



## RIKSADVOKATEN

Agder statsadvokatembeter  
Postboks 504 - Lundsiden  
4605 KRISTIANSAND S

Deres referanse:

Vår referanse:

Dato:

20/2219 - 15 / LSP003

09.06.2021

### **Direktiv om ransaking av datamengder som det er grunn til å tro inneholder opplysninger underlagt beslagsforbudet i straffeprosessloven § 204, jf. § 119**

#### **1. Innledning**

Fra hovedregelen i straffeprosessloven § 203 om at ting som antas å ha betydning som bevis kan beslaglegges, gjøres det i § 204 første ledd unntak for dokumenter eller annet som et vitne kan nekte å forklare seg om etter nærmere angitte bestemmelser. Blant disse er straffeprosessloven § 119, hvor det er bestemt at retten ikke uten samtykke kan ta imot forklaring fra blant annet advokater om noe som er «betrodd» advokaten i hans stilling. For materiale som er omfattet av bevisforbudet i § 119, gjelder et absolutt beslagsforbud, med mindre den som har taushetsplikt er mistenkt for å være medskyldig i det straffbare forhold, jf. § 204 annet ledd.

For å avgjøre om en datamengde inneholder informasjon omfattet av beslagsforbudet, er det som regel nødvendig å gjennomgå materialet først. Det er fordi datamengder typisk har egenskaper knyttet til format, omfang, lagringssted og lesbarhet som gjør at man ikke uten videre kjenner innholdet. Datamengden som er lagret på en telefon er et slikt eksempel.

Fremgangsmåten for hvordan et slikt materiale kan gjennomgås, herunder hvordan beslagsfritt innhold skal utsorteres, er ikke nærmere regulert i straffeprosessloven, men det er trukket opp retningslinjer i rettspraksis. I HR-2018-699-A (avsnitt. 31) oppsummeres dette slik:

*"Ved ransaking hos andre enn advokater er det derimot ikke nødvendig å forelegge det samlede materialet for tingretten, selv hvor det oppdages advokatkorrespondanse eller det pretenderes at slik korrespondanse finnes, se [HR-2017-111-A avsnitt 41](#). Førstvoterende uttaler samme sted at det i slike tilfeller antakelig vil være «vel så nærliggende å se hen til de retningslinjer Høyesterett har trukket opp for håndtering av samtaler sikret ved kommunikasjonskontroll.» Dette innebærer at politiet i utgangspunktet kan gjennomgå det materialet som er sikret, men at det som måtte*

*være taushetsbelagt, umiddelbart må sorteres ut uten ytterligere undersøkelse, se [Rt-2015-81 avsnitt 30](#) og [HR-2017-111-A avsnitt 42-43](#)."*

Den 17. desember 2020 avgjorde Den Europeiske Menneskerettighetsdomstolen (EMD) at mangelen på en klar rettslig regulering og nærmere prosedyrer for gjennomgang av digitalt lagrede opplysninger med potensielt beslagsfritt innhold, er i strid med kravene i EMK art. 8.<sup>1</sup>

Riksadvokaten kom på grunnlag av EMDs dom til at politiet ved beslag av digitale lagringsenheter ikke kunne utsortere opplysninger omfattet av beslagsforbudet i straffeprosessloven § 204, jf. § 119 på samme måte som før avgjørelsen. Av den grunn ble det gitt et midlertidig direktiv 17. desember 2020 som bestemte at når det forelå holdepunkter for at et beslag (en datamengde) inneholdt opplysninger omfattet av beslagsforbud etter straffeprosessloven § 204, jf. § 119, skulle beslaget sendes til tingretten for gjennomgang og utsortering. Dette er imidlertid en liten hensiktsmessig løsning, især fordi det hemmer fremdriften i de aktuelle sakene. Riksadvokaten har derfor hatt som målsetting at direktivet fra desember 2020 skulle være en midlertidig løsning i påvente av et rammeverk som gjør det forenlig med EMK å la politiet selv forestå utsorteringen av beslagsfrie opplysninger. Direktivene her gir et slik rammeverk, og i tillegg arbeider Justis- og beredskapsdepartementet med en mulig en forskriftsregulering av området. Direktivene gir anvisning på en prosedyre som sikrer at beslagsfritt innhold ikke tilflyter etterforskningsenhetene.

Fagutviklingsapparatet har på oppdrag fra riksadvokaten utarbeidet forslag til en prosedyre som skal ivareta disse kriteriene ved at utsortering foretas av en teknisk enhet i politiet i de tilfeller hvor det er holdepunkter for at det finnes beslagsfrie opplysninger i datamengden. Forslaget har vært på høring i politidistriktene og danner utgangspunktet for dette direktivet. Representanter med teknisk og juridisk kompetanse fra ulike fagmiljøer, herunder Kripes, Oslo politidistrikt, PST, Økokrim, Oslo statsadvokatembeter, Det nasjonale statsadvokatembetet, PHS og Advokatforeningen, har bidratt med innspill underveis i arbeidet med direktivet, og har fått anledning til å uttale seg til et utkast.

Det innføres ved dette direktivet et system for utsortering av beslagsfrie opplysninger ved en teknisk enhet som organisatorisk er atskilt fra etterforskningsenheten. Utsorteringsprosedyren skal iverksettes når det er grunn til å tro at datamengden inneholder slike opplysninger. Ordningen skal hindre at de tjenestepersoner som etterforsker saken, får innsyn i opplysninger som er beslagsfrie. Videre stilles krav til forsvarlig og sikker oppbevaring av materiale og notoritet om beslutninger og behandling. Prosedyren er beskrevet i punkt 4.

Direktivet erstatter midlertidig direktiv 17. desember 2020.

## **2. Virkeområde**

Under dette punktet behandles hvilke datamengder direktivet omfatter, betydningen av

---

<sup>1</sup> Se *Saber mot Norge*, sak 459/18, særlig avsnitt 57 der det er uttalt at "lack of foreseeability [...] due to the lack of clarity in the legal framework and the lack of procedural guarantees relating concretely to the protection of LPP, already fell short of the requirements flowing from the criterion that the interference must be in accordance with the law within the meaning of Article 8 § 2 of the Convention".

hvordan politiet har fått tilgang til datamengden og hvilke undersøkelser som kan foretas uten at prosedyren i punkt 4 følges.

Direktivet regulerer politiets undersøkelser av datamengder med egenskaper, herunder relatert til format, omfang og lesbarhet, som innebærer at man ikke uten videre kjenner innholdet. Med "datamengde" forstås i denne sammenheng en avgrenset mengde opplysninger funnet på et digitalt lagringssted, herunder fysiske lagringsenheter (databærere) og nettverksbaserte lagringstjenester. Fysiske lagringsenheter omfatter typisk PC-er, mobiltelefoner, nettbrett, minnepenner, harddisker mv. Med nettverksbaserte lagringstjenester forstås digitale lagringssteder der tilgang kan oppnås gjennom datanettverk (herunder Internett), typisk via pålogging til tjenestekonti hos e-post-, "skylagring"- eller fildelingstilbydere.

Avgrensningen til datamengder "med egenskaper, herunder relatert til format, omfang og lesbarhet, som innebærer at man ikke uten videre kjenner innholdet" innebærer at undersøkelse av datamengder med kjent innhold, ikke omfattes av direktivet. Det kan for eksempel være trafikkdata eller kontoutskrifter som beslaglegges eller utleveres på en lagringsenhet.

Undersøkelse av datamengder med ukjent innhold har gjerne flere stadier, fra sikring fra aktuelle lagringssted (eksempelvis ved speilkopiering), utsortering av opplysninger som er eller kan være undergitt beslagsforbud, og til gjennomgang med formål å gjøre beslag i opplysninger som antas å ha betydning som bevis mv. Med "sikring" forstås her arbeidsprosesser som gjennomføres for at politiet skal sette seg i besittelse av en kopi (f.eks. en sikringsfil) av en nærmere definert datamengde.<sup>2</sup> Sikring foretas typisk ved en teknisk prosess, men kan også skje uten bruk av sikringsverktøy, f.eks. ved at det tas bilde eller video av en dataskjerm.

Undersøkelser som ikke gir tilgang til lesbart innhold, typisk sikring og klargjøring før man begynner å lete etter bevis, kan foretas som tidligere uten at den særskilte prosedyren foreskrevet i punkt 4 må følges, selv om det er grunn til å tro at datamengden inneholder opplysninger med beslagsforbud.<sup>3</sup> Dette gjelder likevel ikke når sikringsmetoden innebærer at etterforsker ved sikringen får innsyn i eventuelt beslagsfrie opplysninger som er lesbare. I slike tilfeller må sikringen og klargjøringen foretas ved teknisk enhet slik som beskrevet i punkt 4.

Hvilket rettslig grunnlag som har gitt politiet tilgang til datamengden, er i utgangspunktet uten betydning. Både beslag og utleveringspålegg omfattes. Direktivet gjelder likevel ikke for gjennomgang av materiale fra kommunikasjonskontroll (straffeprosessloven §§ 216a og b), romavlytting (straffeprosessloven § 216m) eller dataavlesning (straffeprosessloven § 216o). Fremgangsmåten for behandling av slikt materiale reguleres av straffeprosessloven § 216g og innebærer at materiale som omfattes av straffeprosessloven § 119 skal slettes. Det vises til Rt-2015-81, Rt-2015-1456 og HR-2016-1086-U.

---

<sup>2</sup> Sikringsfilen er ikke et nytt beslag i saken, og er heller ikke en del av sakens dokumenter. Det må likevel foreligge notoritet om hvordan sikringen har skjedd, hvor sikringsfilen er oppbevart mv. Dersom politiet ved ransakingen av sikringsfilen finner materiale som antas å ha betydning som bevis, "hentes" disse ut og tas i beslag. Opplysninger som er "hentet ut" blir en del av sakens dokumenter, jfr. Rt-2011-188 og HR-2018-1901-U.

<sup>3</sup> Se Rt-2011-1188, Rt-2012-1645 og Rt-2013-968.

Ransaking av fysiske steder og dokumenter faller også utenfor, slik at direktivet ikke medfører endringer når det gjelder gjeldende praksis etter straffeprosessloven § 204, jf. § 205.

### **3. Krav om ransakingsbeslutning**

Politiets undersøkelser av datamengder med ukjent innhold må antakelig anses som straffeprosessuell ransaking. Høyesterett har lagt dette til grunn for så vidt gjelder gjennomgang av datalagringsenheter.<sup>4</sup> Det kreves derfor en ransakingsbeslutning før man setter i verk undersøkelser, og de alminnelige reglene om ransaking får anvendelse.

En beslutning om ransaking som gjelder den mistenktes oppbevaringssteder, omfatter i utgangspunktet også digitalt lagrede opplysninger.<sup>5</sup> Har politiet oppnådd rådighet over datamengden gjennom forutgående ransaking, kan undersøkelsene derfor foretas i forlengelse av denne, dvs. "som ledd i en pågående ransaking", innenfor rammen av ransakingsbeslutningen. I andre tilfeller, typisk ved beslag uten forutgående ransaking, må det treffes en ransakingsbeslutning før politiet går i gang med undersøkelsen.

Begjæring om ransaking til retten/beslutning om ransaking bør i tillegg til hjemmelsgrunnlag, mistankegrunnlag og formålet med ransakingen, angi hvor det kan søkes etter bevis, og i den grad det er praktisk mulig beskrive hva ransakingen kan omfatte.<sup>6</sup>

Ransakingsbeslutningen og mistankegrunnlaget setter rammen for ransakingen og dermed hva det kan søkes etter bevis for.<sup>7</sup> Det må være en saklig sammenheng mellom mistankegrunnlaget og ransakingen. Ønsker politiet å ransake for å søke etter bevis for andre straffbare forhold enn siktelsen gjelder, må det innhentes ny beslutning. Finner politiet under ransakingen bevis for nye eller ukjente straffbare forhold, vil disse opplysningene kunne beslaglegges, og på vanlig måte kunne gi grunnlag for etterforskning, herunder begrunne en eventuell ny beslutning om ransaking for å søke etter ytterligere bevis for disse forholdene.<sup>8</sup>

Ransakingen kan pågå over tid med gjentatte søk uten at det kreves en ny beslutning for hver gang man går inn i det lagrede materialet, forutsatt at ransakingen skjer innenfor rammen av ransakingsbeslutningen.<sup>9</sup>

## **4. Prosedyren for ransaking**

### **4.1 Innledning**

I det følgende beskrives fremgangsmåten ved ransaking av datamengder omfattet av direktivets virkeområde (se punkt 2). Gjennomgangen skiller mellom tre typetilfeller: Hvor det ikke er grunn til å tro at det foreligger opplysninger omfattet av beslagsforbudet i

---

<sup>4</sup> Se Rt-2011-296 avsnitt 40 og HR-2018-699-A avsnitt 29.

<sup>5</sup> Se HR-2019-610-A (avsnitt 27).

<sup>6</sup> Se LB-2018-87329.

<sup>7</sup> Se også punkt 2 om kravet til relevant etterforskningsformål i riksadvokatens brev av 9. april 2021, "Påtalemyndighetens legalitetskontroll med tvangsmiddelbruk – relevant etterforskningsformål og forholdsmessighet – særlig om ransaking i narkotikasaker".

<sup>8</sup> Se LB-2018-87329.

<sup>9</sup> Se HR-2018-699-A (avsnitt 29).

straffeprosessloven § 204, jf. § 119, hvor det er grunn til å tro at slike opplysninger foreligger og hvor ransakingen foretas hos person som innehar stilling som nevnt i § 119.

#### **4.2 Tilfeller hvor det ikke er grunn til å tro at det foreligger beslagsfrie opplysninger**

Dette er normalsituasjonen og følger de vanlige reglene for ransaking. Det kreves ikke at politiet på selvstendig grunnlag forespør den som er rammet av beslaget eller iverksetter andre undersøkelser for å avdekke om datamengden inneholder beslagsfrie opplysninger. Men også i disse tilfellene må etterforsker eller den som gjennomgår datamengden, være oppmerksom på at slikt materiale kan forekomme. Dersom etterforsker under gjennomgangen kommer over opplysninger som kan være underlagt beslagsforbud, skal gjennomgangen stanses og prosedyren som beskrevet i punkt 4.3 følges.

#### **4.3 Tilfeller hvor det er grunn til å tro at det foreligger beslagsfrie opplysninger**

##### *4.3.1 Innledning*

Dersom det er grunn til å tro at det foreligger beslagsfrie opplysninger i datamengden, skal den særskilte prosedyren for utsortering ved teknisk enhet som beskrives i det videre, følges. Fra dette gjelder det likevel et unntak i situasjoner hvor det er stor fare for at bevis kan gå tapt om man avventer utsortering ved den tekniske enheten, se punkt 4.3.7

##### *4.3.2 Hva ligger i "grunn til å tro"?*

Med "grunn til å tro" menes i denne sammenheng at det foreligger konkrete holdepunkter som med en viss styrke indikerer at den aktuelle datamengden inneholder opplysninger som er beslagsfrie etter straffeprosessloven § 204, jf. § 119. En generell antagelse om at slike opplysninger kan finnes, er ikke tilstrekkelig. Det kreves på den annen side ikke sannsynlighetsovervekt.

Hva holdepunktene bygger på, er i seg selv ikke avgjørende. Det vil kunne være opplysninger i saken fra tidligere innhentet trafikkdata eller kommunikasjonskontroll, eller fra den som er rammet av beslaget eller andre. Noen ganger vil slike holdepunkter foreligge innledningsvis, for eksempel allerede når det tas beslag i en databærer, mens de andre ganger fremkommer etter at ransakingsprosessen har kommet så langt at man har begynte å lete etter bevis. Et eksempel på det siste er at mistenkte i avhør opplyser at e-postkontoen hans inneholder advokatkorrespondanse. Konsekvensen må da være at ransakingen av e-postkontoen stanses inntil en utsortering ved en teknisk enhet har funnet sted, forutsatt at det ikke er grunn til å se bort fra mistenktes anførsel (se like nedenfor).

Når vedkommende selv anfører at det foreligger beslagsfrie opplysninger, legges dette normalt til grunn. Kun i de tilfeller hvor anførselen fremstår som åpenbart uriktig ut fra opplysningene og omstendighetene for øvrig, kan dette utgangspunktet fravikes og ransaking gjennomføres uten å følge den særskilte prosedyren for utsortering. Det kan for eksempel tenkes at siktede har opplyst at han har korrespondert med sin advokat på appen Signal, men at innledende undersøkelser som ikke gir tilgang til lesbart innhold (se punkt 2), viser at appen ikke finnes på telefonen. I slike tilfeller skal spørsmålet forelegges påtalemyndigheten, som avgjør om

ransaking skal gjennomføres uten prosedyre for utsortering. Beslutningen loggføres i eventuell beslutningslogg eller notoritet sikres på annen hensiktsmessig måte.

Når vedkommende som er rammet av beslaget anfører at en datamengde inneholder opplysninger med beslagsforbud, bør han oppfordres til å angi type/mengde beslagsfrie opplysninger og hvor disse finnes (i e-post, sms, notater e.l.). Spørsmål om dette må ikke stilles på en slik måte at det innbyr til et svar som er egnet til å avdekke korrespondansens innhold.

Den som har krav på hemmelighold, kan samtykke til fritak fra taushetsplikt etter straffeprosessloven § 119, og samtykket opphever da beslagsforbudet i straffeprosessloven § 204. Det legges derfor til grunn at vedkommende også kan samtykke i at ransaking foretas uten forutgående utsortering. Samtykket skal være skriftlig.

#### *4.3.3 Hvilken enhet som skal foreta utsorteringen, taushetsplikt mv.*

Utsorteringen skal skje ved Enhet for Digitalt politiarbeid (DPA) eller annen teknisk enhet som er organisatorisk adskilt fra etterforskningsenheten. Politimesteren har ansvaret for å utpeke hvilken enhet i distriktet som skal ha denne oppgaven. Dersom det vurderes som hensiktsmessig, kan politidistriktene samarbeide om én eller flere slike enheter. I det følgende omtales den tekniske enheten for enkelhets skyld som DPA.

Personell ved enheten skal gis opplæring i behandling av denne type beslag. Den som skal foreta utsorteringen, kan ikke opptre i andre roller eller utføre andre oppgaver i etterforskningen av saken.

Taushetsplikten etter politiregisterloven § 24 innebærer at personell som utfører utsortering og blir eksponert for beslagsfrie opplysninger, ikke kan bringe disse videre til etterforskningsenheten eller andre. Dette gjelder selv om opplysningene kan være av interesse for etterforskningen av saken.

#### *4.3.4 Påtalemyndighetens beslutning om å iverksette utsortering ved DPA og utforming av oppdraget*

Påtalemyndigheten beslutter at det skal iverksettes prosedyre for utsortering av opplysninger med beslagsforbud. Politifaglig etterforskningsleder (PEL) sørger for at det utformes et oppdrag til DPA. Oppdraget kan ved behov utformes i samråd med DPA.

Oppdraget til DPA *skal* inneholde:

- Opplysninger om hvem som har fattet beslutning om utsortering
- Beslutning om ransaking
- Opplysninger av betydning for utsorteringen, for eksempel – om det er kjent – hvor i materialet de beslagsfrie opplysningene befinner seg, type, mengde, aktuelle søkeord ol.

Videre *bør* oppdraget inneholde:

- Dokumentasjon som kan være relevant for DPA, f.eks. beslagsrapport eller sikringsrapport.
- Intern prioritet dersom det for eksempel er flere enheter i samme sak
- En vurdering av hvor mye utsorteringen haster basert på sakens alvor og beslagets betydning for etterforskningen

Datamengden og eventuell fysisk lagringsenhet overføres til DPA.

#### *4.3.5 Behandlingen ved DPA*

Det skal være et system for notoritet om mottatt materiale, og dette skal oppbevares på sikker måte.

Det skal etableres en dokumentert original tilstand av det digitale beslaget. Med dette menes for eksempel en såkalt checksum eller hashverdi.

DPA vurderer hvordan arbeidet med utsorteringen av opplysninger teknisk skal gjennomføres. Ved behov kan det anmodes om bistand fra et annet politidistrikt eller fra Kripos, for eksempel ved mangel på kapasitet eller teknisk kompetanse. Etter omstendighetene kan det være fornuftig å ha dialog med mistenkte eller forsvarer for å identifisere og lette utsorteringsarbeidet, og det skal alltid vurderes om det er grunn til å initiere en slik dialog.

Innhold som kan være undergitt beslagsforbud, skal deretter utsorteres.

Dersom det identifiseres mulig beslagsfrie opplysninger som av tekniske årsaker ikke kan utsorteres, kan påtalemyndigheten beslutte at hele materialet oversendes tingretten for vurdering av om opplysningene er beslagsfrie.

DPA utarbeider en sluttrapport om hvordan arbeidet er gjennomført og organisert. Rapporten må redegjøre for de ulike trinnene i prosessen slik at det kan kontrolleres at disse er gjennomført i tråd med direktivet.

Etter utsortering gjøres den resterende delen av datamengden tilgjengelig for etterforskningsenheten.

#### *4.3.6 Den videre behandling ved etterforskningsenheten*

Etterforskningsenheten gjennomfører ransaking av datamengden som er gjort tilgjengelig etter utsortering, jf. punkt 4.3.5. Dersom det under den videre ransakingen avdekkes opplysninger som kan være underlagt beslagsforbud, gjennomføres prosedyren for utsortering ved DPA på nytt.

Påtalemyndigheten kan beslutte at hele eller deler av de utsorterte opplysningene sendes tingretten for vurdering av om opplysningene er undergitt beslagsforbud.<sup>10</sup>

#### 4.3.7 Unntak ved stor fare for at bevis kan gå tapt

Dersom det er stor fare for at bevis ellers vil gå tapt, kan det etter en helhetsvurdering foretas ransaking uten en forutgående utsortering ved DPA selv om det er grunn til å tro at det foreligger beslagsfrie opplysninger. Dette er ment å være et meget snevert unntak. Sentrale momenter ved denne vurderingen vil være sakens alvor og om det vil skade etterforskningen i vesentlig grad om de aktuelle bevisene går tapt. Spørsmålet forelegges påtalemyndigheten, som avgjør om ransaking skal foretas uten forutgående utsortering ved DPA. Beslutningen loggføres i eventuell beslutningslogg eller notoritet sikres på annen hensiktsmessig måte.

Et eksempel på en slik situasjon kan være at politiet ved pågripelsen av en mistenkt i en alvorlig narkotikasak ser at han har en åpen telefon hvor det pågår en aktiv chat på en kryptert plattform som sletter meldinger automatisk etter kort tid. Eventuelle bevis vil dermed gå tapt dersom politiet ikke undersøker chatten på stedet. Selv om det er grunn til å tro at telefonen inneholder advokatkorrespondanse, vil påtalemyndigheten etter en konkret vurdering kunne beslutte ransaking for å sikre chatten uten at den særskilte utsorteringsprosedyren følges.

Dersom politiet ved ransakingen oppdager mulig beslagsfrie opplysninger, skal disse så langt det er mulig sorteres ut fortløpende. Ransakingen kan ikke gå lenger enn det som er strengt nødvendig for å sikre bevis som kan gå tapt. Eventuell ytterligere gjennomgang må utstå til etter at utsorteringen ved teknisk enhet er gjennomført.

Riksadvokaten legger til grunn at unntaket er i samsvar med EMK art. 8 nr. 2, idet det anses både proporsjonalt og legitimt begrunnet i hensynet til kriminalitetsbekjempelse.

#### 4.3.8 Nødrett mm.

Påtalemyndigheten kan beslutte ransaking uten forutgående utsortering i nødrettssituasjoner hvor vilkårene i straffeloven § 17 er oppfylt.<sup>11</sup> Dersom det er stor fare ved opphold, kan beslutningen treffes av polititjenesteperson.

### **4.4 Beslag og ransaking hos en person som innehar stilling som nevnt i straffeprosessloven § 119**

Ved ransaking rettet mot en person som innehar en stilling om nevnt i straffeprosessloven § 119, for eksempel en advokat, er det en presumpsjon for at det vil foreligge opplysninger underlagt taushetsplikt og beslagsforbud.<sup>12</sup> Ransaking av beslag foretatt hos en advokat har vært gjenstand for en rekke rettslige avklaringer de senere årene, men det er fremdeles flere uavklarte spørsmål. Det ligger utenfor rammen av dette direktivet å gi nærmere regler om fremgangsmåten for ransaking i slike tilfeller.

<sup>10</sup> Se Rt-2017-111-A (avsnitt 46): "Aksepteres det at påtalemyndigheten i første omgang gjennomgår beslaget, vil formentlig rettens oppgave i praksis bli avgrenset til å ta stilling til det materiale påtalemyndigheten oversender til prøvelse."

<sup>11</sup> Om nødrett som hjemmelsgrunnlag for tvangsmiddelbruk, se Bruce og Haugland, Skjulte tvangsmidler, side 92 flg.

<sup>12</sup> Se HR-2018-699-a (avsnitt 27).



Riksadvokaten legger til grunn at politiet kan foreta beslag og gjøre undersøkelser som ikke gir tilgang til lesbart innhold, slik som sikring og klargjøring, også i disse tilfellene.<sup>13</sup> For øvrig gjelder prinsippene beskrevet i bl.a. Rt-2018-699-A (avsnitt 22):

*"Rettspraksis har slått fast at materiale som er sikret ved ransaking hos advokat, må overleveres til tingretten for utsortering av beslagsfritt materiale før det resterende kan utleveres til politiet for vurdering av beslag, se blant annet [Rt-2013-968](#), særlig avsnitt 40."*

Jørn Sigurd Maurud

Line Steen Presthus  
statsadvokat

Dokumentet er elektronisk godkjent og har derfor ingen signatur

#### **Mottakere**

Agder politidistrikt	Postboks 514, Lundsiden	4605	KRISTIANSAND S
Det nasjonale statsadvokatembetet	Postboks 2101 Vika	0125	OSLO
Finnmark politidistrikt	Postboks 501	9917	KIRKENES
Hedmark og Oppland statsadvokatembeter	Postboks 4457	2326	HAMAR
Hordaland, Sogn og Fjordane statsadvokatembeter	Markeveien 4 c	5012	BERGEN
Innlandet politidistrikt	Postboks 355	2303	
Kripos	Postboks 2094 Vika,	0125	OSLO
Møre og Romsdal politidistrikt	Postboks 1353 Sentrum	6001	ÅLESUND
Møre og Romsdal statsadvokatembeter	Postboks 2517	6404	MOLDE
Nordland politidistrikt	Postboks 1023	8001	BODØ
Nordland statsadvokatembeter	Postboks 273	8001	BODØ

---

<sup>13</sup> Se Rt-2013-968, HR-2018-699-A og LB-2018-87329.

**Mottakere**

Oslo politidistrikt	Postboks 2093 Vika	0125	OSLO
Oslo statsadvokatembeter	Postboks 2100 Vika	0125	OSLO
Politiets Utlendingsenhet			
Politihøgskolen			
Rogaland	Postboks 180	4001	STAVANGER
statsadvokatembeter			
Sør-Vest politidistrikt	Postboks 240	4001	STAVANGER
Sør-Øst politidistrikt	Postboks 2073	3103	TØNSBERG
Troms og Finnmark	Postboks 2503	9267	TROMSØ
statsadvokatembeter			
Troms politidistrikt	Postboks 6132	9291	TROMSØ
Trøndelag politidistrikt	Postboks 2475 Torgarden	7005	TRONDHEIM
Trøndelag	Postboks 4733 Torgarden	7468	TRONDHEIM
statsadvokatembeter			
Utrykningspolitiet			
Vest politidistrikt	Postboks 85	6901	FLORØ
Vestfold, Telemark og	Postboks 2630	3129	Tønsberg
Buskerud			
statsadvokatembeter			
Økokrim	Postboks 2096 Vika	0125	OSLO
Øst politidistrikt	Postboks 3390	1401	SKI