Dataavlesing som et straffeprosessuelt tvangsmiddel

En konfrontasjon med retten til privatliv etter Grl. § 102 og EMK artikkel 8.

Kandidatnummer: 53

Antall ord: 14 931

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

12. desember 2016

Innholdsfortegnelse

1 Innledning

1.1 Presentasjon av tema og problemstilling

Etter en lengre prosess ble det i høst innført et nytt straffeprosessuelt tvangsmiddel i norsk rett, som kalles dataavlesing. Dataavlesing er ikke et entydig juridisk eller teknologisk begrep, men representerer et teknisk middel som på ulike måter kan gi politiet tilgang til innholdet på en datamaskin. Ved skjult tilstedeværelse i datasystemet, vil politiet kunne overvåke informasjon som produseres, lagres eller kommuniseres.[1] Temaet for avhandlingen er en analyse av gjeldende rett, samt hvordan retten burde være når det gjelder dataavlesing som et straffeprosessuelt tvangsmiddel.

Den teknologiske utviklingen blir stadig mer fremtredende. Utviklingen har medført en økt bruk av sosiale medier, mobiltelefoni, internett og avanserte krypteringer. Samfunnet har generelt en økende bevissthet om informasjonsbeskyttelse og teknologi, og på denne måten har det oppstått nye plattformer for kommunikasjon og arenaer for kriminalitet. Én utfordring er en økende kunnskap om krypteringer, særlig blant kriminelle. Ved bruk av krypteringsprogrammer er det mulig å sørge for at innhold i kommunikasjon ikke vil være leselig eller forståelig.[2] Dette gir politiet utfordringer ved at tvangsmidler som kommunikasjonsavlytting og hemmelig ransaking, ikke gir et tilsvarende informasjonsutbytte som tidligere. Tilgangen til informasjonen er uendret rettslig, men informasjonen har blitt mer utilgjengelig. Det kan ta flere måneder før politiet eventuelt klarer å knekke krypteringene, og i verste fall kan de mislykkes.[3] Informasjon som potensielt kan være et viktig og avgjørende bevis i en straffesak, blir dermed gjenstand for en ressurskrevende dekryptering fra politiets side.

I lys av dette, har det flere ganger vært drøftet hvorvidt politiet skal få adgang til andre metoder som samsvarer med den teknologiske utviklingen.[4] Den nylige vedtakelsen av dataavlesing som et straffeprosessuelt tvangsmiddel, er et tilskudd med formål om å imøtegå politiets utfordringer knyttet til dette.

[1] Prop. 68 L (2015-2016) s. 12.
[2] Prop. 68 L (2015-2016) s. 259.
[3] Prop 68 L (2015-2016) s. 260.
[4] Prop. 68 L(2015-2016) s. 238-239.

Dataavlesing gir mulighet for informasjonsinnhenting *før* det krypteres ettersom kommunikasjonen er i klartekst på vei inn og ut av datamaskinen. Ved at politiet har en skjult tilstedeværelse i datasystemet, kan politiet overvåke informasjonen fortløpende i sanntid. I tillegg kan metoden gi mulighet til dekryptering i transportfasen ved å fange opp kodenøkler.[5] I lys av dette vil dataavlesing løse flere av utfordringene politiet har med krypteringer og dermed være et egnet tvangsmiddel i samsvar med den teknologiske utviklingen.

Metoden kan imidlertid virke svært inngripende og kontroversiell, da det vil gi politiet en skjult tilstedeværelse i datasystemet og dermed åpne for en fortløpende overvåkning av alt mistenkte foretar seg på enheten, i *sanntid*. Mistenktes rettssikkerhet står derfor sentralt. En begjæring om bruk av dataavlesing fra den offentlige myndighet, vil representere et inngrep i mistenktes rett til privatliv som både er vernet av Grunnloven § 102 og EMK artikkel 8. Det er derfor interessant hvordan dataavlesing kan anvendes i tråd med de overordnede rettsregler. I tillegg er det uklart hva dataavlesing innebærer for de fleste, ettersom begrepet verken er selvforklarende eller et entydig teknologisk begrep.[6]

I lys av dette, er det aktuelt å foreta en konfrontasjon med dataavlesing som et straffeprosessuelt tvangsmiddel i forhold til de overordnede rettsregler. Problemstillingen er om det å innføre en inngripende og kontroversiell metode vil samsvare med overordnede rettsregler, hvor retten til privatliv står sentralt. For det første vil EMK artikkel 8 nr. 2 kreve at dataavlesing er et er *nødvendig* inngrep i et demokratisk samfunn. Det vil også være et spørsmål hvorvidt den lovtekniske løsningen for dataavlesing oppfyller kravet til klar lovhjemmel som følger både av Grl. § 102 jfr. § 113 og EMK artikkel 8 nr. 2. Spørsmålet er om bestemmelsene slik de er utformet vil ivareta individets rettsikkerhet. Rettspolitisk vil det være et spørsmål om formålet med å innføre dataavlesing kan realiseres med lempeligere midler.

En konfrontasjon med dataavlesing og de overordnede rettsregler, er ikke blitt foretatt av verken Høyesterett eller Den Europeiske Menneskerettighetsdomstolen (EMD). I lys av dette har problemstillingen aktualitet ved flere implikasjoner. For det første ved hvordan EMK artikkel 8 skal tolkes i relasjon til dataavlesing, ettersom EMD ikke har tatt stilling til dette. For det andre hvorvidt et slikt tvangsmiddel er i samsvar med EMK artikkel 8 og Grunnloven

[5] NOU 2009:15 s. 241-242.
[6] Prop.68 L (2015-2016) side 224.

§ 102. Endelig vil det på selvstendig grunnlag være nødvendig å klargjøre hva metoden innebærer, ettersom dataavlesing er et relativt nytt og lite kjent tvangsmiddel.

1.2 Avgrensning

Nasjonale myndigheter har et overordnet ansvar for å beskytte befolkningen mot kriminelle handlinger som kan krenke borgernes rettigheter og rettssikkerhet. På sentralt nivå er dette ansvaret delt mellom Justisdepartementet og Riksadvokaten, ettersom vi i norsk rett har et tosporet system. Ansvaret for straffesaksbehandlingen hører under Riksadvokaten, mens det daglige politiarbeidet som ordenstjeneste og forebyggende virksomhet hører til Justisdepartementet.[7]

Bruk av skjulte tvangsmidler forekommer både i straffesaksbehandling og i forebyggende øyemed gjennom PST (Politiets sikkerhetstjeneste). Dataavlesing kan for det første begjæres i straffeforfølgende funksjon, ved etterforskning av straffbare handlinger med hjemmel i straffeprosessloven.[8] For det andre kan dataavlesing anvendes som politimetode ved forebygging av alvorlig kriminalitet med hjemmel i politiloven § 17 d.[9]

Av hensyn til omfanget av oppgaven har jeg valgt å avgrense mot dataavlesing som tvangsmiddel i forebyggende og avvergende øyemed. Politilovens hjemmel til bruk av dataavlesing i forebyggende øyemed, har dermed ingen direkte relevans for oppgavens problemstilling og vil ikke bli behandlet.

1.3 Rettskildebilde og metode

Det er to overordnede rettsregler å forholde seg til i denne sammenheng. Grl. § 102 er av Grunnlovs rang, mens EMK artikkel 8 er inkorporert i norsk lov jfr. menneskerettsloven § 3. Grunnloven er *lex superior*, mens konvensjoner og protokoller som er inkorporert i norsk rett, er inkorporert på lovs nivå. Menneskerettsloven § 3, fastslår imidlertid at de konvensjoner og protokoller som er omfattet av loven, skal gå foran annen norsk lovgivning.

[7] Haugland m.fl. (2014) s. 45-46.
[8] Lov av 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven).
[9] Lov av 4. april 1995 nr. 53 om politiet (politiloven).

Menneskerettighetskonvensjonen er således innført med en slags forrang av "semikonstitusjonell karakter" i forhold til annen lovgivning.[10]

Som jeg vil komme tilbake til i kapittel 4.1, har det vært nødvendig å klarlegge det nærmere forholdet mellom Grl. § 102 og EMK artikkel 8. Dette har jeg gjort basert på nyere praksis fra Høyesterett. På bakgrunn av uttalelser fra Høyesterett, vil konfrontasjonen foretas gjennom en tolkning av EMK-retten. Praksis fra Den Europeiske Menneskerettighetsdomstolen (EMD) vil dermed stå sentralt. Ved tolkning og fastlegging av gjeldende rett etter EMK er det en noe annen metodisk tilnærming.[11]Av hensyn til plass og disposisjon er det ikke mulig å gjøre en generell redegjørelse av metodiske spørsmål knyttet til dette. Jeg vil etter beste evne forsøke å anvende metoden for tolkning av konvensjonspraksis.

De siste årene har det vært en utvikling i Strasbourg når det gjelder EMK artikkel 8, hvor det er kommet avgjørelser, som mer utførlig presiserer normen og hvordan den skal tolkes. Det kan blant annet nevnes *R.E mot Storbritannia* og storkammer dommen *Roman Zakharov mot Russland.*[12] Da det foreligger nyere konvensjonspraksis som oppklarende belyser normen på flere punkter, har jeg vært nødt til å gå inn i disse avgjørelsene på selvstendig grunnlag.

1.4 Kort om fremstillingen i oppgaven

Dataavlesing er som nevnt ikke et selvforklarende eller entydig teknologisk begrep. I tillegg er det en forholdsvis ny metode, slik at det kan fremstå noe uklart hva dataavlesing innebærer. I lys av dette finner jeg det nødvendig å belyse hvordan dataavlesing kan gjennomføres på selvstendig grunnlag, samt gi en oversikt over hvordan dataavlesing har vært vurdert som metode tidligere. Dette vil bli foretatt i kapittel 2. Videre vil jeg foreta en deskriptiv redegjørelse for de materielle- og prosessuelle krav som bestemmelsene i norsk rett stiller for å bruke dataavlesing i etterforskning. Dernest vil jeg i kapittel 4 gå over i den normative analysen og foreta en konfrontasjon med de overordnede rettsregler. For det første vil jeg forsøke å klargjøre det nærmere forhold mellom Grl. § 102 og EMK artikkel 8 (kapittel 4.1). For det andre vil jeg belyse de ulike ulike vilkårene for et rettmessig inngrep i EMK artikkel 8.2, ved å klargjøre hvordan EMD tolker normen i praksis. Konfrontasjonen med de norske reglene vil gjøres fortløpende. (kapittel 4.2-4.5).

[10] Skoghøy (2002) s. 340.
[11] Se Skoghøy (2002) og Graver (2003).
[12] Roman Zakharov v. Russia og R.E v. The United Kingdom.

2 Fenomenet dataavlesing

2.1 Dataavlesing i norsk rett

I løpet av de siste tiårene har dataavlesing blitt vurdert og drøftet som en mulig politimetode i norsk rett. Utredningene bærer preg av en usikkerhet rundt hvordan dataavlesing gjennomføres teknisk, samt en forsiktighet begrunnet i at det er en svært inngripende politimetode.[13] Den første utredning av betydning i denne sammenheng, var metodekontrollutvalgets utredning i 2009. Utvalget foreslo å innføre dataavlesing som en gjennomføringsmåte for kommunikasjonsavlytting etter strpl. § 126 a og hemmelig ransaking etter strpl. § 200 a. Hensikten var at politiet ved hjelp av dataavlesing kunne sikre informasjon som var hentet ved kommunikasjonsavlytting eller hemmelig ransaking, men som var kryptert eller på annen måte utilgjengelig. Dataavlesing kunne dermed effektivisere de eksisterende tvangsmidler.[14]

Metodekontrollutvalget la til grunn at dataavlesing som en gjennomføringsmåte ved kommunikasjonsavlytting etter strpl. § 216 a, ville gjøre det mulig å fremskaffe opplysninger som relaterer seg til vanskeliggjøringen av kommunikasjonsavlyttingen. Informasjon om annet enn det mistenkte selv sender og mottar i datasystemet, for eksempel informasjon hentet fra kamera eller mikrofon, ville imidlertid falle utenfor. Det samme gjelder informasjon som er lagret i datasystemet. Dataavlesing som en gjennomføringsmåte for hemmelig ransaking med hjemmel i strpl. § 200 a, ville på den annen side gi tilgang til informasjon som er lagret på mistenktes datamaskin. Metodekontrollutvalget la til grunn at datavlesing ville gjøre hemmelig ransaking mindre integritetskrenkende ettersom politiet ikke behøver fysisk tilgang til mistenktes private bolig. Ransakingen ville foregå elektronisk, fjernstyrt fra politiet gjennom tilgangen i datasystemet.[15] Det ville imidlertid være begrenset slik at politiet ikke kunne utnytte tilstedeværelsen i datasystemet over tid og derav kartlegge mistenktes fortløpende bruk i sanntid. Begrunnelsen var at en generell adgang til innhenting av informasjon ville utgjøre en for stor integritetskrenkelse i forhold til det anførte behovet, slik at tillatelse til hemmelig ransaking, måtte innhentes på nytt hver gang.[16]

[13] Haugland m.fl. (2014) s. 253.
[14] NOU 2009:15 s. 26-27.
[15] NOU 2009:14 s. 27.
[16] NOU 2009:15 s.246.

Utvalget legger videre til grunn at innføringen av dataavlesing er betinget av en forsvarlig kontroll med inngrepet. Det fremheves i utredningen at det kreves en "skjerpet kontroll med og dokumentasjon av bruken av et slikt tvangsmiddel", da det eksisterer en stor fare for misbruk. Utvalget foreslo å innføre et protokollsystem, for å sikre notoritet.[17]

I Prop. 68 L (2015-2016) ble det fremmet et lovforslag om å innføre dataavlesing. Forslaget var en av flere lovendringer som ville gi politiet en utvidet adgang til benyttelse av skjulte tvangsmidler. Departementet legger til grunn at adgangen til å benytte dataavlesing bør være *mer vidtgående* enn metodekontrollutvalgets forslag fra 2009, og foreslår dataavlesing innført som et nytt *selvstendig* tvangsmiddel.[18] Forslaget åpnet for at politiet ved skjult tilstedeværelse i datasystemet, kan skaffe seg tilgang til opplysninger i et datasystem, uten at avlesingen er en del av en begjæring om kommunikasjonsavlytting eller hemmelig ransaking. Politiet vil dermed kunne kartlegge mistenktes bruk av datasystemet i sanntid, over en lengre periode, i tillegg til at lagret informasjon omfattes.[19] Dette står i kontrast til metodekontrollutvalgets forslag, som kun foreslo dataavlesing som et substitutt eller en gjennomføringsmåte for de eksisterende tvangsmidler. Forslaget tar dermed sikte på en metode som metodekontrollutvalget anså å være *for integritetskrenkende* syv år tidligere.

Departementet legger videre til grunn at en forsvarlig kontroll med metodebruken er avgjørende for å sikre notoritet. I likhet med metodekontrollutvalget, foreslår departementet at det skal føres en protokoll med bruken av dataavlesing i hver enkelt sak for at kontrollen skal være tilfredsstillende.[20] Departementet viderefører utvalgets forslag når det gjelder kontrolltiltak, til tross for at omfanget av dataavlesingen etter lovforslaget går *lengre enn* utredningen i 2009. Det kan således problematiseres hvorvidt kontrollen med metodebruken er tilpasset omfanget av dataavlesingen som er foreslått. Dette vil jeg komme nærmere tilbake til i kapittel 4.4.2.

Hjemmel til bruk av dataavlesing i norsk rett ble vedtatt 17 juni 2016, ved tilføyelse av en ny bestemmelse i straffeprosessloven § 216 o og politiloven § 17 d.[21] Bestemmelsene trådte i kraft 9 september 2016. Dataavlesing er innført som et *selvstendig* tvangsmiddel, i samsvar med departementets forslag i proposisjonen. Det endelige vedtaket var imidlertid snevret inn

[17] NOU 2009:15 s.249.
[18] Prop. 68 L (2015-2016) s.264.
[19] Prop. 68 L (2015-2016) s. 264-265.
[20] Prop 68 L (2015-2016) s.272.
[21] Jf. endringslov av 16. juni 2016 nr. 54 om endringer i straffeprosessloven.

på flere punkter. Et eksempel er at det i departementets utredning ble foreslått at dataavlesing kunne brukes når noen med *skjellig grunn* mistenkes for en handling som rammes av *straffeloven § 231*.[22] At dataavlesing ble foreslått tillatt ved simpel narkotikaovertredelse, illustrerer at forslaget til departementet var svært vidtgående. Strl. § 231 er imidlertid ikke med i oppregningen av straffebud i strpl. § 216 o.

2.2 Den tekniske gjennomføringen av dataavlesing

Dataavlesing er en etterforskningsmetode som omfatter ulike fremgangsmåter som kan gi tilgang til informasjon som genereres eller lagres i et *datasystem*. Det er imidlertid ikke en teknisk betegnelse som referer til en klart avgrenset fremgangsmåte.[23] Det kan derfor fremstå noe uklart hva metoden innebærer. I lys av dette er det nødvendig å klargjøre hva dataavlesing er, og hvordan politiet kan gå frem teknisk. Metodens karakter vil videre ha betydning i konfrontasjonen med de overordnede rettsregler i avhandlingens kapittel 4.

Departementet har lagt til grunn at "datasystem" omfatter smarttelefoner, datamaskiner og andre anlegg for elektronisk kommunikasjon som behandler data ved hjelp av dataprogrammer.[24] Etter dette kan dataavlesing foretas på ulike enheter, for eksempel nettbrett, smarttelefon og datamaskin. I prinsippet vil avlesingen kunne omfatte lydstrøm tilknyttet mikrofon, videostrøm, tastetrykk, innhold på harddisk og data som sendes ut eller hentes på internett.[25] I tillegg vil opplysninger som verken lagres eller kommuniseres være omfattet.[26] Dette kan for eksempel være inntastinger, filer eller tekster med personlige tanker eller betraktninger, som aldri var ment å formidles eller lagres.

Selve prosessen av dataavlesingen kan deles inn i ulike deler. Det vil for det første være en innledende fase hvor det teknologiske virkemiddelet installeres eller monteres. Dernest en avlesningsfase, hvor politiet får tilgang til opplysningene og mulighet til å overvåke bruken av datasystemet. Endelig er det en avslutningsfase der virkemiddelet avinstalleres eller fjernes.[27]

I lys av beskrivelsene i metodekontrollutvalgets utredning og departementets vurdering i forarbeidene, samt juridisk teori er det mulig å trekke et skille mellom tre ulike

[22] Prop 68L (2015-2016) s.224.
[23] Prop. 68 L (2015-2016) s. 13.
[24] Prop. 68 L (2015-2016) s. 270-271.
[25] Prop. 68 L (2015-2016) s. 224.
[26] Haugland m.fl. (2014) s. 255.
[27] NOU 2009:15 s. 247.

gjennomføringsmåter. Betegnelsene er ikke rettslige, men bidrar til en systematisk fremstilling.[28] Jeg vil i det følgende skille mellom utstyrsbasert og informasjonsbasert dataavlesing, samt en mellomform.

Ved *utstyrsbasert* dataavlesing benyttes teknisk utstyr eller programvare for å fange opp data fra et datasystem. Utstyrsbasert dataavlesing kan hovedsakelig gjennomføres på to ulike måter; hardwarebasert og softwarebasert.[29]

Ved bruk av software kan politiet hente ut informasjon fra datasystemet ved hjelp av et program som er installert på mistenktes brukerkonto eller datamaskin.[30] Programvaren kan sende data til politiet og programmeres slik at den forholder seg til et avgrenset område i datasystemet.[31] En slik programvare kalles *"trojaner*" på det tekniske fagspråket. Trojanere spres til mistenktes maskin ved å utnytte sikkerhetshull i datasystemet på internett, eller ved å sende e-post hvor trojaneren fremkommer i et skjult vedlegg. En annen løsning er å infisere datasystemet med trojanere som ledd i hemmelig ransaking.[32] Når programvaren blir kjørt i datasystemet, åpnes det en tilgang til maskinen, en såkalt bakdør. Politiet kan deretter benytte seg av bakdøren for å innhente informasjon fra datasystemet, ved at programmet kopierer og sender data. Trojanere kan være avanserte og blant annet inneholde funksjoner som gjør det mulig å lese filer på datamaskinen, overvåke skjermbildet samt avlytte rommet ved hjelp av mikrofonen.[33] Trojaneren kan for eksempel programmeres slik at den gir varsel om aktivitet av interesse for politiet.[34] I forbindelse med dataavlesing er trojaneren et hackerverktøy til bruk for politiet. Denne typen trojaner kan betegnes som "polititrojanere" eller "politiprogram", for å understreke at trojaneren i denne sammenheng brukes av den offentlige myndighet.[35]

Når fremgangsmåten er hardwarebasert, installeres det fysiske komponenter som gir politiet tilgang til informasjon. For det første kan en tastetrykkavleser installeres i tastaturet, såkalt "key-logging". Gjennom key-logging kan politiet lese av tastetrykkene som utføres på mistenktes datamaskin. For det andre kan det monteres utstyr i mikrofonen som gjør det

[28] Sunde (2012) s. 9-10.
[29] Sunde (2012) s. 9. Se også Haugland m.fl. (2014) s. 254-255.
[30] NOU 2009:15 s. 247.
[31] Sunde (2012) s. 10.
[32] NOU 2009:15 s. 247.
[33] NOU 2007:2 s. 24.
[34] Sunde (2012) s. 11.
[35] Sunde (2012) s.11.

mulig for politiet å overvåke lydsignalene ved kommunikasjon over internett.[36] Ettersom hardwarebaserte løsninger krever fysisk tilstedeværelse ved datautstyret, kan dette gi utfordringer operativt. Ved bruk av software vil politiets arbeid kunne effektiviseres ettersom politiet ikke trenger å være til stede ved avlesningen. Trojaneren kan for eksempel programmeres slik at den gir varsel om aktivitet av interesse for politiet.[37]

Ved *informasjonsbasert* dataavlesing utnyttes brukerens tilgangsdata eller teknisk hackerkompetanse for å oppnå tilgang til datasystemet. Politiet bruker ikke teknisk utstyr, men utnytter teknisk kunnskap eller tilgangsdata for å få tilgang til datasystemet. Et eksempel er at politiet kan benytte seg av mistenktes brukernavn og passord slik at tilgang oppnås gjennom ordinær påloggingsprosedyre. En annen løsning er bruk av hackerkompetanse, slik at sårbarheter i programvaren utnyttes for å gi politiet tilgang.[38] Datakrimutvalget bruker betegnelsene ”passord-innbrudd” og ”sårbarhetsinnbrudd” på disse metodene.[39]

Endelig kan det tenkes *mellomformer* som kombinerer utstyrs- og informasjonsbaserte fremgangsmåter. Dersom politiet oppnår tilgang til systemet ved hjelp av en eksisterende sårbarhet, og deretter installerer en trojaner for å kunne foreta avlesning, er fremgangsmåten en kombinasjon av å være utstyrs- og informasjonsbasert. Et annet eksempel er dersom politiet avdekker en eksisterende trojaner ved å bruke et datasystem som søker etter sårbarheter, vil denne delen av prosessen være utstyrsbasert. Men på den annen side vil selve inntrengingen i datasystemet være informasjonsbasert ettersom politiet utnytter sin tekniske kompetanse.[40]

Når det gjelder fremgangsmåten for dataavlesing slik det er innført i norsk rett, fremgår det av straffeprosessloven § 216 p at:

> ”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.”

Sett i sammenheng med redegjørelsen ovenfor, tar lovgiver med betegnelsene “tekniske innretninger*”* og ”dataprogram*”* sikte på utstyrsbaserte fremgangsmåter for dataavlesingen,

[36] Haugland m.fl. (2014) s. 254.
[37] Sunde (2012) s. 11.
[38] Sunde (2012) s. 11-12.
[39] NOU 2007:2 s. 22-23.
[40] Sunde (2012) s. 11.

herunder bruk av software og hardware. Dette understrekes ved at disse kan ”installeres i datasystemet” og ”i annen maskinvare”. Videre åpner formuleringen *”*eller på annen måte”, for informasjonsbaserte løsninger og mellomformer. Ordlyden illustrerer en forholdsvis vid adgang til ulike gjennomføringsmåter og politiet er med dette utdelt et betydelig skjønn ved valg av metode. Ordlyden isolert sett gir ikke en klar anvisning på hva som ligger i gjennomføringen av dataavlesingen. Det kan således problematiseres hvorvidt bestemmelsen er tydelig nok på dette punkt. Men det er klart at løsningen som er valgt i lovteksten åpner for både informasjonsbasert og utstyrsbasert dataavlesing, i tillegg til en kombinasjon av disse.

3 Vilkårene for bruk av dataavlesing

3.1 Materielle vilkår

3.1.1 Generelt

For å anvende straffeprosessuelle tvangsmidler, må de materielle vilkårene være oppfylt. Vilkårene varierer fra tvangsmiddel til tvangsmiddel, men er ment å gjenspeile inngrepets karakter og hvor viktig bruken er for å sikre en effektiv strafferettspleie.[41] I det følgende vil jeg foreta en analyse de lege lata av vilkårene for å anvende dataavlesing etter strpl. § 216 o.

3.1.2 Mistankekravet

Et grunnvilkår for at politiet kan anvende dataavlesing er at det foreligger "skjellig grunn" til mistanke om at en straffbar handling er begått jfr. strpl. § 216 o første ledd. Vilkåret stiller krav til mistankens styrke. En naturlig språklig forståelse av "skjellig grunn" tilsier at det kreves god eller rimelig grunn til mistanke. En sikker overbevisning om skyld er således ikke nødvendig. På den annen side kreves det en kvalifisert mistanke, ved at den må være velbegrunnet. Rettspraksis legger til grunn at vurderingstemaet er om vedkommende er skyldig, herunder om personen oppfyller vilkårene for straff og om det foreligger en straffrihetsgrunn.[42] Høyesterett har videre tolket bestemmelsen slik at det må være mer sannsynlig at vilkårene for straffansvar er oppfylt enn at de ikke er det.[43] Beviskravet er således sannsynlighetsovervekt.

Etter dette må det foretas en skjønnsmessig vurdering av om det foreligger sannsynlighetsovervekt for at vedkommende er skyldig sett hen til straffbarhetsvilkårene. Såfremt det foreligger sannsynlighetsovervekt for at mistenkte er skyldig i det straffbare forholdet mistanken gjelder, er mistankekravet oppfylt jfr. strpl. § 216 o første ledd.

[41] Øyen (2016) s.177.
[42] Se Rt. 2004 s.887 avsnitt 12 og Rt.2012 s.134 avsnitt 10.
[43] Rt. 2011s. 946 avsnitt 13

3.1.3 Kriminalitetskravet

Det stilles videre krav til alvoret av den overtredelsen mistanken gjelder. Bestemmelsen opererer med to ulike strafferammekrav; det alminnelige og det spesielle. Dataavlesing kan for det første benyttes ved skjellig grunn til mistanke for "en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i 10 år eller mer" jfr. strpl. § 216 o første ledd bokstav a. En naturlig språklig forståelse av ordlyden "kan medføre" tilsier at det er strafferammen i det straffebudet mistanken gjelder som er avgjørende. Dette støttes av rettspraksis hvor Høyesteretts kjæremålsutvalg har påpekt at det er straffebudenes abstrakte strafferamme som er avgjørende.[44] Den forventede straffen for den konkrete overtredelsen har således ingen betydning.

For det andre kan dataavlesing anvendes dersom det er skjellig grunn til mistanke for en handling eller forsøk på en handling som omfattes av opplistingen av straffebud i strpl. § 216 o første ledd bokstav b. Dette omtales som det spesielle strafferammekravet ettersom det avgjørende er hvorvidt straffebudet som overtredelsen gjelder, er nevnt i bestemmelsen. Ulovlig etterretning og militær virksomhet, samt oppfordring eller rekrutering til terrorhandlinger er straffbare handlinger som fremkommer i opplistingen. Videre er menneskehandel, grovt heleri, hvitvasking knyttet til narkotika og uaktsom grov narkotikaovertredelse omfattet. Dette illustrerer et vidt spekter av straffebud med ulik grovhet og strafferamme. Adgangen til bruk av dataavlesing er således ikke begrenset til mistanke om de mest alvorlige straffbare handlinger, også mindre alvorlige handlinger med betydelig lavere strafferammer er omfattet. Begrunnelsen er i følge departementet, at dette er eksempler på lovbrudd som kan medføre etterforskningsmessige utfordringer, slik at det bør åpnes for dataavlesing selv om det ordinære strafferammekravet ikke er oppfylt. I slike tilfeller, vil dataavlesing imidlertid være underlagt vesentlige tilleggsbegrensninger ved at forholdsmessighetskravet etter strpl. § 170 a skjerpes i slike saker.[45]

3.1.4 Krav til nødvendighet og forholdsmessighet

Tillatelse til bruk av dataavlesing kan gis såfremt det "antas at dataavlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaringen ellers i vesentlig grad vil bli vanskeliggjort" jfr. strpl. § 216 o tredje ledd. Det stilles med dette et krav om at metoden er

[44] Se Rt. 2006 s.1398.
[45] Prop.68 L (2015-2016) s.268.

nødvendig. Det må etter dette foretas en konkret vurdering i hver enkelt sak om det foreligger et nødvendig behov for dataavlesing. I tillegg til kravet om nødvendighet og de øvrige materielle vilkår, er adgangen underlagt en ytterligere begrensning ved det alminnelige forholdsmessighetsprinsippet i strpl. § 170 a annet punktum. Det følger av bestemmelsen at dataavlesing, likevel ikke kan benyttes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep. En slik begrensning bidrar til å sikre at bruken av dataavlesing skjer innenfor rammene av retten til privatliv i EMK artikkel 8.[46] Avgjørende vil være at skaden eller belastningen som er forbundet med dataavlesingen, ikke står i misforhold til formålet som søkes oppnådd. Forholdsmessighetskravet etter strpl. § 170 a vil ha særlig betydning for adgangen til dataavlesing i saker hvor forbrytelsen har en vesentlig lavere strafferamme enn fengsel inntil 10 år.[47]

Eksistensen av prosessuelle garantier i forbindelse med gjennomføringen av dataavlesingen er et tungtveiende moment i forholdsmessighetsvurderingen. Ved bruk av skjulte tvangsmidler, kan ikke mistenkte gis adgang til å uttale seg på forhånd om avlesingen, ettersom dette vil redusere effekten av tiltaket.[48] Hensynet til kontradiksjon og ivaretakelse av mistenktes rettssikkerhetsgarantier, må derfor sikres på en annen måte. Dette vil jeg komme nærmere tilbake til under punkt 3.2.

3.1.5 Kravet om hensiktsmessighet

Strpl. § 170 a første punktum legger videre til grunn at et tvangsmiddel bare kan brukes når det er tilstrekkelig grunn til det. Bestemmelsen oppstiller med dette et hensiktsmessighetskrav.

Kravet om tilstrekkelig grunn for å bruke et tvangsmiddel kan betegnes som en sikkerhetsventil, ettersom det normalt foreligger tilstrekkelig grunn når bruken av tvangsmiddelet er nødvendig og forholdsmessig.[49]

[46] Prop. 68 L (2015-2016) s.270.
[47] Prop. 68 L (2015-2016) s.268 og 269.
[48] Aal (2014) s. 231.
[49] Øyen (2016) s.179.

3.2 Prosessuelle rettssikkerhetsgarantier og kontrollmekanismer

Det ligger i sakens natur at skjulte tvangsmidler må holdes hemmelige overfor mistenkte. Det stilles derfor særlige krav til prosessuelle garantier i forbindelse med tvangsmiddelbruken for å sikre kontradiksjon og ivaretakelse av mistenktes rettssikkerhet.[50] Videre er betydningen av tilstrekkelig kontrollmekanismer ved innføring av dataavlesing, understreket av både metodekontrollutvalget og departementet.[51] I lys av dette er det hensiktsmessig å redegjøre for hvilke prosessuelle garantier og kontrollmekanismer som er innført i forbindelse med dataavlesing.

Det stilles for det *første* krav til en betryggende personell avgjørelseskompetanse. Begrunnelsen er at dataavlesing er et skjult tvangsmiddel, slik at mistenktes manglende kunnskap om tvangsmidlet, svekker kontradiksjonen.[52] Utgangspunktet er at retten ved kjennelse gir tillatelse til bruk av dataavlesing jfr. strpl. § 216 o første ledd. Påtalemyndighetens ordre kan imidlertid tre i stede for kjennelse, dersom det ved opphold er stor fare for at etterforskningen vil lide jfr. strpl. § 216 o femte ledd og henvisningen til strpl. § 216 d. Ved bruk av påtalemyndighetens hastekompetanse, må politi og påtalemyndighet snarest mulig og senest innen 24 timer, forelegge beslutningen til retten for godkjennelse jfr. strpl. § 216 d første ledd.

For det *andre* kreves det at retten oppnevner en offentlig advokat for mistenkte ved behandling av begjæring om bruk av dataavlesing jfr. strpl. § 100 a første ledd. Advokaten skal imidlertid ikke settes i forbindelse med mistenkte, og har taushetsplikt vedrørende tvangsmidler, begjæring og rettens beslutning jfr. strpl. § 100 a tredje ledd. Hensikten er at den oppnevnte advokaten skal ivareta mistenktes interesser i forbindelse med rettens behandling av begjæringen og har ved anmodning rett på innsyn i sakens dokumenter jfr. bestemmelsens tredje ledd. Departementet påpeker at advokatens primære oppgave er å sørge for at faktum blir grundig og allsidig belyst, samt problematisere om kravet til proporsjonalitet og de øvrige vilkårene for bruk av tvangsmiddel er oppfylt. På denne måten

[50] Aal (2014) s. 231.
[51] Se NOU 2009:15 s. 249 og Prop. 68 L(2015-2016) s. 274.
[52] Aal (2014) s. 231.

kompenseres mistenktes fratatte mulighet til å kontrollere og ta til motmæle mot begjæringen.[53]

Når det gjelder kontrollmekanismer, stilles det for det *første* krav om protokollføring. Det følger av kommunikasjonskontrollforskriften § 7 at det skal føres en protokoll med opplysninger om tvangsmiddelbruken. Tilsvarende protokoll gjelder ved romavlytting og kommunikasjonsavlytting.[54] Hvilke opplysninger som skal fremgå av protokollen er nærmere opplistet i bestemmelsen, og det stilles *særlige krav* til opplysninger ved dataavlesing. Det skal blant annet opplyses hvilke type data som er avlest, om det er benyttet tekniske innretninger eller maskinvare og hvilket personell som har foretatt avlesingen. Hensikten er at protokollen skal sikre notoritet med hensyn til det politiet foretar seg, ettersom kontroll med politiets metodebruk ble ansett å være en betingelse for å innføre dataavlesing.[55] Departementet videreførte dermed metodekontrollutvalgets forslag om protokoll som en kontrollmekanisme.[56] Ved at dataavlesing er innført som et *selvstendig* tvangsmiddel i strpl. § 216 o, er metoden innført i en annen utstrekning enn det metodekontrollutvalget tok sikte på. Det kan dermed problematiseres hvorvidt protokollen er tilstrekkelig tilpasset dataavlesing som et *selvstendig* tvangsmiddel, da departementet videreførte forslaget om protokollføring uten å foreta en nærmere vurdering. Det er ikke gitt at protokollen vil sikre notoritet i den sammenheng dataavlesing nå er innført. Dette vil jeg komme tilbake til i kapittel 4.4.2.

For det *andre* er kontrollutvalget for kommunikasjonskontroll (kk-utvalget), en kontrollmekanisme for dataavlesing i norsk rett. Kk-utvalget skal foreta en etterfølgende kontroll av politiet og påtalemyndighetens behandling av saker om dataavlesing jfr. strpl. § 216 h. Kontrollutvalgets primære oppgave er å kontrollere at politiet og påtalemyndighetens bruk av kommunikasjonskontroll er innenfor rammene av lov og instruks, samt se til at bruken er betryggende og begrenset jfr. kommunikasjonskontrollforskriften § 14. Departementet understreker viktigheten av at det legges til rette for at kontrollutvalget fører en effektiv og reell kontroll med bruken av dataavlesing, og at det sett hen til metodens karakter vil være avgjørende at høy teknologisk kompetanse er tilgjengelig.[57] I kapittel 4.4.2

[53] Ot.prp. nr. 64 (1998-1999) s.84.
[54] Forskrift av 9. september 2016 nr. 1047 om kommunikasjonsavlytting, romavlytting og dataavlesing (kommunikasjonskontrollforskriften).
[55] Prop. 68 L(2015-2016) s.272.
[56] NOU 2009:15 s.249. Se også overfor i kapittel 2.1.
[57] Prop. 68 L (2015-2016) s.274.

vil jeg komme tilbake til hvorvidt kk- utvalget har mulighet til å foreta en *reell* kontroll med dataavlesing, samt hvilke utfordringer dette eventuelt kan medføre.

Endelig skal politimesteren sende innberetning til Riksadvokaten ved utgangen av hvert kvartal jfr. kommunikasjonskontrollforskriften § 10. Innberetningen skal omfatte opplysninger om gjennomføring og resultat av dataavlesingen, i tillegg til eventuell overskuddsinformasjon om overtredelse av andre straffbare forhold. Videre skal Riksadvokaten sende innberetningen med eventuelle merknader, til kk-utvalget som foretar en etterfølgende kontroll.

4 Konfrontasjon med overordnede rettsregler

4.1 Innledning

Utgangspunktet er at alle individer har en privatsfære, hvor de kan være seg selv, handle og kommunisere fritt, uten innblanding fra staten eller andre individer. Privatsfæren er et sentralt element i det å være et selvstendig individ og et fritt menneske. Retten til privatliv er derfor et grunnleggende prinsipp i en rettsstat og i demokratiet.[58] I Norge er retten til privatliv en konstitusjonell rettighet som er forankret i Grunnloven § 102. Bestemmelsen lyder som følger:

> **Grunnloven § 102.**
> Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.

Det oppstilles et generelt vern for privatlivets fred i bestemmelsens første ledd første punktum. Retten til privatliv er dermed utformet som en individuell rettighet og det fremgår uttrykkelig av ordlyden at grunnlovsvernet omfatter respekten for privatlivet, familielivet og kommunikasjon. Et generelt vern av privatlivet i Grunnloven § 102 kom ved Grunnlovsrevisjonen i 2014. I tillegg til grunnlovsvernet er retten til privatliv forankret i Den Europeiske Menneskerettighetskonvensjon (EMK) artikkel 8. EMK artikkel 8 lyder som følger:

> **Art. 8. Right to respect for private and family life.**
> 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 his 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.

I tillegg til at EMK artikkel 8 oppstiller et generelt vern av retten til privatliv, familieliv, hjem og kommunikasjon tilsvarende Grl. § 102, oppstilles det et unntak i annet ledd. For at et inngrep skal være i samsvar med EMK må tre kumulative vilkår være oppfylt; inngrepet må

[58] NOU 2009:15 s.50.

ha (1) legitimt formål, (2) klart rettsgrunnlag og (3) være nødvendig i et demokratisk samfunn jfr. EMK artikkel 8 nr. 2.

Det er dermed to overordnede rettsnormer å forholde seg til når dataavlesing skal konfronteres. Mens Grl. § 102 er en rettsregel med grunnlovsrang, er EMK på den annen side inkorporert i norsk lov jfr. menneskerettsloven § 3. Det er derfor nødvendig å klarlegge det nærmere forholdet mellom Grl. § 102 og EMK artikkel 8.

Det fremgår av nyere rettspraksis fra Høyesterett at det er et nært forhold mellom Grl. § 102 og EMK artikkel 8. Avgjørelsen inntatt i Rt. 2014 s.1105 er et prejudikat for at Høyesterett anvender EMK artikkel 8 ved siden av Grl. § 102, og illustrerer dermed at rettsnormene har en nær sammenheng. Videre uttaler førstevoterende i Rt. 2015 s. 93 at *"Jeg legger til grunn at § 102 skal tolkes i lys av de folkerettslige forbildene (...)",* med den begrensning at "*Det er vår forfatning Høyesterett (..) som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettsbestemmelser."*[59] Ved å lese de nevnte avgjørelser i sammenheng, kan vi utlede to implikasjoner av materiell og strukturell karakter.[60]

For det første gir ordlyden "tolkes i lys av" en alminnelig presumsjon for at vi som alminnelig utgangspunkt kan legge til grunn at Grl. § 102 vil gi det samme minstevernet som EMK artikkel 8. Imidlertid følger dette med begrensning presisert av førstevoterende *"(...) det er vår forfatning Høyesterett som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettighetsbestemmelser".* Det er derfor Høyesterett sin oppgave å tolke Grunnloven i siste instans. Dette følger av at EMK ikke er inkorporert i norsk rett med grunnlovs rang, slik at Grunnloven etter omstendighetene *kan* gi et bedre vern. Men det materielle minstevernet vil *i utgangspunktet* være det samme. For det andre kan vi utlede en strukturell implikasjon ved at Høyesterett har adoptert og lagt til grunn systematikken for EMK artikkel 8 når de tolker Grunnloven § 102, herunder krav til at inngrepet har hjemmel i lov, har et legitimt formål og at det er nødvendig i et demokratisk samfunn.

Ettersom nyere praksis fra Høyesterett viser at systematikken og strukturen for EMK artikkel 8 anvendes ved tolkningen av Grl. § 102, har jeg valgt å konfrontere reglene om dataavlesing med utgangspunkt i tilsvarende struktur og systematikk. Den videre konfrontasjon med overordnede rettsregler vil dermed ta utgangspunkt i EMK artikkel 8. Uavhengig av

[59] Rt. 2015 s. 93 avsnitt 57.
[60] Se også Rt-.2015 s.155 avsnitt 40 som følger opp de overnevnte avgjørelser.

grunnlovsvernet er EMK artikkel 8 i tillegg av stor interesse, ettersom Norge har inkorporert konvensjonen med trinnhøyde over formell lov. Det vil derfor på selvstendig grunnlag være hensiktsmessig å undersøke om dataavlesing er i samsvar med EMK. Dette er særlig interessant ettersom EMD ikke har berørt problemstillingen knyttet til dataavlesing tidligere.

I lys av at EMD ikke har tatt stilling til dataavlesing som et straffeprosessuelt tvangsmiddel, har jeg valgt å undersøke avgjørelser fra EMD som gjelder kommunikasjonskontroll ved tolkningen av EMK artikkel 8. Det er nylig kommet avgjørelser som gir klarere føringer enn tidligere praksis, og som er oppklarende på flere punkt. Særlig storkammer dommen *Roman Zakharov mot Russland* og avgjørelsen *R.E mot Storbritannia*, som begge er avsagt i 2015 er av betydning. Da disse avgjørelsene ikke er nevnt i litteraturen, vil analysen hovedsakelig ta utgangspunkt i praksis fra EMD på selvstendig grunnlag.

4.2 Er dataavlesing et "inngrep" i privatlivet?

Det fremgår av EMK artikkel 8 nr. 2 at "*There shall be no interference by a public authority with the exervise of this right (...)"* Det følger av fast konvensjonspraksis at kommunikasjonsavlytting utgjør et inngrep i retten til privatlivet.[61] Ettersom dataavlesing i likhet med kommunikasjonsavlytting er en form for kommunikasjonskontroll, må tilsvarende legges til grunn for dataavlesing.

Videre vil inngrepets karakter være av betydning i relasjon til EMK artikkel 8 nr. 2. EMD uttaler i *Roman Zakharov mot Russland* at:

> "In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees agianst abuse".[62]

EMD legger til grunn at det vil være avgjørende hvorvidt lovgivningen oppstiller prosessuelle garantier ettersom hemmelig overvåkning er et sterkt inngrep og dermed potensielt kan undergrave demokratiet. Inngrepets karakter har således betydning for lovkravet og nødvendighetsvurderingen, da de prosessuelle garantier har betydning i begge vurderinger. Spørsmålet er i hvilken grad dataavlesing er et *sterkt* inngrep i privatlivet.

[61] Se Klass and others v. Germany avsnitt 41 og R.E v. The United Kingdom avsnitt 179.
[62] Roman Zakharov v. Russia avsnitt 232.

Dataavlesing er en form for hemmelig overvåkning hvor offentlig myndighet kan foreta en fullstendig overvåkning av mistenktes tastetrykk, filer, kommunikasjon over internett, samt mulighet for avlytting ved hjelp av mikrofonen og overvåkning gjennom webkameraet.[63] Materialet som kan hentes ut gjennom disse kanalene, kan gi politiet informasjon om både mistenktes tanker, følelser og kommunikasjon med omverdenen. En fullstendig overvåkning av slik informasjon i sanntid, representerer dermed et *sterkt* inngrep i individets rett til privatliv og kommunikasjon etter EMK artikkel 8. At dataavlesing medfører et sterkt inngrep, vil være et moment i den videre vurdering av lovkravet og nødvendighet i relasjon til EMK artikkel 8.

4.3 Krav om at inngrepet har et legitimt formål

Et inngrep i retten til privatlivet må være begrunnet i et legitimt formål for å være rettmessig etter EMK artikkel 8 nr. 2. Det stilles krav om at eventuelle inngrep, er i tråd med et av de opplistede formål;

> ”(…)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.”.[64]

I relasjon til dataavlesing med hjemmel i strpl. § 216 o, er det kriminalitetsbekjempelse som er formålet. Slik jeg belyste i kapittel 3.1.2 setter bestemmelsen opp et kriminalitetskrav for hvilke kriminelle handlinger det må være mistanke om for å kunne anvende dataavlesing. Ved at det er et straffeprosessuelt tvangsmiddel som kan anvendes når det foreligger en viss mistanke mot vedkommende under etterforskningen, er dataavlesing et inngrep som har til formål å frembringe bevis ved mistanke om alvorlige kriminelle handlinger slik at straffeforfølgning kan gjennomføres. Dataavlesing oppfyller dermed et av de nærmere opplistede formål i EMK artikkel 8 nr. 2, herunder ”interests of national security” og ”public safety”. Kravet til legitimt formål er således oppfylt. Formålet med dataavlesing har imidlertid betydning i forholdsmessighetsvurderingen vedrørende om inngrepet er nødvendig i et demokratisk samfunn. Dette kommer jeg nærmere tilbake til i kapittel 4.5.

[63] Se nærmere om dette i punkt 2.2 overfor.
[64] EMK artikkel 8 nr. 2.

4.4 Lovskravet

4.4.1 Hva kreves for at lovskravet er oppfylt etter EMK?

Et lovlig inngrep fra offentlige myndigheter er videre betinget av at det er " *...in accordance with law (...)"* jfr. EMK artikkel 8 nr. 2. Lovkravet er begrunnet i hensynet til rettssikkerhet, som innebærer at enhver skal være beskyttet mot vilkårlige overgrep fra offentlig myndighet og være i stand til å forutberegne sin rettsstilling.[65]

En naturlig språklig forståelse av ordlyden tilsier at inngrepet må være forankret i nasjonal lovgivning. EMD har imidlertid lagt til grunn at både formell lov og ulovfestet rett oppfyller lovkravet.[66] EMD uttaler i *R.E mot Storbritannia* at det avgjørende er hvorvidt tre betingelser er oppfylt:

> "..the impugned measure must have som 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".[67]

Det er dermed ikke et forbud mot å hjemle et inngrep i rettspraksis, såfremt de øvrige betingelser er oppfylt. Ved at både formell og ulovfestet rett betegnes som "nasjonal lovgivning", og det i tillegg stilles krav til lovgivningens tilgjengelighet og forutberegnelighet, kan vi legge til grunn at EMK krever et forutberegnelig rettsgrunnlag. Avgjørende er at den nasjonale lovgivningen som gir hjemmel til inngrepet er tilgjengelig for individet slik at de kan forutberegne sin rettsstilling. Det er således aspektet med forutberegnelighet som er det sentrale ved lovkravet i EMK, og ikke hvorvidt det er formell lov eller ulovfestet rett.

Når det gjelder kravet til tilgjengelighet må det være mulig å skaffe seg kjennskap til lovgivningen som tillater inngrepet. EMD har lagt til grunn at det normalt kreves en kunngjøring eller publisering, slik at interne instrukser som er utilgjengelig for borgerne ikke er tilstrekkelig.[68]

---

[65] NOU 2009:15 s.60.
[66] Sunday times v. The United Kindom avsnitt 47.
[67] R.E v. The United Kingdom avsnitt 120.
[68] Silver and others v. The United Kingdom avsnitt 87- 89.

Når det gjelder kravet til forutberegnelighet, følger det av fast konvensjonspraksis at inngrep som følge av skjult overvåkning står i en særstilling. I en slik kontekst kan ikke kravet til forutberegnelighet forstås slik at individet må være i stand til å forutse når overvåkningen skjer og dermed kunne tilpasse sine handlinger.[69] Et slikt krav ville forringe effekten av inngrepet, ved at individet foretok atferdstilpasninger slik at inngrepet ikke lenger er formålstjenlig. EMD er imidlertid tydelig på at risikoen for vilkårlig maktbruk er betydelig ved skjulte inngrep overfor borgerne, slik at det må stilles strenge krav til reglene som tillater slik metodebruk.[70] Når det gjelder kommunikasjonsavlytting uttalte EMD i storkammer i *Roman Zakharov mot Russland* at kravet til forutberegnelighet innebærer at:

> "The domestic law must be sufficient clear to give citizens an adeqaute indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".[71]

EMD stiller med dette opp et presisjonskrav ved at nasjonal lovgivning må være tilstrekkelig klar og detaljert i forhold til hvilke omstendigheter og tilfeller hvor offentlige myndigheter tar i bruk skjulte overvåkningsmetoder, slik at borgerne kan forutberegne sin rettsstilling. Det understrekes at dette er særlig viktig vedrørende kommunikasjonsavlytting, da teknologien stadig blir mer avansert.[72] Fra dette kan vi utlede at både den tekniske metoden inngrepet gjøres på, samt hvilke omstendigheter den brukes ved, må være tilstrekkelig klar. Dette har stor overføringsverdi til dataavlesing, hvor teknologien er avansert og stadig utvikles. I tillegg er dataavlesing en overvåkningsmetode som åpner for en mer fullstendig overvåkning enn kommunikasjonskontroll, ettersom det ikke kun er kommunikasjonen som kan avlyttes men alt man foretar på datamaskinen *i tillegg* til eventuell kommunikasjon. Slik kan det argumenteres for at dataavlesing går *lenger* enn kommunikasjonsavlytting, slik at risikoen for vilkårlig maktmisbruk er større. Selv om EMD ikke eksplisitt har tatt stilling til forutberegnelighet vedrørende dataavlesing, må det på bakgrunn av overnevnte redegjørelse legges til grunn at de samme prinsippene fastlagt i overnevnte EMD praksis må gjelde tilsvarende.

[69] Se Malone v. The United Kingdom avsnitt 67 og Roman Zakharov v. Russia avsnitt 229.
[70] Malone v. United Kingdom avsnitt 67, se også Roman Zakharov v. Russia avsnitt 229 som følger opp.
[71] Roman Zakharov v. Russia avsnitt 229.
[72] Roman Zakharov v. Russia avsnitt 229.

Videre fremholder EMD 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 (…)”.[73]

Det stilles dermed krav til klarhet vedrørende hvordan myndighetene går frem ved dataavlesing, herunder gjennomføringsmåte og hva avlesingen omfatter av informasjon. Klarhet på dette punkt er derfor viktig for å sikre forutberegnelighet og rettssikkerhet ved inngrep i privatlivet. Når det gjelder hva som kreves for at lovgivningen er tilstrekkelig presis slik at borgerne kan forutberegne sin rettsstilling, har EMD utviklet ”minimum safeguards” som må fremgå av nasjonal lovgivning. I storkammer dommen *Roman Zakharov mot Russland*, uttaler EMD følgende:

> ” In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards (...) the nature of offences which may give rise to an interception order, a definition of the categories of people liable to have their telephones tapped, a limit on the duration of telephone tapping, the procedure to be followed for examining, using and storing data obtained, the precautions to be taken when communicating the data to other parties and the circumstances in which recordings may or must be erased or destroyed.”[74]

I tillegg til klarhet vedrørende materielle krav, stilles det med dette krav til at eksistensen av prosessuelle rettssikkerhetsgarantier i lovgivningen, for å sikre borgerne mot vilkårlig inngrep fra den offentlige myndighet. Lovgivningen må inneholde en maks grense for lengden på overvåkningen, prosedyrer for håndtering av materialet som innhentes samt regler for sletting eller og formidling av materialet til andre. Uttalelsen er fulgt opp i en nyere dom fra EMD, *R.E mot Storbritannia*, hvor EMD la til grunn at den britiske lovgivningen ikke hadde tilstrekkelige regler for registrering, sletting, lagring og utlevering av materiale fra kommunikasjonskontroll.[75] Ettersom avgjørelsen er forholdsvis ny, kan vi utlede at regler vedrørende håndtering av materiale fra kommunikasjonskontroll, er noe EMD tillegger stor betydning i vurderingen av ”the minimum safeguards”.

Videre fremhevet EMD i *R.E mot Storbritannia* at vurderingen av ”minimum safeguards” ligger nært opp til hvorvidt inngrepet er nødvendig i et demokratisk samfunn, og det

[73] Roman Zakharov v. Russia avsnitt 231.
[74] Roman Zakharov v. Russia avsnitt 231.
[75] R.E v. The United Kingdom avsnitt 141.

presiseres at lovkravet og nødvendighetsvurderingen etter omstendighetene kan tas under ett.[76] De prosessuelle rettsikkerhetsgarantiene har derfor betydning i to relasjoner. For det første ved at de må fremgå tilstrekkelig klart i lovgivningen slik at borgerne kan forutberegne sin rettsstilling. For det andre har det betydning i nødvendighetsvurderingen, da det her må vurderes hvorvidt prosessuelle rettssikkerhetsgarantiene er *tilstrekkelige* for å begrense inngrepet til det som er *nødvendig* i et demokratisk samfunn. Om de prosessuelle rettssikkerhetsgarantiene vurderes under lovkravet eller ved nødvendigheten, må avgjøres i den konkrete sak.

Hvorvidt nasjonal lovgivning oppfyller kravet til forutberegnelighet og presisjon i relasjon til dataavlesing, beror på om lovgivningen oppfyller kravene til den personelle, prosessuelle og materielle inngrepskompetansen.[77]

4.4.2 Konfrontasjon – er den norske lovgivningen i samsvar?

Dataavlesing er i norsk rett forankret i straffeprosessloven § 216 o og § 216 p i lovens kapittel 16 d. Straffeprosessloven er en formell lov som er offentlig tilgjengelig for borgerne. Lovgivningen oppfyller således kravet til forankring i nasjonal lovgivning og kravet til tilgjengelighet. Det kan imidlertid påpekes at det norske legalitetsprinsippet som er innbakt i Grl. § 102 jfr. § 113, krever klar og *formell* lov. Grunnloven går dermed lenger enn minstestandarden i EMK som kun stiller krav til et forutberegnelig rettsgrunnlag.

Avgjørende i relasjon til lovskravet, vil være hvorvidt lovgivningen er utformet slik at borgerne kan forutberegne sin rettsstilling.[78] Avgjørende vil være at både inngrepets metode, vilkår samt prosessuelle rettsikkerhetsgarantier er utformet tilstrekkelig presist. Som nevnt i kapittel 4.4.1 vil presisjonskravet i relasjon til dataavlesing rette seg mot den prosessuelle, materielle og personelle inngrepskompetansen i lovgivningen gjennom minimumskriteriene som er oppstilt i EMD praksis.[79]

Etter strpl. § 216 o første ledd kan dataavlesing foretas overfor personer som ”med skjellig grunn mistenkes” for en straffbar handling. Dataavlesing er dermed betinget av at det foreligger sannsynlighetsovervekt for at den *mistenkte* er skyldig i det straffbare forholdet

[76] R.E v. The United Kingdom avsnitt 122.
[77] Roman Zakharov v. Russia avsnitt 231 og R.E v. The United Kingdom avsnitt 131.
[78] Roman Zakharov v. Russia avsnitt 228 og 229.
[79] Jf. overfor i kapittel 4.4.1. Se Roman Zakharov v. Russia avsnitt 231.

som mistanken gjelder. Den straffbare handlingen må videre kunne medføre fengsel i 10 år eller mer eller omfattes av et av de oppregnede straffebudene i bestemmelsen.[80] Strpl. § 216 o gir etter dette en ganske tydelig indikasjon på hvem dataavlesing kan anvendes ovenfor.

EMD har uttalt at den kriminelle handling ikke må fremgå eksplisitt i en oppregning i lovgivningen, men at *"sufficient detail should be provided on the nature of the offences in question"*.[81] Avgjørende er om fremstillingen i lovgivningen totalt sett gir en indikasjon på terskelen for hvilke straffbare handlinger som må begås for at dataavlesing kan anvendes. Det alminnelige strafferammekravet med fengsel i 10 år eller mer i strpl. § 216 o første ledd bokstav a, understreker at terskelen er høy. Videre omfatter oppregningen av straffebud i bokstav b, handlinger som i seg selv er alvorlige og grove men som likevel har en lavere strafferamme. Her omfattes blant annet menneskehandel og oppfordring eller rekrutering til terrorhandlinger. Samlet sett gir både det alminnelige strafferammekravet og de oppregnede straffebudene en klar indikasjon på at dataavlesing kun er anvendelig dersom mistankekravet *skjellig grunn* er oppfylt i relasjon til *en alvorlig straffbar handling*. Det må derfor legges til grunn at lovgivningen er tilstrekkelig klar vedrørende hvilke straffbare handlinger som kan lede til bruk av dataavlesing, og at det er *den mistenkte* som kan bli utsatt for en slik metodebruk. Den norske lovgivningen er således i samsvar med klarhetskravet på dette punkt.

Videre har EMD stilt krav til at lovgivningen presiserer hva inngrepet kan omfatte overfor den mistenkte.[82] Dette er særlig viktig for å sikre at mistenkte kan forutberegne sin rettsstilling. Ordlyden i strpl. § 216 o fjerde ledd gir anvisning på at dataavlesing *kan* omfatte kommunikasjon, elektronisk lagret data og andre opplysninger om bruk av datasystemet eller brukerkontoen. Ordlyden er forholdsvis åpen, slik at det kan være noe uklart hvilken informasjon avlesingen omfatter. Det fremgår imidlertid av forarbeidene, at informasjonen som kan avleses teknisk, kun begrenses av type informasjonssystem og funksjonaliteten til program- eller maskinvaren. Videre vil dataavlesing i prinsippet kunne innebære alt fra lydstrømmer, tastetrykk, videostrømmer til lagrede filer og kommunikasjon.[83] Dette illustrerer hvordan avlesningen kan omfatte *mer enn* kommunikasjon, elektronisk lagret data og andre opplysninger slik ordlyden legger til grunn. Når det gjelder hva som faller inn under overvåkning, er ordlyden svært uklar ettersom det i prinsippet vil være mulig med en

[80] Jf. overfor i kapittel 3.1.2.
[81] Roman Zakharov v. Russia avsnitt 143.
[82] Roman Zakharov avsnitt 230 og 231.
[83] Prop.68 L(2015-2016) s.224.

fullstendig overvåkning i sanntid med svært lite begrensninger. I lys av inngrepets karakter er det betenkelig at ordlyden ikke er mer utførlig.

Når det gjelder departementets vurdering, er det fremhevet at metoden må omfatte tilgang til samme type elektronisk informasjon som politiet ellers har adgang til gjennom kommunikasjonsavlytting, hemmelig ransaking og beslag. I tillegg understreker departementet at dataavlesing innføres for å imøtegå utfordringene som disse tvangsmidlene har som følge av blant annet krypteringer.[84] Dette er i samsvar med "kommunikasjon" og "elektronisk lagret data " slik det fremgår av ordlyden. Forarbeidene presiserer dermed at det er samme type informasjon som ved kommunikasjonsavlytting og hemmelig ransaking det tas sikte på. Ordlyden åpner imidlertid for at "andre opplysninger" kan være omfattet av overvåkningen. Ettersom dataavlesing *kan* innebære alt fra overvåkning av lydstrøm, videostrøm til tastetrykk, ville det vært hensiktsmessig med en tydeligere presisering av hvilke informasjon som kan omfattes som "andre opplysninger".

Videre uttaler EMD 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 (...)"*.[85] Lovgivningen må derfor presisere hvordan politiet gjennomfører dataavlesingen. Ordlyden i strpl. § 216 p gir anvisning på at avlesningen *kan* gjennomføres ved hjelp av tekniske innretninger, dataprogram *eller på annen måte.* Etter ordlyden er det ingen krav om at gjennomføringen *skal* skje slik bestemmelsen anviser, men den *kan* foretas slik. Lovgiver har dermed tillagt offentlig myndighet et betydelig skjønn når det kommer til valg av fremgangsmåte. Det nevnes at avlesningen kan gjennomføres ved hjelp av tekniske innretninger eller dataprogrammer, men samtidig er det åpent for andre løsninger som følge av formuleringen "eller på annen måte". Det er dermed noe uklart hvilke tekniske gjennomføringsmåter avlesningen kan bestå av basert på ordlyden isolert sett.

Ordlyden skal i henhold til forarbeidene forstås slik at politiet skal kunne benytte tekniske hjelpemidler, programvare og kunnskap. Departementet uttaler videre at det kan foretas installasjon av programvare eller fysiske komponenter i datasystemet.[86] Det er således tale om utstyrs- og informasjonsbaserte varianter av dataavlesing, tilsvarende redegjørelsen ovenfor.[87] Gjennom den nærmere presisering i forarbeidene, gis det en indikasjon på hvilke metoder som

[84] Prop. 68 L(2015-2016) s. 264 og 265.
[85] Roman Zakharov v. Russia avsnitt 230.
[86] Prop 68 L (2015-2016) s. 271 og 272.
[87] Jfr. redegjørelsen ovenfor i punkt 2.2.

hovedsakelig kan anvendes ved avlesningen. På den annen side, er det flere av metodene som representerer et vidt spekter av underliggende metoder og utfordringer. Et eksempel er innstallering av programvarer, såkalte *trojanere*,[88] hvor det ikke er redegjort for hvilke type trojanere det er tale om eller hvor politiet får trojaneren fra. Dersom politiet benytter en alminnelig og kommersielt tilgjengelig trojaner, for å utføre dataavlesingen, kan det medføre en fare for misbruk fra tredjepersoner. Tredjepersoner kan for eksempel utnytte sårbarheten i datasystemet som politiet har laget, slik at overvåkningen ikke nødvendigvis er begrenset til den offentlige myndighet. Videre kan det tenkes at tredjepersoner kan manipulere programvaren etter den er installert, og dermed påvirke eventuell informasjon som politiet senere henter ut som bevis. I lys av dette ville det være hensiktsmessig å stille krav til hvilke programvare politiet kan bruke, for eksempel begrenset til nasjonal teknologi og at politiet utvikler den. For ytterligere trygghet, ville regler om at teknologien byttes med jevne mellomrom være hensiktsmessig. I lys av dette finner jeg det betenkelig at departementet ikke fastsetter nærmere begrensninger når det gjelder de nærmere gjennomføringsmåtene for dataavlesingen. Dersom det foreligger en betydelig fare for misbruk, vil det utfordre individets rettssikkerhet.

I forarbeidene fremholder departementet at det ikke er hensiktsmessig eller mulig å beskrive gjennomføringsmåtene i detalj. Begrunnelsen var først og fremst taktiske ved at politiet selv burde utvikle metodene uten at detaljer ble kjent. For det andre var det hensiktsmessig å holde det åpent, som følge av den teknologiske utviklingen som stadig ville generere nye muligheter.[89] Etter dette har lovgiver bevisst valgt å holde lovgivningen åpen når det gjelder hvordan politiet kan gå frem for å foreta dataavlesingen.

At enkelte tekniske detaljer må holdes unntatt fra offentligheten, kan til en viss grad aksepteres for å unngå at de kriminelle kommer politiet i forkjøpet og dermed forringer politiets adgang til datasystemet. På den annen side er det viktig at detaljer om hvordan en så inngripende overvåkning gjennomføres, er allmenn kjent, for å hindre vilkårlig maktmisbruk og ivareta borgernes rettssikkerhet. Videre vil begrunnelsen om at det er nødvendig å bevisst utelate detaljer om gjennomføringsmåtene, være mer legitimt når det gjelder dataavlesing som tvangsmiddel i forebyggende øyemed etter politiloven. Ved slike tilfeller kan det for eksempel være tale om å bruke dataavlesing ved mistanke om et forestående terrorangrep mot

[88] Se overfor om trojanere i kapittel 2.2.
[89] Prop. 68 L (2015-2016) s. 264 og 265.

Norge. Når det gjelder dataavlesing, som et straffeprosessuelt tvangsmiddel, som brukes ved etterforskning av *begåtte* straffbare handlinger som ledd i straffeforfølgning, må det imidlertid kunne forventes at borgerne får en tilstrekkelig klar og detaljert beskrivelse av hva man kan bli utsatt for av inngrep.

Det faktum at departementet la til grunn at det ikke var hensiktsmessig å beskrive metoden i nærmere detalj, ettersom den teknologiske utviklingen stadig ville generere nye metoder for gjennomføring,[90] står i kontrast til hvordan EMD har fremholdt presisjonskravet ved hemmelig overvåkning. I *Roman Zakharov mot Russland,* påpekte EMD at klare og detaljerte regler var *særlig* viktig i relasjon til kommunikasjonsavlytting ettersom teknologien stadig blir mer avansert.[91] Den teknologiske utviklingen må anses å være den samme for kommunikasjonsavlytting så vel som dataavlesing. At lovgiver velger å bruke den teknologiske utviklingen som argument for å rettferdiggjøre at det *ikke* er hensiktsmessig å beskrive gjennomføringsmåtene i detalj, står derfor i motsetning til uttalelsen. Dette er en forholdsvis ny storkammer dom fra EMD, som ble avsagt i desember 2015. Dommen forelå da arbeidet med reglene om dataavlesing pågikk i Norge. Det er således betenkelig at lovgiver tar dette standpunkt.

I lys av det strenge presisjonskrav EMD har lagt til grunn når det gjelder hvordan inngrepet fra den offentlige myndighet skal presiseres, finner jeg det betenkelig at lovgiver bevisst har valgt å holde lovgivningen relativt åpen på dette punkt. Den norske lovgivningens presisjon av hvordan politiet skal skaffe seg tilgang til datasystemet, står dermed i et spenningsforhold til konvensjonens krav om et forutberegnelig rettsgrunnlag. Et interessant spørsmål er hvorvidt det hadde vært mulig for lovgiver å være klarere på dette punkt. Dette vil jeg komme tilbake til i kapittel 5.

Videre stilles det krav til at lovgivningen må angi *"a limit on the duration of telephone tapping".*[92] Det fremgår av Strpl. § 216 o femte ledd at bestemmelsene i §§ 216 d til 216 k gjelder tilsvarende, men med den begrensning at tillatelse ikke kan gis for mer enn to uker av gangen. Ordlyden gir dermed en klar grense for lengden på dataavlesingen. Begrunnelsen for at dataavlesing ilegges en hyppigere prøving enn ved kommunikasjonsavlytting, er i henhold til forarbeidene begrunnet med at dataavlesing etter omstendighetene kan fremstå som et

[90] Prop. 68 L (2015-2016) s. 264.
[91] Roman Zakharov v. Russia avsnitt 229.
[92] Roman Zakharov v. Russia avsnitt 231.

større integritetsinngrep.[93] Lovgivningen gir dermed en indikasjon på tidsrommet dataavlesingen kan besluttes for, og begrunnelsen i forarbeidene understreker at regelen er utførlig vurdert av lovgiver.

Endelig stilles det krav til tilstrekkelige regler og prosedyrer for informasjonshåndtering, herunder regler om hvordan materialet skal lagres, brukes, utleveres og slettes.[94] Spørsmålet er etter dette om den norske lovgivningen er i samsvar på dette punkt.

Strpl. § 216 o femte ledd fastslår at reglene i strpl. §§ 216 d til 216 k gjelder tilsvarende for dataavlesing. Lovgivningen oppstiller dermed et krav om at materiale fra dataavlesing *snarest mulig* skal *tilintetgjøres* dersom det er uten betydning for etterforskningen av det straffbare forhold eller gjelder opplysninger som retten etter reglene i §§ 117 til 120 og 122 ikke kan kreve vedkommendes vitneforklaring om. Ettersom etterforskningen av det straffbare forhold normalt er avsluttet ved tiltale, vil en naturlig språklig forståelse av bestemmelsen tilsi at materialet skal være slettet på dette tidspunkt. Dette står i motsetning til strpl. § 216 i bokstav b som åpner for at materiale fra dataavlesing kan brukes som bevis under iretteføringen. Lovgivningen fremstår således uklar når det gjelder hvilket tidspunkt materialet fra dataavlesing skal være tilintetgjort.

I Rt. 2014 s. 1105, som gjaldt spørsmål om sletting og oppbevaring av materialet fra kommunikasjonskontroll, uttalte Høyesterett at strpl. § 216 g ikke kan tas helt på ordet. Årsaken er at materiale fra kommunikasjonskontroll tidligere ikke kunne brukes som bevis, slik at ordlyden ikke står i sammenheng til en endret rettstilstand.[95] Etter dette må det legges til grunn at bestemmelsene leses i sammenheng, slik at det er gitt hjemmel til en *fortsatt lagring* av materialet såfremt lagringen skjer med sikte på tilfeller strpl. § 216 i omfatter. Slik vil det være hjemmel til en fortsatt lagring av materialet fra dataavlesing, dersom materialet skal brukes som bevis eller utleveres til kk- utvalget.

Videre påpeker Høyesterett, at reglene om sletting i strpl. § 216 g bokstav a, må leses i sammenheng med innsynsretten til forsvarer i strpl. § 264 første ledd. Innsynsretten gir forsvarer adgang til å gjøre seg kjent med det samlede materialet fra kommunikasjonskontrollen.[96] Ettersom innsynsretten til forsvarer inntrer når tiltale tas ut, vil

[93] Prop. 68 L(2015-2016) s.272 og 273.
[94] R.E v. The United Kingdom avsnitt 139 og 141 og Roman Zakharov v. Russia avsnitt 231.
[95] Rt. 2014 s.1105 avsnitt 37.
[96] Rt. 2014 s. 105 avsnitt 37, se også Rt. 2005 s.1137.

sletting av materialet fra dataavlesingen tidligst være mulig etter tiltale er utferdiget. Det er særlig viktig at innsynsretten overholdes og at materialet ikke er slettet før forsvareren har gått gjennom materialet, da dette har betydning for tiltaltes rett til rettferdig rettergang som er fastslått i Grl. § 95 første ledd og EMK artikkel 6 nr.1. Dette ble også påpekt av Høyesterett i den overnevnte avgjørelsen. Samlet illustrerer dette hvordan ordlyden i strpl. § 216 g, isolert ikke gir en presis regel for når materialet fra kommunikasjonskontrollen skal slettes. For å klargjøre når materialet fra dataavlesing skal slettes, må flere lovbestemmelser leses i sammenheng. Lovgivningen fremstår således uklar og utilgjengelig på dette punkt, og står derfor i spenning med kravet til et forutberegnelig rettsgrunnlag etter EMK.

Videre oppstiller lovgivningen ingen *absolutt grense* for hvor lenge materialet kan oppbevares. Den absolutte grense på 3 måneder i kommunikasjonskontrollforskriften § 9 omfatter kun oppbevaring av o*verskuddsinformasjon*. Nødvendig materiale i etterforskningen av den konkrete sak er dermed ikke omfattet. I lys av de utfordringer jeg påpekte overfor, er det tydelig at materialet fra kommunikasjonskontroll kan oppbevares over *lengre tid*. Det er problematisk at uklare regler som er i utakt med rettstilstanden, kan medføre at materiale fra kommunikasjonskontroll oppbevares lenger enn det som er nødvendig.

I arbeidet med metodekontrollutvalgets utredning, la kontrollutvalget for kommunikasjonskontroll frem et notat som påpekte at reglene om sletting av materialet fra kommunikasjonstroll ikke ble praktisert etter sin ordlyd. Kontrollutvalget påpeker at årsaken skyldes et regelverket om sletting og rettstilstanden har kommet i utakt. Det ble dermed påpekt et behov for en oppklaring i reglene om sletting.[97] Ved at det tidligere er påpekt svakheter og uklarheter vedrørende reglene om sletting, ville det være hensiktsmessig å problematisere dette i arbeidet med å innføre dataavlesing som et nytt tvangsmiddel. De overnevnte problemstillinger vedrørende sletting vil ramme dataavlesing tilsvarende. At lovgiver avstår fra å påpeke de nevnte utfordringer, finner jeg betenkelig ettersom presise regler vedrørende informasjonshåndtering er en prosessuell rettssikkerhetsgaranti som har betydning for individets rettsikkerhet.

Når det gjelder hvordan lagringen av materialet fra kommunikasjonskontrollen skal foretas, gir straffeprosessloven ingen veiledning. Kommunikasjonskontrollforskriften oppstiller imidlertid et krav om at materialet skal lagres på en *forsvarlig* og *hensiktsmessig* måte i § 8.

[97] NOU 2009:15 s. 253.

Videre fastslår bestemmelsen i andre ledd at materialet skal lagres etter reglene i beskyttelsesinstruksen. Beskyttelsesinstruksen betegner materialet som "fortrolig" eller "strengt fortrolig", og oppstiller særregler for hvordan slikt materialet skal oppbevares.[98] Departementet har ikke drøftet hvordan det kan sikres at materialet fra dataavlesing lagres på en forsvarlig og hensiktsmessig måte. I lys av at dataavlesing som en ny metode, trolig vil innebære mer omfattende materiale enn vanlig kommunikasjonsavlytting, ville det være hensiktsmessig av departementet å drøfte hvordan det kan sikres at lagring skjer i samsvar med loven.

Endelig understreker EMD i avgjørelsen *R.E mot Storbritannia* viktigheten av at lovgivningen inneholder *"precautions to be taken when communicating the material to other parties.*[99] Strpl. § 216 i oppstiller en lovbestemt taushetsplikt om begjæring om kommunikasjonskontroll og opplysninger som fremkommer ved denne. Utover dette åpner bestemmelsen for at materialet kan brukes som bevis for det straffbare forhold, i avhør og at det kan overlates til kontrollutvalget samt til mistenkte ved underretning jfr. bokstav a-h. Det gis imidlertid ingen "precautions" eller forholdsregler som skal tas i denne sammenheng, utover taushetsplikten. Enkelte forholdsregler og begrensninger vil få anvendelse gjennom de krav som stilles i beskyttelsesinstruksen.[100] Ved videreformidling av materiale fra kommunikasjonskontroll ville det være hensiktsmessig med forholdsregler vedrørende tilbakelevering av materiale og utdeling av opplysninger, for å sikre at materialet hemmeligholdes. Forarbeidene har imidlertid ingen uttalelser om begrensninger knyttet til videreformidling av materialet fra dataavlesing. Den norske lovgivningen er således mangelfull på dette punkt.

I avgjørelsen *R.E mot Storbritannia*, fant EMD den britiske lovgivningen svært mangelfull vedrørende informasjonshåndtering.[101] I motsetning til den britiske lovgivningen, inneholder den norske lovgivningen regler for utlevering, oppbevaring og sletting av opplysninger fra kommunikasjonskontroll, men på enkelte punkt fremstår det noe uklart og utilgjengelig. Det er derfor ikke tilstrekkelig til å fastslå en krenkelse av lovskravet, men det må påpekes at reglene om informasjonshåndtering fra kommunikasjonskontroll er en svakhet i den norske lovgivningen.

---

[98] Forskrift av 17. mars 1972 om instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen) Se § 9 om oppbevaring.
[99] R.E v. The United Kingdom avsnitt 141.
[100] Se reglene i beskyttelsesinstruksen §§ 7-11.
[101] R.E v. The United Kingdom avsnitt 140 og 141.

Videre stilles det krav til effektive og tilstrekkelige kontrollmekanismer. I *Roman Zakharov mot Russland*, formulerte EMD kravet slik*"the Court must be satisfied that there are adequate and effective guarantees against abuse"*.[102] Det avgjørende er at det stilles tilstrekkelig og presise kontrollmekanismer slik at inngrepet begrenses til det som er nødvendig i et demokratisk samfunn. Spørsmålet er om lovgivningen oppstiller tilstrekkelige kontrollmekanismer for dataavlesing.

Slik jeg redegjorte for i kapittel 3.2, skal det for det *første* føres en protokoll med opplysninger om tvangsmiddelbruken jfr. kommunikasjonskontrollforskriften § 7.[103] Dataavlesing slik det er innført i strpl. § 216 o vil gi en betydelig mengde opplysninger, og det vil kreves en nøyaktig registrering av alt materiale som er lastet ned for å sikre notoritet. Det vil dermed bli ressurskrevende for politiet å foreta en slik registrering, og det er en risiko for at deler av materiale ikke vil bli registrert. I lys av dette, kan protokollen være lite egnet til å sikre notoritet og en reell kontroll ved dataavlesing som et *selvstendig* tvangsmiddel.

Videre må det vektlegges at protokollen er tilsvarende det metodekontrollutvalget la frem i 2009, hvor dataavlesing ble foreslått som en gjennomføringsmåte for kommunikasjonsavlytting og hemmelig ransaking. Ved dataavlesing som en gjennomføringsmåte for kommunikasjonsavlytting og hemmelig ransaking, vil informasjonen som avleses være tilsvarende det politiet ville ha tilgang til uten bruk av dataavlesing. Dette skyldes at dataavlesingen, kun gjør informasjonen mer tilgjengelig.[104] Dataavlesing som et selvstendig tvangsmiddel, vil på den annen side generere et større omfang av materiale, ettersom lagret informasjon og informasjon fra overvåkning i sanntid vil være omfattet. Departementet foretok imidlertid ingen tilpasning eller påpekte utfordringer knyttet til at dataavlesing som selvstendig metode er mer vidtgående. I lys av dette er det betenkelig at protokollen ikke er tilpasset dataavlesing slik det er innført. Det kan således problematiseres hvorvidt protokollen tilfredsstiller kravet til "(…) *adequate and effective guarantees against abuse",* slik EMD fremholdt i Roman Zakharov mot Russland.[105]

Videre skal kk-utvalget som nevnt i kapittel 3.2, foreta en etterfølgende kontroll av politiet og påtalemyndighetens behandling av saker om dataavlesing jfr. strpl. § 216 h. Utvalget skal kontrollere at bruken av dataavlesingen er i samsvar med lov og instruks, samt hvorvidt

[102] Roman Zakharov v. Russia avsnitt 232.
[103] Se kapittel 3.2 om hvilke opplysninger som skal inngå i protokollen.
[104] Jf. overfor kapittel 2.1 og 3.2.
[105] Roman Zakharov v. Russia avsnitt 232.

bruken er betryggende og begrenset jfr. kommunikasjonskontrollforskriften § 14. Ved kommunikasjonsavlytting, kan for eksempel lydopptaket spilles av, slik at utvalget får et reelt bilde av kommunikasjonskontrollen som er foretatt. Departementet har imidlertid ikke drøftet hvorvidt en tilsvarende løsning skal gjelde for dataavlesing, da forarbeidene er mangelfull på dette punkt. Ettersom dataavlesing er et nytt tvangsmiddel, er det uklart hvordan kk- utvalget vil gjennomføre kontrollen i praksis. Det er således vanskelig å vurdere hvorvidt utvalget er i stand til å foreta en tilstrekkelig og effektiv kontroll. Basert på lovgivningen isolert sett, virker protokollen å være det eneste utvalget kan foreta kontroll med. I lys av de svakheter som påpekt overfor i relasjon til protokollen, vil det være vanskelig for kk-utvalget å foreta en *reell* kontroll med bruken av dataavlesing.

Samlet sett står den norske lovgivningen i spenning med kravet til et forutberegnelig rettsgrunnlag etter EMK artikkel 8 nr. 2, da det kan påvises svakheter både ved prosessuelle rettssikkerhetsgarantier og kontrollmekanismene som er innført.

4.5 Nødvendighet

4.5.1 Kravet om at inngrepet er ”necessary in a democratic society”

Et rettmessig inngrep i retten til privatliv er videre betinget av å være ”necessary in a democratic society” jfr. EMK artikkel 8 nr. 2. En naturlig språklig forståelse tilsier at inngrepet må fremstå som mer enn ønskelig, men likevel ikke uomgjengelig.[106] Det følger av fast konvensjonspraksis at inngrepet må være begrunnet i ”a pressing social need”, og at det samtidig fremstår ”proportionate to the legitimate aim pursued”.[107] Kravet om at inngrepet er nødvendig i et demokratisk samfunn består derved av to deler. For det første må det påvises et pressende samfunnsbehov for dataavlesing. Videre må behovet være proporsjonalt i forhold til det formål som søkes oppnådd.

Der inngrep begrunnes i nasjonal sikkerhet og kriminalitetsbekjempelse, har EMD tillagt statene en vid skjønnsmargin når det gjelder hvilke metoder som er nødvendige.[108] Skjønnsmarginen innebærer at statene er tillagt et visst spillerom innenfor konvensjonens rammer, ved at EMD tillegger statenes oppfatning betydning og er mer tilbakeholden i sin

[106] Tilsvarende er lagt til grunn i Handyside v. The United Kingdom avsnitt 48 og 49
[107] Olsson v. Sweden avsnitt 67.
[108] Se Klass v. Germany avsnitt 49 og Roman Zakharov v. Russia avsnitt 232.

prøving. Begrunnelsen er at den enkelte stat er nærmere å avgjøre hvilke tiltak som er nødvendige for å bekjempe kriminalitet og beskytte nasjonal sikkerhet.[109]

Det første som må vurderes er om det foreligger et pressende samfunnsbehov for inngrepet. Som følge av statenes skjønnsmargin på dette området, vil EMD være tilbakeholden med å prøve den rene nødvendighet av inngrepet. I stedet vil domstolen etterprøve den nasjonale myndighets begrunnelse. Avgjørende vil være om den nasjonale myndighet har påvist at det foreligger "relevant and sufficient reasons" for inngrepet.[110]

Nyere konvensjonspraksis viser at EMD i større grad foretar en ytre prosessuell kontroll når det gjelder hvorvidt inngrepet er nødvendig, i motsetning til en indre materiell vurdering av om den nasjonale lovgivningen er i samsvar med konvensjonen.[111] Storkammer dommen *Perincek mot Sveits*, som gjaldt EMK artikkel 10, er et eksempel på dette. EMD uttalte:

> "However, in discussing that point it only analysed the conviction's foreseeability and aim: to protect the rights of the Armenians. It said nothing about the conviction's necessity in a democratic society, and did not engage in any discussion of the various factors that bear on that point."[112]

I lys av den manglende vurderingen av inngrepets nødvendighet fra den nasjonale myndighet, går EMD i neste avsnitt over til å vurdere nødvendigheten og konkluderer til slutt med at inngrepet ikke var nødvendig i et demokratisk samfunn.[113] Dissenterende dommer Nussberger sier seg enig med flertallet når det gjelder vurderingen av inngrepets nødvendighet, og presiserer at det er tale om en prosessuell krenkelse av EMK artikkel 10.[114]

Fra dette kan vi utlede at nasjonal lovgiver må vurdere den rene nødvendigheten med å innføre dataavlesing, slik at både hensyn for og mot må drøftes. Dersom dette ikke er gjort av nasjonal lovgiver, vil EMD kunne konkludere med en prosessuell krenkelse av EMK artikkel 8.

Såfremt det kan påvises et pressende samfunnsbehov for inngrepet, er det videre et krav om at inngrepet er proporsjonalt i relasjon til det formål som søkes oppnådd.[115] Denne delen av nødvendighetsvurderingen tar sikte på forsvarligheten av inngrepet, og det sentrale er

[109] Harris m.fl. (2014) s. 14 og 15.
[110] Se Olsson v. Sweden avsnitt 67 og Handyside v. The United Kingdom avsnitt 50.
[111] Se Ausin and others v. The United Kingdom. Se også Rui (2013).
[112] Perincek v. Switzerland avsnitt 278.
[113] Perincek v. Switzerland avsnitt 279 og 280.
[114] Se dissenterende dommer Nussberger sin redegjørelse i Perincek v. Switzerland, på s. 120.
[115] Olsson v. Sweden avsnitt 67, tilsvarende i Sunday Times v. The United Kingdom avsnitt 67.

hvorvidt det etter omstendighetene var nødvendig å gå frem på en så inngripende måte. I dette ligger en forholdsmessighetsvurdering hvor staten må veie nødvendighet og formål mot viktigheten av å ivareta individets vernede rettigheter etter EMK. For det første må inngrepet være egnet til å oppnå formålet. For det andre må ikke formålet ivaretas ved bruk av lempeligere midler.[116] Avgjørende er således at inngrepet ikke går *lenger enn* nødvendig.

EMD har akseptert at lovgivning som tillater overvåkning av mail, post og telekommunikasjon *kan* være nødvendig i et demokratisk samfunn for å beskytte nasjonal sikkerhet og bidra til bekjempelse av kriminalitet, til tross for at det er et stekt inngrep i privatlivet. EMD påpeker at det avgjørende vil være at det er oppstilt tilstrekkelig og effektive garantier mot misbruk.[117] Tilsvarende er fulgt opp i den nyere storkammer dommen Roman *Zakharov mot Russland*, hvor EMD uttaler:

> ” In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effecitve guarantees against abuse (…)”[118]

Storkammer dommen er med dette et eksempel på at EMD holder tilbake i den materielle vurderingen og prøver hvorvidt det foreligger prosessuelle garantier mot misbruk i lovverket som en del av forholdsmessighetsvurderingen. Fra dette kan vi utlede at dersom det er nødvendig å gripe så langt inn i borgernes rett til privatliv, må det foreligge prosessuelle rettssikkerhetsgarantier for at inngrepet skal være proporsjonalt. Avgjørende vil dermed være hvorvidt de prosessuelle rettsikkerhetsgarantiene er i stand til å begrense inngrepet til det som er ”necessary in a democratic society”.

Ifølge EMD, kan gjennomgangen og kontrollen med hemmelig overvåkning deles i tre steg; begjæringen av dataavlesing, gjennomføringen av overvåkningen og prosessen etter overvåkningen er avsluttet. Når det gjelder de første stegene er det avgjørende at det foreligger prosessuelle garantier som ivaretar vedkommende sine rettigheter, ettersom vedkommende ikke vet om overvåkningen, og derved er avskåret fra å utnytte et eventuelt rettsmiddel eller å kunne ta aktivt del i kontrollprosedyren. Når det gjelder det tredje steget,

[116] Aal (2011) s. 142-143.
[117] Se Klass v. Germany avsnitt 48.
[118] Roman Zakharov v. Russia avsnitt 232.

hvor den hemmelige overvåkningen er avsluttet, er det underretning til vedkommende om at overvåkningen har funnet sted samt muligheten til å benytte effektive rettsmidler.[119]

Etter dette henger nødvendighetsvurderingen tett sammen med lovkravet, hvor det som nevnt i kapittel 4.4.1 stilles krav til at prosessuelle rettsikkerhetsgarantier fremgår tilstrekkelig klart av den nasjonale lovgivning slik at borgerne kan forutberegne sin rettsstilling. Dette er også påpekt av EMD, som i tillegg utaler at vurderingene i noen tilfeller tas under ett.[120] En analyse av rettspraksis vedrørende hemmelig overvåkning i relasjon til EMK artikkel 8 nr. 2, tyder på at i tilfeller hvor den nasjonale lovgivning oppstiller prosessuelle rettsikkerhetsgarantier, vil vurderingen være hvorvidt det er tilstrekkelig klart i relasjon til lovkravet. På den annen side, vil det i tilfeller hvor slike garantier uteblir i lovgivningen, kunne være uproporsjonalt i relasjon til nødvendighetskravet at slike garantier mangler. Dette følger av at de prosessuelle rettssikkerhetsgarantier skal begrense inngrepet til det som er nødvendig i et demokratisk samfunn. Slik sett vil de prosessuelle rettsikkerhetsgarantiene være relevante ved to ulike implikasjoner.

4.5.2 Konfrontasjon – er den norske lovgivningen i samsvar?

Dataavlesing er i forarbeidene begrunnet som nødvendig i lys av den teknologiske utviklingen, som har gitt en større bruk av avanserte krypteringer og utvikling av nye elektroniske kommunikasjonstjenester. Departementet peker på at høringsuttalelsene viser en redusert effekt ved de eksisterende skjulte tvangsmidler, og at selv om adgangen til informasjonen rettslig sett er den samme, har informasjonen i praksis blitt mer utilgjengelig.[121] I lys av disse uttalelsene, peker departementet på et behov for nye metoder. Spørsmålet er imidlertid om det er *nødvendig* å innføre en sterkt inngripende overvåkningsmetode overfor borgerne for å avhjelpe politiets utfordringer. Avgjørende vil være hvorvidt lovgiver har påvist "relevant and sufficient reasons" for å innføre dataavlesing.[122]

Departementet peker på en økende bevissthet i samfunnet om informasjonsbeskyttelse og at en rekke elektroniske kommunikasjonsmidler leveres med sterk informasjonsbeskyttelse. Dette utnyttes av kriminelle som ved å benytte tilgjengelige teknologiske løsninger, kan

[119] Roman Zakharov v. Russia avsnitt 233 og 234.
[120] R.E v. United Kingdom avsnitt 122.
[121] Prop. 68 L (2015-2016) s. 260.
[122] Olsson v. Sweden avsnitt 67.

kryptere store deler av kommunikasjon og lagret informasjon. Ettersom det ofte kan være tale om avanserte krypteringsalgoritmer, vil en eventuell dekryptering av politiet kreve betydelige ressurser i form av tid, datakraft og kompetanse. I tillegg er det ikke sikkert at dekryptering lykkes.[123] Dermed kan deler av kommunikasjon og informasjon som politiet overvåker eller beslaglegger fra mistenkte, være ubrukelig. I lys av dette, kan dataavlesing være et nødvendig middel for å imøtegå disse utfordringene, ettersom metoden vil bidra til at politiet kommer seg forbi krypteringene. Slik sett er begrunnelsen relevant og tilstrekkelig for at dataavlesing er nødvendig.

På den annen side er dataavlesing i denne sammenheng begrenset til et tvangsmiddel ved etterforskningen av en begått straffbar handling. Avanserte krypteringer kan vanskeliggjøre innhenting av bevis og gjøre etterforskningen mindre effektiv, men det er viktig å se hen til graden av inngrep en slik overvåkning vil medføre. Når det ikke er tale om avverging eller forebygging av alvorlige straffbare handlinger, men straffeforfølgning av *begåtte* handlinger, kan metodens inngripende karakter tilsi at politiet må akseptere at dette er ressurs- og tidkrevende.

Straffeprosessloven skiller mellom informasjon som er lagret og informasjon som overføres mellom en avsender og en mottaker. Utviklingen innen elektronisk kommunikasjon har gitt nye plattformer for informasjonsdeling som straffeprosesslovens sondring ikke tar høyde for. For eksempel internettbaserte e-post og fildelingstjenester hvor flere personer kan dele tilgang til samme brukerkonto, og dermed lese, opprette og redigere dokumenter uten at informasjonen utveksles mellom brukerne. Departementet påpeker at dette utvilsomt er å betegne som kommunikasjon, men kommunikasjonsavlytting i medhold av straffeprosessloven § 216 a vil gi ikke et fullstendig bilde av informasjonen som utveksles. Dette skyldes at kommunikasjonen blir værende på brukerkontoen, og ikke overføres til en mottaker.[124] Dataavlesing vil imidlertid gi en tilstedeværelse i datasystemet som gir politiet tilgang til brukerkontoen i sanntid. På denne måten vil politiet ha full oversikt over informasjonen som blir værende på brukerkontoen. Dette taler for at departementet har gitt en relevant begrunnelse for at dataavlesing er et nødvendig tvangsmiddel.

Videre vil det etter departementets oppfatning være en mer skånsom overvåkning ved bruk av dataavlesing, enn ved hemmelig ransaking og kommunikasjonsavlytting. Årsaken er at

[123] Prop. 68 L (2015-2016) s. 260.
[124] Prop. 68 L (2015-2016) s. 260.

dataavlesing vil gi mulighet til å foreta en hemmelig ransaking av et datasystem uten fysisk tilstedeværelse, slik at overvåkningen er mindre integritetskrenkende.[125] Motsetningsvis nevner ikke departementet at dataavlesing innebærer en tilstedeværelse i datasystemet *over tid* med mulighet for overvåkning *i sanntid*, og at dette er et sterkt inngrep. Det kan diskuteres hvorvidt en overvåkning av datasystemet i sanntid over tid, er mer eller mindre inngripende enn fysisk ransaking. Det er imidlertid betenkelig at departementet ikke har påpekt at også dataavlesing har en svært integritetskrenkende karakter i denne sammenheng.

Ved å underbygge utfordringene i relasjon til den teknologiske utviklingen og påvise hvordan kommunikasjonsavlytting og hemmelig ransaking ikke alltid strekker til, har departementet påvist at dataavlesing *kan* være et nødvendig inngrep for kriminalitetsbekjempelse. EMD fremhevet imidlertid i storkammer dommen *Perincek mot Sveits*, betydningen av en tilstrekkelig vurdering av nødvendigheten.[126] Proposisjonen er noe mangelfull når det gjelder potensielle utfordringer knyttet til dataavlesing. Jeg vil i det følgende ta for meg noen av disse utfordringene og drøfte hvorvidt disse kan ha betydning for metodens nødvendighet.

For det *første* la Oslo Statsadvokatembeter til grunn i sin høringsuttalelse at "dataavlesing som fremgangsmåte gir en betydelig mengde overskuddsinformasjon".[127] Straffeprosessloven § 216 g skal gjelde tilsvarende for dataavlesing når det gjelder overskuddsinformasjon, slik at materialet som ikke er fremlagt som bevis, skal slettes dersom det er åpenbart uten betydning for saken.[128] Departementet har således tatt stilling til hvilke regler som gjelder vedrørende sletting av materialet. Det er imidlertid ikke drøftet hvordan kontrollsystemene sikrer at overskuddsmaterialet ikke er gjenstand for misbruk. Det er som nevnt protokollføring som er kontrollmekanismen for å sikre notoritet ved dataavlesing.[129] Protokollen har flere svakheter, og det kan problematiseres hvordan protokollen kan sikre at overskuddsmaterialet som har fremkommet under dataavlesingen er slettet i henhold til lovverket og eventuelt hva slags overskuddsmateriale som foreligger til enhver tid. Som påpekt av Oslo Statsadvokatembeter, må politiet i alle tilfeller registrere og dokumentføre materialet som er innhentet, og en nøyaktig registrering av materialet vil være svært ressurskrevende.[130] I lys av dette gir overskuddsinformasjon ved dataavlesing flere utfordringer når det kommer til registrering,

[125] Prop. 68 L (2015-2016) s. 264-265.
[126] Perincek v. Switzerland avsnitt 278 og 279. Se også overfor kapittel 4.5.1.
[127] Prop. 68 L (2015-2016) s. 259.
[128] Prop. 68 L (2015-2016) s. 273.
[129] Jf. overfor i kapittel 4.4.2.
[130] Prop 68 L (2015-2016) s. 259.

oppbevaring og sletting. Jeg finner det derfor betenkelig at dette ikke er drøftet nærmere av departementet.

For det *andre* kan dataavlesing innebære en atferdstilpasning blant de kriminelle slik at metoden kan miste sin effektivitet og egnethet. Ved at de kriminelle er oppmerksom på at politiet kan foreta en skjult overvåkning av datasystemet, kan det skje en omgåelse i miljøer som driver med organisert kriminalitet. De mistenkte kan for eksempel benytte offentlige datamaskiner eller lignende, og på denne måten vil begjæringen om dataavlesing ikke avdekke relevant informasjon som kan brukes som bevis. På samme måte som ved krypteringer, vil en slik omgåelse skape utfordringer for politiet. En slik omgåelse vil føre til at individet er gjenstand for en svært inngripende overvåkning, uten at inngrepet er formålstjenlig. Problemstillingen er ikke nevnt eller vurdert av departementet i forarbeidene.

For det *tredje* eksisterer det en fare for misbruk ved at andre enn politiet kan skaffe seg uberettiget tilgang til datasystemet eller opplysninger som behandles i systemet. Problemstillingen er til en viss grad drøftet i forarbeidene, hvor departementet langt på vei slutter seg til metodekontrollutvalgets utredning som legger til grunn at skaderisikoen er liten og uansett innenfor det akseptable. Etter departementets oppfatning kan faren for misbruk avhjelpes ved at det stilles krav til politiets fremgangsmåte og krav til personellet som skal utføre avlesningen, for å minimere risikoen.[131] Strpl. § 216 p stiller imidlertid krav til personellet som skal utføre avlesingen, men utover dette er det få begrensninger for å avhjelpe risikoen for misbruk fra tredjepersoner. Særlig må det påpekes manglende begrensninger knyttet til trojaneren som kan brukes ved gjennomføringen av dataavlesing. Dersom politiet bruker en kommersielt og allment tilgjengelig trojaner, kan det medføre en økt fare for misbruk fra tredjepersoner.[132]

I lys av dette er det flere utfordringer knyttet til dataavlesing som departementet ikke har tatt høyde for. Dette viser at departementet til en viss grad har forbeholdt seg å fokusere på fordelene ved å innføre dataavlesing og hvorfor dette er nødvendig, uten å drøfte utfordringer og ulemper tilsvarende. Da EMD i storkammer slo ned på en manglende vurdering av nødvendighet i *Perincek mot Sveits* og konkluderte med en prosessuell krenkelse, burde departementet være mer utførlig i sin vurdering. Den norske lovgivningen er dermed

[131] Prop. 68 L (2015-2016) s. 267.
[132] Se mer om dette overfor i kapittel 4.4.2.

mangelfull på dette punkt, og jeg finner det betenkelig at departementet ikke har foretatt en avveining av hensyn både for og mot.

Videre stilles det krav om at inngrepet er proporsjonalt i relasjon til det formål som søkes oppnådd.[133] I dette ligger en forholdsmessighetsvurdering, hvor inngrepet vil være uproporsjonalt dersom formålet kan nås med lempeligere midler. Spørsmålet er om innføringen av dataavlesing i norsk rett er et inngrep som går *lenger enn nødvendig*.

Dataavlesing med hjemmel i strpl. § 216 o, er et tvangsmiddel som kan begjæres på *selvstendig* grunnlag. Dataavlesing er dermed innført i en annen utstrekning enn det metodekontrollutvalget foreslo i 2009. Utvalget foreslo dataavlesing som et substitutt ved å være en gjennomføringsmåte for eksisterende tvangsmidler, ettersom de mente at dataavlesing på selvstendig grunnlag, medførte en for stor integritetskrenkelse i forhold til det anførte behov.[134] Spørsmålet er hvorfor departementet går lenger enn det metodekontrollutvalget foreslo, når dataavlesing som et selvstendig tvangsmiddel åpner for en fortløpende overvåkning i sanntid, og dermed er et sterkere inngrep. Departementet legger til grunn at det ikke var mulig å tallfeste behovet for dataavlesing. Likevel uttaler departementet at behovet for å supplere bestemmelsene om kommunikasjonsavlytting og hemmelig ransaking er *sterkere* i dag enn ved utvalgets utredning.[135] Det presiseres imidlertid ikke *hvorfor* det er et større behov for å innføre en mer inngripende metode. Begrunnelsen for å innføre dataavlesing var i begge tilfeller å gi politiet en metode som var bedre rustet til utfordringene knyttet til den teknologiske utviklingen. Spørsmålet er om det var *nødvendig* å innføre dataavlesing som en selvstendig metode jfr. strpl. § 216 o, eller om det ville være tilstrekkelig med *lempeligere midler*, herunder dataavlesing slik metodekontrollutvalget foreslo.

I følge departementet vil forslaget til metodekontrollutvalget, ikke løse de problemene som høringsinstansene har pekt på.[136] Økokrim uttaler i sin høringsuttalelse at metodekontrollutvalgets forslag er *" (...) en pragmatisk mellomløsning som vil gi tilstrekkelige muligheter til å ivareta Økokrim's behov i dagens situasjon."* [137] Økokrim støtter imidlertid departementet i at dataavlesing burde innføres som en selvstendig metode,

[133] Olsson v. Sweden avsnitt 67, tilsvarende i Sunday Times v. The United Kingdom avsnitt 67.
[134] NOU 2009:15 s.246.
[135] Prop. 68 L (2015-2016) s. 261.
[136] Prop. 68 L (2015-2016) s. 264-265.
[137] Prop. 68 L (2015-2016) s. 251.

men uttalelsen viser at dataavlesing som en gjennomføringsmåte for hemmelig ransaking og kommunikasjonsavlytting kunne vært *tilstrekkelig*. På den annen side påpeker flere høringsinstanser at dataavlesing som selvstendig metode ville være svært effektiv for å få tilgang til informasjon uten hinder av krypteringer.[138]

Forarbeidene viser at dataavlesing vil være effektivt i relasjon til de utfordringer som foreligger med krypteringer og lignende. Det er imidlertid ikke påpekt hvordan metoden vil være mer inngripende og representere en større integritetskrenkelse ved at det er tale om en fortløpende overvåkning i sanntid. Når metodekontrollutvalget fant at metoden var for integritetskrenkende for syv år siden, må det kunne forventes at departementet belyser hvordan dette har endret seg. I lys av dette kan det være grunnlag for at inngrepet går lenger enn det som er nødvendig i et demokratisk samfunn, og derved er i strid med kravet til nødvendighet i EMK artikkel 8 nr. 2. Det må i det minste legges til grunn at det er en betydelig svakhet ved den norske lovgivningen på dette punkt.

4.6 Konklusjon

Dataavlesing oppfyller kravet til et legitimt formål, ettersom kriminalitetsbekjempelse er et av de opplistede formål jfr. EMK artikkel 8 nr. 2. Når det gjelder lovskravet har den norske lovgivningen imidlertid flere svakheter. Det må særlig fremheves at reglene om hvordan materialet fra dataavlesingen skal utleveres, slettes og lagres fremstår uklart og noe utilgjengelig ved at flere bestemmelser må leses i sammenheng. Dette sikrer på ingen måte forutberegnelighet, og er dermed problematisk i relasjon til kravet om et forutberegnelig rettsgrunnlag etter EMK. I lys av det strenge presisjonskravet EMD har lagt til grunn, er det videre betenkelig at lovgivningen bevisst er holdt åpen, vedrørende hvordan politiet skal foreta dataavlesingen. Dette er en svakhet, da metoden medfører et sterkt inngrep i privatlivet og det må kunne forventes at borgerne får en tilstrekkelig klar og detaljert beskrivelse av hva man kan bli utsatt for. I tillegg er det ikke gitt at protokollføring sikrer notoritet, ettersom dataavlesing gir et betydelig omfang av opplysninger som er innhentet i sanntid. Videre er det noe uklart hvordan kk-utvalget er i stand til å foreta en *reell* kontroll med dataavlesingen. Slik jeg forstår lovgivningen på dette punkt, er protokollen eneste verktøy for dette arbeidet. Det er dermed problematisk at departementet ikke har drøftet hvordan det kan sikres at departementet kan foreta *en reell* kontroll. I lys av at EMD har understreket betydningen av

[138] Prop. 68 L (2015-2016) s. 250-252.

tilstrekkelig og effektive kontrollmekanismer, er dette en betydelig svakhet i den norske lovgivningen. Samlet sett er det svakheter knyttet til hvorvidt lovgivningen sikrer et forutberegnelig rettsgrunnlag. Reglene om dataavlesing står dermed i spenning med lovskravet i EMK artikkel 8 nr.2.

Når det gjelder vilkåret om at dataavlesing må være nødvendig i et demokratisk samfunn, har lovgiver påvist relevante og tilstrekkelige grunner for at dataavlesing kan være *nødvendig* som følge av utfordringer knyttet til krypteringer og lignende. Forarbeidene er imidlertid "ensidige" ved at det i stor grad påvises fordelene ved å innføre et slikt inngrep, uten at utfordringene som dataavlesing kan medføre, er drøftet tilstrekkelig. Videre knytter jeg noe tvil til hvorvidt dataavlesing som en *selvstendig* metode går *lenger enn* det som er nødvendig. Dette skyldes forarbeidenes manglende presisering på hvorfor det er nødvendig med et mer vidtgående inngrep enn det metodekontrollutvalget foreslo i 2009. Dersom det ville være tilstrekkelig med dataavlesing slik utvalget la til grunn, vil formålet kunne realiseres med lempeligere midler. Bestemmelsen slik den er innført i dag, vil dermed kunne anses som uforholdsmessig.

Etter en samlet vurdering, velger jeg å legge til grunn at det ikke kan gis en entydig konklusjon. Det er noe usikkert om dataavlesing er i samsvar med de overordnede rettsregler, da problemstillingen ikke har vært vurdert tidligere. Jeg velger derfor å holde konklusjonen åpen, men understreker at den norske lovgivningen står i et spenningsforhold med hvordan EMD har tolket lignende problemstillinger knyttet til EMK artikkel 8, på flere punkter.

5 Avsluttende bemerkninger

Dataavlesing er potensielt godt egnet til å tjene det formål som søkes, men i lys av dets inngripende og kontroversielle karakter, finner jeg det betenkelig at den norske lovgivningen har svakheter når det gjelder forholdet til de overordnede rettsregler.

Uavhengig av om det er konvensjonsbrudd med EMK artikkel 8 nr. 2, må det for *det første* forventes at det rigges et ordentlig system som ivaretar individets rettssikkerhet gjennom tilstrekkelige kontrollmekanismer og prosessuelle garantier. Når det gjelder de svakheter som er påpekt, kan flere avhjelpes ved enkle grep. Lovgiver kan foreta en innstramming når det gjelder skjønnet den offentlige myndighet er tildelt i forbindelse med gjennomføringen av dataavlesing. Dette vil bidra til forutberegnelighet når det gjelder hva borgerne kan bli utsatt for av inngrep. Det ville videre være hensiktsmessig å oppstille nærmere krav til trojanere som brukes i forbindelse med software basert dataavlesing, herunder krav til hvor den er utviklet. Bruk av trojanere som ikke er kommersielt tilgjengelig, vil redusere faren for misbruk fra tredjepersoner. Når det gjelder hvorvidt kk-utvalget kan foreta en *reell kontroll* med bruken av dataavlesing, kan det være hensiktsmessig at dataavlesingen "tas opp" slik at avlesingen politiet foretar kan spilles av. Dette er tilsvarende løsningen for kontroll med kommunikasjonsavlytting. En slik løsning vil i tillegg være hensiktsmessig for en etterfølgende kontroll av forsvarer, på et senere tidspunkt, hvor materialet fra dataavlesing brukes som bevis mot tiltalte. Når det gjelder de påpekte utfordringer knyttet til at regelverket for sletting av materialet fra kommunikasjonskontroll ikke samsvarer med rettstilstanden, er det vedtatt en lovendring. Endringen har per november 2016 ikke trådt i kraft, men det vil trolig være en klargjøring på dette punkt i nær fremtid.[139]

For det *andre,* er det lovgiver sin oppgave å sørge for at inngrepet ikke går lenger enn det som er nødvendig. Etter min mening burde lovgiver revurdere om det ville være tilstrekkelig å innføre dataavlesing som *en gjennomføringsmåte* for kommunikasjonsavlytting og hemmelig ransaking. En slik løsning vil gi tilgang til mindre informasjon enn dataavlesing som *selvstendig* tvangsmiddel slik det er innført, men de utfordringer politiet har vedrørende krypteringer vil i stor grad være løst. I lys av dette kan det revurderes om en fortløpende overvåkning av datasystemet i sanntid, går *lenger enn* det som er nødvendig.

[139] Lovvedtak 105 (2012-2013) om endringer i straffeprosessloven mv. (behandling og beskyttelse av informasjon).

Selv om det ikke konstateres et konstitusjonelt brudd på EMK artikkel 8, må det kunne forventes at Norge som et demokratisk samfunn og en rettstat, har ambisjoner om å være *godt innenfor* de overordnede rettsregler som verner om individets grunnleggende rettigheter. I forhold til dataavlesing, står den norske lovgivningen i et spenningsforhold som *er* problematisk.

6 Kilderegister

Lover:

Grl. (1814)	Lov 17. Mai 1814. Kongerike Norges Grunnlov.
Strpl. (1982)	Lov 22. mai 1982 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven).
Mrl. (1990)	Lov 21.mai 1990 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).
Politl.(1995)	Lov 4. april 1995 om politiet (politiloven)

Forskrifter:

Forskrift	Forskrift 17. mars 1972 om instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen).
Forskrift	Forskrift 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing (kommunikasjonskontrollforskriften).

Forarbeider:

Ot.prp.nr.64. (1998-1999)	Om lov om endringer i straffeprosessloven og straffeloven mv. (etterforskningsmetoder mv.).
NOU 2007:2	Lovtiltak mot datakriminalitet. Delutredning II.
NOU 2009:15	Skjult informasjon- åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.

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

Juridisk litteratur:

Aal (2011) Aal, Jørgen, Rettsstat og menneskerettigheter, 3 utgave, Bergen, 2011.

Aal (2014) Aal, Jørgen, ”Prosessuelle garantier og forholdsmessighet i straffeprosessen”, *Jussens venner*, 2014, side 227-258.

Graver (2003) Graver, Hans Petter, ”Internasjonale konvensjoner som rettskilde”, *lov og rett*, nr. 8, 2013, side 468-489.

Harris m.fl. (2014) Harris, David. Michael O´Boyle, Edward Bates og Carla Buckley, Law of the European Convention on Human Rights, third edition, Oxford 2014.

Haugland m.fl.(2014) Haugland, Geir Sunde og Ingvild Bruce, *skjulte tvangsmidler*, Oslo 2014.

Skoghøy (2002) Skoghøy, Jens Edvin A, ”Norske domstolers lovkontroll i forhold til inkorporerte menneskerettighetskonvensjoner”, *Lov og rett*, nr. 6, 2002, side 337-354.

Sunde (2012) Sunde, Inger Marie, ”Dataavlesing som etterforskningsmetode”, *tidsskrift for retfærd*, årgang 35 nr. 1/136, 2012, side 3-35.

Rui (2013) Rui, Jon Petter, ”The Inerlaken, Izmir and Brighton declaratuins: towards a paradigm shift in the Strasbourg Court´s interpretation of the European Convention of human rights?, *Nordic Journal of Human Rights*, volum 31 (1), 2014, side 28-54.

Øyen (2016) Øyen, Ørnulf, *Straffeprosess,* 1 utgave, Bergen 2016.

Rettsavgjørelser:

Rt. 2004 s. 887

Rt. 2005 s. 1137

Rt. 2006 s. 1398

Rt. 2011 s. 946

Rt. 2012 s. 134

Rt. 2015 s. 93

Rt. 2015 s. 155

Rt. 2014 s. 1105

Internasjonale rettskilder:

Internasjonale konvensjoner

EMK Den Europeiske Menneskerettskonvensjon, vedtatt av Europarådet 4. november 1950.

Avgjørelser fra Den Europeiske Menneskerettighetsdomstolen (EMD):

Sak 5493/72 Handyside v. The United Kingdom, 7.desember 1976.

Sak 2029/71 Klass and others v. Germany, 6. juni 1978.

Sak 6538/74 Sunday Times v. The United Kingdom, 6. november 1980.

Sak 7136/75 Silver and others v. The United Kingdom, 25.mars 1983.

Sak 8691/79 Malone v. The United Kingdom, 2. August 1984.

Sak 10465/83 Olsson v. Sweden, 24. mars 1988.

Sak 39692/09	Austin and others v. The United Kingdom, 15. mars 2012.
Sak 27510/08	Perinçek v. Switzerland, 15. oktober 2015.
Sak 62498/11	R.E v. United Kingdom, 27. oktober 2015.
Sak 47143/06	Roman Zakharov v. Russia, 4. desember 2015.