Dataavlesing som etterforskningsmetode

En rettslig analyse av straffeprosessloven § 216 o

Kandidatnummer: 208

Antall ord: 14 787

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

1. juni 2017

Innholdsfortegnelse

1 Innledning

1.1 Temaet for avhandlingen

Straffeprosessloven hjemler en rekke virkemidler som politiet kan ta i bruk ved etterforskning av ulike straffbare handlinger. Blant disse finnes de skjulte tvangsmidlene.[1] De senere årene har katalogen av skjulte tvangsmidler blitt utvidet med både nyere og mer vidtgående virkemidler. Senest ved lov av 17. juni 2016 nr. 54 fikk politiet hjemmel til et nytt skjult tvangsmiddel; *dataavlesing*. Lovendringen trådte i kraft 9. september 2016 og utvider politiets fullmakter til å gjøre inngrep i borgernes private sfære. Dette er temaet for avhandlingen.

Kort fortalt er dataavlesing en metode politiet kan ta i bruk for å oppklare og avverge bestemte typer kriminalitet og som er regulert i straffeprosessloven § 216 o og § 222 d. For spesielt alvorlig kriminalitet kan Politiets sikkerhetstjeneste (PST) også benytte metoden til forebygging, jf. politiloven § 17 d. Dataavlesing innebærer at politiet eller PST kan skaffe seg tilgang til alt som blir gjort og skrevet på for eksempel en datamaskin eller en smarttelefon. Dette skjer gjennom hemmelig overvåking av datasystemer. Metoden gir tilgang til opplysninger på et så tidlig tidspunkt at informasjonen ikke er gjort utilgjengelig av kryperting. Det er kun personer som tilfredsstiller mistankekravet "skjellig grunn" i straffeprosessloven § 216 o, "rimelig grunn til å tro" i straffeprosessloven § 222 d eller "grunn til å undersøke" i politiloven § 17 d som kan utsettes for dataavlesing.

Det vil ikke være mulig innenfor rammen av denne avhandlingen å gå inn på alle problemstillinger som kan reises ved innføringen av et nytt skjult tvangsmiddel. Temaet for avhandlingen er derfor politiets adgang til å bruke *dataavlesing i etterforskingsøyemed* slik dette er regulert i straffeprosessloven § 216 o og § 216 p. Det avgrenses mot andre problemstillinger der det dreier seg om avverging og forebygging. Avhandlingen er konsentrert til de prinsipielle spørsmål knyttet til etterforskningsmetodens karakter, og formålet er å redegjøre for de mer gjennomgripende perspektiver ved dataavlesing.

[1] Se særlig straffeprosessloven § 200 a, kapittel 16 a og § 216 m.

1.2 Bakgrunn for regelverket

Spørsmålet om dataavlesing burde innføres som politimetode har blant annet vært vurdert av Lund-utvalget i NOU 2003:18[2] og Politimetodeutvalget i NOU 2004:6[3]. Etter departementets oppfatning i Ot.prp. nr. 60 (2004-2005)[4] etterlot høringen av Politimetodeutvalgets forslag et klart inntrykk av at etterforskningsmetoden burde vurderes nærmere. Det ble påpekt at det særlig var et behov for en ytterligere utredning av kompliserte tekniske spørsmål.

Som en følge av dette ble det ved kongelig resolusjon 15. februar 2008 opprettet et utvalg, Metodekontrollutvalget, som blant annet skulle "utrede og foreslå regler som tillater at politiet tar i bruk dataavlesing som metode i etterforskningen".[5] Til grunn for de ulike utredningene lå behovet for nye politimetoder i forbindelse med forebygging, avverging og etterforskning av alvorlig kriminalitet. Behovet skyldes hovedsakelig økt teknologiforståelse blant profesjonaliserte kriminelle miljøer og fremveksten av krypteringsløsninger, samt andre metoder for informasjonsbeskyttelse som har ført til at de tradisjonelle tvangsmidlene har tapt mye av sin effekt.[6]

Metodekontrollutvalgets utgangspunkt var at en eventuell utvidelse av eksisterende hjemler eller innføring av nye tvangsmidler, ikke bare måtte forankres i en solid dokumentasjon av behovet, men også at metoden ville være egnet til å tilfredsstille dette behovet på en effektiv måte.[7] Utvalget konkluderte med at det *ikke* kunne dokumenteres et tilfredsstillende behov for å innføre dataavlesing med det formål å gi politiet mulighet til å fortløpende overvåke all aktivitet i et datasystem i sanntid.[8] I stedet foreslo Metodekontrollutvalget å innføre dataavlesing som en målrettet metode som kun kunne benyttes i den utstrekning det skulle være nødvendig for å gjennomføre kommunikasjonskontroll etter straffeprosessloven § 216 a og hemmelig ransaking etter straffeprosessloven § 200 a – altså som et ledd i gjennomføringen. Metodebruken ville da skje innenfor rammene av disse respektive

[2] Se s. 126-127.
[3] Se s. 207-208.
[4] Se s. 141.
[5] Jf. mandatet til Metodekontrollutvalget inntatt i NOU 2009:15 s. 14-19.
[6] Prop. 68 L (2015-2016) s. 259-260.
[7] NOU 2009:15 s. 240.
[8] NOU 2009:15 s. 26.

tvangsmiddelhjemlene, og ville etter utvalgets oppfatning ikke innebære noe større personverninngrep enn det de allerede etablerte tvangsmidlene medførte.[9]

Departementet påpekte i Prop. 68 L (2015-2016) at det utvilsomt var et behov for å utvide eller supplere de allerede eksisterende bestemmelsene om skjulte tvangsmidler, slik at de i større grad kunne tilpasses det teknologiske virkelighetsbildet. I likhet med Metodekontrollutvalgets vurdering, la Departementet til grunn at politiets adgang til skjult tvangsmiddelbruk ikke burde utvides i større utstrekning enn det som var nødvendig for å møte behovet for effektiv kriminalitetsbekjempelse. Departementet mente imidlertid at utvalget ikke hadde tatt tilstrekkelig høyde for de teknologiske utfordringer politiet sto over i dagens samfunn, og at behovet ytterligere hadde blitt forsterket de senere årene. En særlig utfordring var fleksible løsninger for elektronisk informasjonshåndtering – som for eksempel internettbasert e-post og fildelingstjenester – som ikke fulgte lovens skille mellom informasjon som er lagret (ransaking) og informasjon som overføres mellom avsender og mottaker (kommunikasjonskontroll).[10] På bakgrunn av dette foreslo departementet å innføre dataavlesing som et nytt skjult tvangsmiddel hvor politiet gis mulighet til *vedvarende overvåking av et datasystem i sanntid*.[11] Lovforslaget avviker fra det som ble lagt til grunn av Metodekontrollutvalget i 2009.

Det endelige lovvedtaket[12] er sammenfallende med hovedlinjene i departementets forslag om å innføre dataavlesing som et tvangsmiddel hvor politiet gis adgang til vedvarende overvåkning av et datasystem i sanntid. Terskelen for å anvende tvangsmidlet er imidlertid hevet på flere områder. Eksempler på dette er at metoden ikke kan brukes for å avdekke narkotikaovertredelse etter straffeloven § 231 eller uaktsomt heleri etter straffeloven § 335, slik som departementet forslo i sin utredning.[13] De vedtatte reglene om dataavlesing er i NOU 2016:24 for det vesentlige foreslått videreført.[14]

[9] NOU 2009:15 s. 244-245.
[10] Prop. 68 L (2105-2016) s. 261.
[11] Prop. 68 L (2015-2016) s. 277, sml. 264-271.
[12] Tilføyd ved lov 17. juni 2016 nr. 54. I kraft 9. september 2016.
[13] Se prop. 68 L (2015-2016) s. 268, sml. med vedtatt § 216 o i straffeprosessloven.
[14] Se s. 107, sml. s. 341-342.

1.3 Hovedproblemstillinger

Vedtakelsen av straffeprosessloven § 216 o rører ved flere av borgernes grunnleggende rettigheter, både etter Grunnloven og Den europeiske menneskerettskonvensjonen (EMK). Eksistensen av tvangsmiddelet utfordrer særlig retten til privatliv etter Grunnloven § 102 første ledd første punktum og EMK artikkel 8. I lys av dette er det aktuelt å undersøke nærmere om de vedtatte regler om dataavlesing tilfredsstiller de minstekrav som følger av Grunnloven og EMK.[15]

Verken Høyesterett eller Den europeiske menneskerettsdomstol (EMD) har tatt stilling til om dataavlesing som etterforskningsmetode er forenlig med retten til privatliv etter henholdsvis Grunnloven § 102 første ledd første punktum og EMK artikkel 8. I den forbindelse må bestemmelsene om dataavlesing sees i lys av de øvrige skjulte tvangsmidler og rettspraksis knyttet til dette. For å kunne vurdere hvorvidt reglene om dataavlesing tilfredsstiller kravene som følger av EMK artikkel 8 og de retningslinjer som følger av EMD sin praksis, fremstår det som nødvendig å plassere dataavlesing i forhold til de øvrige skjulte tvangsmidlene. Karakteren av det integritetsinngrepet dataavlesing innebærer har flere likhetstrekk med ransaking etter straffeprosessloven § 192 og § 200 a og kommunikasjonskontroll etter § 216 a. Det er derfor av interesse å foreta en vurdering av dataavlesing i lys av *disse* tvangsmidlene.

Forskjellen mellom Metodekontrollutvalgets forslag og departementets utredning aktualiserer også spørsmålet om politiets adgang til dataavlesing i etterforsknings øyemed er videre enn det som er nødvendig for å møte behovet for effektiv kriminalitetsbekjempelse. EMD har blant annet gitt uttrykk for at det må være forholdsmessighet mellom den belastningen borgerne påføres og behovet for tiltaket.[16] For å ta stilling til dette fremstår det som nødvendig å gi en redegjørelse for og en vurdering av de ulike hensyn som gjør seg gjeldende ved innføringen av tvangsmidlet dataavlesing.

Fra et rettssikkerhets- og kontrollperspektiv, kan det reises spørsmål ved om dagens regler om dataavlesing oppfyller de kontroll- og kvalitetssikringskrav som kreves etter våre konstitusjonelle og folkerettslige forpliktelser. EMD har blant annet gitt uttrykk for at

[15] Se dokument 6 (2016-2017) s. 50-54 som også har kommet med innvendinger mot tvangsmidlet dataavlesing.
[16] Se punkt 4.2.5.

eksistensen av effektive rettssikkerhetsgarantier og kontrollmekanismer utgjør en sentral del i vurderingen av om inngrepet er forholdsmessig etter EMK artikkel 8 nr. 2.[17]

1.4 Rettskildebilde og metode

Avhandlingens viktigste rettskilder er straffeprosessloven og tilhørende forarbeider – i denne sammenheng spesielt NOU 2009:15 og Prop. 68 L (2015-2016). Overordnet står borgernes rett til privatliv som er forankret i EMK artikkel 8. Etter menneskerettsloven § 3 skal konvensjonsbestemmelsen ved motstrid gå foran annen norsk lovgivning. Retten til privatliv har i tillegg fått en grunnlovfestet forankring i Grl. § 102 første ledd første punktum. Grunnloven er lex superior.

For å besvare avhandlingens problemstillinger brukes vanlig juridisk metode. Ved tolkningen av EMK vil jeg bruke EMDs metode ettersom dette er lagt til grunn av Høyesterett.[18] Foruten tolkningen av forholdet mellom lovskravet og forholdsmessighetskravet i artikkel 8 som jeg vil komme tilbake til i punkt 4.2.2, er det ingen særskilte metodespørsmål som fortjener en mer allmenn behandling innledningsvis.

1.5 Fremstillingen videre

Problemstillingene under punkt 1.3 danner grunnlaget for avhandlingen. For å besvare disse spørsmålene er det først nødvendig å klarlegge adgangen til dataavlesing etter straffeprosessloven § 216 o de lege lata. Ettersom metoden er svært ny, er det også nødvendig å gi en nærmere rettsdogmatisk redegjørelse for hva dataavlesing innebærer, metodens karakter og geografiske virkeområde. Dette er tema i kapittel 2.

Kjennskap til de ulike hensyn som presenteres i kapittel 3 er en forutsetning både for å forstå de rettspolitiske vurderingene som ligger til grunn for regelverket om dataavlesing, og for en fornuftig og forsvarlig bruk av metoden i det enkelte tilfellet.

Bestemmelsen om dataavlesing kan videre verken forstås eller praktiserer uten at et spekter av våre konstitusjonelle og internasjonale forpliktelser tas i betraktning. I avhandlingens kapittel 4 redegjøres det først for om, og på hvilke vilkår det kan gjøres inngrep i retten til privatliv i

[17] Se for eksempel storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 233 og *R.E mot Storbritannia* avs. 122.
[18] Jf. blant annet Rt. 2000 s. 996 på s. 1007 og Rt. 2005 s. 833 avs. 45.

Grunnloven § 102 første ledd første punktum og EMK artikkel 8. Avslutningsvis foretas en vurdering av om dataavlesing slik det er innført i straffeprosessloven § 216 o kan forsvares etter unntaksvilkårene i EMK artikkel 8 nr. 2.

2 Dataavlesing

2.1 Hva er dataavlesing?

2.1.1 Generelt

Ordet ”dataavlesing” brukes i overskriften til straffeprosessloven kapittel 16 d, men defineres ikke. Ut i fra sammenhengen må ”dataavlesing” imidlertid forstås som det tvangsmidlet det er gitt hjemmel for i § 216 o.

Straffeprosessloven § 216 o første ledd gir politiet, på nærmere bestemte vilkår, hjemmel til ”avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem”. Metoden innebærer at politiet gis anledning til å overvåke bruken av datasystemet i sanntid.[19] Terminologien ”datasystem” skal i følge forarbeidene forstås som ”enhver innretning, bestående av maskinvare og programvare, som foretar behandling av data ved hjelp av dataprogrammer”. Et ”datasystem” kan etter dette for eksempel være en datamaskin, smarttelefon eller et nettbrett.[20]

I videste forstand kan dataavlesingen gi politiet innsyn i alle opplysningene som er lagret i eller er innom det aktuelle datasystemet i avlesingsperioden. Slike opplysninger kan for eksempel være programmer, dokumenter, film- og lydfiler eller e-poster som den mistenkte bevisst lagrer, samt tekniske data om bruken av datamaskinen – såkalt metadata. Ved hjelp av dataavlesing kan politiet også få adgang til informasjon som verken kommuniseres eller lagres i datasystemet, men som kun ”passerer gjennom”. Dette kan for eksempel være passord, internettsøk eller filer og tekster som den mistenkte oppretter, men uten å lagre.[21]

Avlesingen kan også rettes mot *deler av et datasystem* som for eksempel “brukerkontoer eller nettverksbaserte kommunikasjons- og lagringstjenester”, sammenlignet straffeprosessloven § 216 o fjerde ledd første punktum. Slike tjenester kjennetegnes ved at bruken ikke er bundet til bestemte datasystemer, men til et virtuelt avgrenset område (dataskyer). Et eksempel er nett-tjenesten Facebook eller Google Mail hvor brukeren identifiserer seg med brukernavn og

[19] Haugland (2016) merknad til straffeprosessloven § 216 o.
[20] Prop. 68 L (2015-2016) s. 270-271.
[21] Bruce (2014) s. 255.

passord, og således får tilgang til tjenesten fra et hvilket som helst passende datasystem.[22] Dette er opplysninger som ikke kan fanges opp ved bruk av de tradisjonelle tvangsmidlene.

På bakgrunn av dette synes det i følge forarbeidene å være informasjon som genereres *i og av* datasystemet, samt mistenktes *bruk* av datasystemet som sådan som er gjenstand for dataavlesing.[23] Avlesingen kan dermed omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruken av datasystemet eller brukerkontoen.

2.1.2 Gjennomføringen av dataavlesing

Straffeprosessloven § 216 p angir rammene for hvordan politiet kan gå frem for å gjennomføre dataavlesingen etter § 216 o. Ved å sammenholde de to bestemmelsene, er det mulig å dele gjennomføringen av dataavlesingen inn i tre ulike faser: i) en innledende fase hvor det teknologiske virkemiddelet som skal foreta avlesningen monteres eller installeres i datasystemet, ii) en avlesningsfase hvor datasystemet blir overvåket og opplysningene tilgjengeliggjort for politiet og iii) en avsluttende fase hvor det teknologiske virkemidlet fjernes eller avinstalleres.[24] Av hensynet til tvangsmiddelets karakter må følgelig hele denne prosessen skje uten den mistenktes kunnskap.

I den innledende fasen; i) hvor det teknologiske virkemiddelet som skal foreta avlesningen monteres eller installeres i datasystemet, er det mulig å skille gjennomføring i ytterligere to deler: a) hvordan foreta avlesingen og b) hvordan skaffe tilgang.

Etter bestemmelsens ordlyd kan avlesningen *foretas* ved hjelp av ”tekniske innretninger, dataprogrammer eller på annen måte”. Gjennom å bruke formuleringen ”på annen måte”, er loven gjort veldig vag og det er ikke uttømmende hva som omfattes. Utgangspunktet er at domstolene ved kjennelse gir tillatelse eller ikke tillatelse til å foreta dataavlesing for et spesifikt tidsrom mot et datasystem som den mistenkte besitter eller antas å ville bruke, jf. straffeprosessloven § 216 o første ledd. Utover denne begrensede legalitetskontrollen, er politiet tillagt en forholdsvis stor frihet til å velge – ut fra en samlet vurdering av teknologiske og taktiske forhold - hvilken praktisk gjennomføringsmåte som til enhver tid er best egnet.[25]

[22] Prop. 68 L (2015-2016) s. 270-271.
[23] Prop. 68 L (2015-2016) s. 264.
[24] Se også Bruce (2014) s. 254.
[25] Prop. 68 L (2015-2016) s. 271.

Til tross for at lovteksten er relativt vag, er det – gjennom å sammenholde departementets forslag, Metodekontrollutvalgets utredning og juridisk litteratur - mulig å se for seg ulike, overordnede gjennomføringsmåter for *hvordan skaffe tilgang*. Det kan skilles mellom "informasjonsbaserte" og "utstyrsbaserte" fremgangsmåter, samt en mellomform av disse. Betegnelsene er ikke rettslige, men bidrar til en mer systematisk fremstilling.[26]

Den *informasjonsbaserte* fremgangsmåten går ut på at politiet får rådighet over den aktuelle brukerkontoen eller datasystemet ved å utnytte den mistenktes brukernavn og passord. Metoden har flere likhetstrekk med utleveringspålegg etter § 199 a, men et vesentlig punkt skiller de ulike metodene; den informasjonsbaserte fremgangsmåten innebærer at politiet, ved å benytte seg av *sårbarheter* i programvaren og ved hjelp av teknisk "hackerkompetanse"[27], kopierer og henter ut informasjon via en "bakdør" til programvaren fra internett.[28] Tilgangen til datasystemet skjer altså – til forskjell fra utleveringspålegg etter § 199 a - uten den mistenktes medvirkning og viten. Metoden krever ikke annet bruk av fysisk teknisk utstyr enn tilgang til et datasystem.[29]

Inntrengning i et datasystem eller en brukerkonto kan også skje ved hjelp av *utstyrsbaserte* fremgangsmåter. Hovedsakelig skjer dette ved hjelp av softwarebaserte eller hardwarebaserte løsninger.[30] Den softwarebaserte fremgangsmåten innebærer at det installeres et dataprogram på mistenktes datasystem – for eksempel i en datamaskin eller brukerkonto på nettet. Dette kan gjøres ved at politiet sender en e-post med et skjult vedlegg som inneholder det aktuelle programmet og som aktiveres idet e-posten åpnes. Et annet alternativ er at politiet forleder den rettmessige bruker av datasystemet til å kjøre en programkode som er programmert av politiet. Dette kan gjøres ved å lage et program som for brukeren fremstår som nyttig, men som i stedet gir politiet tilgang til datasystemet.[31] Et slikt program kalles i denne sammenheng for en polititrojaner og kan både kopiere og sende informasjon til politiet. Dataprogrammet kan forholde seg til et logisk avgrenset område som for eksempel et spesielt nettsamfunn.[32] I klartekst innebærer dette at politiet opererer som hackere.

[26] Sunde (2012) s. 9.
[27] Sunde (2012) s. 11.
[28] NOU 2009:15 s. 248.
[29] Sunde (2012) s. 11.
[30] Sunde (2012) s. 10.
[31] NOU 2007:2 s. 23.
[32] Sunde (2012) s. 10-11.

Ved bruk av en hardwarebasert løsning installerer politiet en fysisk komponent på mistenktes datamaskin eller på linjen ut til omverden. En slik komponent kan for eksempel være utstyr som monteres i tastaturet og som leser av tastetrykkene.[33] Metoden er særlig hensiktsmessig for å avdekke tilgangskoder til kryptert data eller passord til tjenester som krever pålogging. Inntrenging i et datasystem kan også skje ved at det monteres en innretning i overgangen mellom tastaturet og selve datamaskinen som leser av all informasjon som går mellom disse enhetene. Innstallering av de hardwarebaserte løsningene forutsetter fysisk tilstedeværelse, og vil som en følge av dette muligens by på større operative utfordringer enn den softwarebaserte.[34]

2.1.3 Betydningen av at datasystemet befinner seg i utlandet

Straffeprosessloven har ingen bestemmelser som avgrenser lovens stedlige virkeområde. Heller ikke straffeprosessloven § 216 o avgrenser adgangen til metodebruken geografisk. Det følger imidlertid av straffeprosessloven § 4 at "lovens regler gjelder med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat". Etter dette og i tråd med det folkerettslige suverenitetsdogmet, må utgangspunktet rettslig sett være at politiets myndighet, herunder adgangen til å bruke dataavlesing, er begrenset til nasjonalstatens territorium.[35] Utover dette kreves det, enten i det konkrete tilfellet eller som følge av folkerettslig avtale, tillatelse til å etterforske på det aktuelle territoriet. I tillegg kreves det at norske myndigheter forholder seg til de regler som gjelder i utlandet.

Gjennom dagens teknologi har politiet muligheten til å samle informasjon, avlytte og kontrollere personer og gjenstander uten å forlate politihuset.[36] Særlig ved innføringen av dataavlesing som etterforskningsmetode – ettersom metoden i praksis kan brukes mot et hvilket som helst datasystem uavhengig av plassering, samt at datakriminalitet i liten grad påvirkes av landegrenser – er avgrensingen av lovens stedlige virkeområde interessant.

I forlengelsen av dette oppstår et spørsmål om de folkerettslige skranker for myndighetsutøvelse innebærer at *datasystemet som en enhet (hardwaren)* må befinne seg i Norge. Det er ganske klart at norsk politi ikke kan rykke inn i et annet lands territorium rent fysisk uten samtykke. Et spørsmål i så måte er om rettstilstanden er annerledes der det er

[33] Sunde (2012) s.10.
[34] Bruce (2014) s. 254.
[35] Auglend (2016) s. 1389.
[36] Bruce (2014) s. 96.

snakk om digitale løsninger og å bryte seg inn digitalt. Datakriminalitet påvirkes i svært liten grad av landegrenser. Dette aktualiserer spørsmålet om reglene om jurisdiksjon muligens bør avdempes noe hva gjelder dataavlesing og digitale bevis. På den annen side er det vanskelig å forstå at rettstilstanden for digitale bevis skal stå i en særstilling. I fravær av folkerettslige kilder som berører dette temaet, må utgangspunktet være at politiet ikke kan drive med dataavlesing på hardware som befinner seg på utenlandsk territorium. På denne bakgrunn vil det nok være problematisk som sådan om norsk politiet bryter seg inn digitalt i et datasystem som befinner seg på en annen stats territorium uten klar lovhjemmel, samtykke og bistand fra den aktuelle stat.[37]

2.1.4 Nærmere om avgrensningen mot andre tvangsmidler

En forståelse av reglene om dataavlesing etter straffeprosessloven § 216 o og § 216 p forutsetter til en viss grad kjennskap til beslektede tvangsmidler i loven. Dette både for å se når det er påbudt å bruke de nye hjemlene og for når man kan nøye seg med å bruke de klassiske hjemlene. I tillegg vil dette punktet danne grunnlaget for den rettspolitiske vurderingen i punkt 3.5.

Ved bruk av dataavlesing kan politiet skaffe seg tilgang til alle *lagrede opplysninger* i et datasystem samt den *fortløpende bruken* av datasystemet over tid. Metoden gir altså mulighet til sikring av fortidig informasjon og sikring av informasjon i sanntid. Dette skjer gjennom en "form for ´tilstedeværelse´ over tid i datasystemet".[38] Av den grunn befinner dataavlesing seg i grenseland mellom ransaking og beslag i lagrede data (databeslag) og kommunikasjonskontroll.[39] Dersom metoden kun benyttes for å *kopiere innhold* på mistenktes datasystem, har metoden store likhetstrekk med hemmelig ransaking og beslag i lagrede data. Dersom metodebruken tar sikte på å *overvåke* datasystemet over tid, kan dataavlesing karakteriseres som en hybrid mellom kommunikasjonskontroll og romavlytting.[40]

Gjennom hjemlene for kommunikasjonskontroll er politiet gitt mulighet til å avlytte samtaler eller annen kommunikasjon som bilder og filmer til og fra bestemte telefoner, e-post, datamaskiner og nettbrett. Det er kun kommunikasjonen mellom to signalstrømmer som kan avlyttes, og avlyttingen skjer ved at samtalene avlyttes *via* teleselskapenes linjer. Reglene om

[37] Til illustrasjon: Straffeprosessloven § 216 a fjerde ledd.
[38] Prop. 68 L (2015-2016) s. 265.
[39] Se straffeprosessloven § 192, jf. § 203 flg., og § 216 a.
[40] Sunde (2006) s. 276.

dataavlesing gir imidlertid politiet adgang til å avlytte eller lese av kommunikasjonen *direkte* i telefonen, nettbrettet eller datamaskinen. Dette har betydning i to implikasjoner: For det første gir det politiet mulighet til å tilegne seg informasjonen i "klartekst" – altså før kryptering. Dette er svært praktisk med tanke på den stadig økende forekomsten av kommersielle krypteringsløsninger hvor forsøk på å knekke krypteringskodene krever store ressurser i form av datakraft, kompetanse og tid. Dataavlesing innebærer at politiet gis tilgang til informasjonen *før* den krypteres – for eksempel når en mistenkt åpner et tekstdokument for behandling på sin datamaskin, og er et godt eksempel på hvor hjemlene for kommunikasjonskontroll kommer til kort.[41]

For det andre gir hjemlene om dataavlesing politiet tilgang til virtuelle brukerkontoer (såkalte "nettskyer") som for eksempel internettbaserte e-post- og fildelingstjenester hvor flere impliserte – ved én felles tilgang til samme brukerkonto – kan lese, opprette og redigere dokumenter, uten at informasjonen sendes direkte mellom de involvertes datasystemer. Til tross for at dette utvilsomt er en form for kommunikasjon, vil ikke kommunikasjonskontroll etter straffeprosessloven § 216 a gi fullstendig tilgang til informasjonsutvekslingen.[42] Også her vil hjemlene til kommunikasjonskontroll komme til kort.

Gjennom reglene om ransaking og beslag kan politiet i prinsippet skaffe seg tilgang til all informasjon som ligger lagret i et datasystem, jf. straffeprosessloven § 192/§ 200 a og § 203. Dette kan blant annet gjøres ved at politiet i medhold av straffeprosessloven § 199 a kan "pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet". Det er først og fremst *fortidig informasjon* som vil bli fanget opp på denne måten. Til tross for at det hyppig kan begjæres og gjennomføres ny ransaking av samme objekt, vil den aktuelle ransakingen kun gi øyeblikksbilder, og ikke nødvendigvis et fullstendig bilde av situasjonen.[43] Ved dataavlesing gis politiet mulighet til å være "inne i datasystemet" over tid og ikke bare kartlegge den mistenktes fortidige bruk, men også få tilgang til opplysninger som ikke lagres i datasystemet, men som kun passerer igjennom. Metoden vil da ha store likhetstrekk med forslaget om gjentatt hemmelig ransaking.[44] Ved bruk av dataavlesing vil politiet således ikke være hindret i å få tilgang til informasjon som tidligere – ved bruk av ransaking – stod i fare for å bli slettet eller fjernet før politiet kom.

[41] Prop. 68 L (2015-2016) s. 260.
[42] Prop. 68 L (2015-2016) s. 260.
[43] Prop. 68 L (2015-2016) s. 261.
[44] Se nærmere om dette i NOU 2009:15 s. 246.

2.1.5 Representerer dataavlesing noe nytt i forhold til de klassiske tvangsmidlene?

Departementet legger til grunn i Prop. 68 L (2015-2016) at det ved en innføring av dataavlesing som et skjult tvangsmiddel "langt på vei er snakk om å introdusere nye og mer effektive fremgangsmåter for å skaffe politiet tilgang til informasjon som det allerede har rettslig adgang til gjennom kommunikasjonsavlytting og hemmelig ransaking og beslag".[45] At politiet på visse vilkår har hjemler til å bruke inngripende tvangsmidler, og således få innsyn i sensitiv informasjon, er ikke noe nytt.[46] Likevel synes dataavlesing å *utvide* politiets adgang til å få tilgang til og innhente informasjon på flere måter.

Det kan skilles mellom tilgang til informasjon som politiet i) *etter sin art* ikke fikk tilgang til tidligere, tilgang til informasjon som politiet ii) *rent praktisk* ikke fikk tilgang til tidligere og tilgang til iii) *annen type kommunikasjon*.

Ved spørsmålet om dataavlesing er en metode som gir tilgang til opplysninger som politiet etter sin art ikke fikk tilgang til tidligere, kan det sondres mellom *arten av informasjonen* kontra *lokaliseringen av informasjonen.* Dataavlesing er i likhet med ransaking og kommunikasjonskontroll for øvrig, underlagt de samme strenge begrensningene hva kommer til taushetsbelagt informasjon, avlytting av advokatsamtaler etc.[47] Utover dette gjelder det ingen spesielle regler for hvilken type informasjon politiet kan få innsyn i eller skaffe seg tilgang til. Personlige notater eller dagbøker som i aller høyeste grad kan inneholde privat og sensitiv informasjon, kan derfor være gjenstand for ransaking og beslag.[48] At politiet i så måte får innsikt i enkeltindividers personlige betraktninger er altså ikke nytt. Arten av informasjonen er den samme.

Forskjellen synes å være lokaliseringen av informasjonen. Kommunikasjonskontroll fanger primært opp informasjon som den mistenkte utleverer til andre og som derfor har funnet veien ut av den personlige sfære. Det kan derfor anføres at idet den mistenkte har valgt å kommunisere noe til andre, har vedkommende gitt slipp på denne informasjonen.[49] Gjennom dataavlesing gis politiet muligheten til *umiddelbart* å overvåke hva den mistenkte til enhver tid gjør, og mistenkte gis på den måten ikke muligheten til å "slette" nedskrevne tanker,

[45] Se s. 266.
[46] Se punkt 2.1.4 og 2.1.5.
[47] Se blant annet straffeprosessloven § 216 c andre ledd og § 216 i, jf. § 216 d siste ledd.
[48] Prop. 68 L (2015-2016) s. 265-266.
[49] Se til sammenligning Sunde (2013) s. 277.

handlinger og betraktninger. I forlengelsen av dette hevder datatilsynet i sitt høringsinnspill at ”dataavlesing … vil innebære at ´tanker, assosiasjoner og ønsker som kanskje aldri engang var tenkt kommunisert til noen andre blir gjenstand for politiets behandling´”.[50] Det er altså ”ikke det du sier som overvåkes, men det du tenker og vet”.[51] Det som er nytt, synes altså å være at personligheten til den mistenkte overvåkes i enda dypere grad enn tidligere. Lokaliseringen av informasjonen er ny.[52]

Dataavlesing innebærer også at politiet får tilgang til informasjon som de *rent praktisk* ikke fikk tilgang til tidligere. For det første innebærer dataavlesing at politiet ikke er bundet av den straffeprosessuelle sondringen mellom informasjon som er lagret og informasjon som overføres mellom en avsender og en mottaker. For det andre vil metoden kunne brukes for å gjennomføre vedvarende overvåking av datasystemer uten fysisk tilstedeværelse i flere tilfeller enn det gjeldende rett i praksis gir adgang til.[53] Et eksempel på dette er at dataavlesing gir politiet mulighet ”til å overvåke ransakingsobjektet (for eksempel forbli pålogget på en e-postkonto eller en datamaskin) over tid for å fange opp ny aktivitet eller ny informasjon som produseres fortløpende av mistenkte eller andre”.[54]

Endelig gir dataavlesing politiet tilgang til en *annen type informasjon*. Metoden innebærer at politiet fortløpende kan gjøre seg kjent med den kontinuerlige bruken av datasystemet – som for eksempel bruken av en programvare, inntastinger på et tastatur eller behandling av ulike filer hvor dataene ikke blir lagret eller kommunisert. Dette er informasjon som det ikke er mulig å innhente etter dagens regler om kommunikasjonskontroll og ransaking og beslag.[55]

Når departementet på bakgrunn av dette har argumentert med at innføringen av dataavlesing kun er en utvidelse som vil gi politiet ”tilgang til informasjon som det allerede har rettslig adgang til”[56], synes dette imidlertid ikke å være helt heldig. Dataavlesing representerer – ikke bare faktisk, men også rettslig – noe nytt på flere måter.

[50] Prop. 68 L (2015-2016) s. 252.
[51] Elden (2016).
[52] I forlengelsen av dette kan det stilles spørsmål ved om dataavlesing er siste slag før ”hjerneavlytting”.
[53] Prop. 68 L (2015-2016) s. 265.
[54] Prop. 68 L (2015-2016) s. 261.
[55] Prop. 68 L (2015-2016) s. 266. Se også NOU 2009:15 s. 244.
[56] Prop. 68 L (2015-2016) s. 265.

2.2 Vilkårene for å iverksette dataavlesing

2.2.1 Generelt

Straffeprosessloven § 216 o er en omfattende og til dels komplisert lovbestemmelse som gir politiet adgang til å foreta dataavlesing etter strenge materielle og prosessuelle vilkår. Sammenholdt med de øvrige bestemmelsene om skjulte tvangsmidler i straffeprosessloven, er det imidlertid veldig få av disse vilkårene som er genuine for dataavlesing. Til tross for at vilkårene til en viss grad er kjente størrelse, er det, for å danne et bakteppe for diskusjonen i kapittel 4, nødvendig å gi en kort oversikt over regelverket.

2.2.2 Generelle vilkår for metodebruken

Grunnvilkåret for å tillate dataavlesing er at noen med "skjellig grunn" mistenkes for fullbyrdelse av, eller forsøk på en av de bestemte straffbare handlinger angitt i § 216 o første ledd bokstav a eller b. Vilkåret stiller krav til graden av mistanke og finnes i en del andre bestemmelser i straffeprosessloven.[57] Det følger uttrykkelig av forarbeidene at formuleringen "skjellig grunn" i denne sammenheng skal forstås på samme måte som ved andre steder i loven.[58] Det må altså være sannsynlighetsovervekt for at mistenkte er skyldig.[59] Denne mistanken må i tillegg være rettet mot besitteren eller brukeren av det datasystemet eller den brukerkontoen som politiet ønsker å avlese, jf. fjerde ledd.

Videre må den straffbare handlingen mistanken knytter seg til være av en nærmere kvalifisert art. Straffeprosessloven § 216 o første ledd fastsetter at mistanken må gjelde " en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i 10 år eller mer", jf. bokstav a. Ved klarleggingen av strafferammen etter første ledd bokstav a, må det sees hen til straffeloven § 79 bokstav a og b hvor det uttrykkelig fremgår at økt strafferamme som følge av gjentakelse eller konkurrens ikke skal tillegges prosessuell virkning, med mindre dette fremgår av den aktuelle prosessregelen. Forhøyelse av maksimumsstraffen ved konkurrens eller gjentakelse skal etter dette ikke tas i betraktning ved beregningen av strafferammen etter § 216 o første ledd bokstav a. Det følger av straffeloven § 79 første ledd bokstav c at for organisert kriminalitet, skal den økte strafferammen imidlertid tillegges prosessuell virkning.

[57] Se blant annet straffeprosessloven §§ 171, 192 og 216 a.
[58] Prop. 68 L (2015-2016) s. 283.
[59] Se blant annet Rt. 1993 s. 1302, Rt. 2011 s. 946 og Rt. 2005 s. 194.

Etter første ledd bokstav b åpnes det også opp for at retten kan tillate dataavlesing ved etterforskning av handlinger eller forsøk på nærmere angitte handlinger som ikke oppfyller strafferammekravet etter bokstav a, men hvor etterforskningsmessige utfordringer tilsier at det likevel er et behov for å kunne bruke dataavlesing.[60] Eksempler på slike handlinger er straffeloven § 136 om oppfordring, rekruttering og opplæring av terrorhandlinger eller § 232 om grov narkotikaovertredelse.

2.2.3 Kravet om nødvendighet og forholdsmessighet

Straffeprosessloven oppstiller ikke et generelt vilkår om at bruken av et tvangsmiddel må være nødvendig. Etter § 170 a annet punktum kan et tvangsmiddel imidlertid ikke benyttes "når det etter sakens art og forholdene ellers" vil være "et uforholdsmessig inngrep". Et minimum av nødvendighet er derfor en forutsetning for at bruken skal anses som forholdsmessig etter bestemmelsen. Etter plasseringen i loven gjelder bestemmelsen for alle tvangsmidler i straffeprosesslovens fjerde del.

For de mest inngripende tvangsmidlene er det i tillegg lovfestet et kvalifisert nødvendighetskrav som innebærer at tvangsmidlet kun kan tillates hvis metoden "vil være av vesentlig betydning for å oppklare saken" og "oppklaring ellers i vesentlig grad vil bli vanskeliggjort".[61] For dataavlesing fremgår dette av § 216 o tredje ledd første punktum.

Endelig, for de tilfeller der datasystemet som skal avleses er "tilgjengelig for et større antall personer" eller tilhører særskilte angitte yrkesgrupper[62], kan tillatelse til bruk av tvangsmidlet bare gis dersom det foreligger "særlig grunner", jf. straffeprosessloven § 216 c andre ledd, jf. § 216 o tredje ledd siste punktum. Vilkåret kan sees på som en skjerpelse av det alminnelige forholdsmessighetskravet som følger av § 170 a annet punktum, og kan begrunnes i at det under slik omstendigheter er stor fare for at metodebruken vil ramme utenforstående tredjepersoner. Heller ikke dette er genuint for dataavlesing, se blant annet § 202 a femte ledd og § 216 c andre ledd.

[60] Prop. 68 L (2015-2016) s. 284.
[61] Se straffeprosessloven § 200 a annet ledd, § 216 c første ledd og § 216 m tredje ledd.
[62] Forarbeidene nevner for eksempel advokat, lege, prest eller journalist.

2.2.4 Rettsikkerhetsgarantier og kontrollmekanismer

Politiets skjulte etterforskningsmetoder er som følge av dets karakter unntatt flere viktige rettssikkerhetsgarantier; som kontroll gjennom offentlighet, rett til kontradiksjon og mistenktes egenkontroll. For å kompensere for dette, er skjult tvangsmiddelbruk til gjengjeld underlagt en rekke særskilte kontrollmekanismer.[63] Dette er i liten grad spesielt for dataavlesing, men som en følge at kontrollmekanismene blant annet har betydning for om dataavlesing er et lovlig inngrep i retten til privatliv etter våre konstitusjonelle og folkerettslige forpliktelser, er det påkrevd av hensyn til fremstillingen i punkt 4.2.5 og 4.2.6 å si noe kort om dette.

Det stilles for det første *krav til den interne behandlingen* i påtalemyndigheten. Utgangspunktet er at enhver politijurist kan beslutte bruk av tvangsmidler, jf. straffeprosessloven § 67 første ledd. For de mest inngripende tvangsmidlene fravikes imidlertid dette utgangspunktet. Straffeprosesslovens § 216 o siste ledd første punktum viser til § 216 d som fastslår at det primært er politimesteren eller visepolitimesteren som skal beslutte bruken av dataavlesing – dette gjelder både der det er snakk om å sende begjæring til retten og der det er snakk om å begjære det selv ved hastekompetanse. Den interne behandlingen i påtalemyndigheten er ment å sikre en betryggende og rettssikker behandling.

For det andre stilles det krav om at det eksisterer en tilstrekkelig *ekstern legalitetskontroll*. Domstolene representerer en sentral del av kontrollsystemet for politiets skjulte etterforskningsmetoder. Dette kommer gjennomgående til uttrykk i straffeprosessloven ved at retten som det klare utgangspunkt *ved kjennelse* må gi politiet tillatelse til å ta i bruk tvangsmidlet. Utgangspunktet er at slik tillatelse må innhentes *før* tvangsmidlet kan iverksettes. For dataavlesing kommer dette til uttrykk i straffeprosessloven § 216 o første ledd gjennom at "retten ved kjennelse [kan] gi politiet tillatelse (…)".[64] Kravet om en rettslig kjennelse er imidlertid ikke absolutt. Påtalemyndigheten er gitt en hastekompetanse til å beslutte bruk av tvangsmidler dersom "det ved opphold er stor fare for at etterforskningen vil lide", jf. femte ledd og henvisningen til § 216 d første ledd første punktum. Forutsetningen synes å være at viktige opplysninger eller bevis må gå tapt som følge av at politiet må vente på rettens tillatelse. For de tilfellene der påtalemyndighetene benytter seg av hastekompetansen, skal beslutningen forelegges retten for etterkontroll snarest mulig, og

[63] Se nærmere Bruce (2014) s. 117 flg.
[64] Min utheving. Se også blant annet straffeprosessloven § 200 a første ledd og § 216 a første ledd.

senest 24 timer etter at metodebruken ble iverksatt, jf. straffeprosessloven § 216 d første ledd andre punktum.

I forkant av beslutningen om tvangsmiddelbruken settes spesielt et viktig rettssikkerhetsideal på prøve, nemlig mistenktes rett til kontradiksjon. I et forsøk på å møte denne utfordringen skal det etter straffeprosessloven § 100 a oppnevnes en advokat som skal ivareta den mistenktes interesser. Advokatens hovedoppgaver skal være å sørge for en grundig og allsidig gjennomgang av at vilkårene for kommunikasjonskontroll er oppfylt - i så henseende særlig kravet til forholdsmessighet.

Endelig er det et krav om at politiets skjulte tvangsmiddelbruk er gjenstand for *etterfølgende kontroll* gjennom uavhengige utvalg. Med hjemmel i straffeprosessloven § 216 h er det derfor opprettet et utvalg – Kontrollutvalget for kommunikasjonskontroll (kontrollutvalget) – som skal føre etterkontroll med politiets og påtalemyndighetens saker om kommunikasjonskontroll etter kapittel 16 a. Etter § 216 h, jf. § 216 o siste ledd første punktum, skal kontrollutvalget også føre tilsvarende kontroll med politiets bruk av dataavlesing. Utvalgets virksomhet og kontrollområde er regulert i kommunikasjonskontrollforskriften[65] kapittel 2.

[65] FOR-2016-09-09-1047 *Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing.*

3 Rettspolitiske hensyn

3.1 Generelt

Reglene om dataavlesing reiser grunnleggende rettspolitiske dilemmaer. Samfunnets ønske og behov for effektiv kriminalitetsbekjempelse må avveies mot de grunnleggende verdier i en demokratisk rettsstat som rettssikkerhet og personvern.[66] De verdivalg som må foretas i denne sammenheng beror på ulike interesser som står i et spenningsforhold til hverandre.

3.2 Behovet for kriminalitetsbekjempelse

3.2.1 Kriminalitetsutviklingen

Et av de mest fremtredende trekk ved kriminalitetsbildet de siste tiårene er den stadig økende teknologiske utviklingen i samfunnet. Større tilgang til og bruk av internett har ikke bare skapt nye former for kriminalitet og nye arenaer for eller versjoner av tradisjonelle straffbare handlinger, men også lagt til rette for en mer effektiv kommunikasjon over store geografiske områder. E-post og andre elektroniske kommunikasjonsmedier har i stor grad overtatt for det som før forelå i papirform. Dette innebærer at store deler av bevismassen er elektronisk.

I de senere år har også fremveksten av og kunnskapen om krypteringsmuligheter og andre metoder for informasjonsbeskyttelse økt betraktelig. ”Kryptering” innebærer kort fortalt at informasjonen – for eksempel en e-post i en mailkorrespondanse – ”låses ned” med en kodenøkkel og i så måte gjøres uleselig for de uten kodenøkkel. For å få tilgang til denne informasjonen må den krypterte informasjonen låses opp igjen med riktig kodenøkkel.[67] Slik kryptering kan skje både bevisst av den enkelte brukeren eller automatisk gjennom bruk av bestemte dataløsninger. Et eksempel på sistnevnte er mail-tjenesten Google Mail hvor ”… (alle datapakkene mellom Googles server og brukerens anlegg) krypteres uten at brukeren gjør dette valget selv”.[68]

[66] NOU 2009:15 s. 68.
[67] Se nærmere om kryptering: Datatilsynet (2012).
[68] Eksempel hentet fra Høringsinnspillet til Kripos inntatt i Prop. 68 L (2015-2016) s. 250.

Den økende fremveksten av og kunnskapen om krypteringsløsninger og andre former for informasjonsbeskyttelse byr på store etterforskningsrelaterte utfordringer for politiet.[69] Kripos uttaler i sitt høringsinnspill til lovforslaget at: "Det … ikke [er] tilgangen til beslaget som er problematisk, men i hvor stor grad den teknologiske utviklingen hindrer at beviset kan fremkalles. ... den teknologiske utvikling har gjort at elektroniske bevis er mindre tilgjengelige nå enn før".[70]

Departementet fremholder videre at et annet markant utviklingstrekk ved kriminalitetsbildet "synes å være at det i stadig større utstrekning benyttes kommunikasjonstjenester som ikke er bundet til et bestemt kommunikasjonsanlegg eller en bestemt nettverksforbindelse, men derimot til en virtuell brukerkonto [for eksempel Skype eller Dropbox] som innehaveren med et brukernavn og passord, og eventuelt tilpasset programvare, kan benytte fra en rekke plattformer – for eksempel smarttelefoner, nettbrett eller bærbare datamaskiner".[71]

Dagens teknologi gjør det også mulig at flere kan få tilgang til én og samme brukerkonto, og således uavhengig av hverandre gå sammen om å opprette, redigere og lese dokumenter og øvrige filtyper. Dokumentene og filene sendes ikke mellom de implisertes kommunikasjonsanlegg, men lagres på tjenestetilbyderens servere, noe som innebærer at avlytting ikke vil avdekke kommunikasjonen mellom de involverte.[72] Disse tjenestene er svært fleksible og følger – naturlig nok – ikke lovens sondring mellom innhold som overføres mellom ulike kommunikasjonsanlegg (kommunikasjonskontroll) og innhold som er lagret (ransaking og beslag).[73] Ransaking og beslag er ikke anvendelig fordi det er vanskelig å få tak i hardwaremaskinen, og ettersom kommunikasjonen ikke gjelder aktiviteten på ett sted i nettverket, men derimot overføring mellom forskjellige kommunikasjonsanlegg, er heller ikke kommunikasjonskontroll anvendelig.[74]

Poenget synes i følge departementet å være at "adgangen til meningsholdet i informasjonen er rettslig sett uendret, men i praksis vanskeliggjort" som følge av kryptering og andre metoder

[69] Prop. 68 L (2015-2016) s. 259-261.
[70] Prop. 68 L (2015-2016) s. 249 (Min utheving).
[71] Prop. 68 L (2015-2016) s. 260 (Min tilføyelse).
[72] Prop. 68 L (2015-2016) s. 260.
[73] Sunde (2013) s. 269.
[74] Sunde (2013) s. 273-274.

for informasjonsbeskyttelse.[75] Situasjonen er altså at muligheten for politiet til å innhente informasjonen faller mellom to etterforskningsmetoder.

3.2.2 Effektiv etterforskning

Den teknologiske utviklingen representerer ikke bare en utfordring for politiet, men kan også tjene som et nytt verktøy. Straffelovgivningens forutsetning er at straff, og trusselen om dette, er egnet til å beskytte enkeltmennesker og samfunnet som sådan mot kriminalitet.[76] På denne bakgrunn er en av politiets viktigste oppgaver å avdekke og stanse kriminell virksomhet og å forfølge straffbare forhold, jf. politiloven[77] § 2 nr. 3. Av den grunn er det viktig at styrkeforholdet mellom politiet og den trusselen de kriminelle representerer, ikke forrykkes i negativ retning. Politiet er i denne sammenheng avhengig av et lovverk som gir tilfredsstillende prosessuelle virkemidler.[78]

Departementet påpeker at politiets bruk av skjulte etterforskningsmetoder er helt avgjørende for effektiv kriminalitetsbekjempelse av de mest samfunnsskadelige og alvorlige forbrytelsene.[79] Behovet for nye etterforskningsmetoder kan imidlertid ikke i seg selv forsvare at det gis hjemmel til å ta i bruk en ny inngripende etterforskningsmetode. For det første må hensynet til effektivitet ikke gå på bekostning av hensynet til mistenktes rettssikkerhet.[80] For det andre kreves det i tillegg at metoden har betydning for oppklaring av den aktuelle kriminalitetsformen. Et spørsmål som aktualiseres i denne sammenheng er om dataavlesing faktisk er egnet til oppklaring av de aktuelle formene for kriminalitet. Dette vil tas opp igjen under punkt 4.2.6.

3.2.3 Tillitshensyn

Den allmenne trygghetsfølelsen er en forutsetning for borgernes tillit til staten - en tillit som er helt *fundamental* for vårt demokrati og samfunnsorden.[81] Dette aspektet har to dimensjoner; så vel som at straffbare handlinger utgjør en trussel mot denne trygghetsfølelsen, vil også utvidede fullmakter for politiet kunne medføre en følelse av

[75] Prop. 68 L (2015-2016) s. 260.
[76] Bruce (2014) s. 21.
[77] LOV-1995-08-04-53 *Lov om politiet.*
[78] Se også NOU 2016:24 s. 146.
[79] Prop. 68 L (2015-2016) s. 23.
[80] NOU 2016:24 s. 145.
[81] Se blant annet Politidirektoratet (2008) s. 13.

utrygghet. Den usikkerhet overvåkningshjemlene skaper, kan medføre at borgerne mister den nødvendige tillitt til myndighetene.[82] Samtidig kan frykten for overskridelse av overvåkningshjemlene og faren for maktmisbruk ha en negativ innvirkning på borgerens tillit til staten, som igjen kan føre til at balansen mellom borgerne og myndighetene utfordres.[83] Utgangspunktet må derfor være at det er et samsvar mellom borgernes forventninger til politiet og de virkemidler politiet har til rådighet for å imøtekomme kriminalitetsbildet.[84]

3.3 Rettssikkerhet

Den mest vanlige forståelsen av "rettssikkerhetsbegrepet" i straffeprosessen synes å være at begrepet bør reservers for mistenktes vern mot uriktige avgjørelser i form av vilkårlighet og overgrep fra myndighetens side.[85] En slik forståelse av begrepet legges også til grunn for denne avhandlingen.[86] I dette ligger en forutsetning om at borgerne kan forutberegne sin rettsstilling ved å ha mulighet til å innrette seg etter loven. Dette krever at inngrepet skjer innenfor de rettslige rammer som lovgiver har oppstilt.[87] For at disse rettslige rammene skal kunne ivareta mistenktes rettssikkerhet, er det etter min mening en forutsetning at hjemlene for metodebruken er et resultat av en tilfredsstillende fremgangsmåte. I dette ligger et krav om at hjemlene for dataavlesing er underlagt en forsvarlig utredning hvor de ulike hensynene som gjør seg gjeldene og de utfordringer metodebruken reiser, er grundig vurdert og forsøkt balansert på en best mulig måte. Hvorvidt dette er tilfellet for dataavlesing, kommer jeg tilbake til i punkt 4.2.6.

I et lovgivningsperspektiv vil et realistisk rettssikkerhetsideal i så måte være i balansepunktet mellom hensynet til mistenktes rettssikkerhet og samfunnets/fornærmedes interesser (punkt 3.2 og 3.4). Denne vurderingen må gjøres i lys av hensynet til en effektiv straffeprosess.[88]

[82] Jf. også Busch (2011) s. 350.
[83] Schartum (2010) s. 20.
[84] Jf. også NOU 2009:15 s. 21-22.
[85] Se blant annet NOU 2009:15 s. 61-62, NOU 2016:24 s. 145, Doublet (1995) s. 503-504 og Strandbakken (2003) s. 74-79.
[86] Rettssikkerhetsbegrepet kan også brukes i en videre kontekst og omfatter da kriminalitetsofrenes rettsikkerhet og/eller samfunnets rettsikkerhet som sådan. Se blant annet NOU 2016.24 s. 145-146 og Strandbakken (2003) s. 75.
[87] Bruce (2010) s. 71.
[88] NOU 2009:15 s. 62 og Prop. 68 L (2015-2016) s. 21. Se også Ot.prp.nr. 11 (2007.2008) s. 7 og 24.

3.4 Personvern

Kjernen i personvernsbegrepet er å kunne bestemme over opplysninger som gjelder en selv.[89] Metodekontrollutvalget fremhevet særlig at "politiets bruk av skjulte tvangsmidler vil medføre inngrep i enkeltmenneskers personvern" og at selve "eksistensen av regler som åpner for slik tvangsmiddelbruk vil utgjøre inngrep overfor alle som kan rammes … uavhengig av om reglene faktisk brukes".[90] En viktig side av personvernet er derfor å beskytte borgerne mot uberettiget og unødvendig innsamling og bruk av informasjon som stammer fra skjult tvangsmiddelbruk. Dette gjelder både i forhold til hva politiet får innsikt i gjennom dataavlesing, og i hvilken grad metodebruken skaper sikkerhetshull som utenforstående kan utnytte.

Forventningen om en privat sfære står sterkest i det private hjem.[91] Av den grunn utgjør dataavlesing, som følge av metodens karakter, et særlig stort personverninngrep. Direktør i datatilsynet, Bjørn Erik Thon, har særlig fremmet at "det er ikke, og må aldri bli, forbudt å tenke ondsindige eller farlige tanker. Vi må heller ikke frata mennesket dets rett til å gjennomføre gode etiske valg, som for eksempel å *tenke på* å gjennomføre en kriminell handling, men når tiden nærmer seg beslutte å ikke gå videre med planene". I forlengelsen av dette hevder han at det å tillate dataavlesing "et stykke på vei [er] en kriminalisering av tanken".[92]

Avslutningsvis mener jeg at det ikke er tvil om at de skjulte politimetodene står sentralt på etterforskningsstadiet, og i enkelte tilfeller vil være høyst nødvendig for politiet både for å avdekke, avverge og forebygge alvorlige kriminelle handlinger. Det var særlig utredningen i NOU 1997:15 som dannet grunnlaget for de etablerte skjulte tvangsmidlene. Utvalget pekte spesielt på at endringene ville "krenke den enkeltes integritet og personvern i betydelig grad", men at kriminalitetsutviklingen gjorde dette nødvendig.[93] Bak dette utgangspunktet ligger forutsetningen om at dataavlesing kun kan forsvares dersom metodebruken er i stand til å dekke det tilsiktede behovet. Gjør ikke metoden det, må personvernet gå foran.[94]

[89] Se nærmere NOU 1997:19 s. 21 og NOU 2009:1 s. 35-36.
[90] NOU 2009:15 s. 48.
[91] Dette reflekteres både i Grunnloven § 102 og EMK artikkel 8.
[92] Thon (2016) (Min tilføyelse).
[93] NOU 1997:15 s. 92.
[94] Jf. også Keiserud (2015) s. 7.

3.5 Hvilke særlige hensyn gjør seg gjeldende ved dataavlesing?

3.5.1 Rettssikkerhetsmessige utfordringer

Det spesielle med dataavlesing er at bruken av politiprogrammer *skjer på innsiden* av datasystemet. Dette i motsetning til kommunikasjonskontroll og ransaking hvor informasjonen tilegnes fra "utsiden" gjennom for eksempel oppfanging av stråling eller ved å speilkopiere en harddisk. En utfordring i så måte er at metoden kan gi politiet tilgang til store mengder ubeskyttede data som er svært utsatt for både endringer og sletting.[95] Dette har en side til *vernet om bevisets pålitelighet* og knytter seg til rettssikkerheten i straffesaken som sådan. Det er en grunnleggende forutsetning at ethvert bevis skal representere en sann beskrivelse av hendelsesforløpet. Dette ser man også utslag av i andre regler, som delvis er begrunnet i hvordan man skal bevare påliteligheten av et bevis. Et eksempel er at det ikke skal brukes tortur ved avhør, av hensynet til at forklaringen skal være mest mulig pålitelig. Målet er ikke å finne den skyldige, men å finne sannheten – noe man ikke vil finne dersom bevisene er upålitelig og villende. Dette utgangspunktet utfordres når etterforskeren ved bruk av blant annet trojanere og pålogging til virtuelle brukerkontoer, bevisst eller ubevisst kan komme i posisjon til å endre (ved å for eksempel å åpne en ulest fil) eller slette data på det aktuelle datasystemet.[96]

En annen utfordring ved dataavlesing er at metoden etterlater få ytre spor. Dette har en side til kontrollen med politiets bruk av metoden og *rettssikkerheten mot uhjemlet overvåking*. Dataavlesing som etterforskningsmetode byr på potensielle misbruksproblemer. Gjennom dataprogrammet som installeres på mistenktes datasystem får politiet full kontroll over avlesningsenheten. Dette innebærer i praksis at politiet for eksempel kan aktivisere en tilknyttet innebygd mikrofon og foreta romavlytting, aktivere et webkamera eller tilføye, endre eller slette data. Også den avsluttende delen av avlesningsfasen, hvor dataprogrammet skal avinstalleres, kan by på utfordringer i forhold til hvordan kontrollorganene skal kunne verifisere at dataprogrammet faktisk er slettet fra mistenktes datasystem når avlesingsperioden er utløpt.[97] Departementet fremhever at kontroll med metodebruken er særlig viktig ved bruk

[95] Sunde (2012) s. 21.
[96] Sunde (2012) s. 22.
[97] Sunde (2008) s. 475.

av dataavlesing, og at viktigheten med god dokumentasjon er helt avgjørende for at kontrollorganene skal være i stand til å vurdere metodens lovlighet.[98] Et spørsmål er imidlertid om bruken av dataavlesing fullt ut lar seg kontrollere i etterkant. Dette kommer jeg tilbake til i punkt 4.2.6.

Endelig kan dataavlesing by på rettssikkerhetsmessige utfordringer i forhold til det å identifisere partene. Ved kommunikasjonsavlytting er det ofte lett å identifisere de impliserte. Ved dataavlesing er dette vesentlig vanskeliggjort som følge av metodens karakter. Det må derfor tas høyde for faren om at den reelle gjerningsperson er en ukjent som har misbrukt mistenktes datasystem eller virtuelle brukerkonto.[99] Det må også tas i betraktning at politiet i større utstrekning enn tidligere kan få innsikt i fortrolige samtaler mellom for eksempel klient og advokat.

3.5.2 Personvernmessige utfordringer

Den tekniske gjennomføringen av dataavlesing byr på utfordringer - spesielt når det kommer til bruken av polititrojaner for å gjennomføre metoden. Metodekontrollutvalget pekte særlig på at all programvare inneholder mangler eller feil som kan resultere i en sårbarhet for det aktuelle datasystemet. Disse svakhetene kan tredjepersoner utnytte.[100] Det eksisterer derfor en fare for at utenforstående skal få uberettiget tilgang til opplysninger som behandles i datasystemet eller til datasystemet for øvrig.[101] I lys av dette er det to hensyn som er i spill: Vernet om fortrolig informasjon og vernet om personvernet. Et særlig spørsmål som oppstår i forbindelse med dataavlesing er om metoden overhodet *er mulig* å anvende uten risiko for misbruk av utenforstående. Ettersom de øvrige skjulte politimetodene ikke har medført noen vedvarende datasårbarhet for mistenkte, er problemstillingen ny.[102]

Der hvor datasystemet som avleses, brukes av flere personer – for eksempel en datamaskin i en husstand – vil metoden kunne medføre inngrep i andre enn den mistenktes personvern. Metoden kan potensielt også medføre innsamling av store mengder informasjon og vil som en følge av dette generere svært mye overskuddsinformasjon. Fra et personvernrettslig ståsted bør dataavlesing derfor innrettes på en slik måte at metoden ikke gir innsyn i informasjon som

[98] Prop. 68 L (2015-2016) s. 266.
[99] Sunde (2015) s. 627.
[100] NOU 2009: 15 s. 248.
[101] Se prop. 68 L s. 266-267.
[102] Sunde (2012) s. 24.

er irrelevant for etterforskningen. Videre bør politiets dataprogrammer installeres på en slik måte at tredjepersoner i minst mulig grad rammes av politiets metodebruk.[103]

[103] Se nærmere Bruce (2014) s. 22-26.

4 Konstitusjonelle og menneskerettslige rammer

4.1 Generelt

4.1.1 Forholdet mellom Grunnloven og EMK

I det følgende skal jeg klarlegge de skranker som Grunnloven § 102 første ledd første punktum og EMK artikkel 8 utgjør for den norske lovgivningen om dataavlesing.[104] For å gjøre dette er det først nødvendig å peke på noen alminnelige trekk ved samspillet mellom Grunnloven og EMK.[105]

Både Grunnloven og EMK utgjør selvstendige skranker for lovgivningen og annen myndighetsutøvelse.[106] Som nevnt innledningsvis rører dataavlesing særlig ved retten til privatliv og den personlige integritet. I Grunnloven uttrykkes denne rettigheten i § 102 første ledd første punktum:

> "Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon."

EMK artikkel 8 lyder slik:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

EMK artikkel 8 har, i motsetning til Grunnloven § 102, denne avveiningsnormen i nr. 2 og er i så måte mye mer utførlig. Dette aktualiserer spørsmålet om Grunnloven i denne konteksten

[104] Det avgrenses mot statenes *aktivitetsplikt* til å sikre menneskerettighetene sml. EMK artikkel 1.
[105] For de spørsmål som vil bli drøftet i denne kontekst, har også FN-konvensjonen om sivile og politiske rettigheter betydning. Når det likevel bare er EMK som nevnes, skyldes dette at det ikke vil være mulig innenfor rammene av avhandlingen å også redegjøre for FN-konvensjonen om sivile og politiske rettigheter. EMK gir gjennomgående et mer vidtgående vern, og vil i så måte være dekkende for det avhandlingen tar sikte på å belyse.
[106] Dokument nr.16 (2015-2016) s. 245-246.

er langt mer absolutt enn EMK, eller om det må innfortolkes en begrensning tilsvarende det som følger av EMK art. 8 nr. 2.

Spørsmålet om det burde innføres en begrensningshjemmel slik som i EMK artikkel 8 nr. 2 ble drøftet av Lønning-utvalget i Dokument 16 (2011-2012), hvor det ble gitt anmodning om at "… Grunnlovens menneskerettsbestemmelser … må tolkes i lys av de internasjonale menneskerettskonvensjonene og praksis knyttet til disse".[107] Det ble fremmet forslag om en generell forholdsmessighetsbestemmelse i ny § 115 i Grunnloven, men forslaget ble aldri vedtatt.[108] Høyesterett har i sin praksis imidlertid fulgt opp Lønning-utvalgets anbefaling om at Grunnloven § 102 ikke kan være absolutt, slik at selv om § 115 ikke ble vedtatt, må det være en avveining.[109]

I Rt. 2014 s. 1105 tok Høyesterett for første gang stilling til forståelsen av Grunnloven § 102 i lys av EMK artikkel 8. Førstvoterende uttalte: "… at hvorvidt en lov som griper inn i privat- og familielivet … kommunikasjonen eller den personlige integritet, er forenlig med § 102, også beror på om loven ivaretar et legitimt formål og er forholdsmessig".[110] Avgjørelsen kan anses som et prejudikat for at Grunnloven § 102 må suppleres med kravet til et legitimt formål og forholdsmessighetsvurderingen etter mønster fra EMK artikkel 8 nr. 2. Dette synspunktet ble fulgt opp i Rt. 2015 s. 93 hvor det *enstemmig* ble lagt til grunn at "grunnlovsvernet kan ikke være – og er heller ikke – absolutt" og at det som en følge av dette "vil være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom tiltaket har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig".[111]

På bakgrunn av dette kan det antas at Grunnloven § 102 ikke gir et videre materielt minstevern enn EMK artikkel 8. Det synes også å være slik at betydningen av grunnloven § 102 - som skranke for hjemlene om dataavlesing - i stor grad er sammenfallende med det som kan utledes av EMK artikkel 8 slik EMD har fortolket konvensjonsbestemmelsen til nå og som behandles nærmere i punkt 4.2. De to overnevnte dommene kan også tas til inntekt for at Høyesterett, ved vurderingen av om et inngrep er grunnlovsstridig etter § 102 første ledd første punktum, til en viss grad anvender EMKs strukturelle argumentasjonsmønster. Det er

[107] Jf. s. 90.
[108] Se dokument 16 (2011-2012) s. 260, sml. s. 73-74.
[109] Se som eksempel Rt. 2014 s. 1105 avs. 25-31, Rt. 2015 s.81, Rt. 2015 s. 93, Rt. 2015 s. 155 avs. 52 og HR-2016-1286-A avs. 25. Sml. også Bårdsen (2017) pkt. 3.
[110] Se dommens avsnitt 28.
[111] Se særlig dommens avs. 60.

likevel Høyesterett som har "ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettsbestemmelser" i siste instans.[112]

Ettersom Høyesterett i relasjon til tolkningen av Grunnloven § 102 i stor grad forholder seg til samme målestokk som EMK artikkel 8 nr. 2, vil den videre vurderingen hovedsakelig bli foretatt i lys av EMK artikkel 8 og praksis fra EMD.

4.2 Vernet etter EMK artikkel 8

4.2.1 Generelt

EMK artikkel 8 gir en alminnelig beskyttelse av retten til privatliv og korrespondanse. Til tross for at mye kan regnes som et inngrep i konvensjonsrettigheten, utgjør ikke ethvert inngrep automatisk en krenkelse av konvensjonsrettigheten. Det foreligger kun en krenkelse dersom inngrepet ikke kan forsvares etter tre kumulative unntaksvilkår angitt i artikkel 8 nr. 2 – altså at inngrepet er i) "in accordance with the law", ii) forfølger et av de anerkjennelsesverdige formålene og er iii) "necessary in a democratic society". Det følger av fast og langvarig konvensjonspraksis at det nærmere innholdet i unntaksvilkårene må tolkes i lys av "the present day-conditions".[113] Dette skyldes at EMD ser på konvensjonen som et "living instrument", noe som også reflekteres i EMDs dynamiske og formålsorientere tolkningsstil.[114]

For å kunne vurdere om dagens lovgivning oppfyller lovskravet, om inngrepet er "necessary in a democratic society" og har et legitimt formål, må det først klarlegges om artikkel 8 i det hele tatt kommer til anvendelse for dataavlesing. Dette forutsetter at dataavlesing anses som et inngrep i rettighetene etter artikkel 8.

EMD har flere ganger lagt til grunn at innhenting av informasjon om enkeltpersoner ved bruk av skjulte tvangsmidler utgjør et inngrep etter EMK artikkel 8.[115] Selv om EMD ikke eksplisitt har tatt stilling til om dataavlesing utgjør et inngrep, kan det, ved å sammenligne

[112] Rt. 2015 s. 93 avs. 57. Se også HR-2016-2554-P avs. 86 som gjaldt i relasjon til Grunnloven § 101 første ledd.
[113] *Tyrer mot Storbritannia* avs. 31.
[114] Se nærmere om dette: Elgesem (2003) pkt. 3.6.
[115] Den grunnleggende avgjørelsen er *Klass m.fl mot Tyskland*, se avs. 36.

metodens karakter med de øvrige skjulte tvangsmidlene[116], legges til grunn at dataavlesing åpenbart er å anse som et inngrep i EMK artikkel 8 nr. 1. For å være i tråd med EMK må regelsettet derfor tilfredsstille de tre kumulative kravene i EMK artikkel 8 nr. 2.

Videre er det liten tvil om at myndighetens inngrep for å etterforske kriminalitet – herunder bruk av dataavlesing som etterforskningsmetode - faller innunder formålsangivelsen "the prevention of disorder or crime" i artikkel 8 nr. 2. Ifølge Høyesterett gjelder det i relasjon til Grunnloven § 102 et tilsvarende krav om et "legitimt formål".[117] Hvor tungtveiende samfunnshensyn det er tale om og i hvilken grad formålet med et tiltak er vurdert, vil imidlertid ha stor betydning i forholdsmessighetsvurderingen som avgjør om inngrepet er akseptabelt.[118]

4.2.2 Forholdet mellom lovskravet og forholdsmessighetskravet

I nyere EMD-praksis er det flere eksempler på at domstolen har foretatt en samlet vurdering av lovs- og nødvendighetskravet, hvorav eksistensen av effektive prosessuelle rettssikkerhetsgarantier har blitt tillagt betydelig vekt.[119] Som en følge av dette vil noe av det som behandles under lovskravet ha en side mot forholdsmessighetskravet, og omvendt. For å lette fremstillingen vil det imidlertid under punkt 4.2.4 utelukkende drøftes hvorvidt de norske hjemlene om dataavlesing oppfyller kravet til klar lovhjemmel. Avgjørende er om straffeprosessloven § 216 o er utformet med en slik klarhet at borgerne gis mulig til å kunne forutberegne sin rettsstilling og at hjemmelen således isolert sett gir en tilstrekkelig prosessuell rettssikkerhetsgaranti. Hvorvidt lovgivningen for øvrig i tilstrekkelig grad legger opp til en effektiv prosessuell rettsikkerhetsgaranti for å sikre at inngrepet begrenses til det som er nødvendig, vil bli behandlet under punkt 4.2.6.

Etter dette må kontrollen av inngrepet, eller eventuelt den manglende kontrollen, sees i sammenheng med både lovskravet (punkt 4.2.3 og 4.2.4) og eksistensen til og effektiviteten av den etterfølgende kontrollen (punkt 4.2.5 og 4.2.6).[120]

---

[116] Se nærmere punkt 2.1.4 om forholdet mellom dataavlesing, ransaking og beslag og kommunikasjonskontroll for øvrig.
[117] Se Rt. 2015 s. 93 avs. 60.
[118] Se blant annet *Olsson mot Sverige (No. 1*) avs. 68, *Leander mot Sverige* avs. 51 og *Buck mot Tyskland* avs. 45. Se også Dokument nr. 16 (2015-2016) s. 249 og punkt 4.2.6 nedenfor.
[119] Jf. Storkammeravgjørelsen *Roman Zakharov* avs. 236. Se også *R.E mot Storbritannia* avs.122.
[120] Dokument nr. 16 (2015-2016) s. 251.

4.2.3 Lovskravet

Det første grunnvilkåret for lovlig å kunne gjøre inngrep i interessene etter EMK artikkel 8 nr. 1 er at inngrepet må være "in accordance with the law". Hva som nærmere ligger i lovskravet fremgår blant annet av avgjørelsen *R.E. mot Storbritannia* hvor EMD la til grunn at:

> "The requirement that any interference must be "in accordance with the law" under Article 8 § 2 will only be met when three conditions are satisfied: the impugned measure must have some basis in domestic law; the domestic law must be compatible with the rule of law and accessible to the person concerned; *and the person concerned must be able to foresee the consequences of the domestic law for him* …".[121]

Innholdet i lovskravet etter EMK artikkel 8 kan derfor deles inn i tre hovedaspekter: i) om rettsregelen er fast etablert ii) rettsregelens tilgjengelighet og iii) rettsregelens forutberegnelighet.[122] I forhold til avhandlingens tema, er det kun kravet til forutberegnelighet som eventuelt volder problemer[123], og vil være gjenstand for videre drøftelse. Dette som en følge av at hjemlene om dataavlesing i straffeprosessloven § 216 o og § 216 p har en vag utforming.

Forutberegnelighetskravet knytter seg til selve utformingen av rettsregelen og stiller krav til hjemmelens klarhet. Kjernen i forutsigbarhetskravet er å oppstille saklige rammer for den offentlige skjønnsutøvelse.[124]

I forbindelse med skjult etterforskning har EMD akseptert at kravet til forutberegnelighet ikke kan praktiseres på en måte som gjør det mulig for borgerne å forutse akkurat når myndighetene vil overvåke kommunikasjonen deres. Domstolen forutsetter imidlertid at hjemmelsgrunnlaget gir borgerne en tilstrekkelig indikasjon *på hvilke vilkår* og *under hvilke omstendigheter* myndighetene er legitimert til å anvende virkemidler som gjør inngrep i retten til privatliv.[125] Ettersom politiets bruk av skjulte tvangsmidler utgjør et kraftig inngrep i retten til privatliv, og fordi slik tvangsmiddelbruk i liten grad kan kontrolleres av den som rammes

[121] Se avs. 120 (min utheving). Se også Storkammeravgjørelsen *Rotaru mot Romania* avs. 52, *Liberty and others mot Storbritannia* avs. 59 og storkammeravgjørelsen *Amann mot Sveits avs. 50.*
[122] Se nærmere Aall (2015) s. 126-148.
[123] Lovskravet i relasjon til kravet om fast etablering og tilgjengelighet er i denne sammenheng åpenbart oppfylt, jf. blant annet Grl. § 113 og at straffeprosessloven er en offentlig tilgjengelig lov.
[124] *Olsson mot Sverige (No. 1)* avs. 61 (c). Se også storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 230.
[125] Se blant annet storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 229, *Malone mot Storbritannia* avs. 67, *Weber and Saravia mot Tyskland* avs. 93.

eller samfunnet som sådan, har EMD lagt til grunn at ”such measures must be based on a ´law´ that is particularly precise”.[126]

På denne bakgrunn har EMD utviklet minimumsgarantier til lovregelen for å sikre at de overnevnte prinsippene implementeres på en effektiv måte: i) Lovregelen må angi hvilke kriminelle handlinger som legitimerer overvåking, ii) spesifisere den gruppen personer som underkastes slik overvåking, iii) oppstille prosedyrer for gjennomføringen, iv) angi en tidsmessig grense for overvåkingen, v) bruken og oppbevaringen av opplysningene som er oppnådd gjennom overvåkingen, vi) inneholde prosedyrer for videreformidling av opplysningene til andre myndigheter og vii) regulere når opplysningen kan eller må bli slettet eller ødelagt.[127]

4.2.4 Lovskravet og det norske regelverket

I dette punktet skal jeg klargjøre hva straffeprosessloven § 216 o og § 216 p hjemler i forhold til kravet om klar lovhjemmel. Problemstillingen er om reglene om dataavlesing i etterforskningsøyemed på en adekvat måte gir anvisning på en klar og presis hjemmel slik at borgerne gis mulighet til å forutberegne på hvilke vilkår og under hvilke omstendigheter dataavlesing kan skje, jf. overfor punkt 4.2.3.

Når det gjelder hvilke kriminelle handlinger som legitimerer dataavlesingen, kan det utledes av EMDs praksis at det ikke kreves en uttømmende regulering av de spesifikke lovbruddene som kan legitimere bruken av metoden. Imidlertid kreves det at arten av de aktuelle lovbruddene er tilstrekkelig beskrevet.[128]

Straffeprosessloven § 216 o fastsetter at dataavlesing kan skje overfor personer som med ”skjellig grunn” mistenkes for en forbrytelse med en strafferamme på ti år eller mer, eller ved mistanke om overtredelse eller overtredelse av et av de nærmere lovbrudd som er foreskrevet i bestemmelsens første ledd bokstav b. Bestemmelsen gir adgang til en omfattende overvåking av kriminelle handlinger av ulik alvorlighetsgrad, men gir likevel borgerne en tydelig indikasjon på hvilke handlinger som kan legitimere bruken av dataavlesing.

[126] Se blant annet *Kruslin mot Frankrike* avs. 33 som gjaldt kommunikasjonskontroll.
[127] Se blant annet storkammeravgjørelsen *Roman Zakharaov mot Russland* avs. 231 og *Iordachi og andre mot Moldova* avs. 41-46.
[128] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 244.

Lovskravet i relasjon til kriminalitetskravet må etter dette anses for å være tilstrekkelig klart og presist.

For å være i tråd med lovskravet må den nasjonale inngrepslovgivningen videre spesifisere den gruppen personer som underkastes slik overvåking. Straffeprosessloven § 216 o opererer med et ganske vagt mistankekrav, jf. "skjellig grunn". Som en følge av at mistanken til enhver tid vil bero på de nærmere konkrete forhold, kan det nok vanskelig fastsettes et mer presist krav. En slik oppfatning synes å være i tråd med EMDs praksis.[129] I tillegg har "skjellig grunn" en svært innarbeidet betydning.[130] Etter dette må straffeprosessloven § 216 o også i denne relasjon anses å være tilstrekkelig klar og presis.[131]

Det kan imidlertid problematiseres hvorvidt straffeprosessloven § 216 o i tilstrekkelig grad gir en presis nok anvisning på *hva* inngrepet vil innebære overfor den mistenkte og *hvordan* inngrepet nærmere kan gjennomføres.

Etter straffeprosessloven § 216 o første ledd kan politiet foreta avlesing av "ikke offentlig tilgjengelige opplysninger i et datasystem". Betegnelsen "datasystem" er vag, men må sees i sammenheng med lovens fjerde ledd hvor det fremgår at:

> "Det kan bare gis tillatelse til å avlese 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."

Bestemmelsen gir anvisning på hva som er gjenstand for dataavlesing og hvilken informasjon som kan innhentes. Det legges derfor til grunn at lovskravet på dette punkt er tilfredsstilt.

Etter § 216 o første ledd gjennomføres dataavlesingen ved at det foretas en "avlesing" av det aktuelle datasystemet. Det fremgår ikke tydelig av bestemmelsen hva som menes med "avlesing", men ved å sammenholde første ledd med straffeprosessloven § 216 p første ledd andre punktum og følgende, gis det en tydeligere indikasjon på hva den nærmere avlesingen består i. Det fremgår her at:

---

[129] Se blant annet storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 247 hvor EMD la til grunn at det ikke kan forventes at bestemmelsen i detalj oppgir enhver oppførsel som kan legitimere en beslutning om overvåking.
[130] Se overfor punkt 2.2.2.
[131] Se for eksempel Rt. 2015 s. 1456 avs. 22 som gjaldt i relasjon til mistankekravet i straffeprosessloven § 216 a.

> "Avlesingen 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."

Bestemmelsen gir anvisning på hvordan gjennomføringen *kan* foretas. Utover dette er det *ingen* krav om hvilke metoder som brukes. Dette illustreres gjennom formuleringen "eller på annen måte". Den offentlige myndighet er etter dette tillagt et betydelig skjønn hva gjelder valg av teknisk gjennomføringsmåte.[132]

I storkammeravgjørelsen *Roman Zakharov* presiserte EMD viktigheten av at "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".[133] Dette aktualiserer spørsmålet om ordlyden "på annen måte" i tilstrekkelig grad gir borgerne en rimelig mulighet til å forutberegne sin rettsstilling.

At ordlyden på dette området er vag, er svært betenkelig som følge av metodens karakter. På den annen side vil en mer formell og presis beskrivelse av enhver tenkelig gjennomføringsmåte være problematisk på flere måter.

For det første ligger lovgivningsprosessen konstant mange år bak den teknologiske utviklingen. Dette gjør at det er vanskelig å utforme tidsrelevante og presise bestemmelser.[134] Både Metodekontrollutvalget og departementet påpekte at det som en følge av dette verken var mulig eller hensiktsmessig å beskrive gjennomføringsmåten i detalj.[135] Faren med en for presis lovbestemmelse på dette området, er at metodene fort kan blir utdatert som igjen kan resultere i at politiet står uten hjemmel for inngrepet.

For det andre må det av taktiske årsaker gis en viss mulighet til å utvikle og benytte gjennomføringsmåter som ikke umiddelbart og i detalj blir gjort kjent for allmennheten.[136] Formålet bak bestemmelsen er å avdekke og etterforske svært alvorlig kriminalitet. I lys av dette må regelens utforming sees i sammenheng med regelens effektivitet. I så henseende er

[132] Se overfor punkt 2.1.2. Se også Prop. 68 L (2015-2016) s. 271 hvor det gis en nærmere indikasjon på hvilke fremgangsmetoder som kan anvendes. Fremstillingen er imidlertid ikke uttømmende.
[133] Se dommens avsnitt 230.
[134] Sunde (2006) s. 277.
[135] Prop. 68 L (2015-2016) s. 264.
[136] Prop. 68 L (2015-2016) s. 264.

helt avgjørende at politiets gjennomføringsmåter ikke blir beskrevet i en slik grad at metoden mister sin tilsiktede effekt.

På denne bakgrunn må det derfor stilles spørsmål ved om det i det hele tatt er formålstjenlig å ha en mer presis ordlyd.

I forlengelsen av spørsmålet om bestemmelsen i tilstrekkelig grad gir anvisning på hva som er gjenstand for metoden og hvordan inngrepet gjennomføres, kan det problematiseres hvorvidt en lovgivning som ikke konkret angir *hvem* som skal utvikle de ulike metodene, tilfredsstiller det strenge lovskravet. Som nevnt overfor under punkt 3.5.1 innebærer dataavlesing en rekke rettssikkerhetsmessige utfordringer. Blant disse finnes misbruksfaren fra tredjepersoner. Tilstrekkelige refleksjoner av om utviklingen av programvarer og andre tekniske gjennomføringsmåter må gjøres av nasjonale myndigheter eller om de kan kjøpes av utenlandske leverandører synes å være noe fraværende i departementets utredning.[137] Ordlyden i straffeprosessloven § 216 p – slik den er gjengitt overfor - synes derfor å stå i et spenningsforhold til lovskravet.

For å være i tråd med lovskravet må lovbestemmelsen videre angi en tidsmessig grense for overvåkingen.[138] Det stilles som nevnt overfor krav til at lovbestemmelsen angir i) en tydelig indikasjon på lengden av avlesingen, ii) vilkårene for fornyelse og iii) under hvilke omstendigheter avlesingen må opphøre.[139] Gjennom henvisningene til straffeprosessloven §§ 216 d til 216 k i § 216 o femte ledd, og ved at det i § 216 o femte ledd oppgis en særskilt tidsbegrensning for dataavlesing, synes dette å være tilfellet. Adgangen for metodebruken er begrenset til to uker om gangen. Denne tidsbegrensingen er den eneste skranken domstolene oppstiller utover det å gi tillatelse til metodebruken.

Endelig kreves det som angitt overfor at lovbestemmelsen angir i) forsvarlige prosedyrer for bruken og oppbevaringen av opplysningene som er oppnådd gjennom metodebruken, ii) for utlevering av informasjon som stammer fra metodebruken og iii) for når opplysningene kan eller må bli slettet eller ødelagt.[140]

[137] Se Prop. 68 L (2015-2016) s. 271-272.
[138] Se storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 231.
[139] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 250.
[140] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 231.

Hva gjelder spørsmålet om lovgivningen i tilstrekkelig grad har bestemmelser for bruken og utleveringen av informasjon som stammer fra metodebruken, synes også dette å være oppfylt ettersom straffeprosessloven § 216 i[141] gir utførlige regler om dette.

Det som må klarlegges er derfor i hvilken grad lovgivningen angir prosedyrer for oppbevaringen av opplysningene som er oppnådd gjennom dataavlesing. Straffeprosessloven § 216 g regulerer når en opplysning skal bli tilintetgjort.[142] Utover dette gis det *ingen* retningslinjer for oppbevaringen av opplysningene i straffeprosessloven som sådan. Det følger imidlertid av straffeprosessloven § 216 k at det ved forskrift kan gis en nærmere utfylling og gjennomføring av reglene i straffeprosessloven kapittel 16 a.

Av kommunikasjonskontrollforskriften § 8 kan det utledes at opplysningene ” skal lagres på forsvarlig og hensiktsmessig måte”. Bestemmelsen må sees i sammenheng med § 9 andre ledd første punktum hvor det heter at: ”Andre data, opptak eller gjengivelser oppbevares etter reglene i beskyttelsesinstruksen[143] så lenge dette anses nødvendig av hensyn til … etterforskningen.”. Bestemmelsene gir imidlertid ingen klar anvisning på noen tidsmessig grense for hvor lenge materialet kan lagres og begrensningen på tre måneder i kommunikasjonskontrollforskriften § 9 første ledd siste punktum gjelder bare for overskuddsinformasjon. Hvor lenge opplysningene kan oppbevares må derfor sees i sammenheng med reglene om sletting i straffeprosessloven § 216 g. Avgjørende er hvorvidt lovgivningen gir en klar nok anvisning for når opplysningene kan eller må bli slettet eller ødelagt.

Sletting av opplysninger om og fra skjult tvangsmiddelbruk er regulert i straffeprosessloven § 216 g og kommunikasjonskontrollforskriften § 9. Etter ordlyden i § 216 g skal slike opplysninger snarest mulig bli slettet i den grad de ”er uten betydning for … etterforskningen”, jf. bokstav a.[144] Det følger av straffeprosessloven § 226 første ledd bokstav a at formålet med etterforskningen er å avgjøre spørsmålet om tiltale. Det vil derfor være naturlig å knytte sletteplikten til dette tidspunktet.[145] Etter ordlyden i § 216 g bokstav a og

[141] Tilsvarende gjelder for dataavlesing, jf. henvisning i § 216 o femte ledd til første punktum.
[142] Etter straffeprosessloven § 216 o femte ledd får § 216 g anvendelse overfor dataavlesing.
[143] FOR-1972-17-3352 Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter *(beskyttelsesinstruksen*) (Min tilføyelse).
[144] Etter straffeprosessloven § 216 o femte ledd får § 216 g anvendelse i forbindelse med opplysninger om eller fra dataavlesing.
[145] Jf. også Rt. 2014 s. 1105 avs. 45. Avgjørelsen gjaldt tolkningen av straffeprosessloven § 216 i i relasjon til overskuddsmateriale fra en kommunikasjonskontroll. Dommen må antas å ha overføringsverdi ved tolkningen av bestemmelsen i denne relasjon. Dissens 3-2.

kommunikasjonskontrollforskriften § 9 første ledd skal altså opplysningene om og fra metodebruken slettes så snart etterforskningen er avsluttet.

Flertallet i Høyesterett la i avgjørelsen inntatt i Rt. 2014 s. 1105 imidlertid til grunn at straffeprosessloven § 216 g bokstav a måtte tolkes mer restriktivt, og at bestemmelsen særlig måtte suppleres med § 216 i som gir adgang til å bruke opplysninger om og fra dataavlesing som bevis under den senere retterføring. For å ivareta den tiltaltes rett til rettferdig rettergang etter Grunnloven § 95 første ledd og EMK artikkel 6 nr. 1 måtte straffeprosessloven § 216 g og kommunikasjonskontrollforskriften § 9 første ledd også sees i sammenheng med straffeprosessloven § 264 første ledd som innebar at plikten til sletting inntrådte når "forsvaret er gitt anledning til innsyn".[146]

På bakgrunn av dette er det ikke til å komme utenom at reglene for når opplysningene kan eller må bli slettet fremstår som temmelig uklare og utilgjengelige. For å klargjøre gjeldende rett må flere lov- og forskriftsbestemmelser leses i sammenheng. Lovgivningen synes således på dette punkt å stå i et spenningsforhold med forutberegnelighetskravet. Dette *kan* være problematisk i forhold til lovskravet etter EMK artikkel 8 nr. 2 som sådan.

4.2.5 Forholdsmessighetskravet

Endelig må et inngrep i retten til privatliv etter EMK artikkel 8 være "necessary in a democratic society". Ifølge EMD innebærer dette at inngrepet må være begrunnet i "a pressing social need"[147] og at det fremstår som "proportionate to the legitimate aim pursued"[148] – i dette tilfellet av hensyn til "the prevention of disorder or crime".

Av dette kan det utledes to underliggende krav: i) Det må kunne dokumenteres et pressende samfunnsbehov for at dataavlesing skal tillates, og videre at ii) dette behovet er så tungtveiende at inngrepet etter en samlet vurdering anses som proporsjonalt.[149] Den sistnevnte standarden innebærer et krav om at a) inngrepet er egnet til å fremme og ivareta formålet, b) inngrepet ikke går lenger enn nødvendig og c) at inngrepet er forholdsmessig.[150]

[146] Se dommens avs. 37, jf. også Rt. 2005 s. 1137 avs. 73.
[147] *Leander mot Sverige* avs. 58.
[148] Se blant storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 260.
[149] I relasjon til Grunnloven § 102 første ledd første punktum har Høyesterett uttalt at inngrepet må være "forholdsmessig". Det må i så henseende derfor kunne antas at det henvises til den samme målestokken. Se blant annet Rt. 2015 s. 93 avs. 60.
[150] Se nærmere Aall (2015) s. 156-157.

Ved tolkningen av konvensjonen har EMD innrømmet statene en viss skjønnsmargin (”margin of appreciation”).[151] Skjønnsmarginen innebærer at EMD gir statene et visst spillerom til selv å vurdere konvensjonsmessigheten av inngrepet.[152] I denne kontekst innebærer dette at dersom de demokratiske organene i et land samvittighetsfullt har vurdert hva som er nødvendig, bør dette tillegges en viss vekt.

Når det kommer til det første vurderingstema om hvorvidt inngrepet er begrunnet i et pressende samfunnsmessig behov, viser praksis fra EMD at domstolen er relativt tilbakeholden med å overprøve selve nødvendigheten av inngrepet. I stedet etterprøver EMD hvorvidt lovgiver faktisk har *vurdert behovet* for inngrepet på en grundig og holdbar måte.[153] Herunder om formålet bak inngrepet kan oppnås med mindre inngripende tiltak.[154] Dersom EMD finner at behovet for inngrepet ikke er tilstrekkelig vurdert, kan dette være en prosessuell mangel som innebærer en krenkelse av artikkel 8.

Hva gjelder det andre vurderingstemaet, om at behovet for dataavlesing er så tungtveiende at inngrepet etter en samlet vurdering anses som proporsjonalt, er domstolen også på dette felt relativt tilbakeholden med å overprøve nasjonale myndigheters vurderinger. I stedet viser praksis fra EMD at vurderingstemaet heller er hvorvidt lovgivningen i tilstrekkelig grad:

> ”…contains *adequate and effective safeguards* and *guarantees* to meet the requirements of ´foreseeability´ and ´necessity in a democratic society´”.[155]

Avgjørende for om det foreligger slike egnede og effektive garantier er:

> ”…all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law”.[156]

Det avgjørende for om et inngrep kan aksepteres i relasjon til artikkel 8 nr. 2 synes etter dette å være summen av alle rettssikkerhetsgarantiene.

---

[151] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 232. Se nærmere: Sørensen (2004) s. 135.
[152] Se nærmere om statens skjønnsmargin: Aall s. 157-164.
[153] Se blant annet *Olsson mot Sverige (No. 1)* avs. 68 hvor EMD legger avgjørende vekt på om nasjonale myndigheter kan påvise at det foreligger ”relevant and sufficient reasons”.
[154] *Buck mot Tyskland* avs. 45.
[155] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 232 (Min utheving).
[156] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 232.

4.2.6 Forholdsmessighetskravet og det norske regelverket

Det første som må vurderes er om det kan påvises et *klart behov (*"a pressing social need") for dataavlesing i etterforsknings virksomhet. Praksis fra EMD viser at denne standarden ikke krever at metodebruken er uunnværlig eller absolutt nødvendig, men at det må være mer enn ønskelig.[157] Avgjørende er om det kan dokumenteres "relevant and sufficient reasons".[158]

Som redegjort for overfor i punkt 3.2.1 skaper den stadig økende teknologiske utviklingen store etterforskningsmessige utfordringer for politiet. Dataavlesing som metode vil etter departementets syn innebære at politiets etterforskning rettslig sett ikke hindres av disse utfordringene. I forlengelsen av dette har departementet særskilt fremhevet at dataavlesing vil være en *svært egnet* metode for å imøtekomme disse utfordringene.[159] Til tross for dette gjøres ingen nærmere vurdering av hvilken type kriminalitet som begrunner inngrepet. Og det er i følge departementet heller ikke mulig "å tallfeste behovet for" metodebruken.[160] Likevel argumenterer Departementet med at "utredningen og høringen viser … et klart behov for å supplere bestemmelsene om kommunikasjonsavlytting og hemmelig ransaking …".[161]

Metodekontrollutvalget var særlig opptatt av å kartlegge behovet for dataavlesing, men utredningen fra 2009 viser at det ikke fantes god nok dokumentasjon og statistikk for at metoden ville virke.[162] I lys av dette er det betenkelig at departementet ikke i større grad har tatt seg bryet med å belyse de prinsipielle og praktiske spørsmålene dataavlesing reiser. I denne sammenheng vises det til det svenske forslaget om å innføre dataavlesing. Forslaget ble stoppet fordi det svenske datatilsynet mente at det var i strid med nasjonal lovgivning og EMK.[163] Som en følge av dette satte den svenske regjeringen i gang en offentlig utredning som skal leveres høsten 2017. Utredningen skal blant annet ta for seg behovet for dataavlesing, metodens effektivitet, hvor inngripende det samlede antallet av skjulte etterforskningsmetoder er og bruk av programvare.[164] Med andre ord, momenter som ikke er, men som etter mitt syn burde ha vært bedre belyst i Prop. 68 L (2015-2016). På bakgrunn av dette, kan det etter min mening stilles spørsmål ved om departementets utredning i

[157] *Silver and Others mot Storbritannia* avs. 97. Se også nærmere Høstmælingen (2003) s. 123.
[158] *Olsson mot Sverige (No. 1)* avs. 68.
[159] Prop. 68 L (2015-2016) s. 264-265.
[160] Prop. 68 L (2015-2016) s. 261. Se også NOU 2009:15 s. 242.
[161] Prop. 68 L (2015-2016) s. 261.
[162] NOU 2009: 15 s. 236 og s. 240-243.
[163] Innst. 343 L (2015–2016) (Stortinget – møte onsdag den 8. juni 2016 kl. 10, sak nr. 1).
[164] Komittédirektiv 2016:36 s. 1.

tilstrekkelig grad dokumenterer at det forelå et klart behov (”relevant and sufficient reasons”) for å innføre dataavlesing som etterforskningsmetode.

Det neste som må klarlegges er om dataavlesing er ”proportionate to the legitimate aim pursued”. Dette innebærer som nevnt i punkt 4.2.5 at inngrepet a) må være egnet til å fremme og ivareta formålet, b) ikke må gå lenger enn nødvendig og c) må være proporsjonalt. Spørsmålet er om det var *nødvendig* å innføre dataavlesing slik metoden er regulert i straffeprosessloven § 216 o.

Hva gjelder det første vurderingstemaet (punkt a) er formålet bak å innføre dataavlesing som etterforskningsmetode å etterforske og bekjempe alvorlig og organisert kriminalitet.[165] Dataavlesing fremstår således som tilstrekkelig godt egnet til å fremme og ivareta dette formålet. Det kan imidlertid problematiseres hvorvidt metoden *egentlig* er egnet til å ivareta formålet. Ved bruk av dataavlesing er det alltid en fare for at miljøer som driver med alvorlig og organisert kriminalitet kan tilpasse seg metodebruken. Dette kan skje ved at mistenkte ikke benytter sitt eget datasystem, men heller for eksempel en stjålen smarttelefon eller en offentlige tilgjengelig datamaskin. På den måten vil ikke metoden avdekke det som begrunnet inngrepet. Resultatet blir da at den mistenkte utsettes for et inngrep i retten til privatliv uten at dette er formålstjenlig. Problemstillingen er ikke ny, men i lys av metodens karakter[166], er det betenkelig at dette ikke er vurdert nærmere i departementets utredning.

Det er videre et krav om at inngrepet ikke går lenger enn nødvendig (punkt b). Metodekontrollutvalget konkluderte med at det ikke kunne dokumenteres et tilstrekkelig behov for å foreslå dataavlesing innført som metode ”med det formål å gi politiet mulighet til fortløpende å overvåke all aktivitet i et datasystem”.[167] Departementet gikk likevel inn for en mer vidtgående inngrepshjemmel enn det Metodekontrollutvalget la opp til i sitt forslag, se overfor punkt 1.2.

Etter min mening kan mye tale for at Metodekontrollutvalget i tilstrekkelig grad tok høyde for de etterforskningsmessige utfordringene politiet stod overfor som følge av den teknologiske utviklingen.[168] Likevel mente departementet at dataavlesing som en gjennomføringsmåte for kommunikasjonskontroll og hemmelig ransaking ikke i stor nok grad vil møte de

[165] De tillatte formål for etterforskning angitt i straffeprosessloven § 226 vil her utgjøre begrensninger.
[166] Sml. punkt 3.5.
[167] NOU 2009:15 s. 237.
[168] Se nærmere NOU 2009:15 s. 244-249. Se også redegjørelsen overfor under punkt 1.2.

utfordringene politiet per i dag står overfor som følge av den teknologiske utviklingen. At det var et behov for endringer var etter departementets oppfatning helt åpenbart.[169] Problemet er, slik jeg ser det, imidlertid om lovgiver i tilstrekkelig grad tok høyde for og i tilstrekkelig grad vurderte behovet for dataavlesing opp i mot de rettssikkerhets- og personvernsmessige utfordringene lovendringen reiser.[170] En forutsetning for at politiet skal kunne ha den frihet de er tillagt etter loven, er at den etterfølgende kontrollen er tilstrekkelig. Avgjørende er om summen av de prosessuelle rettssikkerhetsgarantiene er egnet til å begrense inngrepet til det som er "necessary in a democratic society".

Det som nå er gjenstand for vurdering er i hvilken grad lovbestemmelsen – i form av kontrollmekanismer og prosessuelle rettssikkerhetsgarantier for øvrig[171] – er egnet til å gi betryggende rettssikkerhetsgarantier. Summen av alle kontrollmekanismer utgjør en integrert del av forholdsmsessighetsvurderingen etter EMK artikkel 8 nr. 2. Som nevnt i punkt 2.2.4 kan disse deles inn i *interne* og *eksterne* kontrollmekanismer *forut for* og *etter* inngrepet.

Ved å sammenholde praksis fra EMD er det mulig å utlede visse minstekrav til den etterfølgende kontrollen.[172] Det kreves at kontrollorganene har en *uavhengig stilling* i forhold til den myndighet som beslutter og gjennomfører overvåkingen. Avgjørende er hvorvidt kontrollorganet er egnet til å foreta en *reell overprøving*.[173]

Kontrollutvalget for kommunikasjonskontroll består av minimum tre medlemmer hvor lederen for utvalget må oppfylle de krav som stilles til høyesterettsdommere, jf. kommunikasjonskontrollforskriften § 13. Funksjonstiden er fire år av gangen, jf. siste punktum. Kontrollutvalget for kommunikasjonskontroll[174] anses for å oppfylle kravet til uavhengighet, og drøftes ikke nærmere her.[175]

[169] Se også Sunde (2013) s. 273-274.
[170] Se særlig punkt 3.3 og 3.5.
[171] Hvorvidt forutberegnelighetskravet (i lovskravet) isolert sett gav en tilstrekkelig prosessuell rettssikkerhetsgaranti ble drøftet overfor i punkt 4.2.4.
[172] Se også dokument nr.16 (2015-2016) s. 251.
[173] Se bant annet *Ekimdzhiev mot Bulgaria* avs. 85.
[174] Se nærmere i punkt 2.2.4 overfor.
[175] Motsetningsvis *Iordachi mot Moldova* avs. 49.

For at kontrollutvalget skal kunne foreta en reell overprøving kreves det at utvalget både har *kompetanse* og *ressurser* til å foreta en slik kontroll.[176] I dette ligger det en forutsetning om at utvalget får *tilstrekkelig* informasjon om det som er innhentet gjennom metodebruken.[177]

Dataavlesing som en gjennomføringsmåte, slik Metodekontrollutvalget forslo, vil kun gjøre informasjon som politiet allerede har hjemmel til (gjennom reglene om kommunikasjonskontroll og ransaking) mer tilgjengelig.[178] Dataavlesing, slik det er innført i straffeprosessloven § 216 o, vil som nevnt overfor i punkt 3.5.1 ikke bare utvide politiets tilgang til informasjon, men i tillegg generere en *betydelig mengde* opplysninger. Dette har betydning i flere relasjoner.

For det første utfordrer metodebruken det kravet til notoritet som kan utledes av kommunikasjonskontrollforskriften § 7.[179] Ifølge forskriftsbestemmelsen skal politiet føre kontroll over nærmere bestemte opplysninger om tvangsmiddelbruken.[180] Som følge av at dataavlesing gir en betydelig mengde opplysninger vil det være *svært ressurskrevende* for politiet å foreta en nøyaktig registrering av alt materiale. Det er derfor sannsynlig at noe av materialet ikke registreres slik § 7 forutsetter. Dette har igjen en side mot den muligheten kontrollutvalget har for å etterprøve om protokollen er fullstendig og riktig. I lys av dette kan det problematiseres hvorvidt protokollen faktisk er egnet til å sikre notoritet.

I forlengelsen av dette oppstår et nytt problem: Kommunikasjonskontrollforskriften fokuserer nokså ensidig på å dokumentere det som *er* gjort. Dette er betenkelig ettersom kontrollgrunnlaget hovedsakelig består av loggdata som etterforskerens dataprogram selv genererer (selvrapporteringsordning) og at dataavlesing er en metode som etterlater seg få ytre spor. En slik løsning forutsetter at programmet er riktig innstilt og egnet til å rapportere alle relevante hendelser. Faren er at både utilsiktede og tilsiktede feil kan oppstå. Loggens troverdig er derfor problematisk. Dette aktualiserer spørsmålet om hvorvidt kontrollutvalget

[176] Sammenlignet storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 232, jf. "adequate and effective guaranties against abuse".
[177] Se blant annet *Kennedy mot Storbritannia* avs. 166.
[178] NOU 2009:15 s. 244- 245.
[179] Se kommunikasjonskontrollforskriften § 7 første ledd om hvilke opplysninger som skal protokollføres.
[180] For dataavlesing gjelder en mer vidtgående protokollføring enn for romavlytting og kommunikasjonskontroll for øvrig. Se særlig kommunikasjonskontrollforskriften § 7 andre ledd nr. 1-8.

har et forsvarlig grunnlag for å kontrollere at det ikke er gjort mer eller noe annet enn det som står i rapporten.[181] Dette utfordrer kravet om en reell kontroll.

For det tredje skal kontrollutvalget for kommunikasjonskontroll etter forskriften § 14 første ledd "kontrollere at politiets bruk av … dataavlesing skjer innenfor rammen av lov og instrukser, at tvangsmiddelbruken begrenses mest mulig, og at den ikke skjer av hensyn til etterforskning i andre saker enn de som er nevnt i straffeprosessloven … § 216o". Ved for eksempel kommunikasjonsavlytting vil utvalget kunne høre igjennom lydopptaket og således få et reelt bilde av den foretatte kommunikasjonskontrollen. Ved dataavlesing vil en tilsvarende løsning være betydelig vanskeliggjort som følge av metodens karakter.[182] Dermed er det også vanskelig å kontrollere om etterforskningen faktisk skjer innenfor lovens rammer.[183] Dersom ikke et slikt dokumentasjonskrav kan oppfylles, bør konsekvensene vurderes, og det bør diskuterer om metoden overhodet bør tillates.[184] Refleksjoner omkring hvordan dette skal løses i praksis synes imidlertid å være relativt fraværende i departementets utredning. Dette er betenkelig.

Den etterfølgende kontrollen må også sees i sammenheng med *hvem* som er berettiget til å foreta beslutningen om å iverksette dataavlesing. Hovedregelen er at en beslutning om dataavlesing skal treffes ved kjennelse, jf. straffeprosessloven § 216 o første ledd – altså av en domstol. Det er ubestridt at dette tilfredsstiller EMDs krav om et betryggende beslutningsorgan.[185] Også politiets hastekompetanse etter straffeprosessloven § 216 d første ledd, jf. § 216 o femte ledd, synes å være forenlig med konvensjonen.[186] Domstolene går imidlertid kun inn på *hvem* som kan være gjenstand for avlesingen, og ikke *hva* selve avlesingen kan gå ut på.[187] Som en følge av dette har domstolen ingen forutsetninger for å kunne kontrollere at den tekniske siden av metodebruken er forsvarlig. Ansvaret ligger dermed hovedsakelig hos lovgiver som må vedta krav til notoritet for å sikre en forsvarlig teknologikontroll.[188]

[181] Sunde (2013) s. 281. Sunde hevder også at Rt. 2011 s. 1188 i avsnitt 44 kan tas til inntekt for at det fra et rettssikkerhetsperspektiv kan være et behov for et negativt dokumentasjonskrav.
[182] Hernes (2010) s. 319.
[183] Sunde (2013) s. 281.
[184] Jf. også sunde (2013) s. 283.
[185] Storkammeravgjørelsen *Roman Zakharov mot Russland* avs. 259.
[186] Storkammeravgjørelse *Roman Zakharov mot Russland* avs. 266
[187] Se nærmere punkt 2.1.2.
[188] Sunde (2008) s. 475.

I lys av de nevnte utfordringene, kan det stilles spørsmål ved om de prosessuelle rettssikkerhetsgarantiene egentlig utgjør en tilstrekkelig garanti. En reell kontroll forutsetter et effektivt kontrollregime.[189] Etter min mening er det betydelig svakheter ved dagens etterfølgende kontroll. Dette skyldes at i) kontrollutvalget for kommunikasjonskontroll er tilpasset Metodekontrollutvalgets modell, og derfor ikke tilpasset dagens lovvedtak,[190] ii) lovgiver ikke i tilstrekkelig grad har tatt høyde for de teknologiske og rettssikkerhetsmessige utfordringene dataavlesing innebærer slik metoden er innført i straffeprosessloven § 216 o og iii) at lovgiver har ikke lyktes i å dokumentere at metoden i tilstrekkelig grad er kontrollerbar.

Slik jeg ser det har departementet vært mest opptatt av å kartlegge behovet for metoden og dens antatte effektivitet i stedet for å dokumentere at de rettssikkerhets- og personvernspørsmål som gjør seg gjeldende, er ivaretatt. Utover dette gjøres nærmest *ingen* vurdering av forholdet mellom dataavlesing som etterforskningsmetode og retten til privatliv etter Grunnloven § 102 og/eller EMK artikkel 8.[191] Etter min mening er hensynet til notoritet og effektiv kontroll så grunnleggende for rettssikkerheten og tilliten til politiets arbeid, at det bør være et minimumskrav at dette ikke bare er tilstrekkelig vurdert, men også at det foreligger lovregulerte tiltak *før* metodebruken tillates. På en rekke områder synes departementets utredning å komme til kort.

[189] *Kennedy mot Storbritannia* avsnitt 71, 166 og 169. Motsatt *Ekimdzhiev mot Bulgaria* avsnitt 92.
[190] NOU 2009:15 s. 249 og Prop. 68 L (2015-2016) s. 274.
[191] Se for eksempel Prop. 68 L (2015-2016) s. 39 flg. og fra s. 258 flg.

5 Kilderegister

Lover

Grunnloven	LOV-1814-05-17 *Kongeriket Norges Grunnlov*
Menneskerettsloven	LOV-1999-05-21-30 *Lov om styrking av menneskerettighetenes stilling i norsk rett*
Politiloven	LOV-1995-08-04-53 *Lov om politiet*
Straffeloven	LOV-2016-12-16-98 *Lov om straff*
Straffeprosessloven	LOV-1981-05-22-25 *Lov om rettergangsmåten i straffesaker*

Forskrifter

Beskyttelsesinstruksen	FOR-1972-03-17-3352 *Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter*
Kommunikasjonskontroll-forskriften	FOR-2016-09-09-1047 *Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing*

Internasjonale konvensjoner

EMK	*Convention for the Protection of Human Rights and Fundamental Freedoms*. Vedtatt 4. november 1950 (Roma), trådte i kraft 3. september 1953.

Forarbeider og andre offentlige dokumenter

Forarbeider:

NOU 1997:15	Etterforskningsmetoder for bekjempelse av kriminalitet
NOU 1997:19.	Et bedre personvern – forslag til lov om behandling av personopplysninger
NOU 2003:18	Rikets sikkerhet
NOU 2004:6	Mellom effektivitet og personvern – Politimetoder i forebyggende øyemed
NOU 2007:2	Lovtiltak mot datakriminalitet.
NOU 2009:1	Individ og integritet
NOU 2009:15	Skjult informasjon – åpen kontroll
NOU 2016:24	Ny straffeprosesslov
Ot.prp.nr. 11 (2007-2008)	Om lov om endringer i straffeprosessloven mv. (styrket stilling for fornærmede og etterlatte)
Ot.prp.nr.60 (2004-2005)	Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)
Prop. 68 L (2015-2016)	Endringer i straffeprosessloven (skjulte tvangsmidler)

Andre offentlige dokumenter:

Dokument 6 (2016-2017)	Melding om året 2016 fra Norges nasjonale institusjon for menneskerettigheter.
Dokument 16 (2011-2012)	Rapport til Stortingets presidentskap fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven. Avgitt 19. desember 2011.
Dokument 16 (2015-2016)	Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings,- overvåkings- og sikkerhetstjeneste (EOS-utvalget). Vedlegg 4: *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og etterretningstjenestens inngrep i menneskerettigheter?*
Innstilling 343 L (2015–2016)	Innstilling fra justiskomiteen om Endringer i straffeprosessloven mv. (skjulte tvangsmidler).
Komittédirektiv 2016:36	Hemlig dataavläsning.
Politidirektoratet (2008)	Politiet mot 2020 Bemannings- og kompetansebehov i politiet.

Rettsavgjørelser

Høyesterett:

Rt. 1993 s. 1302 (Høyesteretts kjæremålsutvalg)

Rt. 2000 s. 996

Rt. 2005 s. 833

Rt. 2005 s. 194 (Høyesteretts kjæremålsutvalg)

Rt. 2005 s. 1137

Rt. 2011 s. 946 (Høyesteretts ankeutvalg)

Rt. 2011 s. 1188

Rt. 2014 s. 1105

Rt. 2015 s. 81

Rt. 2015 s. 93

Rt. 2015 s. 155

Rt. 2015 s. 1456

HR-2016-1286-A

HR-2016-2554-P

Den europeiske menneskerettighetsdomstol:

Amann mot Sveits	Dom av 16. februar 2000 (Søkenummer: 27798/95)
Buck mot Tyskland	Dom av 28. april 2005 (Søkenummer: 41604/98)
Ekimdzhiev mot Bulgaria	Dom av 28. juni 2007 (Søkenummer: 62540/00)
Iordachi m.fl mot Moldova	Dom av 10. februar 2009 (Søkenummer: 25198/02)
Kennedy mot Storbritannia	Dom av 18. mai 2010 (Søkenummer: 26839/05)
Klass mfl. mot Tyskland	Dom av 6. september 1978 (Søkenummer: 5029/71)
Kruslin mot Frankrike	Dom av 24. april 1990 (Søkenummer: 11801/85)
Leander mot Sverige	Dom av 26. mars 1987 (Søkenummer: 9248/81)
Liberty m.fl. mot Storbritannia	Dom av 1. juli 2008 (Søkenummer: 58243/00)
Malone mot Storbritannia	Dom av 2. august 1984 (Søkenummer:8691/79)
Olsson mot Sverige (No. 1)	Dom av 24. mars 1988 (Søkenummer: 10465/83)
R.E mot Storbriannia	Dom av 27. oktober 2015 (Søkenummer:62498/11)
Roman Zakharov mot Russland	Dom av 4. desember 2015 (Søkenummer: 47143/06)
Rotaru mot Romania	Dom av 4. mai 2000 (Søkenummer: 28341/95)

Silver mot Storbritannia	Dom av 25. mars 1983 (Søkenummer: 7136/75)
Tyrer mot Storbritannia	Dom av 25. april 1978 (Søkenummer: 5856/72)
Weber and Saravia	Dom av 29. juni 2006 (Søkenummer: 54934/00)

Litteratur

Bøker:

All (2015) Jørgen Aall, Rettstat og menneskerettigheter, 4. utgave (Bergen 2015).

Auglend (2016) Ragnar L. Auglend og Henry John Mæland, Politirett (Oslo 2016).

Bruce (2014) Ingvild Bruce og Geir Sunde Haugland, Skjulte tvangsmidler (Oslo 2014).

Doublet (1995) David Roland Doublet, Rett, vitenskap og fornuft (Bergen 1995).

Høstmælingen (2003) Njål Høstmælingen, Internasjonale menneskerettigheter (Oslo 2003).

Strandbakken (2003) Asbjørn Strandbakken, Uskyldpresumsjonen (Bergen 2003).

Sunde (2006) Inger Marie Sunde, Lov og rett i Cyberspace (Bergen 2006).

Artikkelsamlinger:

Bruce (2010) Ingvild Bruce og Geir Sunde Haugland, "Personvern, rettssikkerhet og vern mot alvorlig kriminalitet" i Overvåking i en rettsstat, Dag Wiese Schartum (red.) (Bergen 2010) s. 62-83.

Hernes (2010) Helga Hernes, ”EOS-utvalgets kontroll av ”de hemmelige tjenester” i Overvåking i en rettsstat. Dag Wiese Schartum (red.) (Bergen 2010) s. 306-320.

Schartum (2010) Dag Wiese Schartum, ”Overvåking i en rettsstat – Oversikt og innledende observasjoner” i Overvåking i en rettstat. Dag Wiese Schartum (red.) (Bergen 20110) s. 17-35.

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

Juridiske artikler:

Busch (2011) Tor-Aksel Busch, ”Moderne kriminalitet – tradisjonell rettergang” i Referat fra Nordiska Juristmötet i Stockholm 18.-19. August 2011 s. 350-368.

Bårdsen (2017) Arnfinn Bårdsen, ”Grunnloven, straffeprosessen og strafferetten – noen linjer i Høyesteretts praksis etter Grunnlovsreformen 2014” i Jussens venner, 01/2017 Volum 52 s. 1-44.

Elgesem (2003) Frode Elgesem, ”Tolkning av EMK- Menneskerettsdomstolens metode” , i Lov og Rett, 04-05/2003 Volum 42 s. 203-230.

Keiserud (2015) Eirik Keiserud, Øyvind Precht-Jensen og Amna Avdagic, ”Advokatforeningens årstale 2014: En straffeprosess for vår tid – dilemmaer og utfordringer” i Tidsskrift for strafferett 2015/01 s. 27-42.

Sunde (2008) Inger Marie Sunde, ”Beskyttelsen mot overvågning i den fysiske og elektroniske verden” i Det 38. nordiske Juristmøte 2008 s. 459-479.

Sunde (2012) Inger Marie Sunde, ”Dataavlesing som etterforskingsmetode” i Rettfærd årgang 35 nr.1/136, 2012 s. 3-35 (Kan leses fra https://brage.bibsys.no/xmlui/handle/11250/174670).

Sunde (2013) Inger Marie Sunde, ”Straffeprosessuelle metoder rettet mot elektroniske bevis”. I Rettssikker radikaler: Festskrift til Ståle Eskeland 70 år. AP Høgberg, T.E Schea og R. Torgersen (red.) Oslo 2013 s. 266-283.

Sørensen (2004) Christian Børge Sørensen,” Læren om statens skjønnsmargin etter EMK og betydningen for norsk domstolskontroll med forvaltningen” i Tidsskrift for Rettsvitenskap 01-02/2004 Volum 117.

Lovkommentarer:

Haugland (2016) Geir Sunde Haugland, merknad til straffeprosessloven § 216 o, i Rettsdata 21. september 2016. Sist sjekket 29. mai 2017.

Netthenvisninger

Nettsider:

Datatilsynet (2012) Datatilsynet. *"Kryptering av informasjon",* 24. januar 2012. https://www.datatilsynet.no/Sikkerhet-internkontroll/Kryptering/ Sist sjekket 22. mai 2017.

Thon (2016) Bjørn Erik Thon for Datatilsynets blogg om personvernsspørsmål, "Personvernbloggen"https://www.personvernbloggen.no/2016/04/07/dataavlesing-med-datostempling/,7. april 2016. Sist sjekket 18. mai 2017.

Elden (2016) John Christian Elden,*"Når vi lures inn i overvåkningssamfunnet",* 25. mai 2016 (http://johnchristianelden.blogg.no/1464167829_nr_vi_lures_inn_i_ove.html) Sist sjekket 10. mai 2017.