelegging», er likevel vanlig brukt i det norske fagmiljøet. «Examination» kan sies i større grad enn «klargjøring», å uttrykke realiteten i at politiet i denne fasen får et visst innsyn i de sikrede dataene. Skillet mellom klargjøring og analyse er uansett ikke skarpt.
[116] Rt. 2013 s. 968 avsnitt 5.

Også Etterretningsdoktrinen for politiet beskriver klargjøring:

> gjøre innhentet materiale forståelig, enten det er visuelt, hørbart eller lesbart. Data fra de ulike sensorene kommer i varierende form. For eksempel som digitaliserte data (trafikkdata, datapakker fra internettrafikk, m.m.) i et uforståelig språk ved kommunikasjonskontroll, bilder av områder eller personer uten kontekst, eller som massive mengder data fra åpne kilder.[117]

Klargjøringen regnes som egen fase fordi den kan kreve mye arbeid. Oppgavene kan blant annet gå ut på å

- bearbeide binære rådata til lesbar form,
- kontrollere tidsstempler,
- redusere datamengden ved å filtrere bort irrelevante data,
- få frem slettede, skjulte, komprimerte og krypterte data,[118]
- foreta uttrekk av prioritert materiale,[119]
- strukturere gjenværende materiale slik at den taktiske etterforskeren kan analysere det. I den forbindelse har autogenererte metadata så vidt forstås sentral betydning.[120]

I tillegg vil utskillelse av beslagsfrie opplysninger være en oppgave i klargjøringsfasen.

På grunn av datamengdenes størrelse vil datareduksjon som nevnt i tredje kulepunkt være en prioritert oppgave. EMD-dommen *Sigurdur Einarsson og andre mot Island* som gjennomgås i kapittel 15, illustrerer hvor krevende dette kan være, og at arbeidet må skje strukturert med god notoritet.[121] Med et eksempel fra norsk praksis, omtales datareduksjon i HR-2018-699-A:

> Etter en tilrettelegging og *fjerning av duplikater* besto materialet fra [en av siktedes mobiltelefoner] av 107 000 filer.[122]

Det er ikke et skarpt skille mellom klargjøringen og fasene før/etter. Noen verktøy har automatisert prosessene, f.eks. verktøyet Cellebrite som sikrer og klargjør data fra mobiltelefoner.[123] Derfra kan man gå direkte til analysen. Dessuten kan automatiserte

---

[117] Politidirektoratet (2020) s. 34. Dette illustrerer også dataetterforskingsprosessens generelle anvendelse, også utenfor etterforsking.
[118] Flaglien, *ibid.,* s. 35.
[119] F.eks. bildefiler i en sak om seksuelle overgrep; epost i en sak om rettsstridig tilegnelse av forretningshemmeligheter; internettlogger for et tidsintervall som dekker det antatte gjerningstidspunktet, osv.
[120] Se nærmere utredningen punkt 5.5.
[121] *Sigurdur Einarsson og andre mot Island.* Dom 4. juni 2019. (saknr. 39757/15).
[122] Kjennelsen avsnitt 10. Utreders utheving.
[123] Informant B i samtale 22. januar 2021.

datauttrekk av prioritert materiale, anses som en del av analysen (såkalt «teknisk analyse»), se nærmere om dette nedenfor.

5.4.4 Analysefasen

Analysen går ut på

> å finne relevant informasjon i tilknytning til hendelsen som er under etterforskning, kartlegge hvem som kan knyttes til handlingen, samt belyse verdien og påliteligheten av denne informasjonen.[124]

Dataetterforskingsprosessen tilbyr ikke noen mal for hvordan analysen skal foregå eller dokumenteres. *Flaglien* beskriver imidlertid flere fremgangsmåter for analyse, blant annet bruk av søkeord/ tekststrenger, bruk av verktøy som basert på metadata automatisk plasserer informasjon på en tidslinje, verktøy som avdekker og visualiserer sosiale relasjoner og andre sammenhenger, f.eks. at et kontonummer går igjen i flere eposter, at en bil vises på flere bilder osv.[125] Ved analyse av særlig store datamengder som i økonomiske straffesaker, kan bruk av KI-verktøy for å avdekke mønstre mv., være aktuelt.

Faglitteraturen har etter hvert begynt å skille mellom tre former for analyse av databevis, nemlig teknisk analyse, innholdsanalyse og evaluering.[126]

5.4.4.1 Teknisk analyse: Repeterbar prosess

Teknisk analyse er undersøkelser som har teknisk verifiserbare resultater. Utføringen krever liten eller ingen grad av fortolkning eller skjønn fra etterforskerens side. En teknisk analyse er *repeterbar*. Med dette menes at samme resultat vil oppnås av annen som bruker samme fremgangsmåte på den samme sikringskopien. Teknisk analyse kan f.eks. gå ut på å avdekke filer med ulovlig innhold, på grunnlag av en sjekksumliste over kjente ulovlige filer. Lister som nevnt finnes både for overgrepsbilder av barn og skadelig dataprogram (*malware)*. Et annet eksempel er automatiske søk gjort på grunnlag av nøkkelord. Forutsatt at søkeordene og søkeverktøyet er de samme, skal søk gjort av en annen på de samme data gi identisk uttrekk. Teknisk analyse kan også anses som en del av klargjøringen av sikrede data (se punkt 5.4.3).

5.4.4.2 Innholdsanalyse: Vurdering opp mot straffebud

Innholdsanalyse innebærer undersøkelser av observerbart innhold, dvs. slikt som etterforskeren kan se eller høre (film, bilder, lyd, tekst). Problemstillingen gjelder om innholdet alene eller

---

[124] N. Sunde (2019b) s. 60; se også Flaglien (2018) kap. 2.5.
[125] Flaglien (2018) s. 39-44.
[126] N. Sunde, (2019b) s. 61-62 og s. 72-74.

sammenholdt med andre opplysninger, utgjør dokumentasjon for straffbare forhold. For å kunne utføre analysen må etterforskeren ha kunnskap om siktelsen og ransakingsbeslutningen, eller ha en klar bestilling («mandat») fra en som har denne kunnskapen. Vurderingen forutsetter bruk av menneskelig skjønn og er ikke teknisk repeterbar. Derimot kan dokumentasjon av fremgangsmåte og resultater tilrettelegge for at analysen er *reproduserbar og etterprøvbar*. Etterprøvbarhet er viktig, ikke bare for å kunne reprodusere, men også for å kunne vurdere metode og teknikk, om prosedyrer er fulgt, foruten omstendighetene, resonnementene og usikkerhetsmomentene som konklusjonene bygger på.[127] Hvorvidt konklusjonene virkelig blir de samme avhenger av de menneskelige vurderingene av innholdet opp mot straffebudene.

5.4.4.3 Evaluering av databevis: Vurdering av beviskraft

Evaluering er en kvalitetssikringsprosess som skal fremme objektivitet, og sørge for at bedømmelser av bevisets styrke fastsettes og formidles på standardisert måte.[128] Etter det opplyste følges rutinen blant annet for DNA-spor, og er i ferd med å bli implementert i NCFI utdanningen ved Politihøgskolen. Prosedyren er neppe nødvendig i alle saker, men bør utføres for databevis som er komplekse eller av sentral betydning i alvorlige saker.

Evaluering går ut på å vurdere beviskraft og bør gjøres i lys av gjensidig utelukkende hypoteser relatert til databeviset. Databevisets styrke bedømmes i lys av hypotesene og noen gitte omstendigheter som er sentrale for saken. Etterforskingen gjelder f.eks. hvorvidt siktede har medvirket til en terrorhandling (halshugging). Hypotesene (H) kan være relatert til en video på siktedes smarttelefon som viser halshuggingen. H1 kan f.eks. gå ut på at telefonen ble brukt til å filme hendelsen, og H2 at den ikke ble brukt til å filme hendelsen.[129] Vurderingen angår sannsynligheten for at videoen slik den ble funnet på smarttelefonen, er resultat av at den var brukt til å filme halshuggingen, vs. at den ikke var brukt til å filme halshuggingen (f.eks. tilsendt fra en annen eller lastet ned fra YouTube). For å sikre pålitelige vurderinger bør styrkegraden angis i henhold til en standard, f.eks. CAI (*Case Assessment and Interpretation)*.[130] Først når databeviset er evaluert skal det innlemmes i sakens totale bevisbilde.

---

[127] Dette er i tråd med ISO 27037:2012 *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*, pkt. 5.4.2 (oppdatert 2018).
[128] Casey (2020); Ryser m.fl. (2020)
[129] Ryser *ibid.* pkt. 6
[130] Casey (2020); Pollit et al. (2018); Cook et al. (1998).

Evaluering fokuserer på *databevisets* styrke i forhold til et gitt faktum, og skiller seg fra oppgaven til en taktisk etterforsker, som er å vurdere hvorvidt *sakens* hypoteser styrkes eller svekkes av bevisene som avdekkes.

Evaluering forutsetter bruk av menneskelig skjønn, og er i likhet med innholdsanalysen reproduserbar (forutsatt god dokumentasjon), men ikke repeterbar som teknisk analyse. Det er derfor tenkelig at to sakkyndige kan konkludere forskjellig.

5.5 Metadata

En informasjonsenhet på datasystemet består både av innhold og autogenererte metadata. De kan være lagret forskjellig sted, men når dataene er i bruk henger innholds- og metadataene sammen. Det kan sammenlignes med at Munchs signatur lagres et annet sted enn på maleriet. Signaturen har utvilsomt spesiell betydning når den henføres til maleriet, og maleriet får en unik status på grunn av signaturen.

Metadata kommer i mange fasonger. Definisjonen av metadata er at det er data som sier noe om andre data. Metadata til et dokument kan f.eks. være dokumentfilens navn, opprettelsesdato, hvem som skapte den, lokaliseringen og størrelsen. Metadata kan lages av brukeren selv (f.eks. navnet på et dokument eller overskriften i en epost), eller genereres automatisk av datasystemets loggfunksjoner. Autogenererte metadata er nødvendige for å kunne strukturere det sikrede datainnholdet for analyse, avdekke bevis og vurdere pålitelighet. Iblant er de beviset i seg selv.

Dataforskeren *Gard O. Sundby Thomassen* ved Institutt for informatikk, Universitetet i Oslo, forklarer at «mesteparten av data i verden i dag er egentlig ustrukturerte», og at

> på skytjenester blir ikke [filene dine] lagret på ett sted i et hierarkisk system. En sånn løsning hadde ikke gjort prosessen skalerbar for leverandørene. I stedet er filene dine spredt på vidt forskjellige lagringssteder og katalogisert etter metadata. Så når du skal hente dem frem igjen, settes dette puslespillet sammen og presenteres som hierarkisk og ordnet for deg, der du sitter på egen maskin.[131]

Det fremgår at metadataene er viktige for forståelsen av hvilke datafragmenter som hører sammen, noe også dataetterforskerne understreker (se punkt 4.1.2). *Mason & Seng* viser at metadata ikke bare har betydning for å avdekke hvem som var hvor og gjorde hva på et bestemt tidspunkt. Metadata er også nødvendige for å vite når digitalt innhold er produsert og endret, noe som selvsagt kan ha stor betydning for å klargjøre forhold av bevismessig betydning. Et

[131] Sitat hentet fra Kjetil Johansen & Werner Anderson (2021) s. 106.

dokument kan f.eks. finnes i flere versjoner. Ved hjelp av metadataene kan det fastslås hvilken versjon som er relevant for saken.[132] Metadata kan også være beviset i seg selv, f.eks. dersom det anføres at et tidsstempel har blitt manipulert. Da må det kunne føres for retten i lesbar form.[133] Klargjøringen av dataene baseres således på metadataene, og de er nødvendige for å identifisere og vurdere bevis i analysen, og kan være bevis i eg selv.

I saken om det såkalte «Skøyen-drapet» (RG 2012 s. 74) var metadata viktige for tiltaltes alibi. Dersom de skyldte hans egen aktivitet, ville han ha alibi, mens alibiet sto vesentlig svakere dersom de var generert av systemet som følge av at andre hadde sendt ham epost e.l. Slik saken lå an lot dette seg ikke fastslå med sikkerhet.

5.6 Sletting, sperring og skjerming av data

Dataetterforskingsprosessen har fokus på å sikre data og bevare integriteten, begge deler med formål å avdekke relevante opplysninger på en sikker måte. Under etterforsking kan det imidlertid oppstå behov for å skjerme beslagsfrie data fra politiets innsyn. Dette behandles som eget tema i del VI. Dataetterforskingsprosessen sier ikke stort om hvordan dette kan gjøres.

Etter henvendelse fra utreder har imidlertid en faglærer i NCFI-miljøet orientert om følgende muligheter for å skjerme beslagsfrie data:[134]

a. På sikringsstadiet:

Man kan *unnlate å sikre beslagsfrie opplysninger*. Dette skjer på mappe/filnivå, noe som betyr at opplysningene må være lagret i identifiserbare enheter som kan utelates fra kopieringen.

I så fall finnes to varianter:

i. Det kan foretas selektiv «dypsikring», dvs. at sikringen medtar innholdsdata og tilhørende metadata, eventuelt også uallokerte data, men dette skjer avgrenset slik at irrelevante og beslagsfrie kan data holdes utenfor. Fremgangsmåten kan anses som avgrenset speilkopiering. Sikrings-/analyseverktøyet X-Ways Forensics støtter metoden. Så vidt forstås kan verktøyet bare dypsikre fra et avslått system *(post mortem)*.

[132] Mason & Seng (2017a) s. 38, pkt. 3.9; Maria A. Hjort (2016) pkt. 1.3.3.
[133] Mason & Seng, *ibid*.
[134] Informant D i epost 26. april 2021.

I tillegg beskriver *Faust m.fl.* en fremgangsmåte for selektiv dypsikring fra aktive systemer (*live* sikring).[135] Teknologien er foreløpig et *«proof of concept»*, dvs. at den ikke er moden og foreløpig ikke implementert i et praktisk verktøy.

ii. Det kan foretas selektiv filkopiering («overflatesikring»).

b. I klargjørings- og analysefasen*:*

(i) Under klargjøringen og analysen kan man sørge for at dataverktøyet *utelater de beslagsfrie opplysningene*, også i dette tilfellet basert på utelukkelse av mapper/filer. Utelatelsen skjer virtuelt, dvs. at mappene/filene fortsatt finnes i sikringskopien. De kan følgelig hentes frem på et senere tidspunkt. Sikringskopiens integritet ivaretas.

(ii) I tillegg forskes det på muligheten for å foreta selektiv «dypsletting» av beslagsfrie data i sikringskopien, samtidig som integriteten til det gjenværende materialet beholdes.[136] Heller ikke dette er moden teknologi.

Alle alternativene forutsetter forhåndskunnskap om lokaliseringen av de relevante eller beslagsfrie opplysningene, for å kunne innrette sikringen/klargjøringen deretter. Et visst innsyn er derfor nødvendig. Dersom lokaliseringen av relevante data (som kan sikres målrettet) eller beslagsfrie data (som kan skjermes målrettet) er ukjent, er ingen av alternativene er anvendelige.

Det har som nevnt vært vanskelig å få full klarhet i hva som er *teknisk umulig*, og hva som er *teknisk mulig, men så vanskelig og tidkrevende at det ikke anses praktisk gjennomførbart* innen rammen av en etterforsking. I det følgende er imidlertid følgende utgangspunkter lagt til grunn:

Sikringskopien har et fysisk nivå og et virtuelt (logisk) nivå. Det antas å være sletting på fysisk nivå som endrer sikringskopiens integritet. Foruten skjerming, antas sperring av opplysninger å være et mulig alternativ. Skjerming og sperring gjør data utilgjengelige eller uleselige uten at det går ut over sikringskopiens integritet.

[135] Fabian Faust, Aurélien Thierry, Tilo Müller & Felix Freiling (2020).
[136] Christian Zoubeck & Konstantin Sack (2017).

5.7 Oppsummering

5.7.1 Sikring av data vs. dokumentasjon av spor

Sikring av data synes å være noe annet enn ransaking og beslag, og tydeligere rettslig regulering antas å være nødvendig. «Sikring» brukes imidlertid i varierende kontekster, og i et lovgivningsperspektiv er det behov for å klargjøre hvordan begrepet brukes.

Lovens begrepsbruk bør tydelig skille mellom sikring av data, og dokumentasjon som gjelder obeservasjon og undersøkelser av data. Utredningen reserverer sikringsbegrepet for sikring av dataene som sådan, slik dette er beskrevet i punkt 5.4.2.

Noen eksempler belyser forskjellen. Under ransaking av en bolig finner politiet en bærbar datamaskin som er avslått. Denne tas i beslag og bringes til politiets lokaler slik at *dataene* kan sikres (*post mortem).* Politiet speilkopierer dataene og lager en sikringskopi. Dermed er dataene sikret, og beslaget i datamaskinen kan heves slik at den kan returneres til innehaveren.

På den samme ransakingen påtreffer politiet siktede som er opptatt av sin iPhone. Politiet beslaglegger iPhonen og på stedet scroller etterforskeren gjennom bilder og meldinger fordi det haster å komme på sporet av dem som siktede samarbeider med. Politiet bruker sin egen iPhone til å fotografere bilder/meldinger på siktedes smarttelefon, som antas å ha betydning for saken. I dette tilfellet har politiet dokumentert spor, ikke sikret data. Gjennomsynet er å regne som ransaking av smarttelefonen og skal dokumenteres i ransakingsrapporten. Bildene som ble tatt av innholdet, er dokumentasjon for hva politiet observerte at lå der, og må vedlegges ransakingsrapporten. Ytterligere bevis for undersøkelsen og smarttelefonens innhold kan sikres ved avhør av etterforskeren.

Live sikring som ble beskrevet i punkt 5.4.2, er å anse som sikring av data fordi dataene kopieres, og medtar metadata i den utstrekning de er integrert med innholdet. Foto av digitalt innhold derimot medtar ikke dataenes egenskaper, som for eksempel metadata i bildefiler. Hvorvidt et skjermfoto (*screenshot*) er å anse som sikring eller dokumentasjon for det visuelle innholdet på dataskjermen, får stå som et åpent spørsmål.

Forskjellen mellom sikring av data og dokumentasjon av observasjoner og undersøkelser, er viktig. Undersøkelser av originale data medfører endringer som kan være avgjørende for bevisverdien, iblant med risiko for at den går tapt. Betydningen av nøyaktig og pålitelig dokumentasjon for dataenes opprinnelige tilstand, og ikke slik den var *etter* politiets undersøkelse, bør derfor bevisstgjøres. Som nevnt i et tidligere arbeid følger de politiskapte

endringene med ved eventuell etterfølgende sikring av dataene, og det er i et slikt tilfelle viktig å være klar over og kunne redegjøre for, endringene i originalbeviset.[137] I henhold til prinsippet om fri bevisførsel kan de sikrede dataene føres som bevis, men politivitnets forklaring og dokumentasjon som viser hva som ble observert og hvordan databæreren ble undersøkt, blir vesentlig for å belyse hva innholdet besto i da politiet tok hånd om den. Nye retningslinjer bør presisere dette, se nedenfor.

5.7.2 Tydeligere regulering av *live* sikring

Dataetterforskingsprosessen som metodikk er i utgangspunktet utviklet for databevis som sikres fra systemer som er avslått. I dag er både undersøkelser og sikring som skjer *live* svært praktisk. Politipatruljens etterforsking «på stedet» innebærer ofte ransaking og beslag i smarttelefon. For slike undersøkelser gir dataetterforskingsprosessen lite veiledning, og *Andreassen & Andresen* har funnet systematiske svakheter i gjennomføring av bevissikringen i slike situasjoner.[138] Det kan derfor være behov for tydeligere retningslinjer for å styrke kvaliteten av slike undersøkelser.[139]

5.7.3 Data «låses ned» i sikringskopien

Innhentede opplysninger tyder på at alle sikrede data i sikringskopien «låses ned» under ett uavhengig av relevans og om de er rettslig beskyttet mot beslagleggelse. Sletting på fysisk nivå må antas å gå ut over integriteten, mens dette ikke antas å være tilfelle for skjerming og sperring. Det kan være behov for innspill i høringsrunden for å få full klarhet i dette. Det legges også til grunn at sikringskopien inneholder metadata som er nødvendige for å kunne strukturere det sikrede datainnholdet for analyse, avdekke bevis og kunne vurdere pålitelighet. Dessuten kan metadata være beviset i seg selv.

5.7.4 Sikringskopien

Med tanke på regulering synes sikringskopien å være et sentralt omdreiningspunkt. Den bør være utgangspunkt for regulering av beslag og gjennomføring av beslagsfrihet. Det oppstår også spørsmål om regler for oppbevaring av sikringskopien og eventuelt også for en sikkerhetskopi.

Siden teori og rettspraksis gjennomgående taler om «speilkopien», foreligger det her et terminologisk spørsmål. Forskjellen er at mens «speilkopiering» angir en kopieringsteknikk,

---

[137] I.M. Sunde (2015) pkt. 2.6, s. 604.
[138] Leif Erik Andreassen & Geir Andresen (2019), masteravhandling.
[139] Slik også *ibid.*

angir «sikringskopi» den verifiserte kopien av kildedataene uavhengig av hvilken kopieringsteknikk som ble benyttet. «Sikringskopi» betegner derfor en størrelse som finnes i alle saker med sikrede data. Noen eksempler belyser dette.

(i) I Rt. 2012 s. 1645 var spørsmålet om det av strpl. § 170 a kunne utledes en plikt for politiet til å speilkopiere innholdet på datamaskiner beslaglagt hos siktede. Lagmannsrettens hadde lagt til grunn at strpl. § 170 a ikke ga domstolene hjemmel for å pålegge politiet å speilkopiere datamaskinene. Høyesterett var uenig i lovtolkingen og sa at det

> prinsipielt sett ikke [er] noe til hinder for at ulempene for den siktede kan være så betydelige at beslag bare kan anses forholdsmessig om det skjer i form av speilkopiering av de beslaglagte databærere. Det er imidlertid ikke slik at det kan oppstilles en alminnelig plikt for politiet til å foreta speilkopiering. Det må foretas en interesseavveining (…).[140]

Så vidt forstås kunne samme resonnement vært ført for «kopiering». Poenget var at politiets bevismessige behov for å beholde datamaskinene ville bortfalle dersom dataene ble kopiert. Da kunne datamaskinene returneres til siktede. Kjennelsen fokuserer på en spesiell kopieringsteknikk (speilkopiering) uten at teknikken i seg selv var relevant for spørsmålet og burde prinsipielt vært drøftet i relasjon til sikringskopien.

(ii) Rt. 2013 s. 968 gjaldt krav om tilbakelevering av speilkopi sikret hos siktet advokat. Etter å ha speilkopiert advokatens bærbare datamaskin og en harddisk, hadde politiet levert datautstyret tilbake. Advokaten krevde imidlertid selve speilkopien tilbakelevert, under henvisning til at den inneholdt beslagsfritt materiale. Kjennelsen beskriver speilkopien slik:

> Speilkopien er ikke «levende» – tekstdokumenter, bilder mv. kan ikke endres i selve kopien, og kopien forblir upåvirket av søk. Filene og informasjon om filene («metadata») «fryses» ved tidspunktet for kopieringen.[141]

Sitatet beskriver nettopp de egenskapene ved en sikringskopi som er sentrale for problematikken som utredningen behandler, nemlig at dataene er «nedlåst». Siden

[140] Kjennelsen avsnitt 18 og 19.
[141] Kjennelsen avsnitt 22.

«nedlåsingen» skyldes den tekniske verifiseringsprosessen ville det samme vært tilfelle om sikringskopien var opprettet ved filkopiering.

(iii) *Haaland* kritiserer speilkopiering hos advokat.[142] Hun anfører at speilkopieringen i seg selv er et inngrep i privatlivet som krever klar lovhjemmel, og drøfter hvorvidt strpl. § 192 kan anses å gi slik hjemmel. Konklusjonen er at dette nok er tvilsomt og at «rettsgrunnlaget [for speilkopieringen] er uklart».[143]

Etter utreders mening kan det ikke herske tvil om at hjemmelskravet gjelder for sikring av databevis generelt, både hos advokat og andre, og ikke påvirkes av hvilken kopieringsteknikk som er benyttet.[144] Konklusjonen måtte derfor blitt den samme om filkopiering var benyttet, med mindre sikringen begrenses til å gjelde et utvalg konkret spesifiserte filer. Reelt sett er det fremstillingen av en sikringskopi som inneholder en stor mengde beslagsfrie data, som kritiseres.

(iv) *Haaland* kritiserer også politiets etterfølgende gjennomgang av «restmaterialet» som utleveres fra tingretten når utsorteringen av det beslagsfrie materialet er gjort. Hun påpeker at det «ifølge aktører i rettsvesenet (…) aldri vil være mulig å luke ut all taushetsbelagt informasjon ved speilkopiering».[145]

Poenget er relevant og viktig, men gjelder ikke bare data som er sikret ved speilkopiering. Det gjelder for enhver sikringskopi fremstilt av kildedata tilhørende en advokat, også sikringskopier som er resultat av at slike data er filkopiert. Det samme gjelder data ekstrahert fra minnet på advokatens smarttelefon. Konklusjonen ville vært den samme om man talte om en sikringskopi.

(v) I høringsrunden til NOU 2016: 24 *Ny straffeprosesslov* tok Advokatforeningen til orde for å lovfeste speilkopiering som «hovedsikringsform ved databeslag». Det ble vist til at med speilkopiering kan

> det elektroniske innhold (…) sikres raskt slik at den fysiske databærer deretter kan leveres tilbake til eier uten opphold. Ved speilkopiering trenger politiet altså ikke å beholde besittelsen av mobiltelefonen, datamaskinen etc. for å gå gjennom innholdet. [146]

[142] Marita Haug Haaland (2019).
[143] *Ibid.*, s. 197.
[144] Se kapittel 11.1.
[145] Haaland *op.cit.*, s. 203.
[146] Advokatforeningen (2017) s. 61.

Innspillet tar opp spørsmålet som ble behandlet i Rt. 2012 s. 1645 (se over), og som nevnt kan tilsvarende resultat også oppnås ved andre kopieringsteknikker. Det underliggende poenget gjelder nødvendighetsvilkåret, jf. strpl. § 170 a, som sier at et tvangsmiddel bare kan benyttes når det er «tilstrekkelig grunn» til det. Dersom det ikke er nødvendig for politiet å beholde en databærer, skal den returneres til innehaveren. Hvis databæreren ikke skal inndras plikter politiet å returnere den etter å ha sikret innholdet. Loven bør derfor konsentrere seg om å ivareta nødvendighetsvilkåret, kopieringsteknikken har ikke betydning i den sammenheng. En lovbestemmelse som foreslått ville dessuten kunne binde bevissikringen til en spesiell teknologi på uheldig måte.

5.7.5 Lagring av sikringskopien

Dataetterforskingsprosessen stopper ved presentasjonen av analysen. Hva som bør skje med sikringskopien som sådan gir ikke metodikken svar på. Dette bør som allerede antydet, reguleres nærmere, se utredningen punkt 19.3.

Del III. Ransaking, sikring og beslag i data – Rettslige utgangspunkter

Mandatet ber utreder

> identifisere de særskilte problemstillingene databeslag reiser, vurdere om det er behov for lovendringer, samt komme med konkrete forslag til lovendringer.[147]
>
> …
>
> Videre bør utreder vurdere om det gjeldende beslagsbegrepet er treffende for databeslag. I den forbindelse bør utreder gå nærmere inn på grensedragningen mellom ransaking og beslag i data. Som et bakteppe for drøftelsene bør utreder også gi en beskrivelse av de tekniske fremgangsmåtene som benyttes ved databeslag, og redegjøre for hvilke overordnede hensyn som begrunner valget av teknisk fremgangsmåte.
>
> Problemstillingene skal drøftes i lys av grunnleggende straffeprosessuelle prinsipper som kontradiksjon, partslikhet og proporsjonalitet. Videre må forslagene være i samsvar med de menneskerettslige krav som følger av blant annet Grunnloven og Den europeiske menneskerettskonvensjonen, herunder bør forholdet til EMK artikkel 6 og artikkel 8 vurderes særskilt.

[147] Mandatet punkt 2 første avsnitt.

Problemstillingene faller i to grupper, den ene gjelder de rettslige kravene som bør stilles til inngrepene som ransaking og beslag i data innebærer overfor den som rammes. Vurderingstemaet gjelder det straffeprosessuelle regelverket sett i forhold til vilkårene som følger av Grunnloven §§ 113, jf. 102 og EMK artikkel 8 om retten til respekt for sitt privatliv mv. Den andre delen gjelder hensynene til kontradiksjon og partslikhet, hvor vurderingene foretas opp mot Grunnloven § 95 og EMK artikkel 6 om rettferdig rettergang.

6. Lovtekniske overveielser

6.1 Hensynet til teknologinøytralitet

Det er nærliggende at utkast til lovendringer og retningslinjer om databevis i noen grad må utformes teknologispesifikt, og bryte med hensynet til teknologinøytralitet. Som nevnt i punkt 2.2 vil ikke dette representere et prinsipielt nytt innslag i straffeprosesslovgivningen.

Hensynet til teknologinøytralitet gjør seg først og fremst gjeldende ved utformingen av formell lov. Lovgivningsprosessen er vanligvis for tidkrevende til å kunne sørge for at loven til enhver tid kan holdes ajour med teknologiutviklingen. For forskrifter og retningslinjer som enklere kan oppdateres og videreutvikles, har det mindre vekt. Justisdepartementets bok om lovteknikk opplyser at

> tekniske detaljregler ofte med fordel [kan] plasseres i forskrift, særlig hvis de i praksis bare retter seg til avgrenset brukergruppe (fagpersonale). Det samme kan ofte gjelde hvis det må ventes hyppige endringer i regelverket.[148]

Inngrepets rettsgrunnlag må fremgå av loven, jf. Grunnloven § 113 «Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov». Loven må i tillegg inneholde prosessuelle garantier mot misbruk og vilkårlighet. Hvis inngrepets kjerne for eksempel karakteriseres av fremstilling, bruk og oppbevaring av sikringskopien, må dette dekkes av lovens bestemmelser med tilhørende sentrale saksbehandlingsregler. I så fall kan en viss teknologispesifisitet være uunngåelig.

Ytterligere er det viktig at loven utformes klart og forståelig slik at borgerne kan innrette seg etter den og forutse konsekvenser av sine handlinger. For å oppnå tilstrekkelig tydelighet kan det være nødvendig å ty til teknologispesifikke formuleringer.

---

[148] Justisdepartementet (2000) pkt. 2.2.3 *Valg mellom lov og forskrift*.

På generelt grunnlag er det vanskelig å avgjøre hvor langt hensynet til teknologinøytralitet reelt sett gjør seg gjeldende. Teknologibegrepet er så vidt at det slår inn i alt politiet gjør, se *Paulsen* som sier at:

> Teknologibegrepet refererer både til fysiske produkter, til måter å bruke produktene på, til metoder, og dels også til teoriene som ligger til grunn for produktene (Brey, 2017; Hanks, 2010). Derfor er det en rimelig påstand at politiet benytter teknologi hele tiden – i alt fra bekledning til batong, fra avhørsmetodikk til alkometer. Problemstillingen er altså ikke om politiet skal benytte teknologi, men hvilken teknologi politiet skal benytte, hvordan den skal benyttes, og her særlig hvilke vurderinger som bør ligge bak bruken.[149]

Straffeprosessutvalget konstaterte dessuten at det er

> særlige forhold ved moderne informasjons- og kommunikasjonsteknologi som får betydning for praktiseringen av enkeltregler (…) Dette innebærer at man ved utformingen av loven blant annet må ta høyde for de særlige hensyn som gjør seg gjeldende ved innhenting, lagring, sikring og bruk av digitale bevis. Enkelte bestemmelser vil dessuten måtte uformes særskilt for digitale forhold slik tilfellet for eksempel er for tvangstiltak i form av inngrep i kommunikasjon.[150]

FORMOBILE-prosjektets straffeprosessuelle rapport fra 2021 omtalt i utredningen punkt 3.4.3, opplyser at europeiske land i det store og hele mangler straffeprosessuell regulering som direkte gjelder databevis fra mobile databærere. I stedet anvendes eldre bestemmelser om ransaking og beslag «så langt de passer».[151] Rapporten anbefaler mer spesifikk regulering, fordi databevis reiser egne problemer og det kan være vanskelig å trekke holdbare analogier fra fysiske forhold.[152]

Å kreve egne lovbestemmelser for forskjellige databærere (bærbare, stasjonære, skytjenester mv.) er nok å gå noe langt. Men at det er behov for bestemmelser som gir større klarhet med hensyn til forhold som er spesielle for databevis, synes å være ukontroversielt. Det viktigste er å unngå at loven binder håndteringen av databevis til spesifikke fremgangsmåter eller

[149] Jens Erik Paulsen (2019) s. 23.
[150] NOU 2016: 24 Ny straffeprosesslov, s. 153.
[151] FORMOBILE-rapporten pkt. 2.1 *(«mutatis mutandi»).*
[152] *Ibid.*, pkt. 2.3.

teknologier,[153] jf. også Straffeprosessutvalgets målsetting om at loven bør innrettes slik at «de til enhver tid foretrukne digitale løsninger» i rimelig utstrekning kan benyttes.[154]

Oppsummert betyr dette at mens ønsket om teknologinøytral lovgivning kan anses å ha en viss appellativ kraft, er det bare ett av flere viktige hensyn. I og med at teknologibegrepet i seg selv er vidt og vagt, er det heller ikke lett å vite hva teknologinøytralitet konkret innebærer. Til forskjell f.eks. fra hjemmelskravet i Grunnloven § 113, lar ikke hensynets gjennomslagskraft seg angi generelt. Det man nok kan enes om er at detaljert regulering av kopieringsteknikker og tekniske fremgangsmåter i lovs form, ikke er ønskelig.

6.2 Hensynet til rettslig kontinuitet

I høringsuttalelsen til Straffeprosessutvalgets utredning fremholdt riksadvokaten betydningen av rettslig kontinuitet, dvs. at det ikke bør gjøres større endringer enn nødvendig, og at der endringer gjøres bør forarbeidene synliggjøre hvor langt endringene rekker.[155] For regulering av databevis må dette forstås dithen, at dersom man kan bygge på løsninger utviklet i rettspraksis, som kan anses som tilstrekkelig avklarte, bør det ikke innføres nye bestemmelser fordi det kan gi åpne for utilsiktede tolkingsmuligheter og rettsusikkerhet. Synspunktet har gjenklang i EMK artikkel 8 (2), hvor det nettopp er loven slik den er utviklet i rettspraksis, som vurderes i relasjon til vilkåret om nødvendig rettsgrunnlag.[156] Det er således lagt vekt på å få frem tydelige begrunnelser og utfyllende forklaringer for forslagene.

7. Menneskerettslige utgangspunkter for ransaking og beslag

7.1 Grunnloven §§ 113, jf. 102 og EMK artikkel 8

Ransaking av bopæl, arbeidssted eller person for å skaffe atkomst til datautstyr som kan inneholde bevis; undersøkelser av datasystemer (inkludert skytjenester); sikringen av dataene; den etterfølgende identifiseringen av data som er relevante for saken; og lagring av sikringskopien, er inngrep i retten til privatliv, hjem og kommunikasjon, jf. Grunnloven § 102 og EMK artikkel 8 (1). Vernet er ikke absolutt, men inngrep må oppfylle strenge vilkår for ikke å anses som rettsstridige, jf. Grunnloven § 113 og EMK artikkel 8 (2).

---

[153] Jf. dataetterforskernes syn på dette i punkt 4.3. Se også Eurojust & Europol (2019) *"new cybercrime legislation should strive to be technologically neutral to the extent possible, to avoid the need for regular updates in the future or limiting investigative and prosecutorial possibilities"*, s. 4.
[154] NOU 2016: 24 Ny straffeprosesslov, s. 153.
[155] Riksadvokaten (2017) s. 1-2.
[156] Se neste kapittel punkt 2.

Bestemmelsene lyder:

Grunnloven § 102:

> Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Grunnloven § 113:

> Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov.

EMK artikkel 8:

> Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
>
> Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn (…) for å forebygge uorden og kriminalitet (…).

Det ligger ikke noen realitetsforskjell i at § 102 nevner «kommunikasjon», og artikkel 8 «korrespondanse». Ved innføringen av § 102 som en alminnelig bestemmelse om personvern i 2014, ønsket man å bringe språket mer på linje med dagens, og så også hen til ordlyden i artikkel 7 i EUs Charter om fundamentale rettigheter.[157]

7.2 Hovedpunkter i EMDs praksis om ransaking og beslag

Omfattende rettspraksis fra EMD i relasjon til ransaking og beslag, har utpenslet innholdet i inngrepsvilkårene. Utgangspunktet er at tvangsmidlene anses som *alvorlige inngrep* i retten til privatliv. EMD uttrykker det slik:

> The Court would emphasise that search and seizure represent a serious interference with private life, home and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject.[158]

Mange av sakene i EMDs rettspraksis relatert til EMK artikkel 8, gjelder ransaking og beslag hos advokater, eller hos andre som anfører at materialet inneholder beslagsfrie advokatbetroelser. Sitatet over er fra en slik sak. Også *Wolland mot Norge* (2018) gjaldt ransaking hos advokat, mens *Saber mot Norge* (2020) hadde utspring i en anførsel om at sikrede

[157] Menneskerettighetsutvalget (2012) s. 217 (Lovdata). Charter of fundamental rights of the European Union (2012/C 326/02) artikkel 7: **"**Everyone has the right to respect for his or her private and family life, home and *communications*." (utreders utheving).

[158] *Petri Sallinen og andre mot Finland*, dom 27. september 2005 (saknr. 50882/99), avsnitt 90. Saken gjaldt ransaking og beslag hos advokat.

data inneholdt advokatkommunikasjon. Formuleringen er gjentatt i disse dommene.[159] For advokatkorrespondanse gjelder det således ekstra krav til beskyttelse, klart uttrykt i *Michaud mot Frankrike:*

> …while Article 8 protects the confidentiality of all "correspondence" between individuals, it affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, that is at stake. Indirectly but necessarily dependent thereupon is the right of everyone to a fair trial, including the right of accused persons not to incriminate themselves.[160]

Rettspraksis viser imidlertid at ransaking og beslag anses som avorlige inngrep generelt, ikke bare når beslagsfritt materiale står på spill. Se eksempelvis *Harju mot Finland* (2011).[161] Klager var ikke advokat, og saken reiste heller ikke på annet grunnlag spørsmål om beslagsfrihet. EMD gjentok imidlertid formuleringen fra advokatdommen som gjaldt Sallinen (sitert over), og føyde til at *«safeguards against possible abuse or arbitrariness"* også var nødvendig.[162]

Det generelle utgangspunktet er således at ransaking og beslag anses som alvorlige inngrep i rettighetene nedfelt i EMK artikkel 8. For advokatkorrespondanse, skjerpes vernet. Dette må også gjelde i relasjon til Grunnloven § 102. Det stilles dermed strenge krav til lovgivningen, og til nødvendigheten og proporsjonaliteten i det konkrete tilfellet.[163]

For at inngrepene skal være lovlige må de ha grunnlag i lov, ha et legitimt formål og være nødvendige i et demokratisk samfunn (Grunnloven § 113 og EMK artikkel 8 (2)). Etterforskingsformålet som begrunner tvangsmiddelbruken, omfattes av «å forebygge uorden eller kriminalitet» i artikkel 8 (2). Det er derfor legitimt og drøftes ikke nærmere.[164]

---

[159] *Wolland mot Norge*, dom 17. mai 2018 (saknr. 39731/12) avsnitt 62 i.f.; *Saber mot Norge*, dom 17. desember 2020 (saknr. 459/18) avsnitt 50.
[160] *Michaud mot Frankrike*, dom 6. desember 2012 (saknr. 12323/11), avsnitt 118
[161] *Harju mot Finland*, dom 15. februar 2011 (saknr. 56716/09).
[162] *Harju*, avsnitt 42.
[163] Slik Jan Fridrik Kjølbro (2017), s. 869-875.
[164] Kjølbro (2017), s. 766.

De øvrige vilkårene utdyper EMD slik:

(i) Kravet til rettsgrunnlag («i samsvar med loven») innebærer at inngrepet må ha basis i loven slik den tolkes på inngrepstidspunktet.[165]

Dette har betydning for vurderingen av de norske bestemmelsene om ransaking og beslag. Bestemmelsene er av eldre dato, men Høyesterett har hatt anledning til å tolke dem en rekke ganger de senere årene i forbindelse med ransaking og beslag i data. Dersom hjemmelsgrunnlaget etter en materiell vurdering må anses tilfredsstillende, er vilkåret oppfylt.

(ii) Loven må må være tilgjengelig (*accessible*) og ha forutsigbare konsekvenser for den som berøres, slik at personen kan innrette seg etter den (*foreseeable consequences)*.[166] Innrettelseshensynet fordrer at loven er klar og presis (klarhetskravet).

I norsk rett er dette utlagt som krav til at «loven er så presis som forholdene tillater».[167] Som nevnt er det loven slik den tolkes som vurderes. Klarhetskravet kan tilsi at lovteksten omformuleres eller utdypes, selv om hjemmelskravet strengt tatt er oppfylt. Spørsmålet er i så fall om gjeldende ordyd gir tilstrekkelig veiledning slik at innrettelseshensynet er ivaretatt. I *Saber mot Norge* konkluderte EMD med at straffeprosessloven ikke sørger for tilstrekkelig forutsigbarhet i fremgangsmåten for håndtering av sikrede data, når anførsel om beslagsfrihet fremsettes på inngrepstidspunktet. Tilfellet gjaldt beslag i en smarttelefon og påfølgende sikring av data som blant annet inneholdt advokatkorrespondanse. EMD viste til at den prosessuelle fremgangsmåten i norsk rett er basert på analogibetraktninger fra en bestemmelse (strpl. § 205 tredje ledd) som ikke i utgangspunktet er utformet med tilfellet for øye. Underveis i behandlingen av Sabers data ble fremgangsmåten betydelig lagt om som følge av avsigelsen av HR-2017-111-A som trakk opp nye retningslinjer. Dette viste at loven ikke var tilstrekkelig forutsigbar.[168]

(iii) Loven må oppfylle rettsstatskrav *(rule of law*), og med dette menes at den må inneholde prosessuelle garantier *(«proper legal safeguards»)* mot vilkårlighet og misbruk.[169] Garantiene må sikre effektivt vern om rettighetene nedfelt i artikkel 8, herunder

---

[165] Se for eksempel *Harju* avsnitt 36, med henvisning til den mye refererte dommen *Sociéteé Colas Est og andre mot Frankrike,* dom 16. april 2002 (saknr. 37971/97) avsnitt 43.
[166] *Harju* avsnitt 35.
[167] Rt. 2014 s. 1103 (kommunikasjonskontroll) avsnitt 30; gjentatt i HR-2016-1833-A (adgang til å bruke tvang for å åpne biometrisk lås på smarttelefon), avsnitt 15.
[168] *Saber* avsnitt 55-57.
[169] *Harju,* avsnitt 35 og 39.

> beskyttelsen av opplysninger unntatt fra beslagsadgang. Videre må de sørge for at inngrepet gjennomføres innen rammen satt av ransakingsbeslutningen, og inngi tillit til at bevis ikke kan «plantes» eller ødelegges. Garantiene må sikre god notoritet og effektiv uavhengig kontroll (forutgående og/eller etterfølgende). Rettsstatskravet er et krav til lovens kvalitet, og innebærer at rettssikkerhetsmekanismene *samlet sett* må gi de nødvendige garantier mot misbruk og vilkårlighet. I *Wolland mot Norge* sa EMD således at
>
> > Viewing the system in the Code of Criminal Procedure *as a whole*, the Court considers that the law afforded sufficient legal safeguards as concerned the search, collection and eventually seizure, both with respect to the extents of these measures – the amount of documents collected and copied – and including the protection of legal professional privilege.[170]

Rt. 2013 s. 968 illustrerer lovtolking som ivaretar rettsstats-/kvalitetskravet. Saken gjaldt håndtering av beslagsfritt materiale i en sikringskopi fremstilt etter ransaking og beslag hos en siktet advokat (endelig behandlet av EMD (*Wolland)*). Økokrim hadde først tatt med sikringskopien til tingretten i samsvar med fremgangsmåten foreskrevet i strpl. § 205 tredje ledd analogisk. Tingretten hadde deretter gitt tillatelse til at sikringskopien kunne gjennomgås av en medarbeider i Økokrims IT-avdeling som ikke hadde noe med etterforskingen å gjøre. Medarbeideren hadde undertegnet taushetserklæring. Høyesterett fant at ordningen var uforenlig med strpl. § 205 tredje ledd, idet et system basert på taushetserklæringer ikke kunne være tilstrekkelig, selv om det «ikke [var] grunn til å reise tvil om integriteten» til den aktuelle personen. Muligheten for å bli utsatt for utilbørlig press ble også nevnt som en risiko.[171] Sikringskopien ble følgelig beordret ut av Økokrims besittelse og tilbakeført til tingretten. EMD fant at lovens garantier samlet sett var tilfredsstillende, jf. sitatet over. Garantiene kunne i dette tilfellet ikke leses direkte ut av lovens ordlyd, og ble som det fremgår, etablert ved tolking. Det var tilstrekkelig i forhold til EMK artikkel 8.

(iv) Endelig kreves det at tvangsmidlene er nødvendige og proporsjonale i forhold til etterforskingsformålet, dvs. at inngrepet må fylle «a pressing social need» og være proporsjonalt i forhold til det konkrete formål som skal oppnås.

---

[170] *Wolland* avsnitt 71. Utreders utheving i sitatet.
[171] Kjennelsen avsnitt 39.

For tvangsmiddelbruk i etterforskingen følger vilkårene av strpl. § 170 a:

> Et tvangsmiddel kan brukes bare når det er tilstrekkelig grunn til det. Tvangsmidlet kan ikke brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep.

Kravene er i konteksten av ransaking og beslag i data, utlagt som at inngrepet må være «egnet, nødvendig og forholdsmessig».[172]

7.3 Krav til målrettethet

EMD foretar en nokså inngående prøving av kvaliteten på nasjonal lovgivning i forbindelse med ransaking og beslag. I tillegg kontrolleres de konkrete omstendighetene som begrunner inngrepets nødvendighet og proporsjonalitet. De nevnte vilkårene inngår i et nært samvirke.

Når det gjelder «nødvendig i et demokratisk samfunn» går EMD konkret til verks nærmest i henhold til en sjekkpunktliste.[173] Noen av kriteriene kan være krevende for ransaking og beslag når inngrepene gjelder data. Det gjelder

- Hvorvidt ransakingsbeslutningen var tilstrekkelig klart avgrenset, og grunngitt med hensyn til hvilket informasjonsbehov ransakingen og beslaget skulle oppfylle.[174]
- Hvorvidt gjennomføringen av ransakingen og beslaget konkret var slik innrettet at en eventuell overskridelse av rammene i ransakingsbeslutningen kan utelukkes, og
- Hvorvidt gjennomføringen er tilstrekkelig dokumentert og dermed etterprøvbar.[175]

De nevnte kriteriene sikrer målrettethet. Klare begrunnelser for hvorfor inngrepet anses egnet til å oppfylle etterforskingsformålet, og hvorfor det anses å være nødvendig og proporsjonalt, virker bevisstgjørende og tjener til å sikre målrettethet i gjennomføringen. Begrunnelser som nevnt er også nødvendig for å kunne føre legalitetskontroll med inngrepet. Begrunnelsene må foreligge i forkant, og følgelig være forankret i andre opplysninger (bevis) enn de som politiet antar at kan finnes i dataene som man ønsker å sikre i forbindelse med ransakingen. Begrunnelsene skal selvsagt dokumenteres.

---

[172] Slik HR-2018-104-A avsnitt 23 og HR-2018-699-A avsnitt 32.
[173] Se Kjølbro (2017) s. 869 de to nederste avsnitt.
[174] *Van Rossem mot Belgia*, dom 9. desember 2004 (saknr. 41872/98) avsnitt 45 er grunnleggende. Dommen er på fransk og gjengis av EMD for eksempel som i *Iliya Stefanov mot Bulgaria*, dom 22. Mai 2008 (saknr. 65755/01) avsnitt 41 *"According to the Court's case-law, search warrants have to be drafted, as far as practicable, in a manner calculated to keep their impact within reasonable bounds"*. Sml. *Kolesnichenko mot Russland*, dom 9. april 2009 (saknr. 19856/04) avsnitt 35.
[175] Øvrige kriterier, f.eks. om ranskingsbeslutningen var mistankebasert, om den var utferdiget av kompetent myndighet osv., reiser ikke spesielle spørsmål som følge av at inngrepene gjelder data.

Dokumentasjonen skal også gi grunnlag for å kunne kontrollere hvorvidt bevissikringen og analysen konkret var innrettet mot mistanken uttrykt i ransakingsbeslutningen, og var avpasset begrunnelsen for inngrepet. Dokumentasjonen skal vitne om hvorvidt gjennomføringen var tilstrekkelig målrettet, og ikke bar preg av «fisketur».

Kravet til målrettethet bør drøftes i forhold til praksisen med å sikre store datamengder, som skjer både ved speilkopiering og *live* sikring. Det kan reises spørsmål om praksisen er for lite målrettet og derfor uproporsjonal, se utredningen kapittel 19.1.

Målrettethet bør også drøftes i forhold til analysen, som utredningen kommer tilbake til i kapittel 14. Det finnes indikasjoner på at fremgangsmåten for analyse ikke nødvendigvis skjer planmessig og målrettet, og at dokumentasjonen kan være mangelfull. Samtidig er det viktig at målrettethet ikke går på bekostning av kravet til objektivitet i etterforskingen.[176] Mangler i forhold til hvert av disse vilkårene kan lede til at inngrepet anses uproporsjonalt.

Ytterligere bør målrettethet drøftes i forhold til ransaking av datasystemer *før* innholdet er sikret, jf. usikkerhetsmomentene som er beskrevet i punkt 5.7.2. Formål, begrunnelse og gjennomføring bør dokumenteres. Dette er fulgt opp i utredningen kapittel 10.

Loven kan bygges ut med retningslinjer som sikrer målrettethet, objektivitet og etterprøvbarhet, noe som vil bidra til å styrke rettsgrunnlagets kvalitet. Vilkår som nevnt følger allerede generelt av straffeprosessloven hvoretter etterforsking anses som en formålsstyrt aktivitet,[177] som skal skje objektivt,[178] og dokumenteres.[179] For databevis kan det likevel være behov for tydeliggjøring og presisering, særlig fordi situasjonen jevnlig gjelder håndtering av store datamengder, og man på forhånd vet lite om innhold og sammensetning av de sikrede dataene. Det skaper utfordringer for målrettetheten på alle stadier i dataetterforskingsprosessen. Databevis atskiller seg i dette fra de fleste andre typer spor, og kan fordre tydeligere veiledning fra lovgivers side om rettslige rammer og plikter. Lignende hensyn gjør seg gjeldende for undersøkelser av ubeskyttede originale data, som dermed påføres politiskapte endringer. Bedre lovmessig kvalitet tilrettelegger for bedre gjennomføringskvalitet, noe som er positivt for proporsjonalitetstesten.

---

[176] Se punkt 4.2 og kapittel 14.
[177] Dette følger av strpl. §§ 226, jf. 224, og er presisert i Riksadvokatens rundskriv (1999) og (2018) pkt. 4.2.
[178] Strpl. §§ 226 tredje ledd og 55 a siste ledd; Riksadvokaten (2018) pkt. 4.7.
[179] Dokumentasjonskravet følger av strpl. § 199 annet ledd (ransaking), og for beslag av § 205 første ledd annet punktum, § 207 og påtaleinstruksen § 9-5. Kravene er utdypet i Riksadvokaten (2018) pkt. 4.5.2 og 4.11.

Del IV. Fase én: Ransaking og sikring av data

8. Problemstilling og gjeldende rett

8.1 Problemstilling

Mandatet ber vurdert om

> det gjeldende beslagsbegrepet er treffende for databeslag. I den forbindelse bør utreder gå nærmere inn på grensedragningen mellom ransaking og beslag i data.[180]

De rettslige problemstillingene kan henføres til to forskjellige faser i bevishåndteringen. I denne del IV drøftes spørsmålet reist i mandatet slik det gjør seg gjeldende i den første fasen. Fasen anses å omfatte undersøkelser av ubeskyttede originale data i en databærer, sikring av data i forbindelse med ransaking, og hemmelig ransaking av databærer. Spørsmålene gjelder om inngrepene har tilstrekkelig rettsgrunnlag og om de prosessuelle garantiene er tilstrekkelige.

Innledningsvis reises det grunnleggende spørsmålet om hvorvidt «oppbevaringssted» i strpl. § 192 er tilstrekkelig rettsgrunnlag *de lege ferenda* for ransaking etter databevis.

Behandlingen av beslagsfrie opplysninger som politiet kommer over etter at dataene er sikret, er ikke tema i denne første fasen. Adgangen til å sikre data på advokatkontor er behandlet i del VI sammen med de øvrige spørsmålene som beslagsforbudet reiser, se punkt 17.6.

8.2 Gjeldende rett

8.2.1 Undersøkelse av et datasystem – ransakingens første fase

Straffeprosessloven § 192 gir adgang til å foreta undersøkelser av datasystemer og skytjenester for å søke etter bevis. Bestemmelsens første ledd lyder:

> Når noen med skjellig grunn mistenkes for en handling som etter loven kan medføre frihetsstraff, kan det foretas ransaking av hans bolig, rom eller oppbevaringssted, for å sette i verk pågripelse eller for å søke etter bevis eller etter ting som kan beslaglegges eller som det kan tas heftelse i.

[180] Mandatet punkt 2.

Høyesterett har lagt til grunn at «oppbevaringssted» i strpl. § 192 første ledd «kan omfatte et datanettverk, herunder en server som befinner seg utlandet.»[181] Dette omfatter også skytjenester. Lovforståelsen ble ansett å være helt klar.[182]

8.2.2 Sikring og beslag i data

Ting som antas å ha betydning som bevis kan beslaglegges, jf. strpl. § 203.[183] Etter gjeldende rett anses ikke kopieringen av data som beslag, men som et ledd i en handlingsrekke som kan lede til beslag. Dette er lagt til grunn i rettspraksis over en årrekke, sist oppsummert og presisert i HR-2018-1901-U.[184]

8.2.3 Fortsatt ransaking – ransakingens andre fase

Undersøkelser av sikringskopien anses som en fortsettelse *av den ransakingen som opprinnelig ga tilgang* til datautstyret eller skytjenesten, slik at dataene kunne kopieres. Beslag inntreffer først når etterforskeren identifiserer data som antas å ha betydning som bevis, jf. strpl. § 203, *og* en beslutning om å beslaglegge disse dataene er truffet, jf. strpl. § 205 første ledd. Fra dette tidspunkt inngår dataene i sakens dokumenter og blir gjenstand for dokumentinnsyn, jf. strpl. § 242. Da inntrer også retten til å få prøvet beslaget for retten, jf. strpl. § 208, se HR-2018-1901-U avsnitt 16-19. Overprøvingsadgangen gjelder kun de utplukkede dataene. Saken reiste ikke spørsmål om beskyttelse av beslagsfritt materiale, og stadfester følgelig den alminnelige prosessuelle ordningen for sikring av databevis, beslag og innlemmelse i saksdokumentene.

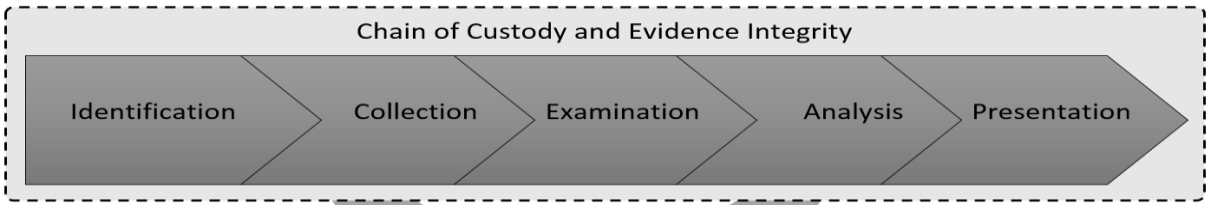
Rettspraksis har også avgjort at forsvareren ikke har rett til å uttale seg om hvordan den fortsatte ransakingen bør innrettes, se HR-2018-1517-U (tingrettens forhåndskontroll av data sikret hos advokat) og HR-2018-1901-U nevnt over. Grunnen er at det er påtalemyndigheten som har primærkompetansen til å beslutte beslag, og som har hovedansvaret for å tilveiebringe bevis til saken. Ordningen ble gjenstand for prøving av EMD i *Mirmotahari mot Norge*. EMD fant ikke noen krenkelse av EMK 8, og avviste klagen som «manifestly illfounded».[185]

---

[181] HR-2019-610-A, avsnitt 27.
[182] *Ibid*.
[183] Rt. 2011 s. 296 «Det er ikke tvilsomt at datamateriale omfattes av [«ting» i § 203]» (avsnitt 23).
[184] HR-2018-1901-U avsnitt 16; HR-2018-1517-U avsnitt 30; HR-2018-699-A avsnitt 29; Rt. 2011 s. 296 avsnitt 40.
[185] *Mirmotahari mot Norge.*Avvisningsbeslutning 8. oktober 2019 (saknr. 30149/19).

Rettstilstanden kan illustreres slik:

Figur 2:



Flaglien (2018)

Fysisk ransaking - Sikring av data

↓

Fortsatt ransaking: Klargjøring og analyse

↓

Relevante data: **Beslag / Sakens dokumenter**

Politiets besittelse av sikringskopien kan ikke overprøves i medhold av strpl. § 208.[186] I *Wolland* anførte klageren at hans rett etter EMK artikkel 8 var krenket fordi loven ikke ga adgang til å overprøve påtalemyndighetens besittelse av sikringskopien i analysefasen, noe som fratok ham muligheten for å gjendrive at det var skjellig grunn til mistanke mot ham. EMD var ikke enig, og viste til at artikkel 8 ikke etablerer en generell rett for mistenkte til prosessuelt å kunne angripe spørsmålet om skjellig grunn til mistanke, selv ikke ved inngrep som ransaking og beslag.[187] EMK artikkel 8 var ikke krenket selv om overprøvingsretten først inntrådte etter at filer var plukket og tatt i beslag.

Loven gir imidlertid adgang til å anke over ransakingen såfremt politiet har tatt med seg materiale som skal være gjenstand for fortsatt ransaking. Da har den som utsettes for ransaking en klar interesse i å motsette seg «den gjennomgang av dokumentene som er nødvendig for å ta stilling til beslagsspørsmålet» (Rt. 1996 s. 1081).[188] Uttalelsen falt i en sak som gjaldt ransaking hos advokat, hvor dokumenter var tatt med til tingretten, jf. strpl. § 205. Men ankeadgangen må gjelde i ethvert tilfelle hvor ransakingen fortsetter etter at politiet har sikret seg materialet, dvs. i alle tilfeller med materiale av noe omfang. Det er følgelig adgang til å anke over ransaking som har resultert i sikring av data. For så vidt gjelder valg av

[186] Rt. 2013 s. 968 og *Wolland*.
[187] *Wolland* avsnitt 72.
[188] Keiserud m.fl. (2020) s.770 note 7.

sikringsmetode har politiet stor frihet. Dette anses nødevdnig i lys av det strenge beviskravet i straffeprosessen.[189] Det er eventuelt krav til nødvendighet og proporsjonalitet som setter begrensninger for fremgangsmåten, se strpl. § 170 a og Rt. 2012 s. 1645.

8.2.4 Ransakingsbeslutningen – en prosessuell garanti for målrettethet

Ransakingsbeslutningen som ligger til grunn for iverksettelsen, er som forklart i punkt 7.3, en viktig prosessuell garanti for målrettethet. Beslutningen, som baserer seg på siktelsen, angir ransakingens ytre rammer, ikke bare ved iverksettelsen, men i hele prosessen, dvs. også mens dataene sikres og analyseres.

Rettspraksis har avklart at det ikke er nødvendig med nye ransakingsbeslutninger for å foreta gjentatte undersøkelser av sikringskopien. Det avgjørende er at undersøkelsene dekkes av den opprinnelige ransakingsbeslutningens angivelse av formålet, og hva som kan ransakes (ransakingssted/-objekt), jf. § 197 tredje ledd og HR-2018-699-A, avsnitt 29.[190]

Politiet har ikke adgang til å søke etter bevis for et annet straffbart forhold enn angitt i ransakingsbeslutningen.[191] Det er f.eks. ikke adgang til å foreta rutinemessig teknisk analyse for å avdekke overgrepsmateriale, utelukkende fordi sjekksumlister over kjente ulovlige filer gjør det mulig.[192]

Hvis mistankegrunnlaget utvides på grunn av nye opplysninger, må ny ransakingstillatelse basert på en utvidet siktelse innhentes, for å undersøke sikringskopien. De vanlige vilkårene etter strpl. § 192 gjelder, dvs. skjellig grunn til mistanke (sannsynlighetsovervekt) om en straffbar handling som oppfyller strafferammekravet. Videre må det være en mulighet for at bevis kan finnes i sikringskopien.[193] For å utelukke muligheten for at politiet har vært på «fisketur» i de sikrede dataene, bør ransakingsbegjæringen vise at den nye mistanken bygger på andre opplysninger enn slike som finnes i sikringskopien.

Dette utelukker ikke at politiet kan bruke opplysninger om andre straffbare forhold som *tilfeldig* avdekkes i sikringskopien. «Tilfeldighetsfunn» om andre straffbare forhold kan inntreffe i en ordinær undersøkelse som lojalt er innrettet på å finne bevis om forhold som omfattes av ransakingsbeslutningen. Tilfeldighetsfunn kan brukes videre i etterforskingen, men dersom det

[189] Rt. 2012 s. 1645; Rt. 2013 s. 968.
[190] I samme retning riksadvokatens brev til Politihøgskolen 21. april 2020 om ransaking og beslag i mobiltelefon.
[191] Se nærmere om formålets betydning som ramme for ransaking og beslag i Riksadvokaten (2021).
[192] Sjekksumanalyse er en type teknisk analyse, se punkt 5.4.4.1.
[193] Slik Keiserud m.fl. (2020) note 5 til § 192, s. 772.

er behov for å foreta flere undersøkelser av sikringskopien for å følge dem opp, må ny ransakingsbegjæring innhentes.[194] Tilfeldighetsfunn er for eksempel ikke å regne som «ferske spor» som gir etterforskeren adgang til å beslutte ransaking, jf. strpl. § 198 første ledd nr. 2. Det sier seg selv at notoritet er særdeles viktig for å kunne dokumentere hvorvidt man har med tilfeldighetsfunn å gjøre, og om analysen skjer innenfor ransakingsbeslutningens rammer.

Riksadvokaten understreker ransakingsbeslutningens betydning som garanti for at ransakingen iverksettes med et relevant etterforskingsformål for øye, og innrettes slik at den ikke går ut over det som er nødvendig og forholdsmessig i lys av siktelsen. Kravet er at ransakingsbeslutningen spesifiseres på en måte som sikrer at ransakingen gjennomføres slik at den *utelukkende* retter seg mot det lovbrudd som etterforskes.[195] Korresponderende krav følger av EMK artikkel 8, jf. EMDs Jurisconsult, gjengitt av riksadvokaten:

> "The Court considers that a search warrant has to be accompanied by certain limitations, so that the interference which it authorises is not potentially unlimited and therefore disproportionate. The wording of the warrant must specify its scope (in order to ensure that the search concentrates solely on the offences under investigation) and the criteria for its enforcement (to facilitate scrutiny of the extent of the operations). A broadly worded warrant lacking information on the investigation in question or the items to be seized fails to strike a fair balance between the rights of the parties involved because of the wide powers which it confers on the investigators (Van Rossem v. Belgium, §§ 44-50 with further references therein; Bagiyeva v. Ukraine, § 52)."[196]

Kravet om streng formålsstyring setter rigide rammer for analyse av store datamengder. Metodene må nøye innrettes i forhold til siktelsen og sakens informasjonsbehov i lys av hypotesene (se nærmere om dette i kapittel 14).

Kravet til målrettethet synes over tid å ha blitt skjerpet. I *Jahres* artikkel fra 1990 om fremgangsmåten ved beslagsfrihet, forutsettes det at politiet har adgang til «generelt innsyn» i dokumenter sikret i forbindelse med ransaking. Dette kobles til at politiet ofte har mistanke «også om andre straffbare forhold, men bevisene for disse er ikke gode nok til å forsvare en siktelse».[197] Implisitt gjaldt det den gang, adgang til å undersøke dokumentene for å få en mistanke be-/avkreftet, selv om mistanken ikke gjaldt forhold som var omfattet av siktelsen.

---

[194] Riksadvokaten (2021) pkt. 2.
[195] *Ibid.*, s. 5. Utreders utheving.
[196] Guide on Article 8 of the European Convention on Human Rights avsnitt 438, oppdatert 31. august 2020, tilgjengelig på https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Riksadvokaten (2021) s. 5.
[197] *Hans-Petter Jahre* (1990) pkt. 3.4.2.1, s. 11-12 (Lovdata).

Slik er neppe gjeldende rett å forstå. Ved analyse av sikrede data kan dessuten tekniske kontrollfunksjoner som dokumenterer hvorvidt politiets undersøkelser ligger innenfor siktelsen, benyttes. Ransaking i sikrede data kan dokumenteres på en mye grundigere og sikrere måte enn ransaking i papirdokumenter. Det forutsetter selvsagt at politiet er utstyrt med hensiktsmessig teknologi.

Siktelsens store betydning for avgrensningen og formålsstyringen av ransakingen, tilsier at utformingen skjer etter grundige overveielser. Kravene som stilles til konkretisering av siktelsen vil ha stor betydning for bevistilgangen. Blir kravene for strenge, risikerer man som påpekt av *Jahre*, at viktige bevis kan gå tapt.[198]

Ransakingsbeslutningen gir som nevnt den ytre rammen for dataetterforskingsprosessen som følges i saken. I tillegg gjelder det krav som ytterligere skal sikre målrettethet, objektivitet og kvalitet i analysen. Disse behandles i kapittel 14.

9. Ransaking av databærer

9.1 Rettsgrunnlaget for ransaking av databærer, jf. strpl. § 192

Det er sikker rett at «oppbevaringssted» i strpl. § 192 omfatter databærere.[199] Det formelle hjemmelsgrunnlaget for ransaking av databærer er derfor tilstede. Generelt å karakterisere et datasystem som et «oppbevaringssted» er imidlertid lite treffende, og tolkingen har mer preg av nødløsning enn å være en robust ordning. Situasjonen kan sammenlignes med den i Rt. 2011 s. 1188 hvor førstvoterende sa:

> Paragrafen ble skrevet og vedtatt i en tid da tradisjonelle dokumenter fremdeles nærmest var enerådende, og lovgiver har ganske sikkert ikke hatt nåtidens forhold i tankene – hvor elektroniske dokumenter er blitt dominerende, og der selv små mobile databærere har enorm lagringskapasitet. Etter min mening åpner dette for å legge betydelig vekt på reelle hensyn ved tolkningen; ikke minst bør de hensyn som ligger bak [bestemmelsen], trekkes inn.[200]

Den nevnte saken gjaldt tolkingen av strpl. § 264 første ledd første punktum (innsynsrett etter at tiltale er tatt ut), men sitatet er talende for det store behovet for aktiv rettsutvikling fra Høyesteretts side på dette området, også ved ransaking og beslag i data.

---

[198] *Ibid.*, s. 11 (Lovdata).
[199] Se punkt 8.1.2.
[200] Kjennelsen avsnitt 38.

En naturlig språklig forståelse av «oppbevaringssted» at det er tale om et slags lager for noe som for øyeblikket ikke er i bruk. Et fysisk dokumentarkiv kan være et oppbevaringssted, så vel som et lagerlokale, et garderobeskap eller en sikkerhetsboks osv. Det typiske for et datasystem er imidlertid at dataene er i bruk, de behandles automatisk av datasystemet. «Oppbevaringssted» er lite treffende for å betegne dette.

Foruten å behandle, så lagrer datasystemer dataene, og kan i den forstand anses som et oppbevaringssted. Dataene skal imidlertid være tilgjengelige når det er behov for det, og lagringen er en beredskap for behandling.[201] Det kan derfor være tilrådelig å bygge ut bestemmelsen til også å omfatte «datasystem» eller «databærer». «Datasystem» brukes allerede i strpl. § 199 a og § 216 o og p, og har en fastlagt betydning, jf. datakrimkonvensjonen artikkel 1 bokstav a. Her defineres datasystem som

> enhver innretning eller gruppe innretninger som er koplet sammen eller som hører sammen, hvorav en eller flere utfører programmert automatisk behandling av data.

Noen hensyn taler imidlertid mot bruk av begrepet. For det første er «datasystem» vanskelig å avgrense, dvs. at selv om det lar seg beskrive, kan det være vanskelig å avgrense rent faktisk. Det er følgelig ikke spesielt velegnet for å oppfylle krav til rettslig presisjon hva gjelder angivelse av ransakingssted. Ransakingsobjektet bør angis presist, enten ved fysisk stedsangivelse, eller ved å angi bestemte tjenester og datatilganger, dvs. brukerkonti. For det andre vil «datasystem» måtte avgrenses i forhold til «oppbevaringssted». Det sistnevnte alternativet bør uansett beholdes i strpl. § 192, fordi det er nødvendig med tanke på fysiske oppbevaringssteder.

En annen mulighet er å gå inn for ordet «databærer», som ikke byr på disse problemene. Motforestillingen er at ordet «databærer» (en oversettelse av det engelske *«data carrier»*) - til forskjell fra «oppbevaringssted» og «datasystem» - neppe kan sies å ha gått inn i dagligspråket og kan anses som lite veiledende. Innvendingen har likevel mindre vekt i lys av at

[201] Tilgjengelighet er et kriterium for informasjonssikkerhet, ved siden av integritet og konfidensialitet, se f.eks. politiregisterloven § 15 første ledd som pålegger plikt til å sørge for tilfredsstillende informasjonssikkerhet med hensyn til «konfidensialitet, integritet og tilgjengelighet» ved behandling av opplysninger. Se også politiregisterforskriften § 40-11 *Sikring av tilgjengelighet.* FOR-2013-09-20-1097.

rettsanvenderne har blitt fortrolige med begrepet. Det har gått inn i rettsspråket med en festnet betydning siden Høyesteretts bruk første gang i 2011.[202]

Alternativene utdypes i det følgende.

9.1.1 «Datasystem»

«Datasystem» vil omfatte en stor og uensartet gruppe innretninger. Bærbare datamaskiner, datasystemer i private og offentlige foretak, nettbrett og smarttelefoner er ganske åpenbart å regne som datasystemer. Det samme gjelder skytjenester, f.eks. epostserver, dokument- og bildebehandlingstjenester, eller eksterne regnskaps- og administrasjonssystemer.

Det er å merke seg at datakrimkonvensjonens definisjon av «datasystem» også nevner «gruppe innretninger som er koplet sammen eller som hører sammen». En lokal datamaskin utnytter en skytjeneste gjennom en forbindelse (sammenkobling), og når forbindelsen er opprettet kan brukerkontoen i skyen anses som en del av brukerens datasystem. Smarttelefonens integrasjon med skytjenesten er et meget praktisk eksempel på dette.[203] Tilsvarende vil gjelde en skytjeneste som ransakes ved bruk av politiets eget datautstyr; brukerkontoen kobles dermed til politiets datasystem.

«Datasystem» vil imidlertid omfatte mer enn dette, og ettersom digitaliseringen utvikler seg er det sannsynlig at «datasystemer» vil finnes i kontekster vi foreløpig ikke er fortrolige med. Eksempler på datasystem som er utbredte i dag er «smarte» innretninger som treningsarmbånd, multifunksjonelle «klokker» og stemmestyrte assistenter. Videre har vi datasystemer i avanserte biler, med stemmestyring og en rekke funksjoner for overvåking, varsling og hendelsesregistrering.[204] Elektroniske system for adgangskontroll til en bygning, og elektronisk bompassering, er også datasystemer.

Typisk for smart teknologi er sammenkoblingen av forskjellige elementer som «snakker sammen» over internett og blåtann («*bluetooth*»), og smart teknologi kan langt på vei forstås synonymt med «Tingenes internett» («*Internet of Things*»). Teknologien sammenkobler sensorer (registreringsenheter) som sørger for datainput til et datasystem som behandler (prosesserer) dem. Dette gir et resultat, f.eks. opplysning om at man har nådd et treningsmål,

---

[202] Avansert søk i Lovdata på «databær*» ga 9 treff på Høyesteretts straffesaker, hvorav en sak inneholdt «databærer» i et sitat fra regelverket for varemerkeregistrering (HR-2019-2213-A). De andre sakene er HR-2019-610-A; 2018-1901-U; 2018-1517-U; 2018-699-A; 2016-846-U; Rt. 2013 s. 968; 2012 s. 1645 og 2011 s. 1188.
[203] Se kapittel 3.2.
[204] Datasystemer i biler er beskrevet i *Prosjekt Cartech-Hovedrapport.* PWC & Statens Vegvesen (2020).

må regulere sukkernivået i blodet, at en person har vært på et bestemt sted på et bestemt tidspunkt (GPS-teknologi), at luftfuktigheten er for lav eller elektrisitetsforbruket for høyt, at en person har rett til å komme inn i en bygning, at bremsesystemet på en bil slår inn automatisk osv. osv.

Stadig økende konnektivitet gjør det vanskeligere å bestemme hva som faktisk er å anse som ett og samme datasystem. Om begrepet likevel benyttes i strpl. § 192, må det klart fremgå av strpl. § 197 at ransakingsbeslutningen tydelig og konkret må spesifisere ransakingsobjektet innenfor alternativet «datasystem».

9.1.2 «Oppbevaringssted» vs. «datasystem»

Dersom strpl. § 192 suppleres med «datasystem» vil «oppbevaringssted» likevel ha selvstendig betydning for databærere som er frakoblet datasystemet. Slike i seg selv, har ikke den nødvendige behandlingsfunksjonen for å anses som «datasystem», jf. datakrimkonvensjonens definisjon «utfører programmert automatisk behandling av data.»

Noen sporsteder som må regnes som «oppbevaringssted» for data, har politiet lenge vært fortrolig med, f.eks. minnepinner, minnekort, harddisker og DVD-plater. Sensorene som inngår i «Tingenes internett» kan også være oppbevaringssted. Formidling av data fra en sensor til datasystemets behandlingsfunksjon (prosessoren), skjer som nevnt over datanettverk. For at teknologien skal anses å være «smart» bør funksjonen utføres i sann tid, dvs. at resultatet (*outputen*) leveres så snart datasystemet mottar data*inputen*. En sensor kan imidlertid ha lagringsfunksjon i tillegg til at den sender data til prosessoren, noe som gjør den relevant som sporsted i seg selv. Sensorer med lagringsenheter antas å bli stadig viktigere som sporsteder som følge av digitaliseringen, blant annet fordi nettverksutbredelsen risikoen for dataangrep øker som følge av at antallet angrepsinnganger *(«attack vectors»)* øker.[205]

9.1.3 «Databærer» vs. «datasystem»

Det enkleste er å bruke ordet «databærer» og la det fullt ut overta som rettsgrunnlag for å søke etter databevis i stedet for «oppbevaringssted». «Oppbevaringssted» må i så fall tolkes snevrere enn i dag, dvs. til å gjelde andre bevis enn databevis.

«Databærer» vil omfatte datasystemer (inkludert skytjenester), brukerkonti og frakoblede lagringsmedier. En supplering av § 192 med «databærer» vil derfor være tilstrekkelig for å gi

[205] Servida & Casey (2019); Europol (2019) pkt. 4.5, s. 14.

et tydelig rettsgrunnlag for å søke etter data som bevis. Av pedagogiske hensyn bør «databærer» antakelig suppleres med «brukerkontoer», sml. strpl. § 216 o fjerde avsnitt første punktum, som spesifiserer objektet for dataavlesing, nemlig «bestemte [databærere] eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller antas å ville bruke.» Formuleringen i § 216 o synes å være vel omstendelig, og det antas å være tilstrekkelig at strpl. § 192 nevner «databærer eller brukerkontoer».

«Databærer» har en generell og vid betydning, noe som gjøre det unødvendig også å innføre ordet «datasystem». Samtidig er «databærer eller brukerkontoer» egnet for konkretisering i en ransakingsbeslutning, gjennom stedsangivelse (f.eks. «databærere fysisk lokalisert på adresse X») og brukerrettigheter (f.eks. «brukerkonto disponert av NN»).

Begrepet «databærer» i strpl. § 192 vil ha en snevrere betydning enn «informasjonsbærer» som brukes i straffelovens inndragningsbestemmelser. Med «informasjonsbærer» forstår straffeloven «trykt skrift eller annet som formidler en skriftlig, visuell, auditiv eller elektronisk lagret informasjon», se strl. § 76 første ledd.[206] «Trykt skrift» omfatter informasjon som foreligger på papir, noe «databærer» ikke gjør. Mens en databærer alltid vil være en informasjonsbærer, er det omvendte ikke nødvendigvis tilfelle.

9.2 Gjennomføring av ransakingen

Teknologiutviklingen innebærer at det kan finnes flere mulige innganger for ransaking av den samme databæreren eller brukerkontoen. Utviklingen innebærer også at de samme dataene kan befinne seg forskjellige steder. Dersom det ikke lar seg gjøre å få tilgang til et håndsett, kan det likevel være mulig å sikre de samme dataene fra en korresponderende tjeneste i skyen. Dette ble forklart i punkt 3.2.6 og 3.2.7. Dessuten kan ransakingen rent teknisk skje direkte fra politiets egne lokaler.

Situasjonen åpner for flere valgmuligheter når det gjelder gjennomføringen, og spørsmålet er om loven burde sette mer presise rammer. Blant hensynene som gjør seg gjeldende kan for det første nevnes, betydningen av å ha visshet om at det faktisk er siktedes (eller en identifisert tredjepersons) databærer eller brukerkonto som ransakes. Dette er i utgangspunktet ivaretatt gjennom den foreslåtte endringen av strpl. § 192, som sammenholdt med strpl. § 197 nødvendiggjør spesifikasjon av databærere og brukerkontoer. Det bør ikke ha betydning om disse formelt er registrert på en annen, f.eks. arbeidsgiver, men at de faktisk disponeres av

[206] Lov om straff av 20. mai 2005 nr. 28 (straffeloven).

siktede. I tillegg vil siktedes tilstedeværelse – eller dennes representant - være en garanti mot at politiet ransaker feil objekt. Siktede skal som hovedregel være tilstede ved ransaking av bolig eller rom, jf. strpl. § 200 annet ledd. Alternativet er at et vitne er tilstede, som bestemt i strpl. § 199, og § 200 annet ledd. Dette bør gjelde tilsvarende ved ransking av databærer eller brukerkonto.

Ransaking og sikring av data er potensielt svært invaderende (se kapittel 10, 11 og 19.1), noe som taler for å ha god kontroll med politiets fremgangsmåte. Ved ransaking av skytjenester må kontroll med gjennomføringen antas å være helt nødvendig, siden dette kan foregå uten at verken siktede eller et vitne er tilstede, med mindre det godtas at en politikollega er vitne. I realiteten er ransaking av brukerkonto uten siktedes eller et vitnes tilstedeværelse, hemmelig ransaking og skal følge reglene for dette (se kapittel 12).

Det kan imidlertid være situasjoner hvor verken siktede eller dennes representant er tilgjengelig, f.eks. fordi de er i utlandet. Vansker med å få fatt i siktede bør ikke være til hinder for etterforskingen, så brukerkontoen bør likevel kunne ransakes. Det er imidlertid betimelig å oppstille noen kvalifiserende vilkår, dvs. at det er strengt nødvendig og etterforskingen ellers vil bli vesentlig skadelidende. Siden en brukerkonto vil være beskyttet, må politiet kunne begå datainnbrudd for at ransakingsadgangen skal være effektiv. Dette kan f.eks. innføres med en formulering tilsvarende den som finnes i strpl. § 216 p første ledd tredje punktum: «Politiet kan bryte eller omgå beskyttelse i [databæreren eller brukerkontoen] dersom det er nødvendig for å kunne gjennomføre [ransakingen].» Adgangen til å ransake etter denne bestemmelsen bør som utgangspunkt omfattes av ransakingsbeslutningen. Hvis problemet med å få fatt i siktede først oppstår etter at ransakingsbeslutning fra retten er innhentet, bør det skje en ekstra kontroll med at vilkårene er oppfylt, gjennom påtalemyndighetens beslutning. For at ransakingen ikke skal anses å være hemmelig, og omfattes av vilkårene som gjelder for dette, må det - såfremt det lar seg gjøre - samtidig gå en underretning til siktede, og notoriteten må være god.

9.3 Konklusjon – forslag

Straffeprosessloven § 192

Utredningen foreslår at strpl. § 192 suppleres med «databærer eller brukerkontoer».

Nytt tredje ledd i straffeprosessloven § 200

Det foreslå at strpl. § 200 suppleres med et nytt tredje ledd om ransaking av databærer eller brukerkonto. Bestemmelsen foreslås å gi hjemmel for å kunne begå datainnbrudd.

10. Undersøkelse av originale data

Kapitlet gjelder den rettslige reguleringen av adgangen til å undersøke originale data. Spørsmålet er om lovens ordning er tilfredsstillende gitt at slike undersøkelser regelmessig påfører dataene endringer. Dette bryter med integritetsprinsippet, se punkt 5.2. Problemstillingen er praktisk blant annet fordi politipatruljen hyppig foretar undersøkelser av smarttelefoner ved etterforsking «på stedet».[207] Ransaking av smarttelefon har også blitt belyst i relasjon til narkotikalovbrudd i rusreformdebatten våren 2021. Reguleringsspørsmålet gjelder imidlertid ransaking av databærere generelt.

10.1 Beslag og samtykke som inngrepsgrunnlag

Tilgang til en bærbar databærer, som en smarttelefon, uten forutgående ransaking, forutsetter beslag eller samtykke, jf. strpl. §§ 203 og 205 første ledd, og da må vilkårene som følger av disse bestemmelsene være oppfylt. Etter § 203 forutsetter beslag skjellig grunn til mistanke om en straffbar handling.[208] I tillegg kreves rimelig grunn til å anta at innsyn i smarttelefonen er egnet til å gi bevis som er relevante for mistanken.

Et samtykke skal være frivillig. Siktede vil være i en presset situasjon og har vern mot selvinkriminering. Det utelukker regelmessig at politiet kan basere seg på samtykket, og kan følgelig ikke «låne» siktedes smarttelefon for et raskt gjennomsyn.

Det kan også være behov for innsyn i fornærmedes eller vitnets smarttelefon. Da er muligheten for å kunne basere seg på samtykke større, men et samtykke skal også være *informert*, og spørsmålet er hva dette betyr i relasjon til beslag og ransaking av smarttelefon.

I England har det vært offentlig debatt om politiets undersøkelser av smarttelefoner. Siden en smarttelefon nærmest inneholder «hele livet» til den det gjelder, regnes undersøkelsen som spesielt invaderende. Særlig fra personer med fornærmet/vitnestatus har undersøkelser registrert svekket tillit relatert til slike undersøkelser. Tillitssvikten er særlig uttalt i voldtektssaker, hvor fornærmede ikke er forberedt på at politiets gjennomsyn kan farge synet på offerets moral. Men det gjelder også ellers.

[207] Andreassen & Andresen (2019).
[208] Keiserud m.fl. (2020) s. 807, note 10 til § 203.

Kritikken gjelder særlig tre forhold:

- For det første at personen blir dårlig informert om hva undersøkelsen omfatter. Fornærmede/vitnet tror f.eks. at politiet bare skal gjennomgå tekstmeldingene, og krenkes av at også bildegalleriet ble undersøkt.
- For det andre at formålet med undersøkelsen fremstår som uklar.
- For det tredje at gjennomsynet ikke legges opp målrettet i forhold til det som antas å være relevant, men tilsynelatende gjelder alt som er tilgjengelig på eller via smarttelefonen.[209]

På denne bakgrunn er det tatt til orde for «a wider review» av fremgangsmåten ved undersøkelser av smarttelefon.[210]

Det kan ikke utelukkes at disse betenkelighetene også gjør seg gjeldende for undersøkelser utført av norsk politi, *Andreassens & Andresens* undersøkelse tyder i hvert fall på dette.[211] Det foreslås følgelig retningslinjer om informasjonsplikt, herunder hvilken informasjon som er nødvendig for å anse samtykke til beslag for å ransake en smarttelefon for å være informert. Samtykke må være avgitt av kompetent person, noe som blant annet er en problemstilling i forhold til mindreårige og voksne rusbrukere. Også for dette kan det være behov for retningslinjer.

10.2 Ransaking vs. gransking

Undersøkelse av innholdet i en smarttelefon er ikke å anse som gransking av et beslaglagt objekt, men som et selvstendig nytt inngrep i form av ransaking.[212] *Gransking* av beslaglagt smarttelefon må begrense seg til å gjelde eksteriøret inkludert skjermbildet, uten at politiet utløser funksjoner på objektet.

I tillegg er ransakingsbeslutning nødvendig, i medhold av strpl. §§ 197 eller 198. Av beslutningen må det fremgå at undersøkelsen anses egnet til å oppfylle etterforskingsformålet. Egnetheten må baseres på opplysninger som foreligger før databæreren ransakes. Det vises til EMDs krav til målrettethet, og riksadvokatens utdyping av vilkåret om at ransakingen må ha et

[209] Punkt 3.2 beskriver det store potensielle informasjonstilfanget, og proporsjonalitetsvilkåret i relasjon til slike undersøkelser problematiseres i punkt 19.1.
[210] UK Law Commission (2020) pkt. 18.8.
[211] Andreassen & Andresens (2019), masteravhandling.
[212] Se nærmere punkt 8.2.3.

relevant etterforskingsformål.[213] Riksadvokatens redegjørelse er spesielt relatert til ransaking av smarttelefoner.

10.3 Vilkår for beslag og ransaking «på stedet»

Undersøkelse av en bærbar databærer forutsetter beslutning både om beslag og ransaking. Vilkårene for at politiet skal kunne gjøre dette på egen kompetanse fremgår av strpl. § 206 første punktum, jf. strpl. § 198 første ledd nr. 3.

Ad beslagskompetansen sier strpl. § 206 første punktum:

> Uten beslutning av påtalemyndigheten kan politimann ta beslag når han setter i verk beslutning om ransaking eller pågripelse, og ellers når det er fare ved opphold.

For politipatruljen / første enhet på åstedet er det særlig «fare ved opphold» som kan by på problemer. Spørsmålet er hva slags fare som berettiger beslag for å kunne ransake en databærer. Farevilkåret gjelder også for ransaking som besluttes av tjenesteperson, jf. strpl. § 198 første ledd nr. 3. Her sies det at «politimann» kan ransake

> når det er sterk mistanke om en handling som etter loven kan medføre straff av fengsel i mer enn 6 måneder, og det er nærliggende fare for at formålet med ransakingen ellers forspilles.

Vilkårene som følger av strpl. § 198 (ransaking) er vesentlig strengere enn de som følger av strpl. § 206 (beslag). Dette fungerer fint når ransaking skjer før beslag, slik strpl. § 192 sammenholdt med § 206 legger opp til. Ved ransaking av smarttelefon eller annen mobil databærer på stedet, må imidlertid beslaget komme først. Dermed oppstår en anomali, fordi det ikke gir mening å foreta beslaget dersom ransakingsadgangen på stedet er avskåret som følge av at vilkårene i strpl. § 198 nr. 3 ikke er oppfylt.

Sammenhengen i loven tilsier at strpl. § 206 bør tolkes i lys av vilkårene i strpl. § 198 første ledd nr. 3. Gode grunner taler for å ha restriktive rammer for ransaking av ubeskyttede originale data. Det er grunnleggende at politiet ikke endrer bevis, og ransaking av originale data på stedet medfører nødvendigvis politiskapte endringer på dataene. Det kan imidlertid være situasjoner hvor integritetsprinsippet bør vike for andre hensyn, og vilkårene angitt i strpl. § 198 første ledd nr. 3 kan anses å gi en rimelig anvisning på dette. Vilkårene utelukker muligheten for å ransake originaldataene i stedet for å sikre dem, f.eks. alene fordi det er tidsbesparende.[214] Derimot

[213] Se nærmere om dette i punkt 7.3 og 8.2.4.
[214] Oppgis å være en grunn som brukes i praksis, se Andersen & Andresen (2019).

åpner de for å ransake dersom politiet ellers må regne med at informasjonen går tapt, f.eks. fordi de er flyktige og vil bli slettet. Hvorvidt risikoen for å gå glipp av informasjon fordi politidistriktet uansett ikke har kapasitet til å sikre innholdet, er relevant for vilkåret i strpl. § 198, er et spørsmål i seg selv.[215] Strenge rammer følger imidlertid også av strafferammekravet som sikrer at inngrepene bare skjer i saker av en viss alvorsgrad, og av det kvalifiserte mistankekravet som ytterligere skjerper inngangen til bruk av inngrepene. Dersom det er tale om beslag og ransaking av smarttelefonen til fornærmede eller et vitne, kreves i tillegg «særlig grunn» til å anta at smarttelefonen inneholder bevis, jf. strpl. § 192 tredje ledd nr. 3. Dette har betydning når fornærmede/vitnet ikke samtykker til beslaget (og ransakingen).

Loven kan sies å være noe vanskelig tilgjengelig med tanke på denne situasjonen som karakteriseres av beslaget inntreffer før ransakingen. Det er neppe grunn til lovendring, men klargjøring i retningslinjer foreslås.

Ransaking «på stedet» etter forutgående beslag i databærer slik som beskrevet, er av en annen karakter enn undersøkelser av databærere som skjer som forberedelse til sikring av data, i forbindelse med ransaking av noens bolig, rom eller oppbevaringssted. Ved forberedelse til sikring har undersøkelsen et foreløpig preg, og kan gjerne foregå i kontrollerte former som gjør det mulig å beskytte usikrede data mot endring.[216] Slike undersøkelser reiser ikke særlige spørsmål. Beslag i smarttelefon for å gjennomføre etterfølgende sikring av innholdet bør derfor følge den vanlige beslagsprosedyren.

10.4 Nødvendig i et demokratisk samfunn

Ransakingen av ubeskyttede originale data må være nødvendig og forholdsmessig, jf, strpl. § 170 a og EMK artikkel 8 (2). Gitt ransakingens negative konsekvenser for dataenes integritet, vil det viktigste elementet være ransakingens nødvendighet. Det bør kreves at opplysningene må antas å ha vesentlig betydning for saken, og at det er nødvendig å ha dem raskt slik at man ikke kan vente til de er sikret. Nødvendigheten må fremgå av dokumentasjonen og være basert på opplysninger som forelå før ransakingen ble gjennomført.

10.5 Konklusjon – forslag

Det foreslås ikke lovendringer på dette punkt, kun et supplement i den nye sikringsbestemmelsen som foreslås i neste kapittel, for å klargjøre at undersøkelser som nevnt

---

[215] *Ibid.*
[216] Se punkt 5.4.2 om bruk av skrivesperre.

her skiller seg fra undersøkelser som forberedelse til sikring. For øvrig foreslås retningslinjer som klargjør lovens vilkår for ransaking «på stedet», informasjonsplikten, og begrunnelses- og dokumentasjonskravene.

11. Sikring av data

11.2 Hjemmelsspørsmålet – gjeldende rett

Etter gjeldende rett anses sikring av data som et ledd i en handlingsrekke som starter med ransaking, jf. strpl. § 192 og ender med beslag, jf. strpl. § 203.[217] Sikringen gjenskaper dataene på den originale databæreren. Undersøkelser av sikringskopien kan anses å tilsvare undersøkelser av originaldataene på den opprinnelige databæreren, hvorfor undersøkelsene av sikringskopien anses som ransaking, slik det er redegjort for. Dette er sikker rett.

I *Wolland mot Norge* ble grensen mellom ransaking og beslag problematisert. Økokrim hadde speilkopiert klagerens datamaskin. Klageren gjorde gjeldende at hans rett under EMK artikkel 8 var krenket fordi overprøvingsretten etter strpl. § 208 ikke inntrådte før data var plukket ut og beslaglagt. Han var derfor nektet rettslig kontroll med inngrepet i perioden mens undersøkelsene av speilkopien pågikk. EMD sa at det ikke var opp til domstolen å vurdere tolkningen av den internrettslige hjemmelen, og la vekt på at tolkningen var fast etablert gjennom langvarig praksis.[218] Lovens ordning fra ransakings- til beslagtidspunktet hadde nødvendig rettsgrunnlag, og var tilstrekkelig tilgjengelig og forutsigbart.[219] Selv om EMD ikke uttalte seg direkte om strpl. § 192 som hjemmelsgrunnlag for sikringen, gis det støtte for at bestemmelsen er tilstrekkelig. EMD fant ikke noen krenkelse av EMK artikkel 8 i denne saken.

11.1 Sikring - et inngrep som krever lovhjemmel

HR-2018-104-A slår fast at sikring av data er et inngrep som krever lovhjemmel.[220] Etter gjeldende rett anses sikringen som et ledd i ransakingen, og skjer i medhold av strpl. § 192. Det kan likevel reises spørsmål om § 192 er holdbar som selvstendig hjemmel for sikringen. Riksadvokaten mener således at sikringen «ikke [er] å anse som ransaking»,[221] og *Haaland*

[217] Utredningen punkt 8.2.
[218] *Wolland* avsnitt 63.
[219] *Ibid., «The Court cannot, accordingly, agree with the applicant's complaint concerning the way the domestic courts had drawn a distinction between search and seizure"* (avsnitt 65).
[220] Kjennelsen avsnitt 22.
[221] Riksadvokaten (2020) s. 1.

mener det er «tvilsomt» at § 192 gir tilstrekkelig hjemmel. Hun synes å argumentere for at sikringen er å anse som beslag.[222]

Spørsmålet er om § 192 er tilstrekkelig hjemmel for sikringen, og i så fall, hvorvidt dagens regulering bør videreføres.

11.3 Hjemmelsspørsmålet *de lege ferenda*

Spørsmålet er om rettstilstanden er tilfredsstillende *de lege ferenda*. Reelt sett synes sikringen nemlig verken å være ransaking eller beslag. Det er også klart fra EMDs praksis at «seizure» er et videre begrep enn beslag, og begrepet synes å tolkes autonomt. Det fremgår både av *Einarsson* og *Wolland*.[223] Det betyr at det finnes en inngrepssone i tilknytning til ransaking og beslag som straffeprosessloven ikke tydelig regulerer.

11.3.1 Sikring vs. beslag

Sikring av data har tilsynelatende fellestrekk med beslag, fordi politiet dermed tilegner seg «ting» som tilhører en annen. Når formålet er bevissikring spiller det ikke noen rolle for beslagsadgangen at dataene ikke tas ut av innehaverens besittelse. Det vesentlige er at politiet har fått beviset i *sin* besittelse, noe sikringen besørger.[224] Men siden det ikke foretas noen konkret relevansvurdering som angitt i strpl. § 203, kan sikringen åpenbart ikke regnes som beslag.

11.3.2 Sikring vs. ransaking

Forholdet mellom sikring og ransaking lar seg analysere i forhold til de grunnleggende rettigheter det gripes inn i. Grunnloven § 102 og EMK artikkel 8 omfatter et stort sett av rettigheter, og HR-2018-104-A som konstaterer at sikringen er et inngrep, opplyser ikke i hvilke av disse inngrepet skjer.

Risikoen for at loven ville bli hengende etter teknologiutviklingen var en viktig del av Menneskerettighetsutvalgets begrunnelse for å innføre en generell personvernbestemmelse i Grunnloven § 102:

> Grunnlovsfesting av retten til privatlivets fred, personvern og personopplysningsvern kan (…) vise seg å bli et viktig rettslig verktøy i møte med fremtidens teknologiske utvikling og utfordringer.

---

[222] Haaland (2019) s. 194.
[223] I *Einarsson* brukes «seized» om alt som er sikret, dvs. hele sikringskopien. Det er et langt videre inngrepsbegrep enn «beslag» etter norsk rett. Saken er nærmere omtalt i kapittel 15.
[224] Utredningen punkt 5.4.2.

> Lovregulering på enkeltområder vil i noen grad måtte ligge i etterkant av den teknologiske utvikling, nettopp fordi fremtidens konkrete problemstillinger kan være vanskelige å forutsi. Dermed oppstår behovet for det generelle og overordnede vern, der prinsippet om privatlivets fred, personvern og personopplysningsvern er nedfelt i den høyeste rettskilde. Det kan ikke utelukkes at den teknologiske utvikling gjør at en slik grunnlovsbestemmelse vil vise seg å bli sentral i de kommende tiår.[225]

Stortingets kontroll- og konstitusjonskomite sluttet seg til dette og bemerket

> K o m i t e e n mener den teknologiske utviklingen gjør at behovet for å formulere kommunikasjon inn i Grunnloven er enda større nå enn tidligere. Teknologiutvikling er et gode, men krever mer av oss i henhold til å sikre personvern.[226]

Databevis er et teknologiskapt fenomen som reiser egne spørsmål, både hva angår sikringen, den videre behandlingsprosessen, og med hensyn til partsrettigheter. I denne konteksten gir uttalelsene i forarbeidene til Grunnloven § 102 oppfordring til å gå dypere inn i forståelsen av sikringens inngrepskarakter.

Hjemmelsgrunnlaget bør være klart med hensyn til hvilket aspekt av Grunnloven § 102 og EMK artikkel 8 det gripes inn i. Det at loven har forskjellige bestemmelser for ransaking av bolig, rom eller oppbevaringssted, og for ransaking av person, vitner som et slikt tankesett. Mens strpl. § 192 hjemler inngrep i retten til respekt for sitt «hjem», hjemler strpl. § 195 inngrep i retten til respekt for sin person, dvs. «privatliv», jf. Grunnloven § 102 og EMK artikkel 8. Dersom sikringen skal forankres i samme hjemmelsgrunnlag som ransakingen, bør sikring og ransaking anses for å gripe inn i den samme rettigheten. Hvis dét ikke er tilfelle, er det behov for klargjøring for så vidt gjelder sikringen.

Ransaking er en fredsforstyrrelse og griper som nevnt inn i retten til respekt for sitt hjem. Sikringen derimot, er det er mer nærliggende å anse som inngrep i retten til privatliv og kommunikasjon.

11.3.3 Retten til privatliv og kommunikasjon

Retten til respekt for «privatliv» omfatter blant annet retten til å utvikle personligheten sin uten ytre innblanding, og til å inngå og utvikle relasjoner. I stor grad handler dette om personlig autonomi, dvs. uforstyrret å kunne velge sin livsvei både privat og yrkesmessig, finne sin

[225] Menneskerettighetsutvalget (2012) s. 215 (Lovdata).
[226] Innst. 186 S (2013-2014) s. 39.

identitet, sosiale tilpasning osv. Et viktig element er at ens sosiale relasjoner privat og yrkesmessig omfattes av privatlivsvernet.[227]

Retten til respekt for sin «kommunikasjon» («korrespondanse») omfatter retten til uhindret og uforstyrret kommunikasjon med andre når dette skjer på en ikke-offentlig måte. Kommunikasjonsretten er en betingelse for og styrker utviklingen av, relasjoner. Siden utvikling av relasjoner også omfattes av retten til privatliv, er det nær sammenheng og delvis overlapping mellom rettighetene. Kommunikasjonsvernet omfatter innhold og metadata både av privat og yrkesmessig art.[228] Kommunikasjon under overføring er åpenbart omfattet, noe som har betydning for reglene om kommunikasjonskontroll. Men også kommunikasjon som er lagret omfattes, f.eks. epost og meldinger i form av tekst, lyd og bilde. Som det fremgikk var Stortingets kontroll- og konstitusjonskomite særlig opptatt av kommunikasjonsvernet.

Personopplysninger generelt omfattes av retten til respekt for privatliv, og i tillegg av kommunikasjonsvernet når de relaterer seg til kommunikasjon. Metadata om kommunikasjon er personopplysninger som er viktige i etterforsking, fordi de kan si noe hvem som har kommunisert, når kommunikasjonen fant sted, og hvor man befant seg da man kommuniserte.

11.3.4 Sikringens inngrepskarakter

Utgangspunktet er at dataene det er spørsmål om å sikre, jevnlig viser en stor del av personens privatliv, forstått både som å omfatte den personlige og private sfæren, og ens profesjonelle liv. På grunn av dataenes rikhet og borgernes avhengighet av dem, har informasjonssikkerhet blitt et viktig hensyn privat og i arbeidslivet. Politiets sikring griper inn i informasjonssikkerheten og innehaveren taper kontrollen over sine data. I tillegg «fryser» sikringen dataenes tilstand på sikringstidspunktet, og fratar innehaveren muligheten til å bearbeide eller slette dem med virkning for omverdenen. Dette er inngrep i retten til privatliv.

I de fleste tilfeller griper sikringen også inn i kommunikasjonsvernet. Det er en naturlig konsekvens av at datamaskiner er koblet til nettverk, og fordi epost-servere og smarttelefoner er vanlige beslagsobjekter. FORMOBILE-prosjektet opplyser at 85% av alle saker som etterforskes i EU inkluderer databevis fra smarttelefoner.[229] *Einarsson*-saken gjaldt spørsmål

[227] Kjølbro (2017) s. 773.
[228] Kjølbro (2017) s. 794 flg.
[229] FORMOBILE Project Page (formobile-project.eu) (besøkt 16. april 2021).

om innsyn i blant annet 20 millioner epost og telefonopptak gjort av foretaket mens det var i virksomhet.[230] Som kjent gjelder mange av de norske sakene korrespondanse med advokat.

Sikringen gjør således inngrep i privatliv og kommunikasjon. Fra et inngrepssynsynspunkt er det politiets *tilegnelse* av data som er det vesentlige. Tilegnelsen er tvungen og gjør borgeren sårbar overfor myndighetenes utnyttelse av dataene. Sikringen griper følgelig inn i privatliv og korrespondanse også når innehaveren beholder sine data.

Dette utelukker ikke at sikringen også kunne anses som en fredsforstyrrelse, jf. alternativet «hjem», og inngrepsmessig kunne likestilles med ransaking. Undersøkelsene av sikringskopien svarer jo rent faktisk til undersøkelser av de originale databærerne, noe som er å anse som ransaking. Sikringen gjelder imidlertid ikke undersøkelsene, men *skaper grunnlaget for* undersøkelsene. Sikring og ransaking er forskjellige handlinger som griper inn i ulike interesser omfattet av Grunnloven § 102 og EMK artikkel 8. Det er heller ikke treffende å si at sikringen går ut på «å søke etter bevis», slik § 192 nevner.

Konklusjonen er at det er behov for et tydeligere rettsgrunnlag for sikringen.

11.4 En ny bestemmelse om sikring av databevis

Sikring av data foreslås regulert i en egen bestemmelse, og ikke f.eks. skrives inn i strpl. § 192. Det tydeliggjør at at rettighetene som ransaking og sikring griper inn i er forskjellige.

11.4.1 Sikringsobjektet

Spørsmålet gjelder hva som er en hensiktsmessig rettslig karakteristikk av sikringsobjektet. I kapittel 5.4.2 er det forklart at sikring av data kan skje *post mortem* og fra aktive systemer (*live* sikring). I det første tilfellet gjelder sikringen data som er lagret. I det andre tilfellet kan sikringen både omfatte lagrete data og data som er under behandling. Det antas at sikringsbestemmelsen ikke bør stille krav til dataenes tilstand, slik det f.eks. gjøres i strpl. § 216 o fjerde ledd «elektronisk *lagrede* data».[231] Et vilkår om at dataene må være lagret vil på en tilfeldig måte innskrenke sikringsadgangen i forhold til i dag.

Når det gjelder gjennomføringsmåten har dataavlesing mye til felles med sikring av data fra databærer/brukerkonto, som skjer i forbindelse med ransaking. Forskjellen er at dataavlesing kan foregå over tid, i perioder inntil to uker av gangen, jf. strpl. § 216 o siste ledd første

[230] *Einarsson*, avsnitt 71.
[231] Utreders utheving.

punktum, mens sikring som ledd i ransaking må avsluttes når formålet «å søke etter bevis» er oppnådd. Mens dataavlesing kan skje fremover i tid gir sikringen bare et «øyeblikksbilde» av dataene på systemet.[232]

For dataavlesing spesifiserer loven hvilke data som kan sikres, jf. strpl. § 216 o fjerde ledd annet punktum: «Avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen.» En formulering som nevnt kunne være dekkende også for data som sikres under ransaking. Det gjelder også alternativet «kommunikasjon», som i konteksten av ransaking omfatter lagrete meldinger (f.eks. sms, chatlogger, epost), og data som sikres fra skytjenester uten at man har et helt konkret forhold til om de er lagret eller er dynamiske.

I dataavlesingsbestemmelsen skal imidlertid «kommunikasjon» forstås i samme betydning som «elektronisk kommunikasjon» i strpl. § 216 a om kommunikasjonsavlytting. Det følger av at dataavlesing skal kompensere for «effekttapet» kommunikasjonsavlytting (og hemmelig ransaking) har på grunn av kryptering.[233] Gjennom dataavlesing kan kommunikasjonen fanges opp før den krypteres og etter at den er dekryptert. Dessuten hadde det vært unødvendig å nevne «elektronisk lagrede data» dersom man ikke bevisst opererte med to kategorier data. Men som man forstår er lovens skille mellom elektronisk lagrete data og kommunikasjon lite hensiktsmessig siden kommunikasjon også kan være lagret.

Sikring som knytter seg til ransaking må skje innenfor ransakingshjemmelens og -beslutningens rammer. For databærere som er tatt i beslag, jf. strpl. § 192, jf. § 206, begrenser sikringen seg til å gjelde innholdet på disse. For sikring fra aktive systemer/brukerkontoer settes rammen av ransakingsbeslutningen sammenholdt med vilkåret om at sikringen gjelder data som var tilgjengelige på ransakingstidspunktet. Sikringen kan ikke strekkes ut i tid for å fange opp nye data som skrives til systemet.[234] Det antas imidlertid verken å være nødvendig eller hensiktsmessig at sikringsbestemmelsen regner opp kategorier av data. Siden forholdene kan variere mye antas en oppregning som nevnt, heller å kunne medføre vanskelige avgrensningsspørsmål og uklarhet. Det vesentlige er at bestemmelsen får frem at

[232] Som nevnt er «øyeblikksbilde» brukt i Prop. 68 L (2015-2016) *Skjulte tvangsmidler* pkt. 14.8.2, s. 262
[233] *Ibid.*, pkt. 14.8.4.
[234] Det er tankevekkende at Politidirektoratets beslagsrundskriv (2010) også nevner «datastrøm under kommunikasjon» blant de espor som kan sikres ved beslag, se punkt 5.4.2.1. Grensedragningen mot kommunikasjonskontroll blir dermed uklar. Utredningen kommer tilbake til spørsmålet i kapittel 20.

sikringsadgangen begrenser seg til å gjelde data som alt fantes på systemet da politiets skaffet seg tilgang.

11.4.2 «Data» eller «elektronisk informasjon»

Loven bør gi sikringsobjektet en entydig betegnelse. Straffeprosessloven §§ 203 og 215 a bruker «elektronisk lagret informasjon», mens § 216 o bruker «elektronisk lagrede data». Det kan ikke ses at forarbeidene til datalagringsbestemmelsen har begrunnet hvorfor man valgte en formulering forskjellig fra den som alt var brukt i §§ 203 og 215 a.[235]

Begrepsmessig er «elektronisk» videre enn «digitalt», fordi det omfatter analoge medier og informasjon i tillegg til digitale data.[236] Men det er de spesielle egenskapene ved det digitale som ligger til grunn for utredningens problemstillinger, ikke minst på grunn av «nedlåsingen» av data i sikringskopien. For eksempel antas ikke utskilling og sletting av lydspor fra kommunikasjonskontroll å by på tilsvarende problemer.[237]

Det foreslås derfor at sikringsbestemmelsen angir objektet som «data». Det bør ikke stilles krav om at dataene er lagret, jf. at sikringsbestemmelsen bør åpne for å kunne sikre dynamiske data fra aktive systemer. Det avgjørende er at sikringen ikke retter seg mot fremtidige data.

11.4.3 Politiet bør ha frihet til å velge sikringsmåte

Spørsmålet er om sikringsbestemmelsen bør regulere fremgangsmåten mer detaljert, for å gi inngrepet tydelige rammer. Risikoen er imidlertid stor for at bestemmelsen dermed vil bryte med den mest tungtveiende begrunnelsen for teknologinøytralitet, nemlig at loven ikke bør binde håndteringen av databevis til spesifikke fremgangsmåter eller teknologier. Begrunnelsen er at den raske teknolgiutviklingen medfører at beskrivelser av spesifikke fremgangsmåter raskt vil bli utdatert. Utredningen punkt 6.1 redegjør for dette, med henvisning til dataetterforskernes synspunkter, Europol & Eurojusts anbefaling, og Straffeprosessutvalgets syn.

Det foreslås derfor at bestemmelsen nøyer seg med å bestemme at sikringen må rette seg mot data som allerede fantes på databæreren da politiet skaffet seg tilgang til den (sml. foregående punkt).

---

[235] *Id.*, kapittel 14.8.
[236] Hjort (2016) pkt. 1.3.2.
[237] Se punkt 4.1.5.

11.4.4 Sikring av irrelevante data

Sikringens formål er å forberede grunnlaget for å kunne ransake data uten å påføre dem endringer. Ransakingsformålet er «å søke etter bevis (…) som kan beslaglegges», jf. strpl. § 192 første ledd. Siden sikringen vanligvis må skje uten forutgående relevansvurdering, medtar den også data som ikke er relevante, og iblant også data som er beslagsfrie, jf. strpl. § 204. Spørsmålet er hvordan sikringsadgangen bør utformes med hensyn til de to kategoriene. Sikring av irrelevante data behandles i dette punktet, og beslagsfrie data i utredningen del VI.

Data som er uten betydning for saken kan naturligvis ikke beslaglegges, men med tilstrekkelig lovhjemmel kan de likevel sikres. Det følger av politiregisterloven § 5 nr. 1, jf. § 4, som bestemmer at opplysninger bare kan behandles når det er nødvendig ut fra etterforskingsformålet, og er i samsvar med reglene i straffeprosessloven. Med eksisterende teknologi og i møte med store datamengder, later det til at sikring av overskuddsinformasjon er en nødvendig bieffekt, selv om sikringen innrettes mot antatt relevante deler av innholdet på databæreren. Manglende lovhjemmel for dette vil rettslig sett være et effektivt hinder for å kunne sikre data for bevisformål. Dersom mer sofistikert teknologi utvikles, kan overskuddsinformasjonens omfang muligens reduseres, men neppe fullstendig unngås fordi datamengdene er for store til at helt presise vurderinger kan gjøres på stedet.

I et lovgivningsperspektiv synes det vesentlige å være at *nødvendighet* oppstilles som vilkår for å sikre dataene. Nødvendigheten bør dokumenteres i sikringsrapporten, som bør redegjøre for omstendigheter av betydning for omfanget av sikringen, og hvordan nødvendighetsvilkåret ble iakttatt. I tillegg bør den inneholde en begrunnelse for valgt fremgangsmåte, og det må fremgå at sikringen så langt som mulig har vært inneretett på å holde seg innen rammen av ransakingsbeslutningen. Rammen overholdes primært ved at sikringen gejlder databærer eller brukekonto som ransakingsbeslutningen nevner, men etter omstendighetene antas det å kunne være mulig å gå enda mer målrettet til verks. En straffeprosessuell bestemmelse som nevnt vil således hjemle sikringsadgangen også for irrelevante data.

Spørsmålet er videre hvilke regler som bør gjelde for adgangen til fortsatt å beholde irrelevante data, etter at de relevante er beslaglagt. Dette må vurderes i lys av at dataene er «låst ned» i sikringskopien, og at sletting er et problem.[238] Utredningen kommer tilbake til spørsmålet i kapittel 19.3.

[238] Det vises til utredningen punkt 5.4.2.

11.4.5 Behov for rettslig beslutning om sikring?

Spørsmålet er om det er behov for en prosessuell garanti som spesielt angår sikringen. Lovmessige rammer vil imidlertid allerede foreligge som følge av at sikringen føyer seg til ransakingen og ikke kan gå ut over ransakingsbeslutningens rammer, jf. forrige punkt. Det antas likevel at loven bør oppstille vilkår om at retten ved behandlingen av ransakingsbegjæringen, også tar stilling til en begjæring om å sikre data. Det gir anledning til å styre inngrepets målrettethet gjennom å stille krav til konkrete opplysninger om behovet, og om hvordan sikringen bør innrettes for å unngå for store mengder overskuddsinformasjon mv.

Krav om bedre begrunnelser for ransaking og sikring av data er begynt å bli et tema, jf. både FORMOBILE-rapporten, og den engelske *Search Warrants* rapporten. I England ser man behov for at retten aktivt stimulerer til økt målrettethet ved å kreve beslutningsgrunnlaget bedre opplyst enn det som har vært praksis. *Haaland* antyder at et tilsvarende behov kan eksistere i Norge.[239] Utredningen kommer tilbake til proporsjonalitetsspørsmålet i kapittel 19.1.

Det foreslås således at strpl. § 197 bygges ut til å omfatte tillatelse til å sikre data.

11.4.6 Behov for en bestemmelse om papirdokumenter?

Spørsmålet er om sikringsbestemmelsen også bør omfatte fysiske dokumenter, siden bevis også i disse tilfellene kan sikres gjennom kopiering. Tilegnelse av informasjon gjennom kopiering må anses som et inngrep uavhengig av om kopieringen gjelder data eller papirdokumenter, og trenger følgelig lovhjemmel, jf. Grunnloven § 113. I Sverige (SOU 2017:100) gikk forslaget til ny bestemmelse om kopiering som alternativ til beslag, ut på at den skulle være teknologinøytral og dermed omfatte både data og papirdokumenter.[240]

På den annen side fremstår nødvendigheten av en særskilt bestemmelse om papirdokumenter som tvilsom. Det er langvarig praksis for at fysiske dokumenter kan sikres ved kopiering, en lovforståelse som støttes av proporsjonalitetshensynet, siden kopiering er mindre inngripende enn at dokumentene varig tas ut av innehaverens besittelse, jf. strpl. § 203. I forhold til EMK artikkel 8 (2) er (det materielle) hjemmelskravet oppfylt, se punkt 7.2, så spørsmålet er om Grunnloven § 113 nødvendiggjør tydeligere formalisering i lov. Det kan anses betenkelig om loven går i en stadig mer spesifiserende retning ved å regne opp hva som kan sikres, med mindre legalitetsprinsippet gjør det helt nødvendig. Loven går riktignok allerede i en slik retning, jf.

---

[239] Haaland (2019) punkt 7.2.1 s. 199.
[240] SOU 2017:100 kapittel 7.6, s. 423. Forslaget er foreløpig ikke fulgt opp.

bestemmelsene om adgangen til å ta fingeravtrykk, fotografi og DNA-prøve, jf. strpl. §§ 158-160, men disse bestemmelsene gjelder inngrep som angår kroppen, og er ikke sammenlignbare med det som er tema her. Det antas også at en mer systematisk gjennomgang av spesifiseringsbehovet for sikring av bevis bør foretas i en helhetlig revisjon av straffeprosessloven.

Dersom uttrykkelig lovhjemmel anses å være nødvendig, kan det muligens gjøres som et supplement til den foreslåtte sikringsbestemmelsen, om at den gjelder tilsvarende for fysiske dokumenter så langt det passer.

Hovedkonklusjonen er at det ikke foreslås en særskilt bestemmelse om kopiering av papirdokumenter eller lignende, for å sikre bevis.

11.5 Konklusjon – forslag

Ny bestemmelse: Straffeprosessloven § 192 a

Det foreslås en ny bestemmelse om sikring av data i tilknytning til ransaking i medhold av strpl. § 192. Bestemmelsen foreslås inntatt som ny § 192 a. Det bør fremgå av ordlyden at sikringsadgangen begrenser seg til å gjelde data som alt fantes på systemet da politiets skaffet seg tilgang, uten at det dermed er et vilkår at dataene er «lagret». Bestemmelsen bør vise til databevisforskriften som regulerer sikringen mer detaljert.

Bestemmelsen kan suppleres med at den gjelder tilsvarende for kopiering av fysiske dokumenter så langt det passer.

Straffeprosessloven § 197

Det foreslås å innføre rettslig forhåndskontroll med sikringsadgangen, ved å utvide ordlyden i strpl. § 197 til også å omfatte tillatelse til å sikre data.

12. Hemmelig ransaking av databærer

12.1 Gjeldende rett

«Hemmelig» ransaking, dvs. ransaking med utsatt eller helt unnlatt underretning til mistenkte eller andre som berøres av inngrepet, er hjemlet i strpl. § 200 a. Bestemmelsen regulerer det som er særegent for hemmelig ransaking sammenlignet med ransaking som skjer åpent. Den angir således de strengere vilkårene for bruk av metoden, beslutningskompetansen, og om og når underretning skal gis. I henhold til bestemmelsens siste ledd gis de alminnelige ransakingsbestemmelsene anvendelse «så langt de passer». Sammenholdt med strpl. § 192

«oppbevaringssted», åpner strpl. § 200 a for hemmelig ransaking av databærer på linje med hemmelig ransaking av bolig, rom og fysisk oppbevaringssted.

12.2 Manglende hjemmel til å kunne begå datainnbrudd

Hemmelig ransaking forutsetter at atkomsten til ransakingsobjektet skjer skjult, om nødvendig ved å begå innbrudd. Rettsgrunnlaget for å begå innbrudd for å gjennomføre ransaking følger av strpl. § 200 annet ledd annet punktum: «Om nødvendig kan det åpnes adgang med makt». Bestemmelsen knytter an til de foregående setningene som gjelder «bolig eller rom» og «redaksjonslokale», og gir følgelig adgang til å begå fysisk innbrudd.

Bestemmelsen nevner ikke «oppbevaringssted», dvs. ordet som er forankringen for at strpl. § 192, etter gjeldende rett, anses å omfatte databærere. Når strpl. § 200 ikke nevner «oppbevaringssted» savnes positiv lovhjemmel for å begå datainnbrudd. Datainnbrudd krever også annen kompetanse og innebærer andre risikofaktorer enn fysisk innbrudd. Reelle hensyn taler derfor mot en utvidende fortolkning av strpl. § 200 til å omfatte datainnbrudd.

Videre gjelder inngrepene forskjellige rettigheter. Mens fysisk innbrudd jevnlig gjør inngrep i retten til respekt for sitt hjem, er datainnbrudd inngrep i retten til respekt for privatliv og kommunikasjon, se punkt 11.3.3. og 11.3.4. Datainnbrudd er dessuten straffbart, jf. straffeloven § 204, så allerede av den grunn er en klar straffeprosessuell hjemmel nødvendig, dersom det skal være lovlig fremgangsmåte for å gjennomføre hemmelig ransaking av databærer. Strafferettslig omfatter datainnbrudd ikke bare «hacking», f.eks. utnyttelse av sårbarheter i datasystemet, men også bruk av innehaverens passord.[241]

Det må derfor legges til grunn at politiet etter gjeldende rett verken har rettslig adgang til å logge seg inn med mistenktes brukernavn og passord, eller bruke «hacking» for å skaffe seg adgang til datasystemet.

12.3 Lovteknisk integrering av hemmelig ransaking og dataavlesing av databærer

12.3.1 Hjemmelsmangelen er utilsiktet

Hjemmelsmangelen for å kunne begå datainnbrudd ved gjennomføringen av hemmelig ransaking, må antas å være utilsiktet fra lovgivers side. Forarbeidene til bestemmelsene om dataavlesing, forutsetter at politiet allerede hadde adgang til å ransake datasystem/brukerkonto

[241] Se I.M. Sunde (2016) kap. 4.6.

både ved fysisk atkomst og over nett.[242] Dataavlesing var bare en «kompenserende» metode for «effekttapet» kommunikasjonsavlytting og hemmelig ransaking har som følge av den teknologiske utviklingen.[243] Det teknologiskapte problemet gjaldt økt bruk av innholdkryptering, ikke at det var vanskeligere enn før å oppnå tilgang til datasystemet. Det må derfor ha vært antatt at politiet hadde lovlig adgang til å begå datainnbrudd i forbindelse med hemmelig ransaking.

Denne hjemmelssvikten bør det nå rettes opp i. Spørsmålet er hvordan.

12.3.2 Fellestrekk mellom hemmelig ransaking av databærer og dataavlesing

Reelt sett har hemmelig ransaking av databærer langt mer til felles med dataavlesing enn med fysisk ransaking, som den er regulert under ett med. Både dataavlesing og hemmelig ransaking av databærer har som formål å sikre data. «Avlesing» er et bredere uttrykk enn «sikring» som også omfatter at data sikres. Sett under ett innebærer metodene adgang for politiet til å foreta hemmelig sikring av data, ved enkeltstående eller vedvarende inngrep.

Dataavlesing og hemmelig ransaking bør derfor anses som grader av samme metode. Dette kan allerede leses ut av loven slik den lyder i dag. Ved å reguleres under ett i bestemmelsene om dataavlesing, løses også hjemmelsproblemet vedrørende adgangen til å begå datainnbrudd for å gjennomføre hemmelig ransaking av databærer. Dette følger av strpl. § 216 p første ledd tredje punktum som gir adgang til «å bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å gjennomføre avlesingen».

Straffeprosessloven § 216 o inneholder en oppregning av hva som kan sikres ved dataavlesing. Oppregningen omfatter blant annet data som kan sikres ved (hemmelig) ransaking, jf. «[a]vlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen.» De to siste kategoriene gjelder lagrete data og metadata, som begge kan sikres i medhold av hjemmelen til å foreta hemmelig ransaking. Forarbeidene til dataavlesingsbestemmelsene utdyper dessuten at dataavlesing kan omfatte data i «fysiske eller virtuelle minneområder».[244] Som forklart i punkt 5.4.2 sikres data politiet har skaffet seg atkomst til gjennom ransaking, også fra aktive systemer, og dermed medtas også

[242] Prop. 68 L (2015-2016) pkt. 14.2.3. Bestemmelsene om dataavlesing ble innført ved lov 17. juni 2016 og trådte i kraft 9. september samme år.
[243] *Ibid.*, pkt. 14.8.4.
[244] Prop. 68 L (2015-2016) kapittel 14.1.

data fra i datasystemets minne (RAM). Det er altså flytende overgang mellom ransaking og dataavlesing.

Tillatelse til dataavlesing gis av retten, jf. strpl. § 216 o siste ledd første punktum. Dersom det er tilstrekkelig for formålet å sikre data som allerede finnes på databæreren, kan retten begrense tillatelsen til å gjelde dette, og følgelig reelt sett begrense dataavlesingen til å gjelde hemmelig ransaking. Loven bestemmer dessuten at dataavlesingen skal stanses dersom vilkårene ikke lenger er tilstede eller avlesing ikke lenger anses hensiktsmessig. Avlesingsperioden kan således være kortere enn to uker, se strpl. § 216 f annet ledd, som gjelder tilsvarende for dataavlesing, jf. strpl. § 216 o siste ledd første punktum.

For ytterligere presisjon og gjøre oppmerksom på at også kortvarig avlesing (ransaking) omfattes av bestemmelsen, kan strpl. § 216 o innta en setning som klargjør dette.

12.3.3 Gjentatt hemmelig ransaking av databærer

Videre bør det åpnes for gjentatt hemmelig ransaking av databærer. *Bruce & Haugland* opplyser at til tross for at *gjentatt* ransaking ikke har positiv straffeprosessuell hjemmel, hender det at tingretten i en og samme beslutning gir tillatelse til flere ransakinger av samme databærer, dette med hjemmel i strpl. 200 a, jf. § 192.[245] Det tyder på at behovet finnes, men praksisen savner klart rettsgrunnlag. Opplysningene gjelder praksis en del år tilbake i tid, og det kan ikke utelukkes at innføring av adgangen til å foreta dataavlesing har fjernet behovet. Dette kan belyses i høringsrunden.

Det antas uansett at politiet bør ha frihet til å bruke fremgangsmåten, dersom det er formålstjenlig. Gjentatt hemmelig ransaking kan også etter omstendighetene anses som mindre inngripende overfor mistenkte enn at databæreren er gjenstand for vedvarende avlesing. Retten bør imidlertid vurdere behovet for å sette et øvre tak på antall gjentakelser.

12.3.4 Oppsummering

Oppsummert må det konkluderes med at dataavlesing og hemmelig ransaking er sammenlignbare metoder. Iblant kan hemmelig ransaking være mer effektivt enn dataavlesing fordi det er enklere å gjennomføre, og dessuten kan gi betydelige mengder data. Dataavlesing kan visstnok føre med seg større risiko for at politiets oppmerksomhet mot databæreren blir avslørt, blant annet dersom politiet har installert et overvåkingsprogram på databæreren. KK-

[245] Bruce & Haugland, s. 188-189.

utvalgets årsrapporter for 2018 og 2019 (2020 er i skrivende stund ikke offentliggjort) opplyser at dataavlesing bare er brukt henholdsvis 7 og 5 ganger. Opplysninger om antall tilfeller av hemmelig ransaking foreligger ikke fordi metoden ikke omfattes av KK-utvalgets mandat. Dette bør uansett endres slik at også hemmelig ransaking undergis etterkontroll, se punkt 12.4. Poenget er at begge metodenes er svært inngripende og reelt sett vanskelig å gradere i forhold til hverandre, fordi begge kan brukes snevert og bredt. Det hele avhenger av bruken i det konkrete tilfellet.

Bestemmelsene om hemmelig ransaking og dataavlesing har tilnærmet likt virkeområde, men ikke identisk. Etter utreders oppfatning burde ikke dette være til hinder for integrering av bestemmelsene.

Forslaget går således ut på å innta et nytt siste punktum i strpl. § 200 a første ledd som klargjør at bestemmelsen ikke omfatter hemmelig ransaking av databærer. Bestemmelsen vil dermed bare omfatte hemmelig fysisk ransaking. Videre foreslås det å innta et nytt annet ledd i strpl. § 216 o som klargjør at bestemmelsen også omfatter hemmelig (gjentatt) ransaking av databærer. Bestemmelsens siste ledd bør presisere rettens plikt til å vurdere behovet for å sette et øvre tak på antall gjentakelser.

12.4 Behov for etterkontroll og særskilt kompetanse

Hemmelig ransaking av databærer bør være gjenstand for etterkontroll av KK-utvalget slik som dataavlesing. I likhet med dataavlesing etterlater hemmelig ransaking få ytre spor, og for dataavlesing forutsatte lovgiver uttrykkelig at

> Det gis retningslinjer for den praktiske bruken av metoden og at det etableres rutiner for å kontrollere at den ikke benyttes utenfor lovens rammer. Departementet legger til grunn at dataavlesing vil etterlate få ytre spor, og at det derfor er særlig viktig at politiets bruk av metoden dokumenteres på en måte som setter kontrollorganene i stand til å vurdere om det som er utført ligger innenfor de lovlige rammene, og så vidt mulig også til å kontrollere at det ikke har blitt utført noe annet eller noe mer enn det som oppgis.[246]

I tillegg ble det stilt krav om at metoden bare kunne utføres av personell med tilstrekkelig datakompetanse, og at den skulle være gjenstand for kontroll av KK- og EOS-utvalgene. Etterfølgende kontroll er en viktig rettssikkerhetsgaranti som virker disiplinerende på bruken

[246] Prop. 68 L (2015-2016) punkt 14.8.4, s. 266.

av hemmelige tvangsmidler, og minimerer muligheten for at bevis endres, slettes eller «plantes». Et system basert på tillit er som nevnt ikke tilstrekkelig.[247]

Videre må det legges til grunn at særskilt datakompetanse er nødvendig for hemmelig ransaking av datasystem. Dette er nødvendig for dataetterforsking generelt, se kapittel 4.2, og i større grad når tvangsmiddelbruken går ut på hemmelig ransaking. Loven bør derfor stille kompetansekrav, foruten særlige krav til dokumentasjonen.

Dersom hemmelig ransaking av databærer i fremtiden omfattes av dataavlesingsbestemmelsene vil man uten videre ha sørget for de nevnte prosessuelle garantiene, fordi de følger av strpl. § 216 p og KK-forskriften. Uansett hvordan man ser på forslaget om å integrere hemmelig ransaking av databærer i bestemmelsene om dataavlesing, bør etterkontroll antas å være helt nødvendig og det er egnet til å overraske at det ikke allerede er en del av KK-utvalgets mandat.[248]

12.5 Konklusjon – forslag

Straffeprosessloven § 200 a

Forslaget går ut på å innta et nytt siste punktum i strpl. § 200 a første ledd som klargjør at bestemmelsen ikke omfatter hemmelig ransaking av databærer. Bestemmelsen vil dermed bare omfatte hemmelig fysisk ransaking.

Straffeprosessloven § 216 o

Det foreslås å ta inn et nytt annet ledd i strpl. § 216 o som klargjør at bestemmelsen også omfatter hemmelig (gjentatt) ransaking av databærer. Bestemmelsens siste ledd bør presisere rettens plikt til å vurdere behovet for å sette et øvre tak på antall gjentakelser.

13. «Ting» i strpl. § 203

Den nære sammenhengen mellom bestemmelsene om ransaking, sikring og beslag gjør det naturlig også å ta opp ordlyden i strpl. § 203. Riksadvokaten har spilt inn at ordet «ting» bør erstattes av det enda mer generelle ordet «noe», eventuelt «det».[249] Forslaget innebærer at

[247] Se utredningen punkt 7.2.
[248] EOS-utvalget kontrollerer hemmelig ransaking utført av Politiets sikkerhetstjeneste (PST) i forebyggende øyemed. Det følger av EOS-kontrolloven § 6 fjerde ledd nr. 1 (som angir kontrolloppgavene overfor PST), jf. politiloven § 17 d som nevner hemmelig ransaking blant de metoder PST kan benytte i sin forebyggende virksomhet. EOS-kontrolloven er lov av 3. februar 1995 nr. 7.
[249] Riksadvokaten (2017) s. 47.

ordlyden klarere uttrykker rettstilstanden, nemlig at objektet for beslag ikke behøver ha en fysisk manifestasjon.

Utreder slutter seg til forslaget.

Del V. Fase to - ransaking og beslag av sikrede data.

14. Problemstilling

Etterforsking går ut på å innhente, systematisere og analysere opplysninger. Loven regulerer innhentingsmetodene forholdsvis detaljert, men sier lite om hvordan de innhentede opplysningene bør systematiseres og analyseres. De viktigste føringene følger av strpl. § 226 om at etterforskingen er formålsstyrt og skal ivareta objektivitet.[250] I tillegg gjelder det kvalitetskrav, herunder krav til dokumentasjon (notoritet). Kravene er utdypet i riksadvokatens retningslinjer for kvalitet i etterforskingen.[251]

De nevnte kravene er av overordnet karakter. I det følgende søkes de operasjonalisert som retningslinjer for analysen. Per i dag finnes det verken en etablert praksis for hvordan analysen bør foregå, mal for analyserapporten hvor bevisene presenteres, eller en festnet begrepsbruk som sikrer mot uklarhet og misforståelser.[252] Det mangler også klare prosedyrer for samhandling mellom dataetterforskere med teknisk fokus og kompetanse, og taktiske etterforskere som er trenet i hypotesetenkning, krav til objektivitet og til å skulle se alle sakens beviser i sammenheng. Samtidig kan analysen være krevende fordi datamengdene er store, og de kan være vanskelige å strukturere og forstå. I punkt 4.1 fremhevet dataetterforskerne kompleksiteten i analysen og etterlyste retningslinjer og metodisk støtte. Dette har støtte i forskning, se f.eks. *Ryser m.fl.* (2020) som sier

> In particular, forensic practitioners are struggling to keep pace with the rising demand for forensic analysis of digital and multimedia evidence, and with the steadily increasing volume, variety, velocity, distribution, and complexity of information (…). In addition, forensic practitioners face

[250] Kravet til målrettethet er utdypet i punkt 7.2 og 8.2.4. For påtalemyndigheten følger objektivitetsplikten av strpl. § 55 a siste ledd.
[251] Riksadvokaten (2018).
[252] I følge N. Sunde (2019b) holder analyserapportene svært varierende kvalitet, s. 77. Sml. Haraldseid (2021), masteravhandling.

> challenges with evaluating and expressing inaccuracies and errors in digital and multimedia evidence.[253]

Kvalitetsmessige mangler av betydning for analysen er rettslig relevante for inngrepsvurderingen. I kraft å være ransaking er analysen et alvorlig inngrep som stiller krav til inngrepets egnethet, nødvendighet og forholdsmessighet, og til prosessuelle garantier mot vilkårlighet og misbruk.[254] Notoritetsmangler kan dessuten gå ut over retten til kontradisjon og partslikhet.

14.1 Tilbakeblikk

Helt fra sin spede begynnelse har «digital forensics /digital forensic science» vært opptatt av å unngå tekniske feil ved databevis, noe som gjenspeiles i dataetterforskingsprosessens tydelige fokus på databevisets integritet. Det betyr at fagmiljøet innen *digital forensics* opp gjennom årene har hatt størst interesse i de mest «tekniske» fasene, nemlig sikring og klargjøring. Faglitteraturen om tekniske aspekter i disse fasene er omfattende, og også Politidirektoratets beslagsrundskriv konsentrerer seg om den tekniske prosessorienterte håndteringen av databevis (rundskrivet punkt 3.3 «Data»).[255]

For disse fasene har behovet for teknisk kompetanse og utstyr vært åpenbart. Oppgavene kan dessuten utføres uten at man nødvendigvis har spesiell innsikt i taktiske aspekter av etterforsking, eller i sakens konkrete informasjonsbehov. En dataetterforsker/spesialist har således kunnet anse oppgaven sin som avsluttet når de sikrede dataene er klargjort, og kunnet overlate analysen til den taktiske etterforskeren som kjenner saken og presumptivt lettere kan finne bevis. I praksis viser det seg imidlertid at den taktiske etterforskeren kan ha behov for støtte til analysen, og retningslinjer antas å kunne gi et visst grunnlag for dette.

I *Saber*-saken konstaterte EMD at det norske regelverket hadde mangler. Det lot seg blant annet lese ut av politirapporten som redegjorde for behandlingen av sakens beslagsfrie opplysninger, og EMD kommenterte:

> As to the report of 9 November 2017 (…), it described the deletion of data in the applicant's case, but did not describe any clear basis or form for the procedure (…).[256]

---

[253] Ryser m.fl (2020) pkt. 1; sml. Servida & Casey (2019). Se også Borhaug (2019) som behandler samspillet mellom teknologi og etterforsker i møte med store datamengder. Masteravhandling.
[254] Se utredningen punkt 7.2.
[255] Politidirektoratet (2010).
[256] *Saber* avsnitt 55.

EMDs kritikk bør neppe anses kun å ha relevans for behandling av beslagsfrie data, selv om saken direkte gjaldt dette. Kritikken bør snarere tas som et signal om at EMD har begynt å intensivere prøvingen av hvordan sikrede data behandles av politiet mer generelt. Som utredningen også gir uttrykk for i punkt 15.3.2 og 17.5, må det forventes en betydelig rettsutvikling i relasjon til EMK når det gjelder spørsmål foranledninget av teknologiutviklingen.

14.2 Tekniske og ikke-tekniske feilkilder

I en kjent artikkel fra 2002 drøfter *Casey* forskjellige feil og svakheter som kan hefte ved databevis, og etterlyser tiltak for kvalitetssikring av prosessene som inngår i bevisbehandlingen.[257]

En type feil angår tekniske forhold, slik som at databeviset skades, i verste fall går tapt, eller manipuleres underveis i prosessen. En annen type feil skyldes svakheter som rammer tolkningen av beviset. Denne kategorien har de senere år fått økt oppmerksomhet, og favner en rekke såkalte «ikke-tekniske» feilkilder.[258] Uttrykket omfatter feilkilder knyttet til person, for eksempel tunnelsyn eller manglende kompetanse, og feilkilder knyttet til organisasjon, f.eks. mangler som gjelder tilrettelegging for å kunne dokumentere hvordan dataene behandles, rutiner for samhandling mellom dataetterforskere og taktiske etterforskere, og prosedyrer for kvalitetssikring av arbeidsprosesser. Feilkilder som nevnt kan lede til at relevant informasjon overses eller feiltolkes, og at holdbarheten av funn vanskelig lar seg kontrollere.

Flere hendelser de senere år har økt oppmerksomheten rundt disse spørsmålene, slik som den danske «teledataskandalen» som gjaldt feil over en årrekke knyttet til politiets bruk av trafikkdata;[259] verktøyet Cellebrite (sikrer data fra smarttelefoner) som inneholdt feil i tidsangivelsen i logger;[260] og Veidirektoratets verktøy og metoder for avlesing av data i bilers ferdsskrivere, data som ble brukt i den videre etterforsking av trafikkulykker.[261]

---

[257] Casey (2002).
[258] Uttrykket stammer fra Nina Sundes masteravhandling *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation*, NTNU (2017). På bakgrunn av avhandlingen ble ikke-tekniske feilkilder inkludert som et eget punkt i et rammeverk for harmonisering av kriterier for forsvarlig dataetterforsking, utgitt av det amerikanske National Institute of Standards and Technology (NIST), se Pollit et al. (2018) punkt 4. En kortversjon av masteravhandlingen finnes i Sunde, N. (2019b).
PhD-prosjektet «Dataetterforskers rolle i konstruksjonen av digitale bevis i straffesaksetterforskning" viderefører temaet i masteravhandlingen Nina Sunde - Politihøgskolen (politihogskolen.no).
[259] N. Sunde & Lene W. Lenz (2021).
[260] Feil i analyseverktøy gjør at Politiet må gjennomgå minst 57 straffesaker (nrkbeta.no) (Ståle Grut & Henrik Lid, 3. november 2020) NRKbeta.
[261] PWC & Statens Vegvesen (2020).

Feilkilder og svakheter ved dataetterforsking i norsk politi og påtalemyndighet, belyses i flere masteravhandlinger.[262] Samlet sett er det grunn til å tro at svakhetene er systematiske, og ikke knytter seg til tilfeldige enkelttilfelle. Riksrevisjonens rapport fra 2021 underbygger dette. Rapporten fremmer alvorlig kritikk av forhold som kan representere ikke-tekniske feilkilder. For denne utredningen er rapportens konstatering av *manglende retningslinjer, rutiner og standarder* for hvordan digitale bevis skal *«sikres, analyseres og etterforskes»* spesielt relevant.[263] Dette sammenfaller med *Jahrens* konstatering av at det verken finnes tilstrekkelige kompetansekrav, standarder for metoder og verktøy, eller instrukser innen kvalitetssikring og kvalitetsstyring i fagfeltet dataetterforsking.[264] Internasjonalt har betydningen av ikke-tekniske feilkilder i dataetterforsking begynt å få stor oppmerksomhet.

Spørsmål om tiltak kan oppsummeres som følger: Hva kreves for å sikre

- Objektivitet og målrettethet i analysen.
- Kvalitet i samarbeidet mellom teknisk og taktisk etterforsker.
- God forståelse av analyseverktøyenes egenskaper og begrensninger.
- Notoritet i behandlingen av dataene (informasjonssikkerhet og dokumentasjon)
- Hva som kreves for å presentere dataene på en rettssikker måte.

De tekniske feilkildene gjør seg særlig gjeldende i fasene for sikring og klargjøring av dataene. De dannet også bakteppet for drøftelsene av ransaking av ubeskyttede originale data (kapittel 10). De ikke-tekniske feilkildene kan særlig påvirke analysen, herunder hvordan databevis avdekkes, tolkes og dokumenteres i saken, og presenteres for bevisbedømmeren.

14.3 Datakriminalteknikk vs. dataetterforsking

En følge av dataetterforskernes tekniske orientering, er at spørsmål om hvordan analysen bør innrettes, har fått mindre oppmerksomhet. Implisitt har det skjedd en arbeidsdeling hvor dataetterforskere/-spesialister håndterer sikring og klargjøring, mens etterforskerne på saken (taktiske etterforskere) har hatt ansvar for identifiseringfasen og analysen. Slik er også DPAens rolle beskrevet i politiets styringsdokumenter (se innledningen i kapittel 4). DPAens rolle tenderer således mot å være rent kriminalteknisk, likevel slik at dette ikke er kategorisk

[262] Masteravhandlingene er oppført samlet under eget avsnitt i litteraturlisten.
[263] Riksrevisjonen (2021) punkt 2.1.3 på s. 9. Se også Andreassen&Andresen (2019) og Heitmann (2019) om manglende struktur i initialfasen (masteravhandlnger).
[264] *Jahren* (2020). Masteravhandling.

gjennomført i praksis. Som bistandsfunksjon synes DPAen å stå i en mellomstilling, dels som kriminalteknikk og dels som etterforsking.

Innen kriminalteknikken spesialiserer man seg på bestemte sportyper, og det gjelder krav om å kjenne grensene for sin kompetanse og ikke rapportere utenfor sin ekspertise.[265] Det forutsettes også at kriminalteknikeren har god innsikt i teknologien og metodikken som brukes for å sikre og analysere spor. Innsikten skal også omfatte begrensninger og mulige svakheter ved verktøyene som er benyttet.[266] Politidirektoratet har utarbeidet en *Kvalitetsstandard for kriminalteknisk etterforsking*. Denne gjelder imidlertid ikke for elektroniske spor, da det for slike «vil (…) bli utarbeidet egne retningslinjer». [267] Retningslinjer som nevnt er foreløpig ikke utarbeidet.

Spørsmålet er hva *dataetterforskere* bør undersøke og rapportere om. Under forutsetning av at de står utenfor etterforskingsteamet og kun sørger for sikring og klargjøring av datamateriale, bør eventuell rapportering om konkrete bevis begrense seg til bevisets objektive/ytre egenskaper. En slik beskrivelse gjelder data som objekt bestående av *«bits&bytes»* og assosierte metadata.[268] Det kan redegjøres for hvor dataene var lokalisert og hvordan dataetterforskeren gikk frem for å finne dem, tilsvarende hvordan det gjøres for fysiske bevis, f.eks. et papirdokument. Man kan f.eks. opplyse at en fil var lokalisert i en bestemt mappe, var i Microsoft Edge pdf-format og at størrelsen var på 1.84 MB. Opplysningene kan etter omstendighetene ha bevisverdi, f.eks. kan det ha betydning om ulovlig bildemateriale befant seg i et mellomlagringsområde eller lå i en mappe i dokumentsystemet, akkurat som det kan ha betydning om et dokument ligger på sin rette plass i bokholderiet eller er nedlåst i nattbordet. Man kan også stusse over at en fil inneholder langt mer data enn normalt for den aktuelle filtypen, noe som kan indikere at den også inneholder skjulte data. Beskrivelse av databevis på grunnlag av slike objektive egenskaper krever lite tolking, og i fagmiljøet tales det om å dokumentere funn (*«objective findings»).*[269]

---

[265] ENFSI Code of Conduct, 16. juni 2005, pkt. 2.6; ENFSI Guidelines for Evaluative Reporting in Forensic Science, 2015, pkt. 1.3; Tilstone et al. (2013) s. 117.
[266] Friheim (2016). Masteravhandling.
[267] Politidirektoratet (2012) s. 3.
[268] Data som et objekt som kan være gjenstand for inndragning, er behandlet av I.M. Sunde (2010). Se avhandlingen kapittel 3 og 7 om representasjonen av data som objekt. Betydningen av metadata behandles i denne utredningen punkt 5.5.
[269] Flaglien (2018), s. 45 og 46.

Også en taktisk etterforsker som er innlemmet i etterforskingsteamet vil kunne rapportere om databevisets objektive egenskaper. I tillegg må etterforskeren vurdere databevisets *utsagnskraft* om en omstendighet som er relevant for etterforskingen. Utsagnskraften kan anses som databevisets subjektive side, fordi det forutsetter tolking, innsikt i sakens hypoteser og kunnskap om informasjonsbehovet. Tendensen til å anse data for å være mer objektive og «sanne» enn det reelt er grunnlag for, representerer imidlertid en risiko for feilslutninger om bevisverdien.[270] Man kan heller ikke regne med at taktiske etterforskere har tilstrekkelig teknisk kompetanse til å kunne undergi datamaterialet overlevert fra dataetterforskerne, kritisk vurdering. Det er de imidlertid ikke alene om. Det antas at også påtalejurister, forsvarere og dommere gjennomgående mangler forutsetninger for å kunne stille relevante kritiske spørsmål om databevis. Utfordringer i kommunikasjonen mellom tingretten og medhjelperen / sakkyndige ved utsortering av beslagsfritt materiale inngår også i dette bildet. Om tilstanden i påtalemyndigheten skriver Riksrevisjonen (2021):

> Påtalemyndighetens kompetanse innenfor digitalt politiarbeid og IKT-kriminalitet har over flere år vært påpekt som mangelfull i både politidistriktene og den høyere påtalemyndighet. Påtalejuristene i politidistriktene baserer seg i hovedsak på erfaringsbasert læring og tar i liten grad etter- og videreutdanning. Etterutdanningstilbudet ved Politihøgskolen for påtalejuristene er også svært begrenset og omfatter ikke opplæring innenfor digitalt politiarbeid.[271]

14.4 Betydningen av kontekstuell informasjon

I et eksperiment med 57 respondenter målte *Sunde* & *Dror* reliabilitet og bias i *avdekking* av digitale spor, *tolkingen* av sporene når de først er funnet, og *konklusjonen* med hensyn til skyld / uskyld.[272] 44 respondenter var fra norsk politi, inklusive noen påtalejurister. Eksperimentet viste generelt lav sannsynlighet for at to etterforskere vil avdekke de samme digitale sporene, tolke dem og konkludere likt. For ett av de digitale sporene mente én respondent at det indikerte skyld, mens en annen mente at det indikerte uskyld.[273]

---

[270] Fenomenet er omtalt av Helene O. I. Gundhus, Niri Talberg og Christin Thea Wathne (2019) i relasjon til data som brukes i politiets etterretningsvirksomhet, se pkt. 3.6 og s. 112. For databevis er det nærmere belyst i eksperimentet til Sunde& Dror omtalt nedenfor.

[271] Riksrevisjonen (2021) pkt. 2.1.1, s. 6. Se også Erlandsen (2019) som har undersøkt kvaliteten på påtalemyndighetens tolking av digitale spor (masteravhandling).

[272] Nina Sunde & Itiel E. Dror (2021). Med *bias* menes kognitiv slagside. Bias er en følge av tendensen til å operere med forenklingsstrategier i informasjonshåndtering, se Sunde, N. (2019b), s. 65. *Reliabilitet* i eksperimentet gjelder sannsynligheten for at flere personer med lik informasjon ville komme til likt resultat.

[273] Undersøkelsen ble en mediesak i The Guardian 31. mai 2021: *Digital forensic experts, prone to bias*, av Linda Geddes.

Eksperimentet viser at kontekstuell informasjon om saken, dvs. informasjon som ikke har betydning for det digitale sporets utsagnskraft eller pålitelighet, påvirker evnen og/eller viljen til å avdekke relevante spor, tolkingen og konklusjonen som trekkes. Kontekstuell informasjon kan f.eks. gjelde at siktede er - eller ikke er - tidligere straffet, at vedkommende er pågrepet, at politiet fant narkotika i forbindelse med ransakingen enda saken gjelder noe annet, at siktede har tilstått, osv. Funnene samsvarer med slike som er avdekket for andre typer kriminaltekniske spor.[274] Det viser blant annet at databevis ikke kan anses som spesielt «objektive» eller «sanne», og at det er behov for tiltak som minimerer sannsynligheten for feil.

Det har følgelig vært reist spørsmål ved om det er behov for organisatoriske tiltak som skjermer den som foretar analysen mot å motta kontekstuell informasjon. Man ser vel da for seg at analysen utføres av en dataetterforsker som ikke kjenner saken, men baserer seg på et mandat fra påtalejuristen/etterforskingslederen. Dagens modell med DPAen i en bistandsrolle kan sies å tilrettelegge for skjerming som nevnt, men det er ikke et definert tiltak som skal gjennomføres systematisk.

Det finnes også hensyn som taler mot at analysen skal være en skjermet funksjon ved DPAen. Det viktigste er at det i praksis viser seg å være vanskelig å utferdige mandater som er tilstrekkelig klare og presise. Selv om mandater brukes er det behov for atskillig kommunikasjon mellom dataetterforskeren og den taktiske etterforskeren som kjenner saken, for å avdekke relevante data. Skjerming mot kontekstuell informasjon er derfor et tiltak som vil være vanskelig å gjennomføre i praksis uten at det går ut over analysen.[275]

Det synes følgelig å være mer hensiktsmessig å legge opp til at den taktiske etterforskeren utfører analysen, men stille krav til hvordan den skal gjennomføres, dokumenteres og presenteres. Dataetterforskerens rolle vil dermed primært bestå i å gi råd om hvordan analysen bør legges opp i lys av en vurdering av bevispotensialet. Videre vil dataetterforskeren ha en viktig rolle gjennom å vite hvordan analyseverktøyene fungerer, kunne utpeke de som er egnet for analysens formål, og informere om eventuelle begrensninger og usikkerhetsfaktorer. På den måten kan dataetterforskeren gi kompetansemessig støtte til den taktiske etterforskeren.

Det foreslås derfor ikke spesielle skjermingstiltak overfor den som utfører analysen.

---

[274] Sunde & Dror, *ibid.*
[275] Haraldseid (2021). Masteravhandling.

14.5 Etterforskingssirkelen og hypotesedrevet etterforsking

14.5.1 Rammeverket

Siktelsen er det viktigste «verktøyet» for å sikre målrettethet. Dette ble utdypet i punkt 8.2.4. Målrettethet må imidlertid ikke gå på bekostning av objektivitet, og analysens resultater må presenteres på entydig vis. Det beste tiltaket for å oppnå målrettethet, objektivitet, entydig presentasjon og gjennomgående kvalitetskontroll, synes å være at analysen systematisk integreres i «etterforskingssirkelen».[276] Etterforskingssirkelen er en anbefalt modell for informasjonsbehandling i etterforsking, som kan anvendes på etterforskingen som helhet, i avgrensede faser og ved utførelsen av bestemte arbeidsoppgaver.[277] I følge *Bjerknes & Fahsing* gir den «metodisk støtte for å kunne undersøke flere ting på en gang og samtidig opprettholde fokus og kvalitet.»[278] Metodikken er basert på de engelske «kjerneordene» [279]

Collect: Samle inn alle tilgjengelige og antatt relevante data.

Check : Kontrollere data for relevans, nøyaktighet og pålitelighet.

Connect: Analysere og koble data fra forskjellige kilder.

Construct: Konstruere alle relevante og konkurrerende forklaringer (hypoteser) fra de tilgjengelige data.

Consider: Vurdere hvordan man kan teste alle forklaringer gjennom rettet informasjonsinnsamling egnet både for verifisering og falsifisering.[280]

Consult: Konsultere andre som kan mate inn ny kunnskap og utfordre egne synspunkter.

---

[276] N. Sunde (2017; 2019b), Haraldseid (2021).
[277] Bjerknes & Fahsing (2018) s. 102-103. Forfatterne presenterer etterforskingssirkelen deskriptivt, dvs. som en «modell» av hvordan politiets informasjonsbehandling i straffesaker faktisk skjer. Men metodikken er ikke implementert i alle politidistriktene og følges ikke konsekvent. Den er derfor mer nærliggende å oppfatte normativt, dvs. som en retningslinje for beste praksis.
[278] Bjerknes & Fahsing (2018), s. 105.
[279] *Ibid.*, s. 102-103.
[280] Eivind Kolflaath (2019) påpeker forskjellen mellom forskning og etterforsking. En etterforskingshypotese gjelder «et konkret fortidig forhold», og kan *styrkes* eller *svekkes.* Hypotesen er ikke egnet for verifisering eller falsifisering slik som naturvitenskapelige hypoteser, som gjelder «universelle utsagn eller teorier om generelle sammenhenger». Den hypotetisk-deduktive metoden er således ofte uegnet for etterforskingshypoteser (Kolflaath særlig på s. 439-443).

Formålet er å sørge for at etterforskingen fremskaffer et så korrekt bilde som mulig om de faktiske forhold, og dermed bidrar til å realisere det straffeprosessuelle prinsippet om materiell sannhetssøken.[281]

14.5.2 Objektivitet

Kjelby skriver at objektivitetsprinsippet blant annet har betydning for «tolkingen av de innhentede bevisene».[282] Analysen bør utføres i henhold til krav om strukturert hypotesebruk, dvs. at det skal arbeides med minst to hypoteser, hvorav én som går ut på at siktede er skyldig, og en annen som gjelder at vedkommende er uskyldig. Det skal hele tiden letes aktivt etter opplysninger som kan peke mot andre forklaringer enn at siktede er skyldig. Riksadvokaten presiserer:

> Selv om etterforsking skal være målrettet, tilsier kravet til objektivitet at det på *et hvert trinn* under saken må utvises både evne og vilje til å vurdere den fra ulike innfallsvinkler og hypoteser. Alle bevis som innhentes må undergis faglige og kritiske vurderinger, og det må utvises åpenhet for nye opplysninger samt vilje til å revurdere tidligere teorier og oppfatninger. Arbeidet skal ikke låses i én hypotese og rettes inn mot å få denne bekreftet uten blikk for andre forklaringer. *Det må tvert imot letes aktivt etter holdepunkter i faktum som kan peke mot alternative og konkurrerende forklaringer.* Eventuelle innvendinger mot eller avvikende synspunkter om etterforskingen eller saksbehandlingen for øvrig skal ikke bare tolereres, men etterlyses, og *møtes med anerkjennelse, åpenhet og konstruktive tiltak*. Dette stiller krav til profesjonalitet og videreutvikling av en politi- og påtalekultur som verdsetter åpenhet og upartiskhet.[283]

I tillegg er evaluering av bevis er et tiltak som styrker objektivitet i analysen. Evaluering anbefales for databevis som er komplekse eller av sentral betydning i alvorlige saker (se punkt 5.4.4.3). Også evaluering involverer bruk av hypoteser, men disse skal utformes med tanke på å teste bevisets verdi for en omstendighet som er relevant i etterforskingen. Evaluering gjelder ikke hvorvidt beviset styrker eller svekker etterforskingshypotesene, men bevisets styrke i forhold til det faktum det er ment å belyse.

Både *riksadvokaten* (sitatet over) og *Bjerknes & Fahsing* understreker at en *second opinion* er essensielt for å sikre objektivitet, og dermed kvalitet. Forskning støtter dette.[284] I

---

[281] De opplyser at etterforsking er «en kontinuerlig innsamling og vurdering av spor og informasjon» (s. 48), og redegjør for innslaget av vurderinger i alle sakens faser (s. 49-50).
[282] Kjelby Påtalerett pkt. 3.3.4 s. 287.
[283] Riksadvokaten (2018) pkt. 4.7.1. Utreders uthevinger.
[284] Sunde & Horsman (2020); og masteravhandlingene N. Sunde (2017; 2019b); Haraldseid (2021); Jahren (2020).

etterforskingssirkelen ivaretas behovet for kritisk gjennomgang av trinnet «*consult*». Videre fremheves *vurderingers* betydning for hvilken retning en etterforsking tar, og for utfallet.[285] I tillegg anses trinnet «*connect*», som går ut på å «analysere og koble data», som kritisk fordi

> den oppsummerer hva etterforskingen nå mener å vite eller ikke vite, og danner derfor utgangspunkt for resten av prosessen. Etterforskerne må altså være ytterst kritiske på dette punktet og *aller helst sørge for at noen utfordrer vurderingene med jevne mellomrom* (…).[286]

14.6 Forslag til tiltak

Det er klare holdepunkter for at dagens praksis ved analyse av sikrede data, verken er tilstrekkelig målrettet eller utføres med tilstrekkelig kvalitet. Dette kan gå ut over tolking av bevis, og hvordan bevis dokumenteres og presenteres. Til tross for dataenes tilsynelatende objektivitet, har bevishåndteringsprosessen store subjektive innslag.[287] Det foreslås derfor retningslinjer for noen tiltak som kan styrke målrettethet, objektivitet og grunnlaget for kontradiksjon.

14.6.1 Krav til analysen

Analysen skal være målrettet og legges opp på en måte som er egnet til å belyse sakens informasjonsbehov. Analyserapporten bør redegjøre for hvordan analysen ble innrettet og avgrenset sett i forhold til ransakingsbeslutningen. Den må også redegjøre for eventuelle feil eller problemer som kan ha påvirket analysen.

Analysen skal utføres under hensyn til objektivitet, og derfor baseres på bruk av hypoteser. Analyserapporten bør opplyse hvilke hypoteser som har vært brukt, og de digitale sporene må henføres til de respektive hypotesene.

Databevis som er komplekse eller har stor betydning for sakens utfall, bør kvalitetssikres gjennom evaluering som beskrevet i punkt 5.4.4.3. Eventuell usikkerhet knyttet til de digitale sporene, bør angis på entydig måte, uavhengig av om evaluering er gjennomført.

14.6.2 Fagfellevurdering av analysen

I tråd med prinsippet om at en ny kritisk vurdering kan tjene som en kvalitetssikring, anbefaler *Sunde & Horsman* rutinemessig gjennomlesing av analyserapporter.[288] Gjennomlesingen bør

---

[285] Bjerknes & Fahsing (2018) opplyser at etterforsking er «en kontinuerlig innsamling og vurdering av spor og informasjon» (s. 48), og redegjør videre for innslaget av vurderinger i alle sakens faser (s. 49-50)
[286] *Ibid.* s. 107. Utreders utheving.
[287] Ryser et al. (2020) s. 3; Sunde & Dror (2019).
[288] Sunde & Horsman (2020).

gjøres av en annen etterforsker («fagfelle») og særlig kontrollere (i) hvorvidt rapporten uttrykker grad av usikkerhet på entydig måte, (ii) hvorvidt databevisene er evaluert når det har vært behov for det, og (iii) om rapportskriver har holdt seg innenfor grensene for sin datatekniske kompetanse, eller trekker konklusjoner om forhold som ligger utenfor kompetansen. Dette er en kontroll med overholdelse av det kriminaltekniske prinsippet om at en *forensic practitioner* skal kjenne grensene for sin kompetanse og rapportere innenfor disse grensene.[289] Krav om fagfellevurdering operasjonaliserer riksadvokatens retningslinjer og etterforskingssirkelens *consult.* Det samsvarer også med *Kvalitetsveilederen for kriminalteknisk etterforsking* (som formelt ikke gjelder for elektroniske spor), som sier at «rapporter og dokumentasjon av undersøkelsene [skal] etterkontrolleres og godkjennes av minst en kvalifisert person i politidistriktet.»[290]

Ved fagfellevurderingen har kravet om skjerming fra kontekstuell informasjon noe for seg. Hvis mulig bør fagfellen følgelig være en som ikke har kjennskap til saken.

14.6.3 Påtalemessig kontroll av bevisets pålitelighet

Påtalemyndighetens bevisbyrde omfatter også bevisets pålitelighet. Riksadvokaten presiserer påtalejuristens plikt til å «foreta en grundig og selvstendig gjennomgang av bevisene».[291]

> Ved bevisvurderingen handler det ikke bare om å være kritisk til eksisterende eller manglende informasjon i det endelige beslutningsgrunnlaget, men også – og kanskje i enda større grad – å være spørrende og kritisk til prosessen hvor bevisene sikres. Mangler ved prosessen, eller manglende notoritet om den, påvirker verdien av bevisene. Bevissthet om dette er en forutsetning for å kunne oppfylle kravet om objektivitet og opplysning av saken som ligger i straffeprosessloven §§ 55 [a] og 226.[292]

For å kunne forvisse seg om databevisets pålitelighet, må påtalejuristen aktivt ettergå grunnlaget for hvordan det materialiserte seg. Det må spørres etter alternative tolkninger/forklaringer/mulige feilkilder. Når det gjelder et drapsvåpen eller fingeravtrykk, vil påtalejuristen vite hvor det ble funnet og sikret, og hvordan dette ble utført.[293] Tilsvarende krav til kunnskap bør stilles for analysen, dvs. hvordan de sikrede dataene ble funnet, og hva som kan sluttes av dem.

---

[289] Se ovenfor i punkt 14.3.
[290] Politidirektoratet (2012) pkt. 6.
[291] Riksadvokaten (2018) pkt. 4.7.3, s. 23.
[292] *Ibid.*
[293] *Id.*

Spesielt når det gjelder databevis kan påtalejuristens kvalitetssikrende funksjon anses å være av vesentlig rettssikkerhetsmessig betydning, siden verken forsvareren eller dommeren har bedre forutsetninger å kontrollere bevisets pålitelighet, heller tvert imot.

Mason & Seng har foreslått et generelt krav om at den som fører beviset bør ha plikt til å dokumentere påliteligheten.[294] I norsk rett følger det av gjeldende prinsipper for bevisførsel og -vurdering at kritiske spørsmål ikke bare kan gjelde bevisets innhold, men også påliteligheten. Det kan lede til at påtalemyndigheten må føre bevis for påliteligheten. Spørsmålet er imidlertid om det er behov for å gå lenger og pålegge påtalemyndigheten plikt til på eget initiativ å gå god for påliteligheten. Begrunnelsen er at de andre aktørene kan mangle forutsetninger for å stille kritiske spørsmål som kan belyse dette. Med mindre påtalemyndigheten pålegges ansvar for å belyse påliteligheten risikerer man at den ikke undergis reell kontradiktorisk behandling, noe som kan svekke rettssikkerheten. Et plikt som nevnt kan dessuten virke bevisstgjørende med hensyn til risikofaktorene knyttet til databevis.

Det foreslås derfor i tråd med *Mason & Sengs* forslag, retningslinjer om at påtalemyndigheten av eget tiltak plikter å dokumentere databevisets ekthet, redegjøre for eventuelle endringer i beviset og forklare dem på grunnlag av en pålitelig metode, og videre, at bevishåndteringskjeden er ubrutt, og at teknikkene som ble brukt til å sikre og analysere dataene har vært testet og var egnet for formålet. [295] I utgangspunktet kan dette gjøres ved påtegning på sluttrapporten (se utredningen punkt 5.3), og følges opp under hovedforhandlingen dersom det er behov for det.

Kravene er i samsvar med de krav som oppstilles for å anse dataetterforskingsprosessen som forsvarlig (*forensically sound)* (se punkt 5.2 og 5.3), og bør følgelig være ivaretatt. Den påtalemessige kontrollen bør derfor ikke innebære en stor byrde i tillegg til den vanlige arbeidsbelastningen. Et vilkår om at den påtaleansvarlige skal gå god for behandlingsmåten og dokumentasjonen vil primært ha som formål å styrke den påtalemessige bevisstheten om betydningen av de nevnte faktorene. I tillegg vil det gi et strukturert grunnlag for kritiske spørsmål fra forsvareren og dommeren, noe som effektiviserer hensynene til kontradiksjon og sakens fulle opplysning, jf. strpl. § 294. Den påtalemessige kontrollen må fremgå av dokumentasjonen.

---

[294] Mason & Seng (2017b) s. 352 flg.
[295] *Ibid.*

14.7 Konklusjon – forslag

I tråd med punkt 14.6 foreslås det retningslinjer for analyse som metodisk støtte for objektivitet og kvalitet, og påtalemessig kontroll av bevisets pålitelighet.

15. Innsynsretten i sikringskopien

Kontradiksjon og partslikhet er rettigheter som er garantert av Grunnloven § 95 og EMK artikkel 6 om rettferdig rettergang. Partslikhet innebærer at partene skal ha «samme stilling med hensyn til å fremføre sin sak, begrunne sitt syn og til å imøtegå den annen parts argumentasjon.»[296] Kontradiksjon er retten til å ta til gjenmæle. Rettighetene forutsetter innsyn i sakens dokumenter. Innsynsretten er således en grunnleggende prosessuell rettighet og en forutsetning for at siktede skal ha «reell mulighet til å forberede sitt forsvar og imøtegå anklagen.»[297] Advokatforeningen omtaler innsynsretten som

> en av de viktigste operasjonelle rettighetene som tilligger mistenkte/tiltalte, og helt konkret den sentrale forutsetningen for å ivareta retten til kontradiksjon – både på mistankestadiet og under hovedforhandlingen: Retten til å begjære etterforskningsskritt, til å føre egne bevis og til å eksaminere vitner på en meningsfull måte blir umulig å utøve uten innsyn i saken.[298]

Innsynsretten under etterforsking følger av strpl. § 242, og suppleres etter at tiltale er tatt ut, av strpl. §§ 264, 264 a, 267 og 269 tredje ledd, som pålegger påtalemyndigheten å opplyse om hvilke bevis man vil føre og eventuelle endringer i bevistilbudet. Av EMK artikkel 6 følger rettigheten av nr. 3 (b), som sier at den anklagede skal få tilstrekkelig tid og *muligheter* til å forberede sitt forsvar.

15.1 Gjeldende rett

Innsynsretten gjelder «sakens dokumenter», se strpl. § 242 (etterforskingsstadiet) og strpl. § 264, 264 a og 267 (etter at tiltale er tatt ut). Innsynsrettens omfang avhenger således av innholdet i dokumentbegrepet. Utgangspunktet er at alle dokumenter som er blitt til eller fremkommet under etterforskingen av saken som tiltalen gjelder, omfattes.[299] Dette gjelder blant annet alle dokumenter som er tatt i beslag. For data gjelder innsynsretten de som konkret

[296] Straffeprosessutvalget (2016) pkt. 5.3.8, s. 143.
[297] Kjelby (2019) pkt. 7.1, s. 339.
[298] Advokatforeningen (2017) pkt. 3.6.1, s. 14.
[299] Kjelby (2019) pkt. 7.2.1, s. 340. Lyd- og videofiler mv. omfattes etter gjeldende rett av lovens dokumentbegrep (Prop. 147L (2012-2013) s. 27).

er vurdert som relevante, og besluttet beslaglagt (HR-2018-1901-U avsnitt 19). Høyesterett la vekt på at

> Situasjonen er ikke ulik den som foreligger ved manuelle søk, for eksempel under politiets ransaking av et forretningslokale. Også da kan en stor dokumentmengde ha blitt gjennomgått, med det resultat at bare enkelte dokumenter er beslaglagt.[300]

I den nevnte saken hadde Økokrim sikret data hos tiltalte, en medtiltalt og to foretak, til sammen ca 8,6 millioner filer. Innsynsspørsmålet gjaldt dataene sikret hos den medtiltalte og foretakene. Saksforholdet svarte således til det i Rt. 2011 s. 1188, hvor innsynsretten i medtiltaltes data ble ansett å gjelde data som var «hentet ut» av sikringskopien. 2018-kjennelsen klargjorde hvordan uttrykket «hentet ut» var å forstå, og konklusjonen var som nevnt at beslagsvilkårene må være oppfylt, og beslutning om beslag truffet. I tillegg omfatter innsynsretten søkekriteriene som har vært benyttet, dataenes egenskaper og hvor de ble funnet.[301]

Av 2018-kjennelsen fremgår det at Økokrim først hadde foretatt et datauttrekk basert på målrettede søk, og deretter gjennomgått uttrekket manuelt for å vurdere relevansen konkret for hvert dokument. Forsvareren hadde begjært innsyn i hele datauttrekket, dvs. også i data som etter en konkret vurdering var funnet ikke å være relevante. Forsvareren begrunnet det med faren for at politiet i sine søk overser relevante dokumenter. Dessuten hindret det tiltaltes mulighet for å se dokumenter i en annen sammenheng enn politiet. Svakhetene gjorde seg særlig gjeldende ved store datamengder. Høyesteretts ankeutvalg mente imidlertid at dette ikke var spesielt for ransaking av en sikringskopi, og at det «også vil være situasjonen ved manuell ransaking.» Hensynet kunne derfor ikke føre til at alle dokumenter politiet får treff på ved sine søk, går inn i sakens dokumenter, uten noen nærmere vurdering. [302] I tillegg ble det med henvisning til Rt. 2011 s. 1188 avsnitt 40-46, vist til de sterke personvernhensyn som gjør seg gjeldende for materialet som er sikret hos andre enn tiltalte, og hensynet taushetsplikten.[303]

Etter gjeldende rett er innsynsretten således begrenset til å omfatte opplysninger som er positivt utskilt fra den sikrede datamengden gjennom beslag. I tillegg omfattes søkekriteriene som ble brukt i analysen mv. Det fremgår for øvrig at tiltalte hadde tilgang på sine egne data (avsnitt 21).

---

[300] HR-2018-1901-U avsnitt 18
[301] Rt. 2011 s. 1188 avsnitt 44.
[302] HR-2018-1901-U avsnitt 7 og 22.
[303] *Ibid.*, avsnitt 20-21.

I ettertid - i 2019 - har EMD avsagt dom i saken *Sigurdur Einarsson og andre mot Island*.[304] Dommen synes å gi innsynsretten noe videre omfang enn det som følger av 2018-kjennelsen.

15.2 EMD-dom: *Sigurdur Einarsson og andre mot Island*

Einarsson-dommen gjelder et meget stort databeslag som blant annet inneholdt 20 millioner epost. Bakgrunnen var den islandske finanskollapsen på slutten av 2010-tallet, og de fire klagerne var blitt dømt til fengselsstraffer på 4 til 5 år for økonomisk kriminalitet.

Den sikrede datamengden *(«the full collection of data»)* var for stor til uten videre å kunne analyseres for å finne bevis. Politiet hadde innledet med å foreta datauttrekk basert på søkeordlister. Uttrekket ble merket elektronisk *(«tagged documents»)*, og gjennomgått for å avdekke materiale som kunne ha forbindelse med etterforskingstemaet *(«documents that might have relevance to the case»)*.[305] Det som ble antatt å kunne være relevant ble merket på nytt og innlemmet i etterforskingsdokumentene (*«the investigation file»)*. Ved gjennomgangen brukte politiet automatiske søkemetoder og manuelt gjennomsyn.[306]

I tillegg fantes det en kategori bestående av det elektroniske materialet påtalemyndigheten førte som bevis i den islandske straffesaken *(«the evidence in the case»).* Bevisene var hentet fra etterforskingsdokumentene.[307]

Klagerne hadde fått kopi av alle data som var sikret hos dem selv. Tvisten gjaldt data som var sikret hos tredjepersoner, så vidt forstås hovedsaklig hos Kaupthing. Saksforholdet ligner derfor på Rt. 2011 s. 1188 og HR-2018-1901-U. Klagerne var gitt innsyn i opplysningene som var innlemmet i etterforskingsdokumentene *(the investigation file»)*, og i sakens beviser *(the evidence in the case»)*.

Klagerne mente at de ikke hadde fått tilstrekkelig mulighet til å forberede sitt forsvar, jf. EMK artikkel 6 nr. 1, jf. nr. 3 (b), for det første fordi de ikke hadde fått full tilgang til det totale sikrede datamaterialet *(the full collection of data)*, og for det andre, fordi de ikke hadde fått tilgang til den delen av bruttouttrekket som var funnet å være uten tilknytning til etterforskingstemaet. Klagerne anførte at dette brøt med partslikhetsprinsippet som sier at siktede skal ha samme mulighet som påtalemyndigheten til å få tilgang til og identifisere bevis.

---

[304] Dom av 4. juni 2019, klagesak nr. 39757/15
[305] *Einarsson* avsnitt 16.
[306] *Einarsson* avsnitt 16 og 88.
[307] *Ibid.*

15.2.1 Ikke uinnskrenket rett til innsyn i sikringskopien.

EMD tok utgangspunkt i at at lik tilgang til bevisene er en grunnleggende forutsetning for rettferdig rettergang, likevel slik at rettigheten ikke er absolutt.[308] Det kan finnes konkurrerende hensyn som taler mot eksponering av bevisene, slik som hensynet til nasjonal sikkerhet, vitnebeskyttelse, eller behov for hemmelighold av visse politimetoder. Inngrep i innsynsretten må imidlertid være strengt nødvendig («strictly necessary») og ulemper for siktede må balanseres ut gjennom rettslig overvåking av prosessen. Saken reiste ikke spørsmål om påtalemyndigheten hadde tilbakeholdt bevis i strid med disse prinsippene.

Kravet om fullt innsyn i sikringskopien ville eksponere uidentifiserte data som ikke hadde inngått i bruttouttrekket. Om dette uttalte EMD at situasjonen kunne sammenlignes med *«any other evidence which might have existed but had not been collected by the prosecution at all»*.[309]

Data som politiet *ikke* hadde sett på ble således ansett som ethvert bevis som kunne ha eksistert, men som av en eller annen grunn ikke hadde blitt sikret av politiet. Dette svarer til Høyesteretts resonnement i HR-2018-1901-U avsnitt 18, sitert i punkt 15.1. Siden påtalemyndigheten ikke hadde kunnskap om innholdet, forelå det ikke noe informasjonsovertak overfor forsvareren. Det var ikke tale om tilbakeholdelse av bevis. Implisitt var kravet til partslikhet ivaretatt.[310]

EMD legger således, i likhet med norsk rettspraksis, opp til at det ikke gjelder en ubeskåret innsynsrett i en sikringskopi med data sikret hos en tredjeperson.

15.2.2 Rett til innsyn i data politiet har sett på

For kravet om innsyn i opplysninger som var blitt vurdert og ikke funnet å være relevante, mente EMD at det stilte seg annerledes, fordi etterforskerne og påtalemyndigheten rent faktisk hadde gjort seg kjent med innholdet.[311] Selv om materialet *a priori* ikke var relevant for saken, var vurderingen foretatt av påtalemyndigheten alene uten involvering av forsvareren, og uten rettslig kontroll.[312]

---

[308] *Einarsson* avsnitt 85.
[309] *Einarsson* avsnitt 90.
[310] *Ibid.*
[311] *Einarsson* avsnitt 91.
[312] Det latinske *«a priori»* kan oversettes med *«åpenbart»*, noe som må bety at etterforskerne med en rask kikk kunne slutte at de omhandlede dokumentene ikke var relevante for saken.

EMD siterte *Rowe and Davis mot Storbritannia:*

> A procedure, whereby the prosecution itself attempts to assess the importance of concealed information to the defence and weigh this against the public interest in keeping the information secret, cannot comply with the above-mentioned requirements of Article 6 § 1.[313]

Til dette kom at forsvareren heller ikke hadde fått lister over bruttouttrekket. For dataene som var blitt ansett *ikke* å være relevante hadde politiet fjernet den elektroniske merkingen, og følgelig mistet oversikten over hvilke data man hadde vurdert med negativt utfall. For å kunne etterkomme innsynskravet måtte analysen vært repetert fra begynnelsen av, noe som ble ansett å være nærmest umulig og uansett enormt ressurskrevende.

Når EMD kom til at artikkel 6 likevel ikke var krenket, skyldtes det at det islandske straffeprosessuelle systemet inneholdt viktige prosessuelle garantier. For det første forelå en rett til å begjære tilgang til *«the full collection of data»*, og få begjæringen behandlet av en domstol. For det andre forelå en rett til å begjære nye etterforskingsskritt, herunder nye søk i datamaterialet. Når klagerne hadde unnlatt å benytte disse mulighetene kunne det ikke statueres noen krenkelse.

Klagerne hadde dessuten løpende fått tilsendt dokumentlister og oversikter med sammendrag av innholdet i etterforskingsdokumentene. EMD la også vekt på at klagerne ikke på noe tidspunkt hadde spesifisert hva slags type bevis de mente var viktig å avdekke og kunne virke til deres gunst.[314] Artikkel 6 kunne ikke forstås å gi siktede rett til til å «gå på fisketur» i datamaterialet, dvs. å kreve nye søk uten å konkretisere hva formålet skulle være.

15.3 Betydningen for norsk rett

15.3.1 Data politiet ikke har sett på

Norsk rettspraksis og EMD er på linje i det at data politiet ikke har sett på, ikke omfattes av innsynsretten. Dvs. at data som nevnt ikke er å anse som «ubearbeidet materiale» som det i henhold til rettspraksis skal gis innsyn i.[315]

15.3.2 Data politiet har sett på

Einarsson går imidlertid noe lenger enn Høyesterett i å gi innsynsrett. I henhold til *Einarsson* omfatter innsynsretten alle data som er vurdert av politiet, uavhengig av om utfallet ble positivt

---

[313] Storkammerdom 16. februar 2000 (saknr. 28901/95). Sitat fra avsnitt 63.
[314] *Einarsson* avsnitt *92.*
[315] Kjelby (2019) s. 341, med henvisning til KK-praksis.

(beslag) eller negativt (ikke relevant). Overført på HR-2018-1901-U betyr det at tiltaltes krav om innsyn i Økokrims datauttrekk som ble gjennomgått manuelt, skulle vært gitt medhold. I stedet ble innsynsretten begrenset til å gjelde beslaglagte data.

Helt klar er *Einarsson* likevel ikke, for det første fordi *Rowe and Davis* som ble sitert, gjaldt tilbakeholdelse av bevis i en situasjon hvor interesseavveiningen gjaldt forholdet til «public interest». Det var ikke tilfelle i *Einarsson.* Det virker også inkonsistent at EMD på den ene siden aksepterte at påtalemyndigheten foretar en foreløpig gjennomgang av sikringskopien *(«sift through information»)* for å redusere datamengden til håndterlig størrelse.[316] Det som påtalemyndighetem da får innsyn i omfattes ikke av innsynsretten. På den andre siden kom EMD til at innsynsretten omfattet dokumenter som åpenbart *(a priori)* ikke var relevante, utelukkende fordi de tilfeldigvis fantes i bruttouttrekket. Dette kunne like gjerne vært ansett som et ledd i datareduksjonen som må til for å kunne lete systematisk etter bevis.

Dommen etterlater derfor uklarhet om når politiets undersøkelser må anses som så intense at dokumenter må sies å være vurdert, og dermed være gjenstand for innsynsrett. Det er heller ikke utelukket at en ordning med god notoritet som sørger for at forsvareren får detajert informasjon om politiets metode for å redusere datamengden, søkekriteriene som har blitt benyttet, supplert med informasjon om de var velegnede eller ikke, vil kunne være tilstrekkelig i forhold til EMK artikkel 6.

Alt i alt er det noe usikkert hvor stor vekt *Einarsson* isolert sett bør tillegges. EMD er åpenbart i en fase hvor retningslinjer stadig må skapes for å løse spørsmål forårsaket av datateknologien, og har lite praksis av samme type å bygge på. Det må forventes å skje en betydelig rettsutvikling på området, en utvikling som vil henge sammen med utviklingen i nasjonalt regelverk, de teknologiske løsningene som brukes i bevishåndteringen og politiets metodiske fremgangsmåte. To anførsler i *Einarsson* som ikke ble direkte besvart er tegn på dette.

Den ene anførselen gjaldt at etterforskingsdokumentene ikke ga tilstrekkelig mulighet for å forberede forsvaret, fordi tilgang til dem ble gitt sent i prosessen. Dette fratok forsvarer mulighet for øve innflytelse på påtalemyndighetens vurderinger.[317] Etter norsk rett ville man i utgangspunktet ikke vunnet frem med dette, fordi påtalemyndigheten har ansvaret for å

[316] *Einarsson* avsnitt 90.
[317] *Einarsson* avsnitt 67.

tilveiebringe bevisene og skal være objektiv. Dertil er beviskravet strengt og påtalemyndigheten har bevisbyrden.

Tanker om at forsvareren bør gis en større rolle i forbindelse med analysen har imidlertid begynt å fremkomme. EMD fremholder i *Einarsson* at

> det i prinsippet er en viktig rettssikkerhetsgaranti at forsvareren gis mulighet til å være involvert i definisjonen av kriterienes som bestemmer relevans.[318]

Den engelske *Search Warrants* rapporten fremholder også betydningen av å samarbeide med forsvarer, og *N.Sunde* og *S. Haraldseid* trekker frem det samme spesielt relatert til analysen.[319] Formålet er å påse at alle omstendigheter til gunst for siktede er hensyntatt. Begrunnelsen er risikoen for tekniske og ikke-tekniske feilkilder, og at både forsvareren og retten reelt sett er i svak posisjon til å kontrollere grundigheten i bevishåndteringen og bevisenes pålitelighet. Forslaget om at påtalemyndigheten bør ha plikt til på eget tiltak å kontrollere databevisenes pålitelighet, er et tiltak for å avbøte dette, se punkt 14.6.3, men det kan også være behov for andre tiltak. For det andre anførte klagerne at påtalemyndigheten hadde et *de facto* monopol på avansert teknologi. Å ekskludere forsvarer fra selv å foreta søk underminerte retten til rettferdig rettergang.[320]

Problemstillingene som anførslene reiser kunne være velegnet for diskusjon i et nasjonalt tverrfaglig organ som foreslått i kapittel 20.

15.3.3 Betydningen av god notoritet

Spørsmålene i *Einarsson* og HR-2018-1901-U oppstår fordi data sikres forut for relevansvurderingen. I *Einarsson* konstaterte EMD at «the mass of information» var sikret "*indiscriminately*». Politiets adgang til å gjøre dette var ikke bestridt, og det er tale om samme fremgangsmåte som ble ansett å være akseptabel i *Wolland* (omtalt i punkt 7.2 og 17.6.3.2).

Den resulterende datamengden er for stor og ustrukturert til uten videre å kunne være gjenstand for søk etter bevis. I forbindelse med klargjøring og analyse må det følgelig legges en plan for *datareduksjon*, som bestemmer hvordan datamengden kan reduseres til håndterlig størrelse, samtidig som man unngår å utelate relevante opplysninger. Blant annet på denne bakgrunn

---

[318] *Einarsson* avsnitt 90: "…in principle an important safeguard in such a process would be to ensure that the defence is provided with an opportunity to be involved in the definition of the criteria for determining what may be relevant."
[319] UK Law Commission (2020) pkt. 17.151; N. Sunde (2019b) og Haraldseid (2021) masteravhandling.
[320] *Einarsson* avsnitt 68.

foreslår § 3-2 i utkastet til databevisforskrift at det skal «utferdiges en skriftlig plan for analysen som sikrer systematikk, målrettethet og objektivitet.» Innskjerping av notoritetskrav synes også nødvendig, jf. bl.a. Økokrim som nevner at det

> i liten grad er praksis i dag for utstrakt notoritet. Dette gjelder trolig både i forhold til mandat fra påtalejurist til etterforsker om rammer for beslagsgjennomgang, og for oppsummering fra etterforsker etter gjennomgang.[321]

Notoritet er en forutsetning for ivaretakelse av innsynsretten. I Ot.prp. nr. 24 (2002-2003) *Begrensninger i retten til dokumentinnsyn og bevisførsel*, understrekes det at «det er viktig at politiet og påtalemyndigheten systematisk og grundig dokumenterer sin fremgangsmåte i saken».[322] Det påhviler følgelig politiet og påtalemyndigheten en plikt til «å produsere dokumenter om etterforskingen, og resultatet av den og føre disse inn i sakens dokumenter».[323] Dokumentfortegnelsen er et utgangspunkt, som suppleres med sakens rapporter og bevisene som sådan. For databevis må dokumentasjonen suppleres og støttes av loggførings- og merkingsfunksjoner i dataverktøyene som brukes i analysen av sikringskopien. Forslaget til databevisforskrift § 3-4 gjelder de nevnte dokumentasjonskravene.

I *Einarsson* var notoriteten delvis gått tapt, noe som ville medført at retten til retterferdig rettergang ble ansett krenket, hadde det ikke vært for at det nasjonale rettssystemet sørget for kompenserende rettssikkerhetsgarantier. Det hadde også betydning at klagerne ikke ga en overbevisende grunn for innsynsbehovet. I en annen sak kan dette stille seg annerledes, og notoriteten kan da få utslagsgivende betydning.

15.4 Rett til sikringskopi av egne data

Som forklart i punkt 5.4.2, må man regne med at originale data endres etter sikringstidspunktet, og det må antas å være viktig for forsvareren å vite nøyaktig hvilke data som ble sikret hos klienten. Sikringskopien inneholder dessuten langt mer enn de dataene som plukkes ut og beslaglegges. Dersom siktede er fratatt databærerne kan han/hun ha behov for dataene som ikke vedrører straffesaken.

Hensynene tilsier at politiet bør pålegges en plikt til å gi siktede / forsvareren en kopi av dataene som er sikret hos siktede. Inntrykket er at dette skjer i praksis, men for å klargjøre og sikre at

[321] Økokrim (2017), s. 19. Se også masteravhandlingene til Jahren (2020) og Haraldseid (2021).
[322] Proposisjonen s. 73.
[323] Kjelby (2019) pkt. 7.2.1, s. 340-341.

praksis er ensartet foreslås en bestemmelse om dette i databevisforskriften. Plikten bør i utgangspunktet gjelde uavhengig av hva slags sak det er tale om, men dersom «sterke hensyn» taler mot oversendelse av sikringskopien bør innsynsretten kunne gjennomføres ved forsvarers oppmøte hos påtalemyndigheten, jf. påtaleinstruksen § 16-2.

15.5 Konklusjon - forslag

Innsyns- og notoritetsspørsmålene i dette kapitlet gir ikke foranledning til forslag om lovendringer, men til noen retningslinjer i databevisforskriften. Disse gjelder behovet for en plan for analysen (forskriften § 3-2), dokumentasjonskrav (forskriften § 3-4) og påtalemessig kontroll med databevisene (forskriften § 3-6). Dette ble behandlet i kapittel 14, og det vises til fremstillingen der. I tillegg er det behov for en forskriftsbestemmelse om sikringskopi til siktede/forsvareren, se databevisforskriften § 2-5.

Del VI. Beslagsfrie data

16. Advokatkorrespondanse

16.1 Mandatet

Mandatet ber utreder om å

> se nærmere på hvordan databeslag skal håndteres når hele eller deler av materialet som vurderes beslaglagt, er eller kan være underlagt beslagsforbud. Utreder bør i den sammenheng vurdere om det er grunn til å endre reglene om beslag i andre ting som kan være underlagt beslagsforbud, slik som papirdokumenter, lydopptak, telefonlogger mv.

16.2 Innledning – advokatkorrespondanse

Beslagsadgangen som følger av strpl. § 203 innskrenkes av strpl. § 204 første ledd, som bestemmer at det ikke kan tas beslag i «dokumenter eller annet hvis innhold et vitne kan nekte å forklare seg om etter strpl. §§ 117-121 og 124-125». Beslagsfriheten forutsetter at det taushetsbelagte materialet «besittes enten av den som kan nekte å forklare seg eller av den som har rettslig interesse i hemmelighold».

Spørsmål om håndtering av beslagsfrie data har særlig kommet opp i forbindelse med advokatkorrespondanse. Det følger av strpl. § 119, som er blant bestemmelsene § 204 viser til, at retten ikke kan ta imot forklaring fra nærmere oppregnede profesjonsutøvere om noe som er «betrodd dem i deres stilling.» Advokatbetroelser omfattes av bestemmelsen. Taushetsplikten

etter denne bestemmelsen er absolutt og straffesanksjonert, jf. straffeloven § 211. Retten kan ikke oppheve taushetsplikten og pålegge advokaten å forklare seg, f.eks. fordi straffesaken er spesielt alvorlig. Det gjelder kun ett unntak, nemlig at forklaringen behøves for å forebygge at noen uskyldig blir straffet, jf. strpl. § 119 tredje ledd. Forøvrig kan taushetsplikten bare bortfalle ved at den som har krav på hemmelighold (klienten) samtykker. I så fall kan dokumenter og data inneholdende slike betroelser beslaglegges. Videre gjør strpl. § 204 annet ledd unntak for betroelser mellom medskyldige, dvs. mellom en siktet advokat og medskyldig klient, se nedenfor.

HR-2018-104-A oppsummerer rekkevidden av taushetsplikten – og dermed beslagsforbudet – jf. strpl. §§ 119, jf. 204:

> Uttrykket «noe som er betrodd dem i deres stilling» omfatter etter Høyesteretts praksis alt det «advokaten i egenskap av sitt yrke og som ledd i et klientforhold innhenter eller får tilgang til på vegne av klienten», jf. Rt-2006-1071 avsnitt 21-22. Dette dekker også den omstendighet at det eksisterer et klientforhold, klientens identitet, timelister og annet som direkte eller indirekte kan gi grunnlag for slutninger om den kontakten advokaten har eller har hatt med klienten og andre i anledning oppdraget. Jeg viser til Rt-2010-1638, Rt-2012-868, Rt-2012-1601, Rt-2013-92, Rt2013-1206 og Rt-2013-1336. Høyesteretts praksis bygger dessuten på den gjennomgående forutsetningen at også informasjon om advokatens egne bearbeidelser av materialet, advokatens overveielser knyttet til gjennomføringen av oppdraget og de råd han gir klienten, er omfattet av beslagsforbudet, jf. Rt-2000-2167 og Rt-2010-740 avsnitt 31.[324]

16.3 Situasjonene

Problemstillingen som skal drøftes gjelder den rettslige fremgangsmåten for å behandle databevis som involverer advokatkorrespondanse. Spørsmålene oppstår i ulike kontekster.

16.3.1 Bevissikring hos advokat

Straffeprosessloven § 204 er ikke til hinder for at en advokat som selv er siktet for en straffbar handling, utsettes for ransaking og bevissikring i sitt kontor eller hjem. Politiet har for det første beslagsadgang i dokumenter/data som ikke har noe med advokatvirksomheten å gjøre. For det andre, dersom advokaten er siktet sammen med sin klient, kan betroelser dem imellom beslaglegges, se strpl. § 204 annet ledd. Bestemmelsen tolkes slik at beslagsadgangen kun gjelder betroelser som er relevante for forholdet beskrevet i siktelsen.[325] Andre betroelser

[324] HR-2018-104-A avsnitt 27.
[325] Rt. 2011 s. 296 avsnitt 41-44.

mellom advokaten og den samme klienten er taushetspliktige og beslagsfrie (forutsatt at det er betroelser i advokatvirksomheten. Kommunikasjon som faller utenfor advokatvirksomheten er uansett ikke beskyttet). For det tredje kan ellers beslagsfritt materiale beslaglegges dersom klienten samtykker. Dette kan være aktuelt blant annet dersom advokaten er siktet for et straffbart forhold begått mot klienten, f.eks. underslag av klientmidler. EMD-dommen *Robathin mot Østerrike* som er nærmere omtalt i kapittel 17, er en slik sak.

I alle tilfellene består problemet i at ransakingen, sikringen av data, klargjøringen og analysen, sannsynligvis vil eksponere opplysninger om klientforhold mv. som *ikke* er relatert til forholdet som etterforskes. For sikring av data fra en advokats elektroniske arkiv kan det være nær sagt umulig ikke å fange opp navn på klienter, da selv et kortvarig innsyn for å bestemme hvordan sikringen bør legges opp og avgrenses, vil kunne fange opp slikt. Det har politiet, forutsatt at loven tas på ordet, ikke har adgang til fordi klientforholdet som sådan er taushetspliktig (se sitatet i punkt 16.2). Det gjelder altså en generell presumpsjon for at politiet vil komme over beslagsfrie opplysninger under ransakingen og sikringen.[326] Problemet vedvarer under klargjøringen og analysen hvor det stadig er risiko for at taushetspliktige data eksponeres.

Norge har vært innklaget for EMD i to saker som gjelder bevissikring hos siktet advokat. Det er *Wolland mot Norge* (dom 17. mai 2018, saknr. 39731/12) og *Mirmotahari mot Norge* (avvisningsbeslutning 8. oktober 2019, saknr. 30149/19). EMD fant ikke noen krenkelse av av EMK artikkel 8 i disse sakene.

Gjeldende regulering av fremgangsmåten for å beskytte beslagsfrie data er likevel ikke tilfredsstillende. Den er svært kostnadsdrivende og tidkrevende, og etterforskingens fremdrift lider. I tillegg er den basert på analogisk anvendelse av en bestemmelse som ikke opprinnelig er utformet med problemstillingen for øye. Det har ledet til rettsusikkerhet og vært prosessdrivende. Spørsmålet er om det for fremtiden lar seg gjøre å finne en prosessuell ordning som ivaretar taushetsplikten og beslagsforbudet, samtidig som politiet gis bevistilgang ved etterforsking av en advokat som med skjellig grunn antas å ha begått straffbare handlinger.

Rettspraksis har lagt til grunn at loven ikke gir adgang til tredjemannsransaking hos advokat som ikke selv er siktet, for å finne bevis mot en klient som er under etterforsking, jf. strpl. § 192 tredje ledd, så dette reises ikke som problemstilling.[327]

---

[326] Presumpsjonen er lagt til grunn i Rt. 1996 s. 1081 og Rt. 2013 s. 968 avsnitt 23.
[327] Rt. 1996 s. 1081.

16.3.2 Tilfeldige funn

Ved klargjøringen og analysen av en sikringskopi som er sikret hos en person som ikke er advokat, kan det hende at politiet tilfeldig kommer over advokatbetroelser, fordi den siktede har eller har hatt et klientforhold til en advokat. Hvordan politiet i så fall skal forholde seg er ikke positivt lovregulert, og spørsmålet gjelder hva den fremtidige ordningen for å beskytte materialet bør være.

16.3.3 Anførsel om beslagsfrihet

En tredje situasjon er at den siktede (ikke advokat) som utsettes for ransaking og bevissikring, hevder at dataene inneholder advokatbetroelser. Situasjonen skiller seg fra den foregående, fordi politiet blir gjort oppmerksom på muligheten allerede på sikringsstadiet. Spørsmålet er om det bør medføre mer proaktiv beskyttelse av beslagsfrie data enn det som er aktuelt for tilfeldighetsfunn. EMD-saken *Saber mot Norge* (dom 17. desember 2020, saknr. 459/18) gjelder et slikt tilfelle. I denne saken konstaterte EMD krenkelse av EMK artikkel 8, se nærmere punkt 16.4.2.[328]

16.4 Tingrettens kontroll

16.4.1 Historikk

Straffeprosessloven inneholder ikke bestemmelser som direkte regulerer fremgangsmåten for bevissikring og beskyttelse av opplysninger som er undergitt *absolutt* beslagsforbud, herunder advokatbetroelser. Straffeprosessloven § 205 tredje ledd regulerer fremgangsmåten når beslagsforbudet er *relativt*, dvs. tilfeller hvor retten etter omstendighetene kan pålegge vitnet som har taushetsplikten likevel å forklare seg. Straffeprosessloven § 205 tredje ledd lyder slik:

> Dokumenter eller annet som besitteren ikke plikter å forklare seg om uten etter særskilt pålegg fra retten, kan ikke beslaglegges uten rettens kjennelse, hvis ikke slikt pålegg allerede er gitt. Dersom politiet vil ta med dokumenter til retten for avgjørelse av om beslag kan tas, skal dokumentene forsegles i lukket konvolutt i nærvær av en representant for besitteren.

Bestemmelsen tok opprinnelig sikte på ransaking i redaksjonslokaler, og ble tatt inn fordi lovgiver mente det var uheldig om politiet skulle få innsyn i slike dokumenter før retten hadde avgjort om den ville pålagt forklaringsplikt, jf. strpl. § 125 tredje, jf. første og annet ledd.[329]

---

[328] Norge har vært innklaget i en fjerde sak om databevis; *Bernhard Larsen Holding og andre mot Norge*, dom 14. mars 2013 (saknr. 24117/08). Saken gjelder Skatteetatens bevissikring i forbindelse med boketterssyn, og reiser ikke spørsmål om beslagsfrihet.

[329] Jahre (1990), s. 9-10 (Lovdata), med henvisning til Ot.prp. nr. 53 (1983–1984) s. 63. Se også Rt. 2013 s. 968 avsnitt 31 og 32.

Straffeprosessloven § 124 er en lignende bestemmelse for forretnings- og driftshemmeligheter. I tråd med dette bestemmer strpl. § 204 første ledd annet punktum at «[i] den utstrekning det etter [§§ 124 og 125] kan pålegges vitneplikt (…) gjelder dette tilsvarende for adgangen til beslag.»

Den foreskrevne fremgangsmåten går ut på at politiet skal forsegle dokumentene i nærvær av en representant for besitteren, og bringe det til tingretten. Politiet har ikke adgang til selv å sortere materialet. Tingretten må gjennomgå materialet og ta stilling til hva som ikke er omfattet av beslagsforbudet. Dette skal utleveres til politiet. For de dokumentene som i utgangspunktet er taushetspliktige, må retten vurdere om taushetsplikten skal oppheves, jf. strpl. §§ 124 og 125, slik at dokumentene (dataene) likevel kan tas i beslag. Materialet utleveres til politiet ved kjennelse. Politiet gjennomgår deretter dokumentene, og påtalemyndigheten treffer beslutning om beslag i det som er relevant, jf. strpl. §§ 205, jf. 203.

16.4.2 Bevissikring hos advokat og pretensjon om beslagsfrihet

I teori og rettspraksis har det vært lagt til grunn at de prosessuelle garantiene for materiale som er undergitt absolutt beslagsforbud, ikke kan være svakere enn når beslagsforbudet er relativt. Rettspraksis har således med støtte i Rt. 1986 s. 1149 og *Jahres* artikkel fra 1990,[330] anvendt strpl. § 205 tredje ledd analogisk, og etablert en obligatorisk prosessuell garanti som gjelder materiale sikret hos advokat (punkt 16.3.1), og når det pretenderes at materialet inneholder advokatbetroelser (punkt 16.3.3).

For databevis er den grunnleggende avgjørelsen Rt. 2011 s. 296 (avsnitt 37 flg.), en sak som gjaldt data sikret hos en advokat siktet for økonomisk kriminalitet. Avgjørelsen er fulgt opp i rettspraksis.[331] For pretensjon om beslagfrihet fremsatt under ransaking er den grunnleggende avgjørelsen Rt. 1986 s. 1149, fulgt opp for datatilfellene av HR-2017-111-A (avsnitt 42-45) og HR-2018-699-A (avsnitt 31). Norge har imidlertid blitt domfelt av EMD i en sak som gjaldt sikring av data fra smarttelefon, hvor smarttelefonens innehaver protesterte fordi den inneholdt advokatkorrespondanse (*Saber-saken* (2020)). EMD la vekt på at en straffeprosessuell ordning som hovedsakelig er utviklet i rettspraksis, basert på analogisk anvendelse av bestemmelser som ikke opprinnelig er utformet med tilfellet for øye, kan bli for uforutsigbar til å oppfylle kravet til klart rettsgrunnlag. I Sabers tilfelle ble den prosessuelle svakheten tydelig fordi prosedyren ble «kastet om» *(effectively reorganized)* av HR-2017-111-A, som ble avsagt mens

[330] *Ibid.*
[331] Rt. 2013 s. 968; HR-2018-104-A; -699-A og -1517-U.

Sabers data var til analyse. Uklarheter ved prosedyren resulterte også i manglende rettssikkerhet ved sorteringen av dataene, noe som fremgikk av politirapporten. Den norske straffeprosessloven manglet rett og slett veiledning med hensyn til hvordan beskyttelsen av det beslagsfrie materialet konkret skulle oppnås, og EMD mente i sum at det manglet tilstrekkelige prosessuelle garantier mot at advokatkorrespondanse ble eksponert i forbindelse med utsorteringsprosessen.[332]

Den prosessuelle reguleringen bør derfor revurderes. Inntil videre gjelder riksadvokatens midlertidige retningslinjer utarbeidet våren 2021. Retningslinjene regulerer ikke ransaking og sikring hos advokat, men de to øvrige situasjonene i tråd med føringene gitt i HR-2017-111-A.

Frem til nå har ordningen vært at tingretten skal kontrollere det sikrede materialet før politiet får anledning til å gjennomgå det. Oppgaven har gått ut på å legge materiale som er taushetspliktig i én kategori og det som ikke er taushetspliktig, i en annen. Det taushetspliktige materialet returneres til innehaveren, og det øvrige utleveres til politiet. For betroelser som nevnt i strpl. § 204 annet ledd, foretar retten i tillegg relevansvurderingen etter strpl. § 203, og beslutter beslag, jf. strpl. § 205 tredje ledd. Dette er et inngrep i påtalemyndighetens primærkompetanse, jf. strpl. § 205 første ledd, og gjøres for å sørge for strengest mulig overholdelse av det absolutte beslagforbudet. Tingrettens innsyn i materialet gjør inngrep i taushetsplikten, men ifølge Rt. 2011 s. 296, er dét mer betryggende enn om politiet forestår innsynet.[333]

16.4.3 Problemer vedrørende data

Den gjeldende ordningen forutsetter to arbeidsoperasjoner fra tingrettens side; en innholdsvurdering som ligger til grunn for kategoriseringen, og faktisk utskilling av materialet i forskjellige kategorier. Når det gjelder betroelser som nevnt i strpl. § 204 annet ledd, skal tingretten i tillegg foreta relevansvurderingen og beslutte beslag.

For papirdokumenter er innholdsvurderingen, inkludert relevansvurderingen, vanligvis en overkommelig oppgave, og den faktiske separasjonen uproblematisk. Når det gjelder data byr alle oppgavene på problemer og gjør den gjeldende ordningen uegnet.

---

[332] *Saber*, avsnitt 55-57.
[333] Rt. 2011 s. 296 avsnitt 38 *i.f.*

16.4.3.1 Innholdsvurderingen

Som redegjort for i utredningen punkt 5.4.2, er mengden sikrede data ofte svært stor. Tingrettsdommeren – eller en medhjelper oppnevnt av tingretten – kan ikke foreta en manuell vurdering av hver enkelt fil, fordi det ville sprenge tidsrammene for en etterforsking. I tillegg er datainnholdet fragmentert og komplekst. Innholdsvurderingen er derfor vesentlig mer kompleks enn for papirdokumenter. For å identifisere det taushetsbelagte materialet må man bruke elektroniske søk basert på lister med søkeord. Fremgangsmåten innebærer bestandig en risiko for at man ikke har identifisert alt. Dermed har det vært ansett problematisk å utlevere restmaterialet til politiet.

I tillegg er man avhengig av siktedes/forsvarerens bistand til å identifisere taushetspliktige data, i praksis ved at de utarbeider lister med søkeord, og utpeker hvilke deler av sikringskopien som er klart taushetspliktig og må skjermes mot innsyn. Disse opplysningene i seg selv kan avsløre klientforhold og konkrete advokatoppdrag, og skal ikke komme til politiets kunnskap. Samtidig er det viktig at politiet faktisk får tilgang på bevismateriale som ikke er taushetspliktig. Tingretten må følgelig påse at siktedes/forsvarerens søkekriterier mv., ikke unntar materiale i større utstrekning enn loven bestemmer.

16.4.3.2 Relevansvurderingen, jf. strpl. § 204 annet ledd

Tolkningen av strpl. §§ 204 annet ledd, jf. 205 tredje ledd, har medført at tingretten har fått en oppgave den mangler forutsetning for å løse selv. Innholdsvurderingen omtalt i det foregående er en kategoriseringsjobb. Spørsmålet om hvorvidt innholdet er advokatkorrespondanse eller ikke, er et oppdrag tingretten kan delegere, noe den også gjør ved oppnevnelse av medhjelper (sakkyndig). *Hjort* opplyser imidlertid at i praksis delegeres også relevansvurderingen til medhjelperen, noe hun kritiserer fordi den er rettslig og tilhører tingrettens alminnelige oppgaver. *Hjort* etterspør følgelig det rettslige grunnlaget for rettens delegering i dette tilfellet.[334] Etter utrederens oppfatning taler gode grunner for at denne ordningen endres, noe som i så fall må skje ved lovendring.

16.4.3.3 Faktisk separasjon av materiale

Det er også et problem faktisk å skille de kategoriserte dataene fra hverandre. Det lar seg vanskelig gjøre fordi dataene er «låst ned» i sikringskopien, og prinsipielt ikke kan skilles fra hverandre uten at sikringskopiens integritet ødelegges.[335] I følge *Hjort* løses problemet i praksis

---

[334] Hjort (2017) pkt. 5 s. 189.
[335] Se punkt 5.4.2

ved at utsortert materiale legges over på harddisk, én disk per kategori.[336] Så vidt forstås betyr det at data kopieres ut fra sikringskopien. Dermed holdes sikringskopien intakt. På den annen side kan det innebære at politiet ikke får tilgang på metadata som er viktige for å vurdere datainnholdets bevisverdi, og som kan være bevis i seg selv. I tillegg tapes konteksten som dataene lå i. Det vises til utredningen punkt 5.4.2 og 5.5.

17. En annen prosedyre

I det følgende presenteres forslag til en annen prosedyre for å verne taushetspliktige opplysninger samtidig som politiet får tilgang til bevis. Først skisseres ordningen, deretter drøftes den antatt rettslige holdbarheten. Kapittel 18 presenterer et alternativ.

En fremtidig prosedyre må ha til formål å være mer forutsigbar og effektiv enn dagens. Beskyttelsesnivået for taushetspliktige opplysninger bør ikke reduseres. Det kan imidlertid herske ulike syn på hvor effektiv dagens beskyttelse er, og også hvor effektiv den vil bli i fremtiden med den foreslåtte ordningen. For lovgiver er det med andre ord et vanskelig farvann å manøvrere i. Uansett må det tas hensyn til de spesielle omstendighetene som følger av at man har med en sikringskopi å gjøre.

Den foreslåtte ordningen er lagt opp som følger:

1) Sikringskopien holdes intakt.
2) Taushetspliktige opplysninger i sikringskopien sperres, de slettes ikke.
3) Sperring foretas av teknisk enhet i politiet.
4) Tingretten i samarbeid med forsvareren gir pålegg om sperring.
5) Politiet kan søke etter bevis i sikringskopien etter at taushetspliktige opplysninger er sperret. Politiet plikter av eget tiltak å sørge for sperring av taushetspliktige opplysninger.
6) Påtalemyndigheten foretar relevansvurderingen for betroelser som nevnt i strpl. § 204 annet ledd.
7) Søk og sperring skal være etterprøvbart med god dokumentasjon støttet av det tekniske systemet.

[336] Hjort (2019) s. 229. Se som eksempel HR-2018-104-A avsnitt 4 (og samme saksforhold HR-2018-699-A avsnitt 11) hvor mandatet beskrev fire kategorier.

17.1 Sikringskopien holdes intakt, taushetspliktige opplysninger sperres

Utredningen har redegjort for at sikringskopien er garantisten for databevisets ekthet og pålitelighet (punkt 5.4.2). Dette bør det ikke rokkes ved. I samme punkt og i punkt 5.6, er det forklart at sikringskopien har et fysisk og et logisk nivå. Sletting på fysisk nivå antas å gå ut over integriteten, mens sperring på logisk nivå ikke gjør det. Sperring gjør at data verken er søk- eller lesbare, men de er ikke fjernet. Utrederen tar imidlertid som utgangspunkt at sperring er tilstrekkelig for å beskytte beslagsfrie data.

Høringsrunden bør belyse hvorvidt sperring må antas å gi tilstrekkelig beskyttelse, og begrunne hvorfor det eventuelt skulle være utilstrekkelig. Hvis sperring er utilstrekkelig kan ikke politiet gis adgang til å søke etter bevis i sikringskopien som forutsatt i punkt 5, og man må velge en annen ordning enn den som foreslås i dette kapitet, se kapittel 18.

17.2 Sperring foretas av Teknisk enhet i politiet

Selektiv sperring av data krever teknisk kompetanse og god systematikk. I høringsuttalelsen til NOU 2016: 24 *Ny straffeprosesslov* illustrerer Økokrim kompleksiteten (i relasjon til innsynsretten, men det er også relevant for sperring):

> Innholdet i et dokument, for eksempel en epost, kan være beslagsfritt eller irrelevant for saken. Metadata, for eksempel når eposten er sendt eller når den er åpnet av mottaker, kan være et viktig bevis i seg selv. Spørsmålet er hvordan dokumentet skal håndteres og hva man skal gi innsyn i. Tilsvarende kan for eksempel deler av systemfiler som benyttes kan ikke nødvendigvis vises på skjerm eller legges i dokumentutdraget. De kan derfor vanskelig oversendes eller arkiveres på vanlig måte, men er likevel en del av sakens opplysninger.[337]

Teknisk kompetanse finnes hos DPAene i politiet og NC3-senteret ved Kripos. I tillegg finnes den i konsulentforetak, bl.a. i større revisjonsselskaper. Domstolene har ikke slik kompetanse. Etter dagens ordning bruker tingretten privat kompetanse som medhjelper/sakkyndig for å løse oppgaven.

I tråd med det som allerede gjelder for materiale innhentet ved kommunikasjonsavlytting, og Høyesteretts føringer i HR-2017-111-A og HR-2018-699-A, bør sperringen for fremtiden kunne skje av en teknisk enhet i politiet som er organisatorisk atskilt fra

[337] *Ibid.*

etterforskingsenheten.[338] Det er mulig at DPAene i distriktene er for tett på etterforskingsenheten, slik at oppdragene bør sentraliseres til NC3.

Forslaget er at Teknisk enhet skal motta sperringsoppdraget fra tingretten for så vidt gjelder data sikret hos advokat, og for øvrig fra påtalemyndigheten i samsvar med retningslinjene som gjelder i dag, se neste punkt.

17.3 Politiet gis adgang til å søke etter bevis i sikringskopien

For at en fremtidig prosedyre skal bli mer effektiv enn dagens, bør politiet få adgang til å søke etter bevis i sikringskopien i samsvar med lovens alminnelige ordning. Hvis det kan lede til at behovet for bolkevis forhåndskontroll og utlevering av materiale vil bortfalle eller i det minste vesentlig reduseres, vil man ha en langt mer effektiv ordning enn i dag. Høringsuttalelsene til NOU 2016: 24 *Ny straffeprosesslov* tyder på et stort behov for dette, jf. at det f.eks. kan ta over et år for tingretten å gjennomgå innholdet på en smarttelefon, og at det i saken behandlet i HR-2018-699-A, var avsagt 20 kjennelser om utlevering av data, uten at behandlingen ennå var fullført.[339]

I tillegg vil tilgangen til metadata medføre at politiet kan gjøre et grundigere etterforskingsarbeid enn det som er tilfelle når politiet får utlevert en disk med data som er kopiert fra sikringskopien.

Det som følgelig bør overveies er å lage en ordning som lar påtalemyndigheten søke etter bevis i sikringskopien. Dersom tingretten med forsvarerens bistand har utpekt hvilket materiale påtalemyndigheten ikke har rett til å få, og sperring er gjennomført, burde dette være akseptabelt. Løsningen vil ligge nær den Høyesterett har trukket opp i HR-2017-111-A avsnitt 42-43, og HR-2018-699-A avsnitt 31. Det fremgår at ved pretensjon om at dataene inneholder beslagsfrie opplysninger, eller politiet mer tilfeldig kommer over slikt materiale, plikter politiet umiddelbart «[å sortere] ut dataene uten forutgående innsyn». Dette gjelder tilfellene nevnt i punkt 16.3.2 og 16.3.3. Utredningens forslag går ut på at påtalemyndigheten i disse situasjonene har plikt til å gi pålegg til den tekniske enheten om å sperre dataene.

Det følger av høyesterettsavgjørelsene at påtalemyndigheten i tvilstilfelle kan sende opplysningene til tingretten for avgjørelse av om de er taushetspliktige eller ikke. Dette må

---

[338] HR-2017-111-A viser til fremgangsmåten for beskyttelse av materiale innhentet gjennom kommunikasjonskontroll, se kjennelsen avsnitt 42 og 43, hvor det vises til Rt. 2015 s. 81, Rt. 2015 s. 1456 og HR-2016-1086-U (Lime kjennelsene). Dette fikk tilslutning i HR-2018-699-A avsnitt 31.
[339] Kjennelsen avsnitt 9.

gjøres uten forutgående innsyn, alternativt må opplysningene umiddelbart slettes. Ordningen kan opprettholdes for fremtiden, med den forskjell at det er tale om sperring, ikke sletting.

Etter at sperring er gjennomført kan påtalemyndigheten fortsette å søke i sikringskopien. Dersom det gjøres nye funn av taushetspliktige opplysninger, plikter påtalemyndigheten på nytt å sørge for at teknisk enhet sperrer dem. Dette gjelder uavhengig av hvor dataene opprinnelig var sikret.

17.4 Bevissikring hos advokat: Tre alternativer

For beslag hos advokat er tingrettens assistanse nødvendig for å skjerme taushetspliktige opplysninger fra å tilflyte påtalemyndigheten. Nøyaktig hvilken type bistand det er behov for må antas å avhenge av konkrete omstendigheter, og nedenfor skisseres noen situasjoner.

17.4.1 Tingretten pålegger sperring i samarbeid med forsvareren

Med utgangspunkt i den gjeldende ordningen er det naturlig å foreslå at tingretten tillegges kompetansen til å gi pålegg om sperring av de taushetspliktige dataene. Årsaken er at utarbeidelsen av lister med søkeord og forslag til skjermingstiltak for å beskytte beslagsfrie data, kan avdekke klientforhold og konkrete oppdrag. Opplysningene må komme fra siktede og forsvareren, men skal ikke tilflyte påtalemyndigheten. Dermed må tingretten tre inn i stedet, i tråd med synspunktet i Rt. 2011 s. 296 avsnitt 38 *i.f.*

Tingretten må samtidig påse at siktedes/forsvarerens innspill ikke går lenger enn det som er nødvendig etter loven, og sikre påtalemyndighetens rett til å søke etter bevis som ikke er taushetspliktige. For dette formål må tingretten ha ransakingsbeslutningen og siktelsen til diposisjon.

Tingretten gir pålegg om sperring direkte til Teknisk enhet uten påtalemyndighetens mellomkomst. Når sperring er utført kan påtalemyndigheten søke etter bevis i sikringskopien. Dersom påtalemyndigheten etter sperring likevel kommer over taushetspliktige data skal disse sperres av eget tiltak, jf. punkt 17.3.

17.4.2 Tingretten utpeker det som kan beslaglegges

Det kan reises spørsmål ved om ordningen i forrige punkt i blant bør snus, slik at tingretten i stedet positivt skal identifisere hvilket materiale som kan utleveres til påtalemyndigheten, ikke hva som skal sperres. Fremgangsmåten kan tenkes å være hensiktsmessig i tilfeller hvor påtalemyndigheten er i stand til å individualisere og konkretisere bevisbehovet. I henhold til påtalemyndighetens spesifikasjoner, kontrollert av tingretten, pålegger tingretten Teknisk enhet

å kopiere disse dataene. Dataene som identifiseres av Teknisk enhet bør kunne utleveres direkte til påtalemyndigheten som kan arbeide videre med dem. Dersom påtalemyndigheten likevel kommer over taushetspliktige data, følges samme prosedyre som i punkt 17.3. Påtalemyndighetens spesifikasjoner bør sendes forsvareren til uttalelse, med mindre det er fare for bevisforspillelse eller andre unntak fra innsynsretten gjør seg gjeldende.

Sett fra påtalemyndighetens side er ulempen at man ikke får søke direkte i sikringskopien. Man får heller ikke alt som ikke er beslagsfritt, bare det som er identifisert gjennom søkekriterier relatert til siktelsen. Avhengig av omstendighetene kan dette likevel tenkes å være tilstrekkelig for bevisbehovet, og kunne gi etterforskingen raskere fremdrift dersom sperringsprosessen må antas å bli komplisert.

17.4.3 Hensynet til konkrete omstendigheter

I praksis må situasjonene antas å kunne variere mye. Eksemplene i det foregående er basert på at sikringen har skjedd ved speilkopiering, dvs. en bred sikringsform. Hvis sikringen derimot har skjedd målrettet slik at mengden taushetspliktige data må antas å være liten, er det ikke utelukket at ordningen nevnt i punkt 17.3 allerede i utgangspunktet bør anses tilfredsstillende. Det betyr i så fall at påtalemyndigheten foretar sperring etter eget tiltak. Som nevnt i punkt 5.6 kan sikring i noen grad skje målrettet, noe som i så fall burde forenkle den etterfølgende prosedyren.

Iblant kan det ligge til rette for både å foreta målrettet og bred sikring. Dette ble gjort i *Robathin mot Østerrike*.[340] Advokaten Robathin var siktet for økonomisk kriminalitet mot to klienter, og i medhold av rettens beslutning ransaket politiet kontoret, med Robathin, forsvareren og et uavhengig vitne fra advokatforeningen i Wien tilstede. Vitnets tilstedeværelse var et krav etter østerrisk lov.

Politiet innledet kopiering av alle data på Robathins datasystem. Vitnet fra advokatforeningen protesterte og viste til at det var uproporsjonalt siden mistanken begrenset seg til å gjelde kriminelle handlinger begått mot to nærmere angitte klienter. Det måtte følgelig være tilstrekkelig å kopiere data som hadde med dem å gjøre. Politiet ringte etterforskingsdommeren, som godkjente den brede sikringsformen (dommen opplyser ikke hvilken sikringsmetode som ble benyttet). Men politiet etterkom vitnets anmodning i tillegg. Løsingen ble således at dataene knyttet til de to klientene ble kopiert til en egen disk, og alle de øvrige dataene til en annen

[340] *Robathin mot Østerrike*, dom 3. juli 2012 (saknr. 30457/06) avsnitt 50.

disk.[341] Ved å bruke to sikringsformer sørget politiet for at den påfølgende analysen i første omgang kunne gjelde sikringskopien som gjaldt de to klientene og formodentlig inneholdt minst beslagsfritt materiale. Hvis bevisbehovet dermed var tilstrekkelig dekket, kunne man se bort fra, og dermed slette den andre kopien.

17.4.4 Konklusjon

I alle situasjonene som har vært nevnt synes tingrettens medvirkning å være nødvendig, enten for å beskytte siktedes /forsvarerens opplysninger fra å bli eksponert, eller for å gi påtalemyndigheten tilgang til bevismateriale under en viss kontroll. Samtidig varierer situasjonene mye. Det taler for at tingretten kan bestemme hvilken prosedyre som skal følges, dog slik at loven oppstiller alternativene for å sikre forutberegnelighet.

17.5 Egnet teknologi - en forutsetning for prosessuelle garantier

Den foreslåtte ordningen fratar tingretten oppgaven med å sortere materiale, henholdsvis mellom hva som er og ikke er taushetsbelagt. I tillegg forelås det å fjerne tingrettens oppgave med hensyn til å vurdere relevans og beslutte beslag i betroelser som nevnt i strpl. § 204 annet ledd. Dette er etterforskingsoppgaver som tingretten er påført gjennom rettspraksis, fordi man ønsket å etablere et ekstra sikkert vern for advokatbetroelser. Det er imidlertid tvilsomt at dagens ordning virkelig representerer en effektiv prosessuell garanti mot eksponering av advokatbetroelser.

Problemet med dagens ordning er at den i realiteten legger opp til manuell innholdskontroll med opplysningene. I møte med store datamengder er oppgaven nærmest ugjennomførlig. Den lar seg verken gjennomføre innenfor et tilfredsstillende tidsrom eller med tilstrekkelig god kvalitet. Høyesterett stiller imidlertid meget strenge krav til beskyttelsen, jf. HR-2018-699-A som oppsummerer beskyttelsesnivået slik:

- Beslagsforbudet er absolutt (avsnitt 40).
- Det er ikke rom for en situasjonsbestemt nyansering av taushetsplikten (avsnitt 43), dvs. at det ikke kan tas praktiske hensyn i den konkrete situasjonen (avsnitt 39 og 51).
- Det klare målet må være at alt som er beslagsfritt er luket ut før utlevering til påtalemyndigheten (avsnitt 49).

[341] Robathin avsnitt 10.

- Risikoen for at restmaterialet fortsatt inneholder taushetspliktig materiale må være lav (avsnitt 49).

Det mest tankevekkende punktet er kravet om at «Det klare målet må være at alt som er beslagsfritt er luket ut før utlevering til påtalemyndigheten». Vilkåret synes å være basert på en antakelse om at påtalemyndigheten faktisk ser på alt utlevert materiale. Antakelsen overser at påtalemyndigheten selv, i møte med store datamengder, må bruke målrettede søk for å finne bevis. Eksponering av taushetspliktige data avhenger av om de elektroniske søkene treffer dem, og analysen bør være innrettet på å unngå at så skjer. Dette bør fremgå av analyserapporten, og dokumenteres av logger. Lovens målsetting bør derfor være å sørge for sperring av data som åpenbart er beslagsfrie, jf. siktedes/forsvarerens innspill. Å gi pålegg om sperring i en dialog med siktede /forsvareren er en oppgave tingretten har forutsetninger for å utføre, sannsynligvis uten ekstern bistand. Etter sperring kan påtalemyndigheten søke i det resterende med sperringsplikt som nevnt i punkt 17.3.

For ytterligere å peke på svakheter ved gjeldende ordning, kan det nevnes at den fremstår som lite troverdig hva gjelder det påstått strenge beskyttelsesnivået. Det er tydeligvis urealistisk at alt beskyttet materiale lar seg identifisere og fjerne i forhåndskontrollen. I den ovennevnte 2018-kjennelsen avdekket man til tross for 20 utleveringskjennelser at ca 2% var taushetpliktig materiale, dvs. i overkant av 2000 filer. *Haaland* opplyser at det ikke finnes

> tilstrekkelige søkemetoder som luker ut alle opplysninger vernet av retten til konfidensiell rettslig bistand. Realiteten er derfor at politiet ved speilkopiering alltid får tilgang til taushetsbelagte opplysninger. Rettssikkerhetsgarantien som ligger i rettens gjennomgang, vil derfor ikke – per i dag – være en tilstrekkelig rettssikkerhetsgaranti til å verne om en absolutt rettighet.[342]

Manuell kontroll kan derfor ikke anses å være en effektiv prosessuell garanti. Videre er det problematisk at tingretten ikke utfører oppgaven selv, men delegerer den til en medhjelper/sakkyndig.[343] Problemet gjelder ikke bare det rettslige grunnlaget for delegeringen, men også at taushetspliktige opplysninger dermed spres til andre enn tingretten. Dette bryter med begrunnelsen for tingrettens kontroll, jf. Rt. 2011 s. 296, som sier at selv om tingrettens gjennomgang av materialet er et inngrep i advokatkonfidensialiteten, er dét mer betryggende enn at påtalemyndigheten gjør det.[344] Da fremstår det som et paradoks at kontrollen ikke lar seg

[342] Haaland (2019) pkt. 7.2.3 s. 203.
[343] Se utredningen punkt 16.4.3.2.
[344] Rt. 2011 s. 296 avsnitt 38 *i.f.*

gjennomføre innenfor domstolsapparatet som sådan, men at man må innhente kapasitet utenfra, med den spredningskonsekvensen det innebærer.

Gitt de store datamengdene som databærere inneholder, blir de sikrede datamengdene store, og tingretten har blitt påført en oppgave den på ingen måte er rustet til å utføre. Høyesterett som i Rt. 2011 s. 296 la oppgaven til tingretten, synes senere å ha fått betenkeligheter. I HR-2017-111-A kalles ordningen for en «særregulering» som ikke behøver utvides til «alle situasjoner hvor det oppdages advokatkorrespondanse i et større beslag.»[345] Høyesterett begrenset således rekkevidden av de tidligere avgjørelsene så langt man kunne. I tillegg bemerket førstvoterende i HR-2018-699-A at «[det nok er er slik] at Høyesterett i 2011-avgjørelsen ikke hadde for øye slike store databeslag som er tema i denne saken.»[346] Her peker Høyesterett således på kjernen i dagens problem.

Gjennomgang av store datamengder må skje strukturert og med god teknisk støtte. Det indikerer behov for en annen ordning enn dagens, som legger avgjørende vekt på dommerens individuelle vurdering av hvert dokument.

Når det gjelder tingrettens oppgave relatert til relevansvurdering og beslag i betroelser som nevnt i strpl. § 204 annet ledd, kan man tenke som følger: Ideelt sett bør ikke betroelser mellom medskyldige som ikke er relevante for etterforskingen, komme til påtalemyndighetens kunnskap. Samtidig må det antas å være viktigere at opplysninger om klientforhold og advokatoppdrag som er helt urelaterte til etterforskingen, ikke kommer til påtalemyndighetens kunnskap. Det som den fremtidige ordningen bør konsentrere seg om er å gjøre sperringen av taushetspliktige opplysninger så treffsikker som mulig, basert på så enkle kriterier som mulig. Det blir vanskelig dersom opplysninger fra ett og samme klientforhold skal vurderes konkret av tingretten for å skjelne mellom hva som er og ikke er relevant.

EMDs praksis kan ikke ses å stille krav om at retten skal gjennomgå dokumenter eller data som er sikret hos advokat, før påtalemyndigheten får tilgang på materialet.[347] I de to norske advokatsakene *Wolland* og *Mirmotahari* anså EMD riktignok ordningen med rettslig forhåndskontroll av de sikrede dataene som betryggende, men ga ikke uttrykk for at det var en betingelse. Av *Saber* kan man lese at det vesentlige er hvorvidt man har et lovbasert system

[345] Kjennelsen avsnitt 41.
[346] Kjennelsen avsnitt 36.
[347] F.eks. Petri Sallinen (2005); Smirnov (2007); Koleshnichenko (2007); Iliya Stefanov (2008), Robathin (2012).

som er utformet med sikte på dagens forhold, med prosessuelle garantier som er relevante for dagens forhold.

Dette inviterer til tilsvarende refleksjoner som for innsynrett og notoritet i utredningen punkt 15.3.2: Det må forventes en betydelig rettsutvikling hos EMD relatert til EMK artikkel 8 på dette området, en utvikling som vil henge sammen med utviklingen i nasjonalt regelverk, de teknologiske løsningene og den metodiske fremgangsmåten. Når det gjelder vernet mot innsyn i advokatkorrespondanse er selvsagt de prosessuelle garantiene spesielt viktige. Etter utreders syn er god og stabil teknologisk støtte, med gode funksjoner for dokumentasjon og logging av helt sentral betydning. Håndtering av store datamengder kan bare skje på betryggende vis med egnet teknologi.

Utredningens forslag begrenser kontrollen til noe tingretten antas å kunne håndtere, samtidig som det opprettes en prosessuell mekanisme som sørger for sperring uten at taushetspliktige opplysninger tilflyter påtalemyndigheten underveis i prosessen. Etter sperring vil ikke sikringskopien inneholde mer taushetspliktig materiale enn det som kan være tilfelle i enhver sak, hvor påtalemyndigheten allerede etter Høyesteretts retningslinjer er tillagt ansvaret for sperringen/slettingen. Det bør derfor kunne legges til grunn at den foreslåtte ordningen ikke svekker dagens beskyttelsesnivå.

Lovgiver må videre kunne legge til grunn at politiet disponerer egnet teknologi, *in casu* teknologi som sørger for sperring av taushetspliktige data på sikker og etterprøvbar måte. Derved kan den prosessuelle kontrollen effektiviseres uten at det går på bekostning av rettssikkerheten. Den foreslåtte ordningen antas således å gi en forutsigbar rettstilstand, effektive effektive prosessuelle garantier, og bidra til effektivitet i etterforskingen.

17.6 Spørsmål på sikringsstadiet – bevissikring hos advokat

17.6.1 Rettens forutgående beslutning – en viktig rettssikkerhetsgaranti

Den prosessuelle ordningen diskutert i det foregående inntrer i likhet med dagens, *etter* at dataene er sikret. I forkant er rettens kontrollfunksjon begrenset til å gjelde utferdigelse av beslutning om ransaking og sikring av data, jf. strpl. § 197. Påtalemyndighetens hastekompetanse, jf. strpl. § 197 annet ledd brukes visstnok ikke i advokattilfellene. Det er uansett klart at EMD legger stor vekt på rettens beslutning som rettssikkerhetgaranti.

17.6.2 Innsyn og speilkopiering hos advokat

Under ransakingen og ved sikringen av data har politiet frihet til å velge fremgangsmåte, hensyn tatt til nødvendighet og proporsjonalitet, jf. strpl. § 170 a. På sikringsstadiet oppstår to spørsmål med betydning for fremgangsmåten ved sikring av data hos advokat. Det ene gjelder at sikringen kan nødvendiggjøre et innsyn i databæreren som kan eksponere taushetspliktige opplysninger. Det andre gjelder hvorvidt det er adgang til å bruke speilkopiering siden metoden også tar med taushetspliktige opplysninger.

Spørsmålene henger til dels sammen. Ad innsynsspørsmålet er utgangspunktet at politiet bør begrense innsynet i databæreren så mye så mulig, for ikke å eksponere taushetspliktige klientforhold mv. En nærliggende mulighet er i så fall å stenge ned advokatens datasystem og foreta speilkopiering.

Speilkopiering som metode for å minimere innsyn, krysses av spørsmålet om hvorvidt speilkopiering hos advokat i det hele tatt er lovlig; for det første fordi advokatkonfidensialiteten er vernet av Grunnloven § 102 og EMK artikkel 8, og beslagsforbudet er absolutt; for det andre fordi det må anses som uproporsjonalt gitt at den taushetspliktige mengden kan være stor enda bevisbehovet bare gjelder en begrenset mengde opplysninger. *Haaland* mener således at speilkopiering ikke kan tillates hos advokat så lenge man må gå ut fra at de taushetspliktige opplysningene ikke lar seg fjerne fullstendig fra sikringskopien.[348]

17.6.3 Drøftelse

17.6.3.1 Utgangspunktet

Den prosessuelle ordningen på sikringsstadiet bør neppe løses utelukkende ut fra hensynet til vern om advokatkonfidensialiteten. Det er også behov for å strafforfølge kriminelle handlinger begått av advokater alene eller med medskyldige klienter. Høyesterett har som nevnt trukket en grense ved tredjemannsransaking hos advokat,[349] men kan ikke ses å ha hatt innvending mot fremgangsmåten for bevissikring hos advokat i de tillatte tilfellene. Det skjer også en streng prøving av nødvendigheten og proporsjonaliteten ved behandlingen av ransakingsbegjæringen.

Heller ikke EMD har hatt innvendinger mot speilkopiering hos advokat. Etter EMDs praksis i tilknytning til artikkel 8, er det først og fremst av betydning hvorvidt rettens beslutning er begrunnet i konkrete opplysninger, og er klart avgrenset for å sikre at innsamlingen av bevis

[348] Haaland (2019) pkt. 7.2.3 s. 203.
[349] Se punkt 16.3.1.

gjelder et klart formål.[350] Videre er det viktig med tilstedeværelse av et kompetent vitne som påser at politiet holder seg innenfor rammene av ransakingsbeslutningen og begrenser seg til det nødvendige.[351] Dette er ikke et vilkår etter norsk rett, men bør nok innføres, f.eks. med krav om tilstedeværelse av en representant fra Advokatforeningen. Det bør i så fall skje med en tilføyelse i loven, f.eks i strpl. § 204. Endelig tillegges notoriteten stor betydning, slik at politiets fremgangsmåte er etterprøvbar.

17.6.3.2 Sikringsmetoden

Når det gjelder valg av sikringsmetode redegjør utredningen punkt 5.6 for noen muligheter for *å skjerme* taushetspliktige data fra å bli sikret i forbindelse med ransaking. Det ble imidlertid presisert at skjerming forutsetter forhåndskunnskap om lokaliseringen, enten av de relevante eller de beslagsfrie opplysningene. Et visst innsyn er uansett nødvendig, noe som medfører risiko for at taushetspliktige opplysninger, f.eks. om klientforhold, eksponeres. Dersom lokaliseringen, f.eks. av relevante data, er ukjent, kan det være mulig å bruke målrettede søk, men også dette må antas å gi risiko for slikt innsyn.

Etter omstendighetene kan speilkopiering anses å gi *bedre* vern mot innsyn enn selektive kopieringsteknikker, noe som illustreres av *Wolland*-saken. Klageren (en siktet advokat) anførte at politiets speilkopiering av innholdet på datamaskinen hans var uproporsjonal, fordi politiet i stedet kunne ha nøyd seg med å kopiere filer identifisert ved målrettede søk basert på søkeord. På denne måten kunne politiet styrt utenom beslagsfritt materiale. Staten innvendte at å utføre søk som nevnt på klagerens datautstyr, uunngåelig og i stor utstrekning ville ha eksponert beslagsfritt materiale. Materialet ble bedre beskyttet ved simpelthen å bli kopiert og overlevert til tingretten, jf. strpl. § 205.

EMD konstaterte at speilkopiering ikke uten videre kunne sammenlignes med tilfeller hvor politiet tar med seg dokumenter «wholesale» og «indiscriminate», slik som i den eldre dommen *Miailhe mot Frankrike* (1993).[352] Tolletaten hadde tatt med seg all korrespondanse og alle dokumenter som de kunne finne - totalt 15 000 - uten å gjøre noen vurdering på stedet, noe

---

[350] *Iliya Stefanov* avsnitt 41 «According to the Court's case-law, search warrants have to be drafted, as far as practicable, in a manner calculated to keep their impact within reasonable bounds (see Van Rossem v. Belgium, no. 41872/98, § 45, 9 December 2004). *This is all the more important in cases where the premises searched are the office of a lawyer, which as a rule contains material which is subject to legal professional privilege* (see Niemietz, cited above, p. 35-36, § 37).” Utreders utheving.
[351] *Robathin* avsnitt 44; *Iliya Stefanov* avsnitt 43; *Smirnov* avsnitt 44
[352] Dom 13. februar 1993 (saknr. 12661/87).

EMD fant at ikke var akseptabelt.[353] EMD mente imidlertid at *Wolland* ikke lignet på *Miailhe*. I *Miailhe* var det tale om fysiske dokumenter, slik at en viss gjennomgang på ransakingsstedet for å begrense dokumentmengden, hadde vært mulig å gjennomføre. I *Wolland* hadde påtalemyndigheten gitt en saklig grunn for hvorfor speilkopieringen var nødvendig, og fremgangsmåten ble følgelig ansett akseptabel.[354]

Også i *Robathin* (omtalt i punkt 17.4.3) ble speilopieringen anført å være uproporsjonal. EMD tok ikke stilling til dette, men konstaterte krenkelse av EMK artikkel 8 fordi det østerrikske klageorganet ikke hadde gitt en klar og overbevisende begrunnelse for *hvorfor det hadde vært nødvendig* å kopiere alle dataene til Robathin når mistanken var klart avgrenset til å gjelde forbrytelser mot to klienter, og det vitterlig viste seg mulig å begrense bevissikringen til det som gjaldt dem. Med manglende begrunnelse var ikke den etterfølgende kontrollen effektiv, og inngrepet ble av den grunn ansett uproporsjonalt. Men av dette følger også at dersom klageorganet hadde gitt en overbevisende begrunnelse for den brede kopieringen, ville det ikke foreligget en krenkelse av EMK artikkel 8.

Av EMDs praksis fremgår det at speilkopiering er brukt også i andre advokattilfeller, uten at det i seg selv har vært gjenstand for kritikk. Det kan derfor ikke antas at speilkopiering hos advokat skulle stride mot EMK artikkel 8. Tvert imot må det legges til grunn at politiet har stor frihet ved valg av fremgangsmåte. Det vesentlige er hvorvidt fremgangsmåten er velbegrunnet og godt dokumentert.

17.6.3.2 Konklusjon

Konklusjonen er at både etter norsk rett og EMK er et visst innsyn på sikringsstadiet akseptabelt. Politiet har stor valgfrihet med hensyn til fremgangsmåten for bevissikring, men den må begrunnes og dokumenteres.

17.7 Beskyttelse av papirdokumenter, lydlogger mv.

Mandatet ber som nevnt utreder

> vurdere om det er grunn til å endre reglene om beslag i andre ting som kan være underlagt beslagsforbud, slik som papirdokumenter, lydopptak, telefonlogger mv.

Lydfiler som er sikret etter fremgangsmåten i punkt 5.4.2 og kapittel 11, er «nedlåst» i sikringskopien og omfattet av utredningens forslag til løsninger. For så vidt gjelder lydopptak

---

[353] *Miailhe*, avsnitt 39.
[354] *Wolland*, avsnitt 76.

og telefonlogger som er fanget opp ved kommunikasjonskontroll, er utskillingen - slik utredningen flere ganger har vært inne på - vesentlig enklere å utføre enn for data «nedlåst» i en sikringskopi. Det antas at for lydopptak og telefonlogger er muligheten for å slette data tilstede, uten at det går ut over de øvrige opplysningenes integritet, og da er det ingen grunn til å endre den gjeldende ordningen. Dersom det anses hensiktsmessig for fremtiden at opptak og logger som nevnt omfattes av den foreslåtte ordningen for sikringskopien, antas det å kunne gjøres med en henvisning i straffeprosessloven kapittel 16 a om kommunikasjonskontroll, til de bestemmelsene som utredningen foreslår (se punkt 17.9). Forskjellen vil være at materialet skal slettes, ikke sperres.

Det foreslås ikke at papirdokumenter omfattes av bestemmelsene som gjelder data. Beskyttelse av taushetspliktige papirdokumenter, helt eller delvis, antas fremdeles å kunne utføres av tingretten som en manuell ordning. Dette bør imidlertid klargjøres i loven, f.eks. med tilføyelse av et nytt ledd i strpl. § 205. Denne bestemmelsen bruker uttrykket «dokumenter eller annet», noe som har vært ansett å omfatte data. Det bør fremgå at det er tale om fysiske dokumenter eller lignende, og ikke data som beskyttes av egne bestemmelser.

17.8 Konklusjon – forslag

Nye bestemmelser i straffeprosessloven §§ 205 a og b.

Det foreslås to straffeprosessuelle bestemmelser som regulerer prosedyren for søk etter bevis i sikrede datamengder som kan inneholde data som er undergitt beslagsfrihet. Bestemmelsene foreslås innført som strpl. §§ 205 a og b, og gjelder henholdsvis påtalemyndighetens pålegg om sperring, og tingrettens beskyttelse av beslagsfrie data.

Nytt fjerde ledd i straffeprosessloven § 205

I tillegg foreslås et nytt fjerde ledd i strpl. § 205 som klargjør tingrettens oppgave for fysiske dokumenter mv. som omfattes av strpl. § 204. Dersom dokumentomfanget er stort bør tingretten ha adgang til å oppnevne medhjelper.

18. Et alternativt forslag

Ordningen foreslått i kapittel 17 avhenger av at sperring anses som en tilfredsstillende prosessuell garanti for ivaretakelse av taushetsplikten og beslagsfriheten. Dersom det ikke er tilfelle og sikringskopien uansett skal holdes intakt, må en fremtidig ordning gå ut på at påtalemyndigheten får utlevert opplysninger som er relevante for siktelsen, istedet for selv å kunne søke etter dem direkte i sikringskopien. Det vil også ha som konsekvens at

påtalemyndigheten må avstå fra sikringskopien dersom taushetspliktige opplysninger tilfeldig oppdages, og ved pretensjon om beslagsfrihet.

I så fall bør oppgaven med å forestå utsorteringen i sin helhet legges til domstolsapparatet. Det må være tale om en sentralisert enhet som mottar alle oppdragene, og er satt opp med tilstrekkelig teknologi og teknisk kompetanse, foruten nødvendig juridisk kompetanse til de rettslige vurderingene. Etter dette forslaget fratas den stedlige tingretten oppgavene som i sin helhet overføres til det sentrale domstolsorganet.

Det antas ikke å være hensiktsmessig å gå direkte løs på en ordning som nevnt, siden domstolsapparatet foreløpig ikke har et slikt organ. Ordningen foreslått i kapittel 17 kan derimot innføres umiddelbart, med teknologi og teknologisk kompetanse som allerede finnes i politiet. Det bør vurderes heller å la et nasjonalt organ som foreslått i kapittel 21, følge utviklingen og evaluere den foreslåtte ordningen, etter gjennomgang av behandlete saker. Det vil kunne bedre kunnskapsgrunnlaget om behovet for endringer.

Del VII. Diverse spørsmål

19. Proporsjonalitet, heving og lagring av databeslag

19.1 Proporsjonalitetsvilkåret

Sikringen av data er et tvangsinngrep som må være nødvendig og forholdsmessig i forhold til det som skal oppnås. Proporsjonalitetsvilkåret reiser imidlertid problemer langs to akser. Datamengdene som sikres av politiet er nærmest ufattelig store og bevisinnholdet utgjør bare en marginal andel. I *Einarsson* sikret politiet ca 20 millioner epost. 6500 av disse ble plukket ut som relevante. Det utgjør 0,03%.

I høringsuttalelsen til NOU 2016: 24 *Ny Straffeprosesslov* opplyser Økokrim at

> Størrelsen på dagens (og fremtidens) databeslag er i seg selv en utfordring. ØKOKRIM jobber aktivt for å begrense størrelsen på beslagene, men databeslag kan likevel bli på over 100 millioner individualiserte dokumenter/eposter. (…) I [2017] er så store beslag unntak, men ØKOKRIM mener det vil bli mer og mer vanlig i fremtiden pga. økt digitalisering.[355]

[355] Økokrim (2017).

Problemet har vært velkjent i en årrekke, f.eks. gjaldt Rt. 2011 s. 1188, 16 millioner datafiler. Saken behandlet i HR-2018-1901-U hadde sin bakgrunn i sikring av 8,6 millioner datafiler.

Hvorvidt det er mulig å innrette sikringen mer målrettet og avgrenset, har ikke utreder forutsetninger for å gå inn på. Det antas imidlertid å være behov for at lovgiver engasjerer seg aktivt i spørsmålet, og leter etter muligheter for å fremtvinge en reduksjon av omfanget. Problemet må muligens ses i sammenheng med lagringsspørsmålet nevnt i punkt 19.3, hvor det fremgår at Kripos har ønsket seg mulighet for fortløpende filtrering og sletting av overflødige data. Det kan være formålstjenlig ut fra tekniske og konstnadsmessige kriterier, men bør også vurderes normtivt som et spørsmål om proporsjonalitet.

Den andre aksen gjelder inngrepet i privatlivet. De omfattende datamengdene gir potensielt omfattende innsyn i privatlivet til dataenes innehaver og vedkommendes sosiale nettverk.[356] Smarttelefonen er et vanlig ransakingsobjekt i norske saker. I rapporten *«Mobile phone data extraction by police forces in England and Wales"* (2020) fra det engelske Information Commissioner's Office, sies det noe om inngrepets omfang og dybde:[357]

> Smartphone users each process around 1.9 GB per month (roughly twice the contents of the Encyclopedia Britannica). The extent to which these devices effectively record a user's everyday activities, whether it be their movements, their associations, their personal preferences, or the services they access online, is unprecedented. (rapporten punkt 1.2).

Hittil har politiets fremgangsmåter stort sett vært akseptert, muligens fordi det er vanskelig å fremme kritikk i møte med påstander om hva som er teknologisk nødvendig. Proporsjonalitetsspørsmålet er imidlertid brennbart også i Norge, noe som viste seg i reaksjonene etter bevisførselen i saken mot *Bertheussen* høsten 2020.[358] Se for eksempel *Per-Olav Sørensen* kronikk i Nettavisen 4.oktober 2020 (oppdatert 12. oktober 2020)

> I løpet av rettssaken som nå pågår har vi fått vite at PST vet når du åpner og lukker ytterdøren. Når du shopper i Sverige. Når du betaler kontant eller med kort. Når du setter seg i bilen. Hvor langt du kjører. Når du stanser. Hvor lenge du sitter i bilen før du går ut av den. Når du er på nett. Hva du søker etter på nett. Hvor lenge du er på nettsidene. Hvem du chatter med i en lukket privat gruppe.

---

[356] Dette er belyst for smarttelefoner av N. Sunde (2019a), se også utredningen punkt 3.2.3.
[357] Vist til i UK Law Commission (2020) kapittel 15.
[358] Oslo tingretts dom 15. januar 2021 (20-020518MED-OTIR/04). Om de elektroniske bevisene i saken, se I.M.Sunde (2021) *Bruken av elektroniske spor i etterforskning kan ha avgjørende betydning for domfellelser, men reiser også spørsmål om personvern*. Forskersonen.no, 18. januar 2021(https://forskersonen.no/kriminalitet-kronikk-meninger/kunne-laila-bertheussen-blitt-dømt-om-saken-skjedde -for-15-år-siden/1800215 (besøkt 26. februar 2021)).

> Hva du chatter med venner om. Når du tekster. Hva du tekster. Når du ringer. Når du beveger deg i eget hus, og ikke minst … den utrolige detaljen … hvor mange skritt du går inne i huset ditt.[359]

Proporsjonalitetsvilkåret bør derfor ha oppmerksomhet fremover, og foreslås fulgt opp av det nasjonale organet foreslått i kapittel 20.

19.2 Heving av beslag

Straffeprosessloven § 213 bestemmer at beslag skal heves så snart det ikke lenger er behov for det, og når saken er endelig avgjort. «Tingene» skal da returneres til eieren, med mindre de skal inndras eller utleveres til fornærmede, se strpl. § 214. Det kan være behov for å klargjøre hva disse pliktene innebærer for sikringskopien, som både inneholder data som er beslaglagt, og data som ikke er det.

Gjeldende bestemmelser er utformet med fysiske gjenstander for øye, dvs. slikt som ikke kan være på to steder samtidig. Det kan imidlertid data. Utredningen har dessuten foreslått at siktede/forsvareren tilsendes en kopi av sikringskopien som inneholder siktedes data (se punkt 15.4). Formålet var å tilrettelegge for kontradiksjon, men det fyller også hensynet bak tilbakeleveringsplikten. Unntak gjelder dersom innholdet er av en slik karakter at det må inndras. Dette blir likt som for fysiske objekter. Det er således først og fremst politiets adgang til å beholde sin kopi som må reguleres, se nedenfor.

Det foreslås ikke noen lovendringer på dette punkt.

19.3 Lagring av sikringskopien

Straffeprosessutvalget foreslo at lagring av bevismateriale burde reguleres i forskrift, og viste til at lagringsspørsmålet befant seg på et for detaljert nivå til å reguleres i selve loven.[360] Riksadvokaten var enig i behovet for regulering, og påpekte at lagring av bevismateriale er svært viktig i et rettssikkerhetsperspektiv. Riksadvokaten fremholdt at

> [f]lere straffesaker er gjenåpnet med fellende dom som resultat, etter at sporene i sakene er reanalysert på bakgrunn av ny teknologi og kunnskap.[361]

---

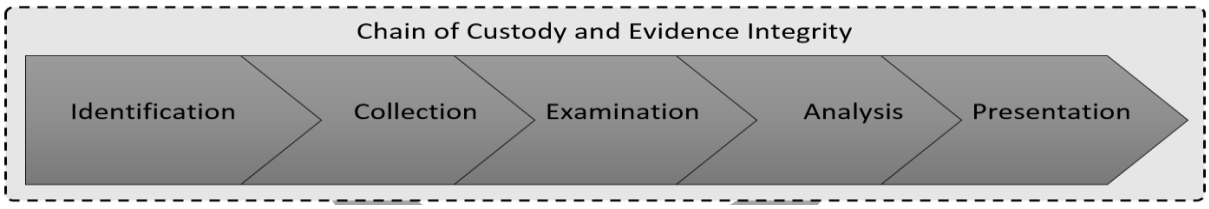
[359] https://www.nettavisen.no/nyheter/the-ways-norway-sees-laila-anita-bertheussen/s/12-95-3424027498 (besøkt 26. februar 2021). Se lignende betraktninger fra Petter Bae Brantzæg *Saken mot Laila Bertheussen viser til fulle hvor lite privatliv vi har i 2020*, Aftenposten 21. september 2020, kronikk. (https://www.aftenposten.no/meninger/kronikk/i/Kyv1LE/saken-mot-laila-bertheussen-viser-til-fulle-hvor-lite-privatliv-vi-har) (besøkt 26. februar 2021).
[360] NOU 2016: 24 *Ny straffeprosesslov* pkt. 13.2.2.2.
[361] Riksadvokaten (2017), kapittel 7.

Dette hensynet gjør seg også gjeldende for databevis, hvor nye analysemetoder og styrket teknologisk kompetanse kan tenkes å gi ny informasjon. Etter en undersøkelse av saker vurdert av Gjenopptakelseskommisjonen for straffesaker, reiser *Nina Sunde* spørsmål om hvorvidt risikoen for systematiske feil vedrørende databevis kan utelukkes. Av 100 saker som kommisjonen hadde besluttet *ikke* å gjenåpne, forekom databevis mye hyppigere enn i de sakene som kommisjonen hadde gjenåpnet. I tillegg var misforståelser og feilvurderinger av databeviset ofte anført som grunn for gjenåpningsbegjæringen.[362] På denne bakgrunn synes at databevisforskriften å burde inneholde en lagringsbestemmelse.

For datamateriale er det imidlertid et godt spørsmål hvor mye som bør lagres. Data som er plukket ut og beslaglagt er lagt til sakens dokumenter, og i strengt terminologisk forstand er det kun dette som diskuteres når man taler om lagring av «bevis». Men i tillegg har man selve sikringskopien som inneholder mengder metadata og kontekstuelle data som kan være viktige for vurderingen av databevisene som er plukket ut, foruten irrelevant informasjon og iblant, beslagsfrie data.

Prosessen kan illustreres slik:

Figur 3:



Flaglien (2018)

Søk etter datakilder

Fysisk ransaking: Sikring - tilrettelegging - **Ransaking** av sikringskopien

Oppbevaring av sikringskopi

Beslag: Relevante data - **Sakens dokumenter**

Dataene vil jevnlig inneholde personopplysninger, ofte sensitive, jf. politiregisterloven § 7, og lagringen må ha lovhjemmel for å være lovlig. Dette følger av Grunnloven §§ 102, jf. 113 og

[362] N. Sunde (2019c).

EMK artikkel 8. Når dataene ikke lenger er nødvendige for formålet, skal de slettes eller sperres, jf. politiregisterlovgivningen.

Det enkleste hadde vært å innføre en bestemmelse som ga hjemmel for å bevare sikringskopien, slik at alle dataene var tilgjengelige for fremtiden. Det medfører imidlertid lagring av datamengder som etterhvert blir ganske enorme, og spørsmålet er om det bør gjelde noen begrensninger eller prosedyrer for sletting. Kripos har således etterlyst

> et regelverk som gir mulighet til å gjøre et relevant utvalg av de digtale bevisene som samles inn, enten ved en fortløpende filtrering eller ved å hente ut de data som antas å være av interesse for å opplyse saken, Informasonen som filtreres bort, bør slettes, eller helst ikke lagres i det hele tatt, hvis mulig.[363]

Spørsmålet er altså komplekst. Det har ikke vært mulig innenfor utredningens rammer å gå nærmere inn på spørsmålet, men også lagringsspørsmålet kunne som et utgangspunkt være egnet for behandling i en et tverrfaglig organ som foreslått i neste kapittel.

20. Et nasjonalt tverrfaglig organ

I høringsuttalelsen til den nye straffeprosessloven foreslo Økokrim oppnevnelse av et «teknologiforum», som

> arbeider løpende med aktuelle problemstillinger, kan bidra til utviklingsarbeid og fremtidsrettede løsninger, samtidig som det vil sikre en helhetlig tilnærming.[364]

Dette er et godt forslag som bør følges opp. Som nevnt i punkt 2.2 er det vanskelig å utvikle et regelverk som fullt ut og på lengre sikt, ivaretar bredden og kompleksiteten i problemstillingene som følger med databevis. Den engelske *UK Law Commission* foreslår således etablering av et organ som nevnt, som kan behandle problemstillinger på tvers av gjeldende kategorisering av tvangsmidler. Organet skal ikke selv utrede alle problemene, men kunne løfte blikket og bidra til at regelverkets forskjellige deler utvikles i felles retning, som gjør det klart og sammenhengende, ivaretar personvern og proporsjonalitet, og oppstiller prosessuelle garantier som er relevante for dagens problemer.[365]

[363] Kripos (2017) s. 5.
[364] Økokrim (2017) s. 4, se også s. 19.
[365] UK Law Commission (2020), kapittel 18.

Straffeprosessloven preges av uklare grensesnitt mellom tvangsmidlene, foruten at det også kan være behov for å vurdere om politiets metoder bør suppleres i forhold til i dag. Svakheter i lovverket går ut over effektiviteten, og kan svekke personvern og rettssikkerhet. Dette er bakgrunnen for utredningens forslag om å integrere hemmelig ransaking av databærer i bestemmelsene om dataavlesing. Det er tale om et meget inngripende skjult tvangsmiddel som kan anses som en variant av dataavlesing, men som likevel ikke har vært undergitt etterkontroll av KK-utvalget.[366]

Høringsuttalelser til Straffeprosessutvalgets utredning har etterlyst behovet for en helhetlig gjennomgang av bestemmelsene om ransaking og beslag, utleveringspålegg og kommunikasjonskontroll, romavlytting og dataavlesing. Et fremtidig regelverk kunne f.eks. gå vekk fra det vanskelige skillet mellom data som er lagret vs. data under overføring. Man kunne tenke seg at relevante skillelinjer heller gikk etter hvorvidt en metode er åpen eller skjult, retter seg mot én eller flere, er kortvarig eller vedvarende, avhenger av manipulasjon eller datainnbrudd osv. I lys av internasjonaliseringen både av kriminaliteten og kriminalitetsbekjempelsen, er det også behov for en løpende diskusjon om hva som er «grunnleggende norske verdioppfatninger», jf. Rt. 2002 s. 1744. Dette fordi bevis tilflyter norsk politi fra utenlandsk politi, til tross for at fremgangsmåten ikke er tillatt etter norsk rett. *Encrochat* og *Trojan Shield* er slike eksempler, hvor utenlandsk politi i den ene saken hacket og avlyttet en chatserver brukt av mange, og i den andre saken distribuerte krypterte håndsett med chattjeneste politiet selv kontrollerte, til forbrytermiljøer. Det at metoden ikke er tillatt etter norsk rett betyr ikke nødvendigvis at lovgiver har tatt et aktivt standpunkt imot, men kan skyldes at man ikke har tenkt på og vurdert muligheten. Det er hele tiden behov for å følge med og ha et aktivt forhold til hvor grensen går for bruk av bevis som er fremskaffet på denne måten.[367]

Organet behøver ikke nødvendigvis begrense seg til å gjelde etterforsking, også teknologibruk i forebyggende øyemed blir et stadig mer presserende tema.[368] Det kunne inviteres til åpne drøftingsmøter og økt transparens om teknologiutnyttelsen i politiet. På sikt må transparens antas å være viktige for opprettholdelsen av befolkningens tillit til politiet. Til organet bør det også være knyttet et etisk oppdrag og en konsultasjonsmulighet, siden nye spørsmål foranlediget av de teknologirelaterte mulighetene stadig vil dukke opp, og loven ikke bestandig

[366] Se kapittel 12.
[367] Se også problemstillinger vedrørende «digital etterforsking» beskrevet av av Kjetil Haukaas (2019) s. 285 flg.
[368] I.M. Sunde (2019b; 2020).

gir klare svar. Utreder kjenner til at en ordning etter disse linjer er opprettet i politiet i Nederland, og anses som en strategisk prioritet.

Utredningen har vært innom noen problemstillinger som kan være egnet for videre diskusjon av et tverrfaglig organ som nevnt:

- *Skytjenester:* Bevissikring fra skytjenester reiser mange problemer som kunne være verdt en utredning i seg selv. Utviklingen bør følges nøye.
- *Tingenes internett:* Når «alt» står i nettverk kan nettverksanalyse være en metode for bevissikring. Dette gjøres i dag såvidt forstås med hjemmel i bestemmelsene om ransaking og beslag, men kan også anses som en form for kommunikasjonskontroll. Spørsmålet er om gjeldende regulering er hensiktsmessig.
- *Forsvarerinvolvering:* Spørsmål om behov for økt forsvarerinvolvering ble reist i punkt 15.3.2, mend et ble ikek konkludert. Problemstillingen kunne trenge et mer solid kunnskapsgrunnlag.
- *Tydeligere skille mellom digital kriminalteknikk og dataetterforsking?* I dag er det ikke et tydelig skille mellom dataetterforsking og digital kriminalteknikk. DPAens rolle kan i praksis anses å være noe uklar, til tross for beskrivelsen i Politidirektoratets styringsdokument.[369] Det gjelder særlig rollen ved analysen av de sikrede dataene, se utredningen punkt 14.3. Det er heller ikke avklart hvilke kompetansekrav som skal stilles for å kunne anses som ekspert. I Nederland har man f.eks. et register til bruk for domstolen ved oppnevnelse av sakkyndige for slike spørsmål (Netherlands Register of Court Experts https://english.nrgd.nl/). For fremtiden kan det være formålstjenlig å trekke opp et klarere skille mellom hva som er dataetterforsking og hva som er vitenskapelige undersøkelser av digitale spor, slik at feltet kommer mer på linje med grensedragningen mellom kriminalteknikk og etterforsking som gjelder for andre spor.
- *Proporsjonalitetsvilkåret*: Det vises til kapittel 19.1
- *Lagringsspørsmålet:* Det vises til kapittel 19.3.

21. Økonomiske og administrative konsekvenser

Utredningen har forutsatt at politiet disponerer egnet teknologi og kompetanse som kan følge opp utkastet til regelverk. Dette er nok ikke helt realistisk for øyeblikket, men i lys av Riksrevisjonens kritikk (2021), skal tiltak for å bedre situasjonen være iverksatt. Den foreslåtte

[369] Politidirektoratet (2017).

reguleringen i seg selv kan derfor ikke ses å medføre kostnader. Administrativt inneholder den forslag om sentralisering av funksjonen Teknisk enhet, ved behandling av beslagsfrie data.

Del VIII. Forslag til lov og forskrift

Forslag til endringer i straffeprosessloven

Ransaking av databærer og brukerkonto

Straffeprosessloven § 192

Ref. utredningen kapittel 9 og 13.

Bestemmelsen første ledd foreslås endret til å lyde:

«Når noen med skjellig grunn mistenkes for en handling som etter loven kan medføre frihetsstraff, kan det foretas ransaking av hans bolig, rom, oppbevaringssted, *databærere eller brukerkontoer* for å sette i verk pågripelse eller for å søke etter bevis eller etter *noe* som kan beslaglegges eller som det kan tas heftelse i.»

Sikring av data

Ref. utredningen kapittel 11, oppsummert i punkt 11.5.

Ny § 192 a

I forbindelse med ransaking for å søke etter bevis kan politiet sikre data direkte fra databærere og brukerkontoer. Sikringen skal begrenses til å gjelde data som allerede finnes på datasystemet. Forutsatt at det er nødvendig og ikke uforholdsmessig inngripende, kan politiet beslaglegge databæreren for å sikre dataene i etterkant. Politiet kan foreta de undersøkelser av databæreren og brukerkontoen som er nødvendige for å beslutte sikringsmetode. For øvrig gjelder bestemmelsene i databevisforskriften kapittel 2.

Ransaking av ubeskyttede data for å finne bevis, følger bestemmelsene i databevisforskriften kapittel 1.

[Bestemmelsen gjelder tilsvarende for fysiske dokumenter så langt den passer.][370]

§ 197 første ledd

Bestemmelsen foreslås endret til å lyde:

«Uten vedkommendes skriftlige samtykke kan ransaking *og sikring av data* etter §§ 192, *192 a*, 194 og 195 bare foretas etter beslutning av retten.»

---

[370] Se utredningen punkt 11.4.6.

Nytt tredje ledd i straffeprosessloven § 200

Ref. utredningen punkt 9.2.

Dette gjelder tilsvarende ved ransaking av noens databærer eller brukerkonto. Dersom innehaveren eller dennes representant ikke kan være tilstede, kan ransakingen likevel gjennomføres dersom det anses å være strengt nødvendig og utsettelse antas å være til vesentlig skade for etterforskingen. Spørsmål om gjennomføring av ransaking i tilfelle som nevnt skal på forhånd forelegges påtalemyndigheten for avgjørelse. Siktede skal så vidt mulig underrettes samtidig eller like etter gjennomføring av ransakingen.

Hemmelig ransaking og dataavlesing

Ref. utredningen kapittel 12, oppsummert i punkt 12.5.

Straffeprosessloven § 200 a

Det foreslås å tilføye et nytt siste punktum i første ledd:

For ransaking av databærer uten underretning gjelder straffeprosessloven §§ 216 o og p.

Straffeprosessloven § 216 o

Det foreslås et nytt annet ledd:

Dataavlesing kan utføres som enkeltstående, gjentakende eller vedvarende sikring av data.

I siste ledd foreslås et nytt tredje punktum:

Ved gjentatt avlesing skal retten om nødvendig bestemme det øvre antall gjentakelser i avlesingsperioden.

Beslag

Ref. utredningen kapittel 13.

Straffeprosessloven § 203

Bestemmelsen forslås endret til å lyde:

«*Det* som antas å ha betydning som bevis, kan beslaglegges inntil rettskraftig dom foreligger i saken. Det samme gjelder *det* som antas å kunne inndras eller å kunne kreves utlevert av fornærmede.»

Beskyttelse av taushetspliktige data

Ref. utredningen kapittel 17, oppsummert i punkt 17.9.

Nytt fjerde ledd i strpl. § 205 *Beslagsfrie papirdokumenter mv.*

Tilsvarende gjelder for papirdokumenter eller lignende som helt eller delvis er beslagsfrie, jf. straffeprosessloven § 204. Dersom dokumentomfanget er stort kan tingretten oppnevne medhjelper til å sortere ut dokumenter og slette beslagsfrie opplysninger. Dokumenter som i sin helhet er beslagsfrie skal returneres til innehaveren.

Ny § 205 a *Sperring av data etter pålegg fra påtalemyndigheten*

Sikrede data som er beslagsfrie, jf. strpl. § 204 første ledd skal sperres. Sperring foretas av teknisk enhet i politiet. Teknisk enhet har taushetsplikt om de sperrede dataene overfor etterforskingsenheten og skal være organisatorisk atskilt fra denne.

Sperring foretas etter pålegg fra påtalemyndigheten unntatt i tilfelle som nevnt i strpl. § 205 b. Etter sperring skal påtalemyndigheten gis fortsatt adgang til sikringskopien for å søke etter bevis, jf. straffeprosessloven § 192, og beslutte beslag jf. straffeprosessloven §§ 203 og 205 første ledd.

Påtalemyndigheten plikter av eget tiltak så langt som praktisk mulig å unngå innsyn i taushetspliktige opplysninger. Dersom påtalemyndigheten tilfeldig kommer over opplysninger som nevnt, skal teknisk enhet umiddelbart anmodes om sperring uten videre undersøkelser fra påtalemyndighetens side. I tvilstilfelle kan påtalemyndigheten begjære rettens avgjørelse om hvorvidt opplysningene er taushetspliktige. Begjæringen skal fremsettes uten forutgående innsyn i opplysningene, hvis ikke skal opplysningene sperres.

Ny § 205 b *Rettens kontroll med beslagsfrie data*

Sperring skal skje med rettens bistand i ethvert tilfelle hvor dataene er sikret hos den taushetspliktige. Påtalemyndigheten skal umiddelbart bringe sikringskopien til teknisk enhet uten forutgående innsyn, samtidig som begjæring om bistand til sperring sendes til retten med kopi av siktelsen og ransakingsbeslutningen. Tilsvarende gjelder dersom den som har krav på hemmelighold pretenderer at sikringskopien inneholder beslagsfrie data, såfremt pretensjonen er konkretisert og troverdig.

I tilfeller som nevnt bestemmer retten fremgangsmåten for beskyttelse av de beslagsfrie dataene. Rettens beslutning kan gå ut på

a) at de beslagfrie dataene skal sperres under tingrettens ledelse, eller
b) at data som ikke er beslagsfrie skal utleveres til påtalemyndigheten.

Ved avgjørelsen skal retten skal blant annet ta i betraktning hvorvidt sikringen har skjedd målrettet eller bredt, mengdeforholdet mellom antatt taushetspliktige data og data som er tilgjengelige for beslag, hvorvidt data må antas å være lett identifiserbare, og graden av kompleksitet ved sperring eller utlevering. Retten treffer avgjørelsen ved kjennelse.

Ved sperring som nevnt i annet ledd bokstav a, kan retten pålegge siktede og den som har rett til hemmelighold, å bidra til å identifisere hvilke data som skal sperres. Identifiserende opplysninger skal ikke tilflyte påtalemyndigheten og retten skal kommunisere direkte med teknisk enhet om sperringen. Retten skal kontrollere at sperringen ikke omfatter data som påtalemyndigheten etter loven har rett til å søke i for å finne bevis. Etter sperring skal påtalemyndigheten gis adgang til å søke etter bevis i sikringskopien som bestemt i straffeprosessloven § 205 a annet og tredje ledd.

Utlevering som nevnt i annet ledd bokstav b, skal baseres på siktelsen og ransakingsbeslutningen. Forsvareren skal gis adgang til å uttale seg dersom det kan skje uten skade for etterforskingen. Når data er utlevert i medhold av denne bestemmelsen skal ikke påtalemyndigheten gis adgang til etterfølgende søk i sikringskopien. Utlevering av opplysninger til påtalemyndigheten skjer ved kjennelse.

Forøvrig gjelder bestemmelsene i databevisforskriften kapittel 3.

Forslag til forskrift om ransaking, sikring og beslag i data for å finne bevis (databevisforskriften).

Kapittel 1. Ransaking av databærer

Ref. utredningen kapittel 10, oppsummert i punkt 10.5.

§ 1-1 *Ransaking av databærer*

Med ransaking av databærer menes undersøkelser av databærerens innhold for å avdekke opplysninger som kan tjene som bevis.

Politiet kan beslutte beslag i databærer for å søke etter bevis i ubeskyttede data, jf. straffeprosessloven §§ 206 første ledd, jf. 198 første ledd nr. 3. Det betyr at følgende vilkår gjelder: Det må foreligge sterk mistanke om en handling som etter loven kan medføre straff av fengsel i mer enn 6 måneder, og være nærliggende fare for at opplysninger som er vesentlige for sakens opplysning ellers går tapt, eller være av vesentlig betydning å få opplysningene før de er blitt sikret som nevnt i straffeprosessloven § 192 a og forskriften kapittel 2.

Dersom beslutningen rettes mot en annen enn siktede kreves i tillegg at det er særlig grunn til å anta at databæreren inneholder bevis, med mindre det er innhentet samtykke i samsvar med forskriften § 1-2.

Undersøkelser av databærer som forberedelse til sikring følger bestemmelsene i forskriften kapittel 2.

§ 1-2 *Informasjonsplikt ved samtykke til beslag i mobil databærer for å ransake den*

Ref. utredningen punkt 10.1

Et samtykke som skal gi grunnlag for beslag må være frivillig, informert og avgitt av kompetent person. Vilkåret om frivillighet utelukker samtykke fra den som er siktet, men ikke fra andre. For at et samtykke til beslag i databærer med formål å ransake den, skal være informert, skal følgende informasjon være gitt på forhånd:

- Det skal gjøres klart at undersøkelsen gjelder innholdet på databæreren.
- Undersøkelsens formål skal opplyses, og hvorfor den anses å være nødvendig.
- Det skal så langt som mulig informeres om hvilke deler av innholdet som antas å være nødvendig å undersøke, f.eks. om undersøkelsen gjelder tekstmeldinger, bilder, nærmere angitte applikasjoner osv., eller om en generell undersøkelse anses å være nødvendig.

Samtykket må være avgitt av den som har rett til å disponere databæreren, uavhengig av om telefonen er registrert på en annen, f.eks. arbeidsgiver. Ved ransaking av databærer som disponeres av personer under 15 år skal foresatte kontaktes.

§ 1-3 *Krav til gjennomføring av ransakingen*

Ransaking av databærer uten beskyttelse medfører endringer av de originale dataene og bryter med integritetshensynet nevnt i forskriften § 2-2. Ransakingen skal derfor begrenses til det som er strengt nødvendig for formålet.

Hvis mulig skal skrivesperre som sikrer mot endring av originale data benyttes.

§ 1-4 *Dokumentasjon og ransakingsrapport*

Ransakingen skal dokumenteres i en rapport. Det skal fremgå hvem som utførte ransakingen, dato og tidspunkt, stedet hvor ransakingen ble utført, hvilken databærer den gjaldt og hvordan det ble gjort.

Rapporten skal beskrive opplysningene som ble avdekket, og være vedlagt dokumentasjon som viser dataenes originaltilstand og hvilke endringer politiets undersøkelser medførte. Ransaking av databærer bør dokumenteres med videoopptak.

Kapittel 2. Sikring av data

Ref. utredningen kapittel 11, oppsummert i punkt 11.5.

§ 2-1 *Sikring av elektronisk informasjon*

Med sikring menes kopiering av data fra avslåtte eller aktive databærere og brukerkontoer, og ekstrahering av data fra hardware. Sikring skjer i medhold av straffeprosessloven § 192 a.

§ 2-2 *Krav til den elektroniske informasjonens integritet*

Sikringen skal så langt som mulig bevare den elektroniske informasjonens integritet. Sikret informasjon skal lagres i en sikringskopi. Sikringskopien skal holdes intakt frem til slettingsplikten inntrer, jf. § X.[371]

Integriteten skal bekreftes med elektronisk integritetskontroll. Ved sikring fra avslått databærer skal sikringskopiens identitet med de originale dataene verifiseres elektronisk. Ved sikring fra aktiv databærer skal sikringskopien umiddelbart gis en elektronisk bekreftelse som stadfester tidspunktet for sikringen. Tilsvarende gjelder så langt det passer for data ekstrahert fra hardware.

§ 2-3 *Krav til nødvendighet og proporsjonalitet*

Sikring av data er inngripende for den det gjelder og skal begrenses til det som er nødvendig for å dekke sakens informasjonsbehov, slik dette er beskrevet i rettens beslutning.

Nødvendighetshensynet kan krysses av integritetshensynet og behovet for å minimere innsyn i databæreren før sikring. Sikringsrapporten skal redegjøre for hvilke overveielser som er gjort for å begrense omfanget av sikringen.

Omfanget av sikringen skal for øvrig ta hensyn til sakens alvor og forholdene ellers, jf. straffeprosessloven § 170 a.

§ 2-4 *Plikt til å føre sikringsrapport*

Sikringen skal dokumenteres i en sikringsrapport. Av rapporten skal det fremgå hvem som utførte sikringen, dato og tidspunkt, stedet hvor sikringen ble utført, hvilken databærer den gjaldt og hvordan det ble gjort.

Rapporten skal opplyse om eventuelle endringer i sikringskopien i forhold til de originale dataene, redegjøre for årsaken og betydningen for informasjonens meningsinnhold og pålitelighet.

Rapporten skal redegjøre for hvilke vurderinger som er gjort for å innrette sikringen mot sakens informasjonsbehov, og for å begrense den til det som er nødvendig og forholdsmessig i lys av sakens art og forholdene ellers, jf. forskriften § 2-3.

Rapporten skal føres i et klart og enkelt språk. Den bør støttes av dokumentasjon som er generert av dataverktøyene som er brukt i sikringsprosessen.

§ 2-5 *Kopi til siktede eller forsvareren*

Ref. utredningen punkt 15.4.

Politiet skal sende et eksemplar av sikringskopien til siktede eller forsvareren såsnart den foreligger, vedlagt sikringsrapporten. Dette gjelder kun sikringskopi med data fra siktedes egen databærer eller brukerkonto. Verken siktede eller forsvareren har rett til sikringskopi av data sikret hos andre. Dersom sterke hensyn taler mot oversendelse, kan sikringskopien gjøres

[371] Se utredningen punkt 19.1.

tilgjengelig for for forsvareren på annen forsvarlig eller hensiktsmessig måte, jf. påtaleinstruksen § 16-2.

§ 2-6 *Data mottatt fra andre*

Ref. utredningen punkt 5.4.2.2.

Data politiet mottar fra andre, for eksempel tilbydere av elektroniske kommunikasjonsnett eller -tjenester, skal umiddelbart gis en elektronisk bekreftelse som stadfester informasjonens tilstand og tidspunktet den ble mottatt. Bestemmelsene i dette kapitlet gjelder tilsvarende så langt de passer.

Kapittel 3. Analyse av sikrede data

Ref utredningen kapittel 14, oppsummert i punkt 14.7.

§ 3-1 *Analyse av sikrede data*

Analyse av sikrede data regnes som fortsatt ransaking og skal utføres innen rammene satt av ransakingsbeslutningen. For å utvide analysen til å gjelde andre straffbare forhold enn nevnt i siktelsen som ligger til grunn for ransakingsbeslutningen, må ny ransakingsbeslutning som dekker dette innhentes. Vilkårene i straffeprosessloven § 192 må være oppfylt.

§ 3-2 *Krav til målrettethet og objektivitet*

Analysen skal innrettes slik at den er egnet til å dekke sakens informasjonsbehov. Det skal utferdiges en skriftlig plan for analysen som sikrer systematikk, målrettethet og objektivitet. Analysen skal utføres strukturert ved bruk av gjensidig utelukkende hypoteser som ivaretar skyld og uskyld.

Data som ikke antas å være relevante skal så langt som mulig skjermes mot innsyn.

§ 3-3 *Evaluering*

Databevis som er særlig komplekse eller av sentral betydning i en alvorlig sak, skal evalueres for å vurdere bevisets styrke.

Evaluering skal gjøres i forhold til gjensidig utelukkende hypoteser relatert til en omstendighet som er relevant i saken.

Bevisets styrke skal angis på entydig vis i henhold til en standard.

§ 3-4 *Dokumentasjonskrav*

Analysens resultater skal dokumenteres i en rapport. Av rapporten skal det fremgå hvordan analysen ble lagt opp for å sikre at den rettet seg mot sakens informasjonsbehov, og hypotesene som ble brukt. Analyseplanen nevnt i forskriften § 3-2 bør inngå i rapporten.

Rapporten skal også redegjøre for hvilke tiltak som ble benyttet for å skjerme data som nevnt i forskriften § 3-2 annet ledd.

Analysen skal suppleres med logger som viser tidspunkter for utførelse, hva som ble gjort, herunder avgrensningene som ble foretatt, søkekriteriene som ble benyttet, og hvem som utførte analysen.

§ 3-5 *Fagfellekontroll*

Analyserapporten og tilhørende dokumentasjon skal etterkontrolleres og godkjennes av en kvalifisert tjenesteperson i politidistriktet. Kontrollen skal særlig gjelde

- Hvorvidt rapporten uttrykker usikkerhet på entydig måte;
- Hvorvidt databevis har vært evaluert når det er behov for det; og
- Hvorvidt rapportskriver har holdt seg innenfor grensene for sin kompetanse.

§ 3-6 *Påtalemessig kontroll*

I saker med positivt påtalevedtak skal påtalejuristen på forhånd ha kontrollert databevisenes pålitelighet, herunder

- betydningen av eventuelle endringer i dataene som har skjedd i løpet av dataetterforskingsprosessen,
- dokumentasjonens godhet,
- hvorvidt analysen var lagt opp på en måte som var egnet for formålet, og
- hvorvidt dataverktøyene som ble benyttet var egnet for formålet.

Kontrollen dokumenteres med påtegning på sluttrapporten.

Litteraturliste

Advokatforeningen (2017) Høringsuttalelse. NOU 2016: 24 Ny straffeprosesslov. juni 2017.

Bjerknes, O.T. & Fahsing, I. (2018) *Etterforskning – prinsipper, metoder og praksis.* Fagbokforlaget, Bergen, 2018.

Bruce, I. & Haugland, G.S. (2018) *Skjulte tvangsmidler*, Oslo: Universitetsforlaget, 2. utg.

Casey, E. (2002) "Error, Uncertainty, and Loss in Digital Evidence". *International Journal of Digital Evidence*, 2002

Casey, E. (2011) *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet.* San Diego: Academic press. 2011.

Casey, E. (2020) "Standardization of forming and expressing preliminary evaluative opinions on digital evidence". *Forensic Science International: Digital Investigation.* 32/2020.

Cook et al. (1998) "A hierarchy of propositions: Deciding which level to address in casework."*Science& Justice.* 1998, s. 231-239.

Eriksen, T. H. (2021) *Appenes planet – Hvordan smarttelefonen forandret verden.* Oslo: Aschehoug. 2021.

Europol (2019) "Do criminals dream of electric sheep? – How technology shapes the future of crime and law enforcement." Europol, 2019.

Europol & Eurojust (2019) Common Challenges in Combating Cybercrime, 2019.

Faust, F., Thierry, A., Müller, T. & Freiling, F. (2020) "Selective Imaging of File System Data on Live Systems". Technical Report. CC BY-NC-ND. ArXiv:2012.02573v1 [cs.OH] 3 December 2020.

Flaglien, A. (2018). «The Digital Forensics Process». I Årnes, A. (red.), 2018, s. 14-49.

Gundhus, H.O.I., Talberg, N., (2019) «Politiskjønnet under press». I Sunde, I.M. & Sunde, N. Wathne, C. T. (red.) *Det digitale er et hurtigtog – vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi.* Bergen: Fagbokforlaget, 2019, s. 83-115.

Haaland, M. H. (2019) «Speilkopiering av databærere hos advokat og retten til konfidensiell rettslig bistand.» *Tidsskrift for Strafferett,* 2/2019, s. 186-208.

Hamm, J. (2018) «Computer Forensics», i A. Årnes (red.) 2018, s. 147-190.

Haukaas, K. (2019) «Cyberkriminalitet og digital etterforsking – noen betraktninger, især om innhenting og bruk av bevis». I Sæther, K-E., Kvande, K., Torgersen, R. og Stridbeck, U. (red.) *Straff og frihet: Til vern om den liberale rettsstat – Festskrift til Tor-Aksel Busch.* Oslo: Gyldendal, 2019, s. 285-299.

Hjort, M.A. (2016) *Tilgang til bevis i sivile saker – særlig om digitale bevis.* Oslo: Universitetsforlaget. 2016.

Hjort, M.A. (2017) «Sorteringsprosessen i bevissikringssaker og ved beslag inneholdende taushetsbelagt informasjon». *Lov&Rett*, 3/2017, s. 178-191.

Hjort, M.A. (2019) «Mandat til å sortere digitalt materiale», *Tidsskrift for Strafferett*, 2/2019, s. 209-234.

Horsman, G. (2020) "ACPO Principles for digital evidence: Time for an update?" *Forensic Science International*, Elsevier, 2020, *in press.* Tilgjengelig her: (4) (PDF) ACPO principles for digital evidence: Time for an update? (researchgate.net)

Jahre, H.-P. (1990) Ransaking og beslag hos advokater og revisorer i økonomiske straffesaker - Særlig om forholdet til taushetsplikt. I Christie, N. (red.) «*...den urett som ikke rammer deg selv: Festskrift til Anders Bratholm 70 år*». Universitetsforlaget, 1990, s. 251-266.

Johansen, K. & Anderson, W. (2021) «Datalagring som evighetsprosjekt», Aftenposten Innsikt, april 2021, s. 105-112.

Justisdepartementet (2000) «Lovteknikk og lovforberedelse - Veiledning om lov- og forskriftsarbeid», Justisdepartementet, 2000.

Justis- og beredskapsdepartementet & Forsvarsdepartementet (2019) *Nasjonal strategi for digital sikkerhet*. Oslo: Departementenes sikkerhets- og serviceorganisasjon, 5/2019.

Keiserud, E., Sæther, K. E., Holmboe, M., Jahre, H.-P. Matningsdal, M. & Smørdal, J. G. (2020) *Straffeprosessloven – Lovkommentar*, 5. utg., Oslo: Universitetsforlaget, 2020.

Kjelby, G. J., (2019) *Påtalerett.* Oslo*:* Cappelen Damm, 2019, 2. utg.

Kjølbro, J. F. (2017). *Den Europæiske Menneskerettighedskonvention for praktikere*. København: Jurist- og Økonomforbundets Forlag. 2017. 4. utg.

KK-utvalget (2019-20) *Årsrapport 2018 og Årsrapport 2019.*

Kolflaath, E. (2019) «Litt om vitenskapeliggjøringen av etterforskningsfaget»». I Sæther, K-E., Kvande, K., Torgersen, R. og Stridbeck, U. (red.) *Straff og frihet: Til vern om den liberale rettsstat – Festskrift til Tor-Aksel Busch.* Oslo: Gyldendal, 2019, s. 435-444.

Koops, B.-J. (2018) "Privacy Spaces". 121 *West Virginia Law Rev.* 611 (2018), s. 612-233. Tilburg Law School Research paper.

Kozhuharova, D., Gyffroy, P., Bogia, H., Krumova, S. (2021) *From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (FORMOBILE).* D2.2 Criminal Procedure Report version 0.1. Forskningsrapport. EU Horizon 2020.

Kripos (2017) Høringsuttalelse. NOU 2016: 24 Ny straffeprosesslov. 27. juni 2017.

Magnussen, T. (2019) «Politiet må kunne beskytte befolkningen i cyber og utøve politimyndighet i og gjennom cyber». *Politiforum,* 4. juli 2019.

Mason, S. & Seng, D. (red.) (2017) *Electronic Evidence.* 4. utg., 2017, s. 36-69. Open access, School of Advanced Study, University of London. Humanities Digital Library http://www.humanities-digital-library.org.

Mason, S. & Seng, D. (2017a) "The foundations of evidence in electronic form". I Mason, S. & Seng, D. (red.), 2017, s. 36-69.

Mason, S. & Seng, D. (2017b) "Draft convention on Electronic Evidence". I Mason, S. & Seng, D. (red.), 2017. Appendix II.

McKemmish, R. (2008) «When is digital evidence forensically sound?". IFIP International Conference on Digital Forensics. Boston: Springer. 2008.

Menneskerettighetsutvalget (2012) Dokument 16 (2011–2012) Rapport til Stortingets presidentskap fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven.

Paulsen, J. E. (2019) «Holdninger til høyteknologi». I Sunde, I.M. & Sunde, N. (red.) *Det digitale er et hurtigtog – vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi.* Bergen: Fagbokforlaget, 2019, s. 23-49.

Politidirektoratet (2010) *Behandling av beslag i straffesaker.* RPOD-2010-7. Oppdatert 19. juni 2017.

Politidirektoratet (2012) *Kvalitetsstandard for kriminalteknisk etterforsking.* 2012.

Politidirektoratet (2017) *Rammer og retningslinjer for etablering av nye politidistrikter.* 16. juni 2017.

Politidirektoratet (2020)	*Etterretningsdoktrine for politiet*, v 1.2, Oslo: Politidirektoratet, 2020.
Pollit, M., Casey, E., Jaquet-Chiffelle, D. & Gladyshev, P. (2018).	*A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*, OSAC/NIST.
PWC & Statens Vegvesen (2020).	*Prosjekt Cartech – Hovedrapport*. Oslo: 27. august 2020.
Riksadvokaten (1999)	*Etterforsking.* Rundskriv nr. 3/1999. Del II.
Riksadvokaten (2017)	Høringsuttalelse. NOU 2016: 24 Ny straffeprosesslov. 1. desember 2017.
Riksadvokaten (2018)	*Kvalitetsrundskrivet.* Rundskriv nr. 3/2018.
Riksadvokaten (2020)	*Ransaking av databærere.* Brev til Politihøgskolen 21. april 2020.
Riksadvokaten (2021)	*Påtalemyndighetens legalitetskontroll med tvangsmiddelbruk – relevant etterforskingsformål og forholdsmessighet – særlig om ransaking i narkotikasaker.* Brev til statsadvokatembetene 9. april 2021.
Riksrevisjonen (2021)	«Riksrevisjonens undersøkelse av politiets innsats mot IKT-kriminalitet», rapport 2. februar 2021, Dokument 3:5 (2020-2021).
Ryser, E., Spichinger, H., Casey, E. (2020)	"Structured decision making in investigations involving digital and multimedia evidence." *Forensic Science International.* 34/2020.
Sandvik, J.-P. (2018)	«Mobile and Embedded Forensics». I Årnes, A. (red.), 2018, s. 191-273.
Servida, F. & Casey, E. (2019)	"IoT forensic challenges and opportunities for digital traces". *Digital Investigation.* 28 (2019), s. 22-29.
Strandbakken, A. (2003)	*Uskyldspresumsjonen.* Bergen: Fagbokforlaget. 2003.
Straffeprosessutvalget (2016)	NOU 2016: 24 *Ny straffeprosesslov*
Sunde, I. M. (2010)	*Automatisert inndragning.* Universitetet i Oslo. PhD-avhandling. 2010. Trykket i Complex 3/2011, Senter for rettsinformatikk, juridisk fakultet. Tilgjengelig online.
Sunde, I. M. (2015).	«Databevis». I Hedlund, M.-A., Aarli, R. & Jebens, S.E. (red.). *Bevis i straffesaker - Utvalgte emner*. Oslo: Gyldendal Juridisk, s. 599-633.
Sunde, I.M. (2016)	*Datakriminalitet*, Bergen: Fagbokforlaget, 2016.

Sunde, I.M. (2019a)	«Har vi behov for straffebud om datakriminalitet?» *Tidsskrift for strafferett.* 2/2019 s. 168-185.
Sunde, I.M. (2019b)	«Patruljering på internett». I Sæther, K-E., Kvande, K., Torgersen, R. og Stridbeck, U. (red.) *Straff og frihet: Til vern om den liberale rettsstat – Festskrift til Tor-Aksel Busch.* Oslo: Gyldendal, 2019, s. 597-608.
Sunde, I.M. (2020)	«Bør rettssikkerheten i politiets kriminalitetsforebyggende arbeid styrkes?» *Tidsskrift for strafferett.* 1/2019.
Sunde, N. (2019a)	«Min smartmobil er min borg – Smartmobilens rolle i privatlivet og i kommunikasjon». I Boucht, J. & Høgberg, A.P. (red.) *Vennebok til Ulf Stridbeck ved hans 70-årsdag,* Institutt for offentlig rett, det juridiske fakultet, Oslo, 2019, s. 199-223 (2019)
Sunde, N. (2019b)	«Digitale bevis – menneskelige feil». I Sunde, I.M. & Sunde, N. (red.) *Det digitale er et hurtigtog - Vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi.* Bergen: Fagbokforlaget, 2019, s. 53-82.
Sunde, N. (2019c)	«Digitale bevis i norske gjenåpningssaker – kan vi utelukke systematiske feil?». *Tidsskrift for strafferett*. 1/2020.
Sunde, N. & Dror, I.E (2019)	"Cognitive and Human Factors in Digital Evidence: Problems, Challenges, and the Way Forward". *Digital Investigation.* 29/2019.
Sunde, N. & Dror, I.E. (2021)	"A Hierarchy of Expert Performance (HEP) applied to Digital Forensics: Reliability and Biasability in Digital Forensics Decision Making", *Forensic Science International: Digital Investigation,* 2021.
Sunde, N. & Horsman, G. (2020)	"Part I: The need for peer-review in digital forensics." *Forensic Science International: Digital Investigation.* 2020:35.
Sunde, N. & Lentz, L. (2021)	«The use of historical call data records as evidence in the criminal justice system - lessons learned from the Danish telecom scandal". *Digital Evidence and Electronic Signature Law Review*, 18 (2021)
Tilstone, W.J., Hastrup, M.L. & Hald, C. (2013)	*Fisher's Techniques of Crime Scene Investigation – First International Edition.* Boca Raton: CRC Press. 2013.
UK Law Commission (2020)	"Search Warrants". Rapport nr. 396. 7. oktober 2020.
Zoubek, C. & Sack, K. (2017)	"Selective deletion of non-relevant data", *Digital Investigation,* 20 (2017), s. 92-98.

Økokrim (2017) Høringsuttalelse. NOU 2016: 24 Ny straffeprosesslov. 15. august 2017.

Årnes, A. (2018). "Introduction". I Årnes, A. (red.), 2018, s. 1-11.

Årnes, A. (red.). (2018). *Digital Forensics*. Hoboken: John Wiley & Sons Ltd.

Masteravhandlinger

Andreassen, L. E. & Andresen, G. (2019) *Live Data Forensics - A quantitative study of the Norwegian Police University College students LDF examinations during their year of practice.* University College Dublin, 2019.

Borhaug, T.S. (2019) *The Paradox of Automation in Digital Forensics*. NTNU, 2019.

Erlandsen, T. E. (2019) *Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service*. NTNU, 2019.

Friheim, I. (2016) *Practical use of dual tool verification in computer forensics.* University College Dublin, 2016.

Haraldseid, S. (2021) *«Kan du stikke opp og gå gjennom databeslaget?» - Fremgangsmåter for innholdsanalyse av databeslag og behovet for metodisk støtte.* Politihøgskolen, 2021.

Heitman, O. (2019) *Digital investigation: The malnourished child in the Norwegian police family?* NTNU, 2019.

Jahren, J. (2020) *Is the quality assurance in digital forensics in the Norwegian police adequate?* NTNU, 2020.

Sunde, N. (2017) *Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation,* NTNU, 2017.

Rettspraksis

Høyesterett

Rt. 1986 s. 1149

Rt. 1996 s. 1081

Rt. 2008 s. 1659

Rt. 2011 s. 296

Rt. 2011 s. 1188

Rt. 2012 s. 1645

Rt. 2013 s. 968

Rt. 2014 s. 1103

Rt. 2015 s. 81

Rt. 2015 s. 1456

HR-2016-1086-U

HR-2016-1833-A

HR-2017-111-A

HR-2018-104-A

HR-2018-699-A

HR-2018-1517-U

HR-2018-1901-U

HR-2019-610-A

Tingrettsdommer

RG 2012 s. 74

Oslo tingretts dom 15. januar 2021 (20-020518MED-OTIR/04)

Den Europeiske Menneskerettighetsdomstolen

Bernhard Larsen Holding og andre mot Norge. Dom 14. mars 2013 (saknr. 24117/08).

Harju mot Finland. Dom 15. februar 2011 (saknr. 56716/09).

Iliya Stefanov mot Bulgaria. Dom 22. mai 2008 (saknr. 65755/01).

Kolesnichenko mot Russland. Dom 9. april 2009 (saknr. 19856/04).

Miailhe mot Frankrike (sak 1). Dom 13. februar 1993 (saknr. 12661/87).

Michaud mot Frankrike. Dom 6. desember 2012 (saknr. 12323/11).

Mirmotahari mot Norge. Avvisningsbeslutning 8. oktober 2019 (saknr. 30149/19).

Petri Sallinen og andre mot Finland. Dom 27. september 2005 (saknr. 50882/99).

Robathin mot Østerrike. Dom 3. juli 2012 (saknr. 30457/06).

Rowe and Davis mot Storbritannia. Dom 16. februar 2000 (saknr. 28901/95) (Storkammer).

Saber mot Norge. Dom 17. desember 2020 (saknr. 459/18).

Sigurdur Einarsson og andre mot Island. Dom 4. juni 2019 (saknr. 39757/15).

Smirnov mot Russland. Dom 7. juli 2007 (saknr. 71362/01).

Van Rossem mot Belgia. Dom 9. desember 2004 (saknr. 41872/98).

Wolland mot Norge. Dom 17. mai 2018 (saknr. 39731/12).