NORGES HØYESTERETT

Den 28. mars 2019 avsa Høyesterett bestående av dommerne Webster, Kallerud, Falch og Høgetveit Berg og kst. dommer Lindsetmo kjennelse i

HR-2019-610-A, (sak nr. 19-010640STR-HRET), straffesak, anke over kjennelse:

Tidal Music AS	(advokat Fredrik Berg – til prøve)
mot	
Påtalemyndigheten	(advokat Henrik Horn – til prøve)

S T E M M E G I V N I N G :

(1) Dommer **Kallerud:** Saken gjelder tredjemannsransaking hos det norske selskapet Tidal Music AS i Oslo, jf. straffeprosessloven § 192 tredje ledd nr. 3. Spørsmålet er om politiet fra dataterminaler i selskapets kontorlokaler i Oslo kan laste ned elektronisk materiale selskapet har lagret i utlandet, eller om slik tvangsbruk faller utenfor norske myndigheters jurisdiksjon.

(2) Tidalgruppen består av en rekke selskaper med tilhørighet blant annet i USA og flere europeiske land og tilbyr en strømmetjeneste hvor abonnenter blant annet kan spille av musikk. Tidal Music AS er et norsk selskap i Tidalgruppen. Det norske selskapet omtales i det følgende stort sett som Tidal.

(3) Økokrim fremsatte 3. desember 2018 begjæring til Oslo tingrett om tredjemannsransaking rettet mot Tidal på selskapets forretningsadresse i Oslo. Det fremgår av begjæringen at mistanken er rettet mot «ukjent gjerningsperson», og at den gjelder databedrageri i form av manipulasjon av antall avspillinger for å påvirke vederlagsberegningen til fordel for noen rettighetshavere. Tidal Music AS har etter det opplyste ikke status som siktet eller mistenkt i saken. Det politiet ønsker tilgang til er materiale som antas å kunne kaste lys over det mulige straffbare forholdet som mistanken gjelder. Dersom informasjon av betydning som bevis viser seg å være lagret elektronisk, omfatter begjæringen også «de aktuelle

databærere og elektronisk lagret informasjon som vedkommende har tilgang til», herunder «online databærere i form av servere m.m.».

(4) Oslo tingrett tok 5. desember 2018 Økokrims begjæring om ransaking hos Tidal til følge.

(5) Ransakingen ble satt i verk 17. desember 2018 i selskapets lokaler i Oslo. Tidal motsatte seg ransaking og beslag som innebar at det fra selskapets terminaler i Norge ble lastet ned materiale som Tidal hadde lagret på servere i utlandet.

(6) Konkret gjelder tvisten for det første 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. Materialet ble lagret på en minnepinne som nå befinner seg hos Økokrim.

(7) Det andre omstridte forholdet gjelder 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. Nedlasting ble satt i gang etter instruks fra politiet, men viste seg å ta lang tid. Økokrim ba derfor eieren av epostkontoen om å kopiere materialet over på en harddisk som Økokrim etterlot på stedet for senere avhenting. På grunn av uenigheten om adgangen til å foreta ransaking, er dette materialet ikke overlevert Økokrim.

(8) Tidal anket tingrettens beslutning til Borgarting lagmannsrett, som 18. januar 2019 forkastet anken. Lagmannsretten kom til at vilkårene for ransaking var oppfylt etter straffeprosessloven § 192 tredje ledd nr. 3. Det forelå etter rettens oppfatning skjellig grunn til mistanke, og det var særlig grunn til å anta at det kunne finnes bevis som kan beslaglegges ved ransaking hos Tidal. Inngrepet var ikke uforholdsmessig. Tidal bestred ikke at disse vilkårene var oppfylt.

(9) Når det gjaldt det omstridte spørsmålet – om ransakingen kunne gjennomføres til tross for at materialet var lagret i utlandet – kom lagmannsretten til at tvangsmiddelbruken måtte anses foretatt under norsk jurisdiksjon. Ransaking ville derfor ikke krenke noen annen stats suverenitet. Retten la her blant annet vekt på at tvangsmiddelbruken foregår i Norge, ved at en ansatt i Tidal – etter pålegg – gir politiet tilgang til serverne i utlandet fra selskapets kontor i Norge. Det er dermed ikke tale om noen inntrengen i serveren i utlandet. Retten vektla også at beslag av materiale fra serverne vil oppnås fra Norge.

(10) Tidal har anket lagmannsrettens kjennelse til Høyesterett. Ved Høyesteretts ankeutvalgs beslutning 7. februar 2019 ble ankesaken overført til avgjørelse av Høyesterett i avdeling, jf. domstolloven § 5 første ledd andre punktum.

(11) *Tidal Music AS* har i det vesentlige gjort gjeldende:

(12) Det bestrides ikke at vilkårene for ransaking etter straffeprosessloven § 192 tredje ledd nr. 3 sammenholdt med § 192 første ledd isolert sett er oppfylt. Det «oppbevaringssted» som ønskes ransaket er imidlertid servere hvor Tidals data er lagret. Disse serverne er ikke i Norge. Materialet befinner seg på et territorium hvor andre stater har eksklusiv tvangsmyndighet. Det er altså utenfor norsk jurisdiksjon. Den ransakingen lagmannsretten har godtatt har virkning i det landet hvor serverne befinner seg blant annet i form av datastrøm gjennom et fysisk ledningsnett i utlandet. Ransakingen krenker derfor disse

statenes suverenitet.

(13) Norge er ikke part i noen traktater som gjør unntak fra suverenitetsprinsippet i dette tilfellet. Statspraksis varierer, og det finnes ingen folkerettslig sedvanerett som kan gi den nødvendige hjemmel.

(14) Tillates ransaking i et tilfelle som dette, er det fare for at det gis tilgang til opplysninger oppbevaringsstaten har sterk interesse av å beskytte, for eksempel av personvernhensyn. Norge må i tilfelle være forberedt på at andre stater tillater at deres politi foretar ransaking av servere som befinner seg på norsk jord. Dette kan være svært betenkelig.

(15) Tidal Music AS har lagt ned slik påstand:

> **«Lagmannsrettens kjennelse oppheves.»**

(16) *Økokrim* har i det vesentlige gjort gjeldende:

(17) Den internrettslige hjemmelen er utvilsom. Norge er ikke bundet av noen traktat eller folkerettslig sedvane som hindrer ransaking i dette tilfellet. Tvangsbruken foregår her ved at politiet skaffer seg adgang til et norsk selskaps oppbevaringssted for mulig bevismateriale gjennom lovlig tilgang til selskapets datasystem fra dets kontorlokaler i Norge. Dette er intet inngrep i en annen stats suverenitet.

(18) Politiet er bare til stede på norsk territorium, tvangen er utelukkende rettet mot et selskap hjemmehørende i Norge og det etterlates ingen fysiske spor i den stat materialet er oppbevart. Politiet foretar seg ikke noe annet enn det selskapet selv lovlig kan gjøre på lagringsstedet i utlandet.

(19) Mulige innsigelser mot at politiet får tilgang til nedlastet materiale, må avgjøres på dokumentnivå etter reglene om hva som kan beslaglegges.

(20) Ved vurderingen bør det også legges vekt på behovet for effektiv bekjempelse av internasjonal nettbasert kriminalitet.

(21) Økokrim har lagt ned slik påstand:

> **«Anken forkastes.»**

(22) *Mitt syn på saken*

(23) Høyesteretts kompetanse er begrenset til å prøve lagmannsrettens saksbehandling og generelle lovtolking, jf. straffeprosessloven § 388 første ledd.

(24) *Internrettslig hjemmel for ransaking*

(25) De påberopte og anvendte ransakingshjemlene er straffeprosessloven § 192 første og tredje ledd. De aktuelle delene av § 192 har denne ordlyden:

> **«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 søke etter bevis eller etter ting som kan beslaglegges … .**

…

Hos andre kan ransaking foretas når det er skjellig grunn til mistanke om en slik handling, og

…

3) det for øvrig er særlig grunn til å anta at … det der kan finnes bevis eller ting som kan beslaglegges … .»

(26) Lagmannsretten har slått fast at både de alminnelige vilkår for ransaking etter bestemmelsens første ledd og det særlige vilkår for tredjemannsransaking i tredje ledd er oppfylt. Lagmannsretten la videre til grunn at inngrepet ikke er uforholdsmessig, jf. straffeprosessloven § 170 a. Tidal har heller ikke for Høyesterett bestridt lagmannsrettens forståelse av ordlyden i § 192 og aksepterer at den internrettslige hjemmelen i og for seg er oppfylt.

(27) Etter mitt syn oppstår det ingen tolkingsspørsmål knyttet til straffeprosessloven § 192 i saken her. Som lagmannsretten forstår jeg § 192 tredje ledd nr. 3 slik at det ved tredjemannsransaking kan ransakes på de samme steder som etter første ledd, altså blant annet på «oppbevaringssted». Dette kan omfatte et datanettverk, herunder en server som befinner seg utlandet.

(28) Tidal har imidlertid anført at lagmannsretten gjennom en henvisning til straffeprosessloven § 199 a i sine premisser må forstås slik at retten legger til grunn at denne bestemmelsen utvider adgangen til ransaking i utlandet. Jeg leser ikke lagmannsrettens kjennelse på denne måten. Men jeg er enig med Tidal i at § 199 a ikke utvider ransakingsadgangen. Bestemmelsen gir – ved ransaking av et datasystem – hjemmel for å «pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet». Vilkårene for ransaking, for eksempel etter § 192 tredje ledd nr. 3 sammenholdt med § 192 første ledd, må imidlertid være oppfylt for at det skal kunne gis pålegg etter § 199 a.

(29) Selv om vilkårene etter straffeprosessloven § 192 er oppfylt, har Tidal videre vært inne på at bestemmelsen ikke er klart nok formulert dersom meningen også er å gi hjemmel for ransaking av servere i utlandet. Jeg kan ikke se at legalitetsprinsippet skaper vansker her. Ordlyden – «oppbevaringssted» – omfatter utvilsomt lagringssted for datamateriale. Og det er intet i ordlyden som kan lede til den oppfatning at visse steder for oppbevaring skulle være unntatt.

(30) Som jeg straks kommer til, kan imidlertid tvangsmidler bare brukes innenfor norske myndigheters jurisdiksjon. Dette gjelder som en selvsagt forutsetning for all bruk av straffeprosessuelle tvangsmidler, og er ikke noe særegent for ransaking av datasystemer. Jeg kan ikke se noen grunn til å kreve at grensene for norsk jurisdiksjon av hensyn til legalitetsprinsippet må angis særskilt når det gjelder ransaking av datasystemer. Den nærmere grensedragningen må gjøres ut fra folkerettslige prinsipper og etter en konkret vurdering av tvangsmiddelet og hvordan det ønskes brukt.

(31) Jeg legger etter dette til grunn at det ikke er noe ved den generelle tolkingen av straffeprosessloven § 192 – basert på interne norske kilder – som hindrer at ransakingen gjennomføres slik de tidligere instanser har godtatt.

(32) *Folkerettslig begrensning av ransakingsadgangen*

(33) Reglene i straffeprosessloven gjelder etter § 4 med «de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat».

(34) *Traktater*

(35) For Høyesterett har partene særlig drøftet Europarådskonvensjonen om datakriminalitet fra 2001 som medlemstatene i Europarådet er bundet av, og som også blant annet USA har sluttet seg til.

(36) Konvensjonen pålegger statene å iverksette nærmere angitte tiltak for å bekjempe datakriminalitet. Eksempelvis er det i artikkel 18 bestemt at statene skal sørge for at det etableres en slik tilgang som i norsk rett er fastsatt i straffeprosessloven § 199 a. I artikkel 29 følgende er det gitt bestemmelser om gjensidig bistand. Konvensjonen fastsetter imidlertid bare minimumsforpliktelser for statene, jf. blant annet NOU 2007: 2 Lovtiltak mot datakriminalitet side 47. Ingen av konvensjonsbestemmelsene angår direkte et tilfelle som i saken her. Jeg går derfor ikke nærmere inn på denne konvensjonen.

(37) Det finnes heller ingen andre spesifikke traktatbestemmelser som hindrer den aktuelle type ransaking. På den annen side er det ikke etablert et traktatrettslig grunnlag for å foreta ransaking i et tilfelle som i saken her.

(38) For ordens skyld nevner jeg at det ikke er lagt frem opplysninger som kunne tilsi at Den europeiske menneskerettskonvensjon (EMK) i dette tilfellet setter skranker for tvangsmiddelbruken. Dette er heller ikke anført av noen av partene.

(39) *Begrensninger anerkjent i folkeretten – suverenitetsprinsippet*

(40) Det klare folkerettslige utgangspunktet er at statene bare kan utøve tvang på eget territorium. Tvangsjurisdiksjonen er eksklusiv; ingen stat kan anvende tvangsmidler på en annen stats territorium uten samtykke fra vedkommende stat. Norsk lovgivning er basert på dette. Det er eksempelvis på det rene at norsk politi og påtalemyndighet ikke kan foreta pågripelser utenlands eller ransake et hus i et annet land. I slike tilfeller er rettshåndhevende myndigheter avhengig av bistand fra – eller avtaler med – andre land.

(41) Disse alminnelige utgangspunktene gir imidlertid mindre veiledning når det gjelder ransaking og beslag av elektronisk lagret materiale. Slikt materiale kan ikke bare lagres på brukerens personlige lagringsenheter – for eksempel egen datamaskin, minnepinne eller harddisk – men kan også plasseres «i skyen». Dette skjer gjerne ved bruk av lagringstjenester som tilbys av utenlandske selskaper, slik som Google og Amazon i saken her. Også ved slik lagring befinner imidlertid materialet seg på en eller flere fysiske lagringsenheter – for enkelhets skyld ofte omtalt som servere. Etter det opplyste kan det være nokså tilfeldig på hvilken server en norsk brukers data lagres. Og lagringsstedet kan over tid endres uten at brukeren blir informert eller kan kontrollere dette. Selv om det skulle være på det rene at det fysiske lagringsstedet ikke er i Norge, kan det – slik saken her viser – være ukjent i hvilket land materialet til enhver tid er lagret.

(42) De rettslige spørsmål som den teknologiske utviklingen aktualiserer ved bruk av tvangsmidler rettet mot lagringssteder «i skyen» er lite avklart, både i norsk rett og internasjonalt.

(43) *Norsk praksis*

(44) Det finnes ingen avgjørelser fra Høyesterett som belyser grensen for norsk tvangsjurisdiksjon i et tilfelle som i saken her.

(45) Norsk politi og påtalemyndighet har etter det opplyste lagt til grunn at det er anledning til å foreta ransaking av servere i utlandet når fremgangsmåten er som her. Det vises særlig til Metodeutvalgets utredning NOU 1997: 15, hvor det tas som utgangspunkt at «det dreier seg om ransaking i Norge når tilgang til dataene oppnås fra en terminal som befinner seg i Norge», se punkt 4.2.1.3. Etter utvalgets oppfatning må det kunne undersøkes «hvilke data som er tilgjengelig på den aktuelle terminal, uavhengig av om opplysningen er lagret i utlandet.»

(46) Jeg nevner videre at norsk praksis på andre områder trolig bygger på noe av den samme tankegangen. Eksempelvis har det ikke vært problematisert om det kan gjennomføres kommunikasjonskontroll selv om den ene samtalepartneren viser seg å være i et annet land. I praksis gis det etter det opplyste pålegg om utlevering i medhold av straffeprosessloven § 210 også om den tingen som antas å ha betydning som bevis skulle befinne seg utenlands.

(47) Synspunktene i NOU 1997: 15 ledet ikke til endringer i lovgivningen, og den beskrevne praksisen ser ut til å ha blitt fulgt uten at jurisdiksjonsspørsmålet tidligere har blitt problematisert.

(48) *Praksis fra andre land – internasjonale utredninger*

(49) Praksis i andre land varierer. Jeg nevner noen eksempler og utredninger til illustrasjon.

(50) Dansk Højesteret avgjorde 10. mai 2012 at politiet kunne få adgang til siktedes Messenger- og Facebook-profiler selv om opplysningene knyttet til profilene befant seg på servere i utlandet. Politiet hadde blitt kjent med de nødvendige koder for å skaffe seg tilgang gjennom telefonavlytting.

(51) Etter svensk rett har synspunktet derimot vært at territorialprinsippet hindrer politiet å gå inn på internettbaserte kommunikasjons- eller lagringstjenester dersom leverandørens servere kan befinne seg utenfor Sverige. Dette gjelder selv om politiet har fått tilgang til de nødvendige innloggingsopplysningene. Jeg viser her til den omfattende utredningen i SOU 2017: 89 Hemlig dataavläsning – ett vikitigt verktyg i kampen mot allvarlig brottslighet side 444. Utvalget bemerker imidlertid at det finnes «stärka skäl att nyansera denna hittillsvarande officiella svenska hållning», se sammendraget på side 28 i utredningen og nærmere på side 465 følgende. I utvalgets avsluttende vurdering heter det blant annet på side 482:

> **«Såvitt avser de praktiska skälen för att förändra den svenska hållningen är det enligt vår mening starkaste argumentet att det, när en brottsutredning (eller ett underrättelseärende) pågår i Sverige och riktas mot en person som befinner sig här samt avser ett brott som begåtts (eller planeras) i riket, framstår som tämligen märkligt att**

> **svenska brottsbekämpande myndigheter inte ska kunna samla in elektroniskt lagrade uppgifter trots att de kan tillgängliggöras i Sverige utan att någon risk t.ex. för informationssäkerheten uppstår i den stat (eller i förekommande fall de stater) där uppgifterna lagras. Än mer märkligt blir detta med hänsyn till att lagringsplatsen i de allra flesta fall torde vara både irrelevant och okänd för den som äger eller disponerar informationen, och som alltså finns i Sverige, så länge hen kan få fram informationen på eget kommando. Med så många anknytningspunkter till en svensk utredning är det helt enkelt svårt att se varför lagringsplatsen i dessa fall ska avgöra den exekutiva jurisdiktionsfrågan.»**

(52) For så vidt gjelder øvrige europeiske land nøyer jeg meg med å vise til gjennomganger av praksis i rapporter fra ekspertgrupper i Europarådet i 2012 og 2016 og en arbeidsgruppe under EU-kommisjonen i 2018.

(53) Resultatene av undersøkelsen fra Europarådets ekspertgruppe i 2012 er det grundig redegjort for i SOU 2017: 89 på side 469 følgende. Denne gjennomgangen viser at det ikke er uvanlig at stater mener seg berettiget til å foreta en slik ransaking som i saken her, også om det er klart at materialet er lagret på en utenlandsk server. En annen ekspertgruppe i Europarådet avleverte 16. september 2016 en rapport med tittelen «Criminal justice access to electronic evidence in the cloud …». Om praksis heter det blant annet på side 16 avsnitt 45:

> **«It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country.»**

(54) Undersøkelsen foretatt av EU-gruppen etterlater det samme inntrykket. Det heter på side 11 i rapporten betegnet SWD (2018) 118 og datert 17. april 2018:

> **«The national law in at least 20 Member States empowers authorities, subject to judicial authorisation, to seize and search a device and remotely stored data accessible from it …»**

(55) Det fremgår i fortsettelsen at dette er stadig mer relevant ettersom data nå regelmessig er lagret «… on servers in a different location, possibly outside of the Member State concerned or even outside of the EU.»

(56) For så vidt gjelder internasjonal litteratur begrenser jeg meg til å vise til «Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations» fra 2017. Manualen er utarbeidet med deltakelse fra en rekke internasjonale eksperter etter invitasjon fra «the NATO Cooperative Cyber Defence Centre of Excellence». Under den forklarende teksten til «Rule 11 – Extraterritorial enforcement jurisdiction» fremheves at det kan være vanskelig å avgjøre jurisdiksjonsspørsmål «in the cyber context», se avsnitt 12. Jeg oppfatter rapporten slik at ekspertene – i favør av å godta territorial jurisdiksjon – blant annet legger vekt på om det aktuelle materialet «is meant to be accessible from the State concerned», se avsnitt 13, og om tilgang til materialet kan oppnås ved å anvende statens tvangsjurisdiksjon overfor rettssubjekter som befinner seg i landet, se avsnitt 16 og 17.

(57) *Oppsummering av praksis*

(58) Gjennomgangen viser at det ikke er etablert noen folkerettslig sedvane på dette området. Etter det opplyste finnes også lite rettspraksis som kan tjene til veiledning.

(59) Likevel er det av interesse at mange land i praksis synes å godta en slik ransaking som i saken her. Det er heller ikke opplyst noe om mellomstatlige reaksjoner knyttet til at et lands myndigheter gjennom tvangsmidler overfor rettssubjekter på eget territorium har fått tilgang til materiale lagret i en annen stat.

(60) *Utgangspunkt for vurderingen av om suverenitetsprinsippet er krenket*

(61) Så lenge det ikke finnes noen internasjonal konsensus, eller anvendelige konvensjonsbestemmelser, må norske rettsanvendere på selvstendig grunnlag ta stilling til om bruk av tvangsmidler krenker en annen stats suverenitet. Ved vurdering av om norske myndigheters tvangsjurisdiksjon begrenses av suverenitetsprinsippet ved ransaking av et datasystem med lagringsenheter utenlands, kan det etter mitt skjønn være hensiktsmessig å ta utgangspunkt i en overordnet vurdering som denne: Griper den aktuelle ransakingen inn i en annen stats eksklusive tvangsjurisdiksjon på en slik måte at denne statens suverenitet krenkes?

(62) Den endelige vurderingen må nødvendigvis bli konkret og avhengig av de nærmere omstendighetene ved den aktuelle ransakingen.

(63) De faktiske omstendighetene som fremgår av lagmannsrettens dom, og som jeg oppfatter at lagmannsretten har lagt vekt på, er etter mitt syn relevante. Begrunnelsen viser at lagmannsretten har lagt riktig rettsoppfatning til grunn. Jeg oppsummerer kort de sentrale momentene.

(64) *Ransakingen hos Tidal – momenter i vurderingen*

(65) Lagmannsretten la vekt på at tvangsmiddelet – beslutning om ransaking hos Tidal og pålegg om å gi tilgang til selskapets datasystem – er satt i verk på norsk territorium; i Tidals kontorlokaler i Oslo.

(66) Som saksgangen viser, er beslutning om ransaking truffet av norske domstoler med ivaretakelse av alminnelige rettssikkerhetsgarantier.

(67) Videre er det på det rene at materialet gjøres tilgjengelig gjennom bruk av tvangsmidler overfor et norsk selskap med kontor i Norge. Det er altså her ikke tale om at norske myndigheter på egenhånd trenger seg inn i materiale som ligger lagret i utlandet.

(68) I denne forbindelse nevner jeg at norske myndigheter utvilsomt har tvangsjurisdiksjon overfor det norske selskapet og dets ansatte som befinner seg her i landet. På dette grunnlaget kan norske myndigheter pålegge selskapet og disse personene å gi nødvendige opplysninger, slik at norske myndigheter får tilgang til lagrede data. Straffeprosessloven § 199 a gir nasjonal hjemmel for dette. Den aktuelle ransakingen ble utført ved å benytte de tilgangsopplysningene selskapet hadde gitt til Økokrim.

(69) Det fremgår av lagmannsrettens avgjørelse at ransakingen bare vil gi tilgang til materiale som selskapet selv har lagret. Og selskapet kan selv fritt hente materialet tilbake fra det utenlandske lagringsstedet.

(70) Endelig er det klart at materialet er i behold på den utenlandske serveren. Det gjøres heller ingen endringer i det lagrede materialet, for eksempel i form av sletting eller sperring. Et eventuelt beslag gjøres tilgjengelig ved kopiering til politiets egne lagringsenheter i Norge.

(71) I alle fall når situasjonen er som her, kan jeg ikke se at ransakingen berører en annen stat på en slik måte at det innebærer en krenkelse av suverenitetsprinsippet.

(72) Lagmannsretten har etter dette lagt til grunn en riktig forståelse av de rettslige normer som kommer til anvendelse, og anken må forkastes.

(73) Jeg føyer til at spørsmål knyttet til om det er begrensninger i adgangen til å ta beslag i materiale som finnes ved ransakingen – her som ellers – må avgjøres etter straffeprosesslovens regler om dette, se særlig § 204 som blant annet viser til vern av advokatkorrespondanse og forretningshemmeligheter. Tvist om bevistilgang kan på vanlig måte forelegges domstolen, jf. § 205 andre og tredje ledd og § 208. Også anførsler om at beslag vil føre til krenkelse av siktedes rettigheter – for eksempel etter bestemmelser i Grunnloven og EMK om rett til privatliv og rett til rettferdig rettergang – kan prøves rettslig på denne måten.

(74) Jeg stemmer for denne

K J E N N E L S E :

Anken forkastes.

(75) Dommer **Falch:** Jeg er i det vesentlige og i resultatet enig med førstvoterende.

(76) Kst. dommer **Lindsetmo:** Likeså.

(77) Dommar **Høgetveit Berg:** Det same.

(78) Dommer **Webster:** Likeså.

(79) Etter stemmegivningen avsa Høyesterett denne

K J E N N E L S E :

Anken forkastes.