Det dynamiske beslag

Om politiets rettslige adgang til innkommende kommunikasjon ved ransaking av databeslag

En juridisk oppgave

BACHELOROPPGAVE (BOPPG30)
Politihøgskolen
2019

Kand.nr : 978
Antall ord: 6593

Innholdsfortegnelse

1. Innledning

1.1 Presentasjon av tema

Straffeprosessloven gir politiet hjemmel til å blant annet ransake etter, og beslaglegge, ting som tilhører andre. Dette er ofte nødvendig for å etterforske et potensielt straffbart forhold, for å finne ut av hva som har skjedd og hvem som kan klandres for det. For å sikre borgerne mot maktmisbruk fra myndighetenes side, er det viktig med et godt utarbeidet og tydelig regelverk.

Utviklingen av data- og nettverksteknologi har medført store endringer i etterforskningssituasjoner som straffeprosesslovens tvangsmiddelbestemmelser opprinnelig tok sikte på.[1] I dagens praksis kan dette lede til enkelte, tilsynelatende, hull i lovgivningen. Mangel på relevant rettspraksis har heller ikke vært til hjelp i tolkningen av lovverket. På grunn av dette har det oppstått noen uklarheter i det straffeprosessuelle skillet mellom ransaking og beslag, og politiets skjulte tvangsmidler som kommunikasjonskontroll. Dette fremstår problematisk når de skjulte tvangsmidlene i utgangspunktet er klart mer inngripende i retten til privatliv enn hva gjelder ransaking og beslag.

Med denne oppgaven er hensikten å gjøre et forsøk på å utforske disse uklare skillene, for å kartlegge dets begrensninger og muligheter. Målet er å bli tryggere på hvilke etterforskningsmessige avgjørelser som på best måte sikrer de involvertes rettssikkerhet og en objektiv etterforskning ved behandling av databeslag.

1.2 Problemstilling

Som ledd i etterforskningen av en straffesak blir A sin smarttelefon beslaglagt. A ønsker å samarbeide med politiet, og oppgir tastelåskoden. Den beslaglagte smarttelefonen er automatisk innlogget på en rekke nettbaserte tjenester som telefonen mottar innkommende meldinger fra. I tillegg til at den beslaglagte enheten mottar meldinger, svarer A på disse gjennom de nettbaserte tjenestene fra en annen enhet enn den beslaglagte. Som politietterforsker har man nå muligheten til å lese all korrespondanse inn- og ut, som A foretar seg på de nettbaserte tjenestene, og som i praksis tilsvarer en form for telefonavlytting. Hvorvidt man i mange tilfeller rent teknisk har tilgang på denne informasjon, kan ikke

[1] Inger Marie Sunde, "Straffeprosessuelle metoder rettet mot elektroniske bevis", *Rettssikker Radikaler: Festskrift til Ståle Eskeland 70 år*, Oslo 2013 s. 266-283 (s. 266).

bestrides. Om politiet har *rettslig adgang* på innkommende kommunikasjon som oppstår etter at beslaget er tatt, er en annen sak, som skal undersøkes nærmere i denne oppgaven.

1.3 Avgrensning

Av hensyn til oppgavens ordbegrensning vil den derfor ikke ta for seg en juridisk analyse hva angår den innhentede informasjonens faktiske bevisverdi i retten. Oppgaven vil ei heller ta for seg i hvilken utstrekning politiet kan benytte seg av innhentet informasjon i annet etterforsknings- eller etterretningsøyemed. Det vil heller ikke foretas en mer inngående analyse av Grunnlovens- og det folkerettslige vernet om privatliv, annet enn å fastslå de poengene som er avgjørende for at politiet kan foreta inngrep.

Begrepet *kommunikasjon* vil i denne oppgaven ikke begrense seg til kun overføringsprosessen av informasjon fra sender til mottaker, men bli brukt i betydningen av korrespondanse.

1.4 Rettskildebildet og metode

Det er ingen tvil om at ordlyden i straffeprosessens lovtekst ikke nødvendigvis gir noe klart svar når det kommer til problemstillinger av informasjonsteknologisk natur. Derfor har oppgaveløsningen vært nødt til å se til straffeprosesslovens forarbeider, spesielt i henhold til de endringer som er gjort opp mot skjulte etterforskningsmetoder og de forsøk på å holde loven oppdatert i arbeidet mot datakriminalitet. Det er lite relevant rettspraksis på området, og vurderinger av de reelle hensyn blir mer aktuelt i så tilfelle.

For å besvare problemstillingen brukes alminnelig juridisk metode til å undersøke de ulike tvangsmidlene i straffeprosessloven som kan tenkes å hjemle en slik informasjonsinnhenting fremstilt i problemstillingen. Oppgaven vil ta utgangspunkt i ransaking og beslag, og vurdere dette opp imot de skjulte metodene kommunikasjonsavlytting og dataavlesing. Ved å se hen til disse tvangsmidlenes lovforarbeider, tolkes lovgivers intensjon og argumenter, og tvangsmidlets tiltenkte hensikt. Dette skaper et grunnlag for vurderinger *pro et contra* av de øvrige rettskildene. Lovtekst, forarbeider, rettspraksis, reelle hensyn og annen juridisk teori tolkes i lys av hverandre, og drøftes for å utlede en gyldig rettsregel.

2. Konstitusjonelle og menneskerettslige rammer

Når politiet bruker makt for å foreta inngrep i borgernes privatliv, foreligger det både folkerettslige- og grunnlovfestede prinsipper som skal sikre borgernes rettsvern. Dette er en grunnpilar i det demokratiske samfunn.

2.1 Grunnloven

Borgernes rett til generelt vern mot statens inngrep i ens privatliv er nedfelt i Grunnloven § 102, ved at "Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon.". Samtidig er det formulert et legalitetsprinsipp i Grunnloven § 113: "Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov".

Dette setter klare rammer for når myndighetene har rett til å foreta slike inngrep, som spesifiseres blant annet i straffeprosessloven. Sistnevnte lov er utformet for å sikre alle parters rettsikkerhet i en straffesak, og legger til grunn for når, hvordan og hvorfor staten eventuelt kan gripe inn i borgernes rett til privatliv og kommunikasjon.

Ransaking av smarttelefoner, eller avlytting av disse, medfører klare inngrep i retten til privatliv. Grunnloven legger ingen andre begrensninger for problemstillingen enn at eventuelle inngrep fra statens side hjemles i lov, henholdsvis straffeprosessloven i oppgavens tilfelle.

2.2 Den Europeiske Menneskerettighetskonvensjonen

I tillegg til Grunnloven, utgjør også Den Europeiske Menneskerettighetskonvensjonen en selvstendig skranke for norsk lovgiving, ved dens inkorporering i norsk rett.[2] Dens artikkel 8 nr. 1, tilsvarer formuleringen i Grunnlovens § 102 første avsnitt første punktum.[3]

Alle inngrep vernes imidlertid ikke automatisk, og staten kan gripe inn i borgernes rettssfære under de tre vilkårene i artikkelens nr. 2, som alle må være tilstede for å legitimere inngrepet. Kun hvis inngripen er (i) i samsvar med loven, (ii) nødvendig i et demokratisk samfunn, og

[2] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)
[3] Se pkt. 2.1

(iii) formålsbestemt etter spesifikasjoner i artikkelen, herunder forebygge kriminalitet og uorden, eventuelt for å beskytte andres rettigheter og friheter, vil det være å anse som et legitimt inngrep.

3. Hva kan ransakes etter, og beslaglegges?

3.1 Ting og bevis

Ransakingsbestemmelsen[4] gir politiet anledning til å "søke etter bevis eller etter ting som kan beslaglegges". Av bestemmelsen vedrørende beslag[5], legger den til grunn at "ting som antas å ha betydning som bevis, kan beslaglegges ...". Dette medfører at politiet har anledning til å beslaglegge en smarttelefon, hvis det kan antas at den inneholder informasjon som kan kaste lys over spørsmålet om hvorvidt det er blitt begått et straffbart forhold, og hvem som eventuelt kan ha skyld.

Ut ifra lesing av lovtekstens ordlyd, er det noe uklart hva som faller innunder begrepet "ting", spesielt når man snakker om tilsynelatende abstrakte enheter som elektronisk lagret informasjon.

3.2 Elektronisk lagret informasjon som ting

Straffeloven § 69 fastslår at elektronisk lagret informasjon er å anse som ting, ved "Som ting regnes også rettigheter, fordringer og elektronisk lagret informasjon". Lovgivers intensjon ved denne lovendringen var å presisere begrepet ting til å gjelde "informasjon som er egnet til elektronisk behandling, i dagligtalen ofte omtalt som 'data'".[6] Det er således tydelig at datafiler er å regne som ting, og kan ransakes etter og beslaglegges.

3.3 Kommunikasjon som elektronisk lagret informasjon

Datakrimutvalgets definisjon av "data", baserer seg på en tredelt hierarkisk modell.[7] Datasystem og elektronisk kommunikasjonsnett utgjør modellens nederste nivå, og representerer fysiske størrelser som infrastruktur. Det samme kan sies om data og dataprogram i modellens midterste nivå. Dette nivået representerer de "elektroniske signalene

[4] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) §§ 192 og 195
[5] Straffeprosessloven § 203
[6] Ot.prp. nr. 90 (2003:2004) s. 463
[7] NOU 2007: 2 s. 60

som lagres, behandles eller overføres på eller ved hjelp av et datasystem eller via et elektronisk kommunikasjonsnett". Det er denne definisjonen og forståelsen som ligger til grunn for lovens fortolkning av "elektronisk lagret informasjon", eller "data", i nevnte straffeloven § 69. Det øverste nivået i den hierarkiske forståelsen av data, er den semantiske data, som kalles "databasert informasjon". Dette betegnes gjerne som meningsinnholdet og budskapet som mennesket selv tolker ved sansing og persepsjon av innholdet på en dataskjerm eller av en innkommende melding som kan ha betydning som bevis.

Inger Marie Sunde, professor ved Politihøgskolen, er tydelig i sin doktorgradsavhandling på at slik uttrykket "elektronisk lagret informasjon" brukes i lovteksten, ikke vil innbefatte databasert informasjon.[8] Derfor vil det råde noe tvil om politiet kan ta beslag i innkommende meldinger fra en nettbasert kommunikasjonstjeneste, hvis meningsinnholdet i disse vil være å anse som databasert informasjon. Likevel er det klart at databasert informasjon er avhengig av et medium eller en "informasjonsbærer". Når meldingen kommer inn på telefonen, vil den lagres, og gjør sitt utspring via et medium - en datafil. Den vil følgelig kunne beslaglegges som "elektronisk lagret informasjon". Politiet har dermed adgang til å beslaglegge innkommende meldinger som er elektronisk lagret.

3.4 Adgangen til ransaking i det virtuelle rom

Det er tydelig av forarbeidene i "Endringer i straffeprosessloven mv. (skjulte tvangsmidler)" at adgangen til å ransake rom tolkes utvidende til å også gjelde ransaking av elektroniske rom, herunder virtuelle brukerkontoer.[9] I lovproposisjonen står dette spesifikt uttrykt under tvangsmiddelet hemmelig ransaking. Likevel må en slik forståelse av ransakingsbestemmelsen også omfatte ordinær ransaking, slik Kripos uttaler i sitt høringssvar til Metodekontrollutvalget: "Eksempelvis kan en slik ordinær ransaking være at politiet ransaker mistenktes e-post- eller facebookkonto etter at mistenkte er pågrepet, ved at brukernavn og passord beslaglegges eller at mistenkte opplyser dette til politiet".[10]

Ransaking av brukerkontoer tilknyttet slike nettbaserte kommunikasjonstjenester vil ofte reise spørsmål om tvangsmiddelet faller utenfor norske myndigheters jurisdiksjonsområde. Dette fordi informasjonens opphav rent teknisk sett ofte befinner seg på en dataserver i et annet

[8] Inger Marie Sunde, *Automatisert inndragning*, 2010 s. 57
[9] Prop. 68 L (2015-2016) s. 226
[10] Kripos' høringsuttalelse 19. april 2010 til NOU 2009: 15 s. 16

land. Denne problemstillingen med server- og skylagrede data medfører at det er vanskelig å trekke et skille for når ransakingen strekker seg over landegrenser og således underlegges folkerettslige begrensninger. Metodeutvalget fastslår likevel følgende: "Etter utvalgets oppfatning må utgangspunktet være at det dreier seg om ransaking i Norge når tilgangen til dataene oppnås fra en terminal som befinner seg i Norge.".[11] Dette begrunnes blant annet i reglene om utleverings- og vitneplikt, hvis sistnevnte plikt "ikke begrenses i forhold til opplysninger som befinner seg i Norge".

Det aktuelle jurisdiksjonsspørsmålet ble nylig diskutert i Høyesterett[12], som henviste til, og konkluderte på lik linje med, Metodeutvalgets utredning fra 1997. Under ransaking hos tredjeperson etter straffeprosessloven § 192 tredje ledd, vil "oppbevaringssted" utvilsomt kunne omfatte dataserver i utlandet, og en enstemmig Høyesterett kunne ikke se at suverenitetsprinsippet krenkes når datamaterialet i utenlandsk server oppnås fra Norge.

3.5 Forholdsmessighetsprinsippet og speilkopiering

Utfra ovennevnte argumentasjon er politiets adgang til å ransake etter, og beslaglegge, Facebook-meldinger og chat gjennom en allerede beslaglagt smarttelefon, udiskutabel. Likevel er straffelovgivningens forholdsmessighetsprinsipp avgjørende for politiets adgang til ransaking og beslag. All bruk av tvangsmidler er kun legitim hvis den samtidig følger kravene i straffeprosessloven § 170 a: "Et tvangsmiddel kan kun brukes når det er tilstrekkelig grunn til det. Tvangsmiddelet kan ikke brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep".

Første punktum angir en hensiktsmessighetsbegrensning, hvor grunnen til inngrepet *skal* være "tilstrekkelig". Dette er i de aller fleste beslag- og ransakingssituasjoner oppfylt ved at inngrepet eksempelvis vil kunne føre til oppdagelsen- eller sikring av bevis. Andre punktum leder over i en forholdsmessighetsvurdering, som baserer seg på en interesseavveiing hos de involverte parter, sakens art og forholdene ellers. Dette kan for eksempel være bevisforspillelsesfare, siktedes sosiale- eller personlige forhold. Vil politiets ransaking og

[11] NOU 1997: 15 s. 80
[12] HR-2019-610-A

beslag av smarttelefon og Facebook-konto være å anse som uforholdsmessig eller uten tilstrekkelig grunn, vil det da følgelig være illegitim bruk av makt.

I dagens moderne samfunn kan et beslag i ens smarttelefon oppleves som omfattende og inngripende. Telefonen benyttes i alle slags hverdagslige situasjoner, samtidig som i dens funksjon av å være en datamaskin kan inneholde og oppbevare store datamengder av privat og sensitiv karakter. Likevel vil eksempelvis hensynet til bevisforspillelsesfaren og den offentlige interessen for etterforskningen av kriminalitet ofte veie tyngre enn de involverte parters interesser, slik at politiet kan iverksette inngrepet.

Av hensyn til hensiktsmessighetsbegrensningen og forholdsmessighetsvurderingen i lovteksten kan ikke politiet uten videre bruke så lang tid de ønsker på å undersøke beslaget, eller holde beslaget tilbake uten grunn. Så fort databeslaget er gjennomsøkt etter bevis, bortfaller den tilstrekkelige grunnen til å gjennomføre videre granskinger, samt beslagsadgangen til selve enheten som gjennomsøkes.

3.5.1 Direkte gransking og speilkopiering

Et beslag i en smarttelefon vil naturligvis medføre store mengder data som skal gjennomsøkes. Det vil da reises spørsmål om en direkte, manuell gransking av et slikt databeslag vil være forholdsmessig. Med dette menes at man ransaker, eller gransker, enheten uten hjelp av tekniske innretninger, og selv søker etter og dokumenterer bevis ved avfotografering og kopiering av filer. Dette kan, men må nødvendigvis ikke, være tid- og kapasitetskrevende.

Per i dag har politiet likevel muligheten til å benytte seg av teknologi som gjør det mulig å *speilkopiere* et databeslag, som smarttelefoner. Dette vil si at man i praksis tar en eksakt kopi av dataverdiene i beslaget, uten at dette skal gå på bekostning av muligheten til å gjennomgå beslaget i etterkant.

Teoretisk sett, vil dette være den mest skånsomme og forholdsmessige måten å gjennomføre etterforskingen på. Dette gjelder både overfor bevisets integritet, og forholdsmessigheten sett opp mot siktedes behov for sin egen telefon ved muligheten til å få utlevert denne raskt fra politiets undersøkelse. En slik speilfil vil også lettere la seg automatisk granske etter bevis, ved bruk av søkefunksjoner i datasystemet. Dette gir mulighet til å gjennomgå store mengder

data på kort tid. Likevel medfører denne speilkopieringen visse praktiske ulemper, fordi denne prosessen fortsatt i dag er ressurskrevende og spesialisert. Enkelte tjenesteenheter har heller ikke tilgang på denne teknologien og kompetansen i dag, og det kan fort ta flere dager å ta en speilkopi av et beslag hvis det er flere enheter i andre saker som prioriteres.

3.5.2 Plikten til å speilkopiere databeslag

Det kan reises spørsmål om hvorvidt forholdsmessighetskravet i straffeprosessloven § 170 a fører til at politiet er pliktig å foreta en speilkopiering av beslaglagte dataenheter. Dette spørsmålet er behandlet av Høyesterett[13], i en sak hvor politiet hadde beslaglagt datagjenstander blant annet med hensikt å sikre bevis. Tingretten påla politiet, etter straffeprosessloven § 170 a, å speilkopiere innholdet i beslagene. Lagmannsretten var på sin side uenig i denne tolkningen av loven, mens Høyesterett i sin uttalelse mente at det ikke lå noe i veien for at et beslag prinsipielt sett kun er forholdsmessig der man foretar en speilkopiering. Likevel utspiller ikke dette seg som en generell plikt til å foreta speilkopiering.[14] I praksis ender dette i en forholdsmessighetsvurdering av de involverte parters interesser.

Selv om det ikke foreligger en plikt til å foreta speilkopiering av databeslag, er det likevel en hel rekke med hensyn som tilsier at man bør foreta speilkopiering før innsyn i beslag. Ved datatekniske undersøkelser er etterprøvbarhet og dataenes integritet viktige prinsipper. Ved speilkopiering av databeslaget, verner man om rettssikkerheten på en mye bedre måte enn ved manuell undersøkelse og sikring av beslaget. Sistnevnte metode kan blant annet endre metadata, og på en slik måte forringe beslagets bevisverdi.

Likevel er man nødt til å foreta forholdsmessighetsvurderinger i de sitasjonene det ikke nødvendigvis er hensiktsmessig å foreta speilkopieringen, med tanke på kompetanse, tidsbegrensning, tilgjengelige ressurser og sakens tilstand. Da må dette veies opp mot blant annet potensiell fare for kontaminasjon av databeslaget.

Samtidig vil forholdsmessighetskravet i mange tilfeller være avgjørende om man i det hele tatt kan speilkopiere beslaget. Som nevnt tidligere, kan en smarttelefon inneholde millioner

[13] Rt. 2012 s. 1645 avsn. 14
[14] Inger Marie Sunde, "Databevis" i *Bevis i straffesaker*, Oslo 2015 s. 599-633 (s. 608)

med datafiler og sensitiv informasjon. I en bagatellmessig sak kan det derfor tenkes at speilkopiering av siktedes smarttelefon ikke vil være forholdsmessig, hvorpå man med manuell gransking kunne gjennomført ransakingen på en mindre inngripende og mer forholdsmessig måte.

Av dette kan det konkluderes med at det allerede er en rekke hensyn som må tas, både om og hvordan informasjonen i det hele tatt kan sikres.

4. Det dynamiske beslag

I utgangspunktet regnes en ransaking etter gjeldende rett "utført som en enkeltstående og tidsmessig avgrenset handling. ... inngrepet skal avsluttes så snart objektet er gjennomsøkt.".[15] Ved ordinær ransaking av et åsted, fryses dette og beslag tas med og representerer åstedet som stillbilde slik politiet fant det. Situasjonen blir noe annerledes hvis en tar dataransaking- og beslag i betraktning. Dette skiller seg fra et ordinært åsted i den grad en ofte er nødt til å gjennomgå beslaget på nytt i etterkant, og deretter ta nye beslag ved den etterfølgende granskingen.

Ved beslag av eksempelvis en smarttelefon, kan bevis nemlig oppstå etter at politiet har gjort tilslag, men før man har rukket å granske beslaget etter bevis. Telefonen kan motta chat-meldinger eller oppringinger mens den ligger i en beslagspose på vei til kontoret. Dermed står man i en situasjon hvor sjansen til å avdekke "bevis" gjennom innkommende meldinger, øker med tiden som går. Spekulasjon i hvor lang tid man bruker på å sette i gang selve speilkopieringen av beslaget, kan derfor ha noe å si for de "innkommende bevisene".

4.1 Ransaking og beslag av "innkommende bevis"

I tillegg til å kunne kartlegge siktedes tidligere foretatte kommunikasjon, kan man derfor i praksis få tilgang til innkommende kommunikasjon. I enkelte tilfeller vil en slik ransaking også innebære at politiet overværer siktedes toveiskommunikasjon, hvis siktede selv opptrer på brukerkontoen som ransakes gjennom en annen enhet, slik som forestilt i problemstillingens tilfelle. Her blir skillet fort utydelig på hvorvidt slike innkommende meldinger faller innunder begrepet "elektronisk lagret informasjon" og om politiet da kan ta

[15] Prop. 68 L (2015-2016) s. 263

beslag i dette. Kommunikasjonen vil fremdeles rent teknisk materialisere seg som elektronisk lagret informasjon som anført i argumentasjonen over, dette være seg lokalt på beslaget eller i en dataserver tilknyttet den nettbaserte kommunikasjonstjenesten. Informasjonen kan derfor i utgangspunktet ransakes og beslaglegges. Likevel medfører dette visse betenkeligheter, når informasjonens natur skiller seg fra historisk lagret, statisk informasjon ved at den er aktiv og kan "overvåkes" på lik linje med kommunikasjonskontroll. Dette blir en utfordring når ransaking- og beslagsreglene ikke er dimensjonert for moderne informasjonsteknologi.

4.1.1 Har politiet plikt til å hindre "innkommende bevis"?

I Rt. 2000 s. 1345 fremgår Høyesteretts behandling av spørsmålet om hvorvidt et bevis skulle avskjæres som ulovlig ervervet. Beviset gjaldt en etterforsker som hadde plukket opp en innkommende samtale til en beslaglagt telefon, uten å opplyse om sin identitet. Forholdet kan sies å være direkte sammenlignbart til situasjonen hvor en etterforsker i dag mottar innkommende chat-meldinger når han ransaker en beslaglagt telefon, sett bort ifra provokasjonsmomentet. I nevnte sak konkluderte Høyesterett med at beviset kunne føres, fordi politiet blant annet "ikke kunne ha plikt til å slå av den beslaglagte mobiltelefonen".[16] Det vil derfor være tvilsomt at politiet har plikt til å for eksempel sette beslaglagte telefoner i flymodus eller logge av Facebook-kontoen, slik at man unngår innkommende kommunikasjon. Dette er dog en påstand som tilsynelatende står ubegrunnet, og som i dagens etterforskning vil medføre særdeles mye større bevisforspillelsesfare enn for 20 år siden, med tanke på fjernsletting av innhold i databeslag tilkoblet telekommunikasjon.

Høyesterett konstaterte også at politiet må "ha adgang til å lese tekstmeldinger eller høre mobilsvarmeldinger som kom inn til mobiltelefonen". Det trekkes paralleller til, og argumenteres med: "I så måte har situasjonen likhetstrekk med den som foreligger når politiet lovlig beslaglegger privat korrespondanse og deretter leser denne." Spørsmålet blir hvorvidt denne analogien egner seg til bruk i lignende saker, i et samfunn med andre forutsetninger for kommunikasjon, hvor den kan sies å være rikere og potensielt sett inneholde mer enn kun tekstmeldinger og mobilsvarmeldinger. Kjennelsen ble avsagt for snart 20 år siden, og det kan tenkes at førstvoterende hadde en annen forståelse av hva slags informasjon en kunne få ut av å lese innkommende meldinger på en telefon den gang, enn det man har tilgang på i dag.

[16] Rt. 2000 s. 1348

Doktorgradsstipendiat Anett Osnes skriver følgende om beslagsanalogien i sin avhandling:

> "Etter Høyesteretts kjennelse i Rt. 2000 s. 1345 har imidlertid oppfatningen om nødvendigheten av en positiv, rettslig forankring når myndighetene tar seg tilgang til noens private gjemmer beveget seg noe i motsatt retning på dette punkt ... Den jevnførelse som fremholdes i kjennelsen med at det tas beslag i privat korrespondanse og dokumenter med sensitivt innhold, dekker ikke det dynamiske elementet som innkommende kommunikasjon til den beslaglagte enheten representerer. Betraktningen er derfor etter min vurdering ikke vidtrekkende nok når man ser hen til dagens rettskildebilde."[17]

Det er her tydelig at en kan argumentere for at den informasjonsteknologiske utviklingen over de siste 20 årene har ført til at argumentasjonen som ligger til grunn for kjennelsen ikke lenger har like tydelige likhetstrekk opp mot oppgavens problemstilling. Analogien til ransaking og beslag av privat korrespondanse står ikke i stil til hvor enkelt man nå kan gjennomsøke all "post", personlige brev, og mer til, ved kun noen få tastetrykk og målrettede søk. Samt har utviklingen av internett utvilsomt ført til en særdeles mer utbredt dokumenterbar informasjonsutveksling enn hva gjelder tilsvarende tidligere brevkorrespondanse. Med henblikk på dagens teknologi, vil et beslag i mistenktes dynamiske kommunikasjonsanlegg, eksempelvis en smarttelefon, medføre et klart større integritetsinngrep enn ved beslag i statisk innhold som eksempelvis analog brevkorrespondanse.

Reelle hensyn taler for at innkommende meldinger som oppstår etter opprinnelig beslag av smarttelefon bryter med den tradisjonelle forståelsen av et fryst åsted og ransakingen som en enkeltstående og tidsmessig avgrenset handling. Selv om disse meldingene materialiserer seg som datafiler som ellers er tilgjengelige som ting og bevis etter ransaking- og beslagsreglene, vil en med dette kunne argumentere for at det dynamiske elementet i beslaget ikke dekkes av de straffeprosessuelle reglene man har i dag.

4.2 Aktiv innhenting av "innkommende bevis"

En ransakningstillatelse gjelder for nettopp kun én ransaking, og Metodekontrollutvalget konkluderer med at: "Det er alminnelig antatt at det ikke kan gis adgang til gjentatt eller

[17] Anett Beatrix Osnes, *Bruk av materiale fra hemmelig avlytting av kommunikasjon som bevis i straffesak : abusos non tollit usum?* 2013 s. 19

fortløpende ransaking etter norsk rett i dag"[18], og at politiet må se seg nødt til å innhente en ny ransakingsbeslutning for hver ny ransaking. Bruker man kriminalåstedet igjen som analogi, gjelder ransakingen for én ransakingssituasjon. Selv om ransakingssituasjonen kan foregå over flere dager i de alvorligste sakene, og at samme objekt kan ransakes flere ganger i samme sak, avsluttes inngrepet så snart objektet er gjennomsøkt. Hvis man går tilbake til samme åsted for å søke etter nye spor, fordrer dette en ny ransakningsbeslutning.

4.2.1 Fortløpende ransaking i virtuelle rom

Når det kommer til ransaking av virtuelt rom, uttalte Kripos et behov for gjentatt ransaking av elektroniske lagringsrom hvis innhold ofte endres. De foreslo at lovens ordlyd i hemmelig ransaking ikke står i veien for at retten kan gi tillatelse til flere ransakinger i samme beslutning, gitt at situasjonen fortsatt oppfyller kravene i straffeprosessloven §170 a.[19] Kripos viser til at dette har vært prøvd i tingretten, som ga tillatelse til gjentatt ransaking da kjennelsen ikke ble påanket av den offentlige oppnevnte forsvarer. Avgjørende vilkår for at det ikke er å anse som overvåking og "fortløpende ransaking", er at politiet forlater stedet, herunder også virtuelle rom, etter hver undersøkelse. Sett opp imot problemstillingens tilfelle, vil en slik beslutning om gjentatt ransaking i praksis åpne for muligheten til å lese inn- og utgående meldinger fra en beslaglagt smarttelefon, over tid.

Reelle hensyn tilsier likevel at dette ikke vil gjøre seg gjeldende i oppgavens problemstilling med en beslaglagt telefon som mottar meldinger ved spesialisert chat-tjeneste. Dette med bakgrunn i at Kripos' intensjon i anført argument siktet til informasjonsinnhenting som var utilgjengelig for datidens skjulte metoder på grunn av krypteringsproblematikk, som blant annet var grunnlaget for ønsket om å innføre dataavlesing som ny metode. Nå har man dataavlesing som kan nyttes i de sakene som kvalifiserer til skjult metodebruk, hvor kryptering er et aktuelt moment. At generelle saker, typisk oppgavens problemstilling, ikke kvalifiserer til skjult metodebruk, er heller regelen enn unntaket.

4.2.2 Gjentatt ransaking

Spørsmålet kan da være hvorvidt den gjeldende rettstilstand kan gi politiet tillatelse til gjentatt ransaking, slik Kripos foreslår det som en mellomting mellom enkeltstående ransaking og

[18] NOU 2009: 15 s. 246
[19] Høringsuttalelse 19. april 2010 s. 17

forløpende ransaking. Metodekontrollutvalget var på sin side klar i sin konklusjon, og anså at gjentatt ransaking innebærer en "klar utvidelse" sammenlignet med dagens regler, og "en for stor integritetskrenkelse i forhold til det anførte behovet".[20] Lovendringsforslaget uttaler seg ikke om legitimiteten av Kripos' praksis. I møte med Riksadvokaten, ble likevel Metodekontrollutvalget anbefalt å vurdere å gi retten tillatelse til å gi beslutning om gjentatt ransaking, på lik linje med dansk rett. Det vises til at den danske retten i kjennelse kan gi tillatelse til gjentatt hemmelig ransaking over en bestemt tidsperiode, innført allerede i 2002.[21] Dette gjelder også ved gjentatt hemmelig ransaking mot elektronisk lagret informasjon og brukerkontoer på nettbaserte kommunikasjonstjenester.[22]

Sett opp i mot situasjoner som nevnt i oppgavens problemstilling, vil man kunne si at en beslutning fra retten om gjentatt ransaking uansett kun vil være snakk om et mer hypotetisk og lite anvendelig tankeeksperiment. Kripos uttaler at gjentatt ransaking som regel vil være lite aktuelt i en åpen etterforskning.[23] Dette begrunnes med at siktede har mulighet til å innrette sin kommunikasjon når åpen bruk av tvangsmidler "etter sin art er avslørende".

Derfor vil reelle hensyn kunne tale for at ved et ordinært beslag av en smarttelefon hvor siktede ikke er inkapasitert ved pågripelse eller fengsling, at det ikke vil være tilstrekkelig grunn etter straffeprosessloven § 170 a til å ransake den innkommende kommunikasjonen. I den grad siktede er klar over politiets tilgang til kommunikasjonen og vil han nemlig kunne innstille sin atferd deretter.

4.2.3 "Overvåkende" informasjonsinnhenting "over tid"

Tidligere nevnte høyesterettskjennelse slo fast at politiet "ikke kunne ha plikt til å slå av den beslaglagte telefonen"[24], og sannsynligheten for at det oppstår nye potensielle bevis i "det dynamiske beslaget"[25] vil derfor øke desto lenger tiden går. Likevel er departementets vurdering tydelig i lovendringsforslaget til dataavlesing der "En ransakningstillatelse gir derimot ikke adgang til å overvåke ransakingsobjektet (for eksempel forbli pålogget på en e-postkonto eller datamaskin) over tid for å fange opp ny aktivitet eller ny informasjon som

[20] NOU 2009: 15 s. 246 i Prop. 68 L (2015-2016) s. 263
[21] Retsplejeloven § 799, stk.3
[22] Dansk Højesterets kjennelse 10. mai 2012 i sak 129/2011, jf. retsplejeloven § 793, stk. 1, nr. 1, jf. § 799, i Prop. 68 L (2015-2016) s. 228
[23] Prop. 68 L (2015-2016) s. 254
[24] Rt. 2000 s. 1345
[25] Se oppgavens pkt. 4

produseres fortløpende av mistenkte eller andre."[26] Av dette kan man tolke at den informasjonsinnhenting som er "overvåkende" og foregår "over tid", helt klart vil falle utenfor ransaking- og beslagsbegrepet dersom hensikten er å fange opp ny aktivitet eller ny informasjon som produseres. Reelle hensyn tilsier at karakteristikken "overvåkende" må kunne tilfalle all systematisk informasjonsinnhenting som strekker seg utover det med et tilfeldig preg, som eksempelvis meldinger i automatiske varsler. Tidsaspektet "over tid" kan heller ikke sies å strekke seg særlig langt, og må nødvendigvis også være oppfylt så fort ransakingsobjektet er ferdig gjennomsøkt.

Selv om departementet i sin vurdering bruker "forbli pålogget" i sitt eksempel, vil argumentet vært nødt til å gjelde også i de tilfellene man ikke opprettholder en kontinuerlig tilstedeværelse i det virtuelle rommet, ved å logge inn og ut. Osnes bekrefter også langt på vei en slik tolkning av ransakingshjemmelen, ved at hun i sin avhandling skriver: "Når det å få tilgang til innkommende kommunikasjon er det reelle formål med beslaget, må beslaget oppheves og rettens tillatelse til avlytting begjæres".[27]

Man kan derfor argumentere med at forarbeidene til straffeprosessloven her tilsier at en innhentning av slike innkommende meldinger helt klar vil falle utenfor ransaking- og beslagsbestemmelsene hvis intensjonen og det reelle formålet med ransakingsbeslutningen er å få tak i ny, innkommende kommunikasjon. Samme argumentasjon vil gjelde i de tilfeller etterforskeren med hensikt om å få størst mulig sannsynlighet for å avdekke bevis, utsetter eller bruker unødvendig lang tid på undersøkelsen av beslaget.

4.3 Alternativer til ransaking og beslag av "innkommende bevis"

Rent instinktivt vil det være naturlig å se hen til straffeprosessens regler om kommunikasjonskontroll gitt det beskrevne dynamiske beslag, hvor etterforskeren potensielt sett har tilgang til aktiv kommunikasjon. Kommunikasjonskontroll er samlebetegnelsen på politiets avlytting og annen form for kontroll av kommunikasjonsanlegg, hvor de ulike formene for kontroll er hjemlet utover i straffeprosesslovens kapittel 16 a.

[26] Prop. 68 L (2015-2016) s. 261
[27] Osnes 2013 s. 19-20

4.3.1 Kommunikasjonsavlytting

I dagligtalen er kommunikasjonskontroll ofte brukt for å beskrive inngrepet kommunikasjonsavlytting[28]. Hva denne avlyttingen innebærer fremgår av straffeprosessloven § 216 a tredje ledd, og: "kan bestå i å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke."

Ved umiddelbar lesing virker det som lovteksten vil kunne anvendes på oppgavens problemstilling. Innkommende meldinger som chat eller annen kommunikasjon på nettbaserte tjenester, vil det være naturlig å tolke som "annen kommunikasjon". En smarttelefon må også regnes for å være både telefon og datamaskin, og nettbaserte tjenester som Facebook, Snapchat eller Messenger vil en umiddelbart kunne tolkes til å være "andre anlegg for elektronisk kommunikasjon", som "mistenkte kan antas å ville bruke". Det er dog noen nyanser i de teknologiske begrepene som gjør det nødvendig med en ytterligere presisering, hvorpå en er nødt til å henvende seg til lovtekstens forarbeider.

Lovtekstens "samtaler eller annen kommunikasjon" er ment å omfatte absolutt all informasjonsutveksling mellom kommunikasjonsanlegg. Det er uttrykkelig formulert at denne informasjonsutvekslingen er å regne som kommunikasjon uavhengig hvilken form den måtte inneha, enten det være seg overføring av tekst, bilde, film eller lyd.[29] Det er derfor tydelig at chat-funksjonen til eksempelvis Facebook dekkes av lovtekstens kommunikasjonsbegrep. Forarbeidene har på dette punktet tatt høyde for den kommunikasjonsutviklingen vi har sett de siste årene med stadig økende bruk av chat som primærmetode for informasjonsutveksling mellom enheter.

Videre er det kun kommunikasjonen mellom "bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon" som det gis adgang til å avlyttes. Med slike anlegg, menes det i lovtekstens forarbeider både telefoner, datamaskiner, telefaks og personsøkere. Allerede her vil det oppstå uklarheter i forhold til oppgavens problemstilling. Informasjonsutveksling gjennom Facebook er tilknyttet en brukerkonto som uavhengig av et fysisk kommunikasjonsanlegg. Ved avlytting av en nettbasert kommunikasjonstjeneste vil avlyttingen kunne skje selv om mistenkte bytter ut fysiske kommunikasjonsanlegg. Dette står

[28] Straffeprosessloven § 216 a
[29] Ot.prp. nr. 64 (1998-1999) s. 156

i motsetning til lovteksten om at avlyttingen skal rette seg mot bestemte kommunikasjonsanlegg. Kommunikasjonsavlytting kan derfor ikke gi adgang til avlytting mot nettbaserte kommunikasjonstjenester, med mindre når den skjer via avlyttede kommunikasjonsanlegg.[30]

I tillegg til overnevnte begreper, er også avlyttingsbegrepet mer komplisert enn det tilsynelatende fremstår. Forarbeidene presiserer at det begrenser seg til avlyttingen av *signalstrømmen* mellom kommunikasjonsanleggene.[31] Avlyttingen av kommunikasjonen kan derfor kun skje i transporten mellom to anlegg. All annen innhenting av informasjon som er lagret, enten hos avsender eller mottaker, faller derfor utenfor avlyttingsbegrepet. Så fort slik informasjon ikke lenger er i en transportfase, er politiet nødt til å se til reglene om beslag og utlevering. Forarbeidene skriver uttrykkelig at: "Politiet kan heller ikke på grunnlag av en avlyttingstillatelse koble seg på en datamaskin for å hente ut annen informasjon"[32].

4.3.2 Dataavlesing

Metodekontrollutvalgets utredning fant det tilstrekkelig dokumentert at kommunikasjonsavlytting har blitt, og vil bli i enda større grad, vanskeliggjort på grunn av den teknologiske utviklingen.[33] Som illustrert ovenfor, oppstod det et behov for å effektivisere kommunikasjonskontrollen på nye plattformer som tilbyr effektiv kryptering og lagring av kommunikasjon. Riksadvokaten støttet oppunder Metodekontrollutvalgets anbefalinger om å utvide politiets adgang til kommunikasjonskontroll gjennom dataavlesing grunnet dette. Selv om Metodekontrollutvalget kun anbefalte å utvide de allerede eksisterende kontrollmetodene til å gjelde dataavlesing, ble dataavlesing stadfestet som egen metode[34].

Etter straffeprosessloven § 216 o, kan retten "gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing)". Fjerde ledd samme paragraf, sier at det bare kan gis tillatelse til å avlese:

[30] Ingvild Haugland og Geir Sunde Bruce, *Skjulte tvangsmidler*, 2. utgave, Oslo 2018 s. 201
[31] Ot.prp. nr. 64 (1998-1999) s. 156
[32] Ot.prp. nr. 64 (1998-1999) s. 157
[33] NOU 2009: 15 s. 245
[34] Prop. 68 L (2015-2016)

> "... bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller kan antas å ville bruke. Avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen.".

Med dette gjøres det klart at bestemmelsen retter seg spesifikt mot blant annet kommunikasjonen mellom brukerkontoer på nettbaserte kommunikasjonstjenester, og informasjon om brukerkontoen ellers, ved for eksempel en Facebook-konto. Denne typen elektronisk informasjon, eller kommunikasjon, er kjernen i oppgavens problemstilling. Selv om politiet kan ta beslag i en brukerkonto, har man automatisk ikke gjort dette ved beslag i smarttelefonen. Mistenkte kan fritt benyttes seg av brukerkontoen, og dette vilkåret i lovteksten vil således være oppfylt. Mistenkte besitter fortsatt brukerkontoen, og vil kunne antas å bruke denne videre gjennom andre enheter.

Dataavlesing er dog ikke et entydig juridisk definert begrep. Selve avlesingsprosessen beskrives videre i straffeprosessloven § 216 p, ved at den

> "... kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. § 199 a gjelder tilsvarende. Politiet kan bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen. Tekniske innretninger og dataprogram kan installeres i datasystemet og i annen maskinvare som kan knyttes til datasystemet. Når retten ikke bestemmer noe annet, kan politiet også foreta innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen.".

Det fremkommer av dette, at politiet har relativt stor mulighet til å skaffe adgang til dataavlesing, ved blant annet fysiske og virtuelle innbrudd. I tillegg til bruk av tekniske innretninger og dataprogram, kan avlesingen foretas "på annen måte". Det vil ikke være unaturlig å tolke en slik formulering dithen at avlesingen kan foretas ved mindre inngripende metoder enn uttrykkelig nevnt. En manuell undersøkelse av en beslaglagt, pålogget, enhet må derfor kunne sies å falle innunder begrepet "på annen måte".

Ved slik lesing av lovteksten, gis det anledning til å avlese brukerkontoer tilknyttet beslag. I problemstillingens tilfelle vil man ikke ha mulighet til å avlese informasjon som ikke er tilknyttet brukerkontoer til nettbaserte kommunikasjons- og lagringstjenester. Dette fordi mistenkte ikke "besitter eller vil kunne antas å bruke" denne smarttelefonen (datasystemet)

når den er beslaglagt. Er siktede inkapasitert, vil man derfor heller ikke ha mulighet til å lese innkommende meldinger, når siktede ikke kan antas å ville bruke kontoen. All annen informasjon som er lagret lokalt på enheten, kan innhentes ved beslagsreglene. Det blir derfor en mer teoretisk problemstilling enn noe annet, da politiet allerede har beslaglagt telefonen og gis adgang gjennom dette. En slik forståelse av lovteksten, samt at tvangsmiddelet er underlagt kapitlet "skjulte tvangsmidler" i straffeprosessloven, tyder på at dataavlesing ikke er tiltenkt enheter som allerede er beslaglagt.

4.3.3 Kommunikasjonskontrollens hinder

Selv om det kan diskuteres hvorvidt en slik dataavlesing vil være enda mer inngripende i retten til privatliv enn alminnelig kommunikasjonsavlytting, er begge metodene forståelig nok underlagt et mye strengere hjemmelsgrunnlag enn ransaking og beslag. Metoden er særdeles ressurskrevende, og utløser også krav til spesielt utpekte mannskaper og kontroll[35]. Av hensyn til disse faktorene er bruken av dataavlesing foreløpig i stor grad forbeholdt politiets særorganer, og lensmannskontoret selv blir i praksis henvist til reglene om ransaking og beslag i ordinære saker.

5. Avsluttende betraktninger

5.1 Kommunikasjonskontroll

Ut fra poeng anført i overstående kapittel, vil derfor kommunikasjonskontroll neppe gjøre seg gjeldende i oppgavens problemstilling. Kommunikasjonsavlytting faller direkte utenfor problemstillingen, i det den retter seg mot signalstrømmen mellom kommunikasjonsanlegg. Å lese innkommende meldinger med direkte tilgang på beslaget, innebærer ikke å avlese en signalstrøm. Dataavlesing vil i teorien gi mulighet til å innhente informasjon tilknyttet nettbaserte brukerkontoer i beslaget såfremt mistenkte kan ville antas å bruke kontoen. I praksis vil metoden sjeldent nyttes i en åpen etterforskning hvor siktede er innforstått med politiets beslag.

5.2 Elektronisk lagret historisk kommunikasjon

Lovteksten i beslagsparagrafen er tydelig på at elektronisk lagret informasjon er å anse som ting, og ut fra forarbeidene til ransakingsparagrafen ser vi at denne tolkes utvidende til å

[35] Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften)

gjelde det virtuelle rom. Derfor er det utvilsomt fastslått at politiet kan beslaglegge historisk lagret kommunikasjon på en beslaglagt smarttelefon eller nettbasert kommunikasjonstjeneste som bevis, hvis inngrepet ellers er forholdsmessig.

5.3 Innkommende kommunikasjon

Politiets rett til å beslaglegge innkommende meldinger i et dynamisk beslag er dog noe tvilsomt. Rettspraksisen[36] som tilsier at politiet kan lese innkommende meldinger, vil ikke kunne gis særlig tyngde som analogisk tolkning. Sammenligningsgrunnlaget har på grunn av den teknologiske utviklingen begrensede likhetstrekk til oppgavens problemstilling.

I Høyesterettskjennelsen[37] fastslås det at politiet ikke kan ha plikt til å slå av en beslaglagt telefon. Det er et argument førstvoterende tilsynelatende ikke begrunner, så det vil således kun gis noe tyngde. Reelle hensyn taler sterkt for at politiet ikke burde ha tilgang til informasjon som etter dens natur er av typen en innhenter ved kommunikasjonskontroll. Ved direkte gransking av databeslaget vil likevel informasjon en kommer over ved "tilfeldig preg" og ikke ved bevisst intensjon, sies å falle innenfor legitim informasjonsinnhenting.

Angående spørsmålet om hvorvidt politiet har ransakings- og beslagsadgang på innkommende meldinger, bør departementets vurderinger i forarbeidene til innføringen av dataavlesing veie tungt. Departementet i forarbeidene skriver at ransakningstillatelsen ikke gir adgang til å "... overvåke ransakingsobjektet ... over tid for å fange opp ny aktivitet ...".[38] Grensen for politiets adgang til innkommende kommunikasjon må derfor sies å trekkes der ny aktivitet eller innkommende meldinger er intensjonen for selve innhentingen. På tross av at forarbeidene kunne tilsi at det ville vært mulig for retten å gi politiet beslutning om fortløpende eller gjentatt hemmelig ransaking, tilsier de reelle hensyn at dette ikke burde være tilfellet sett opp mot oppgavens problemstilling med tanke på innhentingens intensjon.

Selv om det ble fastslått at politiet ikke er pliktige til å speilkopiere eller sette beslag i flymodus, vil dette være en forholdsmessighetsvurdering avhengig av sakens alvorlighet med tanke på bevisenes integritet og de involverte partenes interesser ellers. Ofte vil god etterforskningspraksis tale for at en gjør nettopp dette, i de saker hvor det er sannsynlighet for

[36] Se pkt. 4.1.1
[37] Rt. 2000 s. 1345
[38] Prop. 68 L (2015-2016) s. 261

at siktede har kapasitet til å eventuelt fjernslette innhold på nettbaserte kommunikasjonstjenester og således forspille bevis. I tillegg er det en rekke andre faktorer som tilsier at speilkopiering av databeslag ellers også sikrer etterforskningens objektivitet og etterprøvbarhet på en langt bedre måte enn manuell, direkte gransking.

5.4 Politiets rettslige adgang på kommunikasjon

De presenterte rettskildene er ikke fullt ut harmoniske, og heller ikke arbeidet med ny straffeprosesslov[39] ser ut til å reise liknende problemstillinger vedrørende "det dynamiske beslag". Likevel er det tydelig at argumentene anført i lovforarbeidene til dataavlesing[40] bør vektes med en slik tilstrekkelig tyngde i vurderingen *pro et contra* av de presenterte rettskildene, at man kan utlede en rettsregel basert disse.

Rettsregelen anvendes på følgende måte i oppgavens problemstilling: Hvis granskingen av A sin smarttelefon forholder seg til de konstitusjonelle- og menneskerettslige rammer og begrensningene i straffeprosessloven § 170 a, vil man ha tilgang på innkommende meldinger som eventuelt har tilkommet smarttelefonen etter det opprinnelige beslaget ble foretatt. Ved manuell gransking vil også meldinger som tilkommer beslaget samtidig som granskingen gjennomføres, kunne dokumenteres. Derimot, så fort etterforskeren foretar aktive tiltak som retter seg mot selve kommunikasjonen, som å følge med på innkommende meldinger, er dette illegitim informasjonsinnhenting. I tillegg vil det å utsette gransking, drøye denne, eller innhente ny ransakingsbeslutning, med hensikt om innsyn i den nye aktiviteten, også klart falle utenfor politiets innhentingsadgang ved beslutning om ransaking- og beslag, og dataavlesing må eventuelt begjæres.

[39] NOU 2016: 24
[40] Se pkt. 4.2.3

6. Kildeliste

Lover og forskrifter

Forskrift 09. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften)

Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven)

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)

Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

Lov 20. mai 2005 nr. 28 om straff (straffeloven)

Forarbeider mv.

Høringsuttalelse 19.april 2010 *NOU 2009: 15 "Skjult informasjon – åpen kontroll" - Høringssvar fra KRIPOS*

NOU 1997: 15 *Etterforskningsmetoder for bekjempelse av kriminalitet – Delinnstilling II*

NOU 2007: 2 *Lovtiltak mot datakriminalitet – Delutredning II*

NOU 2009: 15 *Skjult informasjon – åpen kontroll*

NOU 2016: 24 *Ny straffeprosesslov*

Ot.prp. nr. 64 (1998-1999) *Om lov om endringer i straffeprosessloven og straffeloven m v (etterforskningsmetoder m v)*

Ot.prp. nr. 90 (2003-2004) *Om lov om straff (straffeloven)*

Prop. 68 L (2015-2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)*

Rettspraksis

HR-2019-610-A

Rt. 2000 side 1345, side 1348

Rt. 2012 side 1645

Annen litteratur

Bruce, Ingvild og Haugland, Geir Sunde, *Skjulte tvangsmidler*, 2. utgave (Oslo 2018)

Osnes, Anett Beatrix, *Bruk av materiale fra hemmelig avlytting av kommunikasjon som bevis i straffesak : abusos non tollit usum?* (Doktorgradsavhandling) Universitet i Tromsø Det juridiske fakultet (Tromsø 2013)

Sunde, Inger Marie, *Automatisert inndragning* (Doktorgradsavhandling) Universitetet i Oslo Det juridiske fakultet (Oslo 2010)

Sunde, Inger Marie, "Databevis" i *Bevis i straffesaker*; Ragna Aarli, Mary-Ann Hedlund og Sverre Erik Jebens (red.) (Oslo 2015) s. 599-633

Sunde, Inger Marie, "Straffeprosessuelle metoder rettet mot elektroniske bevis", i *Rettssikker radikaler: Festskrift til Ståle Eskeland 70 år*; Alf Petter Høgberg, Trond Eirik Schae og Runar Torgersen (red.) (Oslo 2013) s. 266-283