UiT

NORGES ARKTISKE UNIVERSITET

Det juridiske fakultet

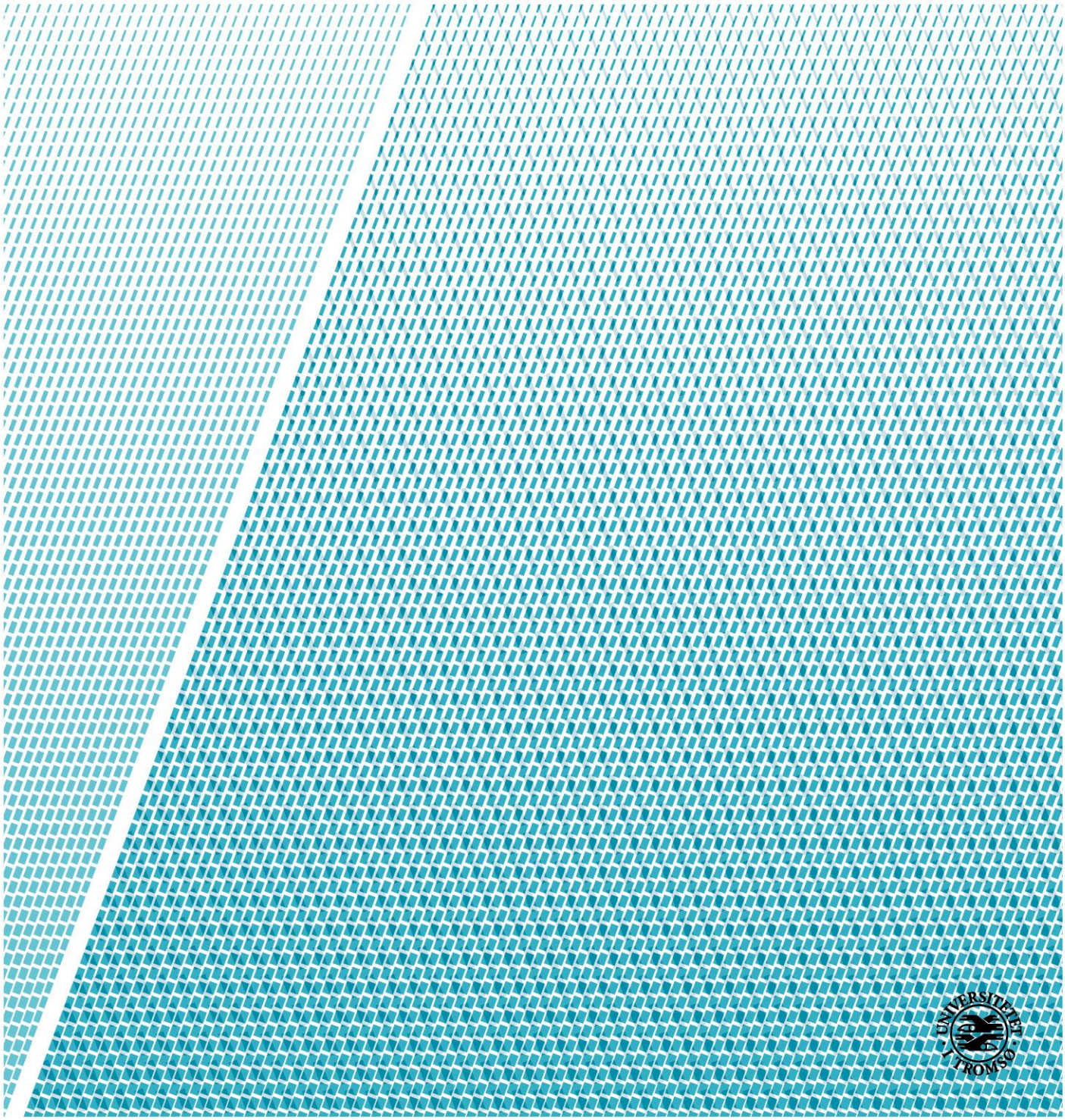
PSTs adgang til å benytte dataavlesing i forebyggende øyemed

En analyse av om dataavlesing i forebyggende øyemed etter politiloven § 17d er i samsvar med retten til privatliv etter Grunnloven § 102.

—

Av Fredrik Hemmingsen

Liten masteroppgave i rettsvitenskap våren 2017



Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

Ved lov 17. juni 2016 nr. 54 ble dataavlesing lovfestet som selvstendig metode i straffeprosessloven og politiloven.[1] *Dataavlesing* er ikke et entydig juridisk eller teknologisk begrep, men kan betegnes som en politimetode hvor politiet ved tekniske midler skaffer seg tilgang til innholdet i et datasystem.[2] Etter lovendringen kan nå Politiets sikkerhetstjeneste (PST) bruke dataavlesing som tvangsmiddel i forebyggende øyemed etter pl. § 17d. Temaet for avhandlingen er om lovfestingen av dataavlesing som selvstendig metode i forebyggende øyemed er i samsvar med retten til privatliv etter Grunnloven § 102.

1.2 Aktualitet

Ved overgangen til det 21. århundre skjøt globalisering og teknologisk utvikling fart ved at man gikk over til et informasjonssamfunn. Økt digitalisering av enkeltpersoners hverdag har medført at både den private og offentlige sfæren i større grad er forflyttet over i det digitale rom,[3] der den enkelte levner enorme mengder digitale spor på sin atferd. I dag produseres, bearbeides, kommuniseres og lagres informasjon ofte elektronisk og ved bruk av mobile tjenester. I tillegg foregår mye av kommunikasjon over internett gjennom moderne kommunikasjonstjenester. Samtidig som denne utviklingen har gitt den enkelte nye muligheter for kommunikasjon og livsutfoldelse har den skapt nye utfordringer og problemstillinger både når det kommer til sikkerhet og personvern.[4]

Et utslag av denne utviklingen er fremveksten av krypteringsløsninger og andre måter for informasjonsbeskyttelse som gjør det i større grad mulig å sørge for at innholdet i kommunikasjonen blir uleselig.[5] Slik informasjonsbeskyttelse er heller ikke forbeholdt aktører med spesiell kunnskap og interesse, men tilbys i dag ofte som «standardløsning» i kommersielle produkter som er tilgjengelig for allmenheten. Den teknologiske utviklingen og

---

[1] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (strpl.) og Lov 4. august 1995 nr. 53 om politiet (pl.).
[2] Prop. 68 L (2015-2016) s. 12 og s. 224, og Sunde (2012) s. 3
[3] Bruk av IKT i husholdningene, 2. kvartal 2016 (https://www.ssb.no/teknologi-og-innovasjon/statistikker/ikthus) - sist besøkt 29. april 2017.
[4] Problematikken knyttet til møtet med 'end-to-end encryption' er også drøftet internasjonalt, se Olsen, Schneier & Zittrain m.fl., *Don't Panic: Making Progress on the "Going Dark" Debate* (2016) (https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf) – sist nedlastet 29. april 2017.
[5] Prop. 68 L (2015-2016) s. 259 flg.

bruken av krypteringsløsninger gjør at politiet i dag oftere står uten faktisk tilgang til informasjon som de rettslig sett har adgang til gjennom de eksisterende tvangsmidlene om kommunikasjonskontroll og hemmelig ransaking.[6] Departementets forslag til lovfesting av dataavlesing var «i hovedsak begrunnet med at det er et stort og udekket behov for effektiv tilgang til elektronisk lagret og kommunisert informasjon».[7] I lys av den teknologiske utviklingen fremstår det som klart at politiet har et behov for metoder som effektivt kan imøtegå de teknologiske utfordringene, og sette politiet i stand til å gjennomføre sine lovpålagte oppgaver. Imidlertid er spørsmålet *hvordan* metoden er innført, og om dette svarer til det anførte behovet.

Lovfestingen av dataavlesing reiser særlige problemstillinger ettersom metoden er svært inngripende i privatlivet til den som rammes. I norsk rett er retten til privatliv konstitusjonelt forankret i Grl. § 102. Avhandlingen vil derfor undersøke om hvorvidt lovfestingen av dataavlesing i forebyggende øyemed er forenelig med retten til privatliv etter Grunnloven § 102.

1.3 Avgrensning

I Norge har man opprettet et tosporet system for politiet ettersom vi følger prinsippet om integrert påtalemyndighet i politiet og prinsippet om uavhengig påtalemyndighet.[8] Det tosporede systemet går ut på at det straffeforfølgende aspektet av politiets kriminalitetsbekjempende virksomhet er underlagt den faglige og instruksjonsmessige ledelsen til riksadvokaten, mens politiets øvrige oppgaver, som ordenstjeneste og forebyggende virksomhet, er underlagt Justisdepartementet. Regelverket i de forskjellige sporene er forskjellig både med hensyn til innhold og formål. Avhandlingen vil følgelig ikke ta for seg bruk av dataavlesing i etterforskningssporet.

1.4 Rettskildebilde og metode

Dataavlesing er et forholdsvis nytt skjult tvangsmiddel, og har i begrenset grad vært behandlet i norsk rettsvitenskap.[9] Kildetilfanget om dataavlesing som metode vil dermed i stor grad bygge på det eksisterende lovforarbeidet med tilhørende litteratur. For øvrig vil avhandlingen suppleres ved det eksisterende rettskildebildet mht. skjulte tvangsmidler, menneskerettigheter,

[6] NOU 2004:6 s. 207-208, NOU 2009:15 s. 241-243 og Prop. 68 L (2015-2016) s. 12
[7] Prop. 68 L (2015-2016) s. 12.
[8] Om forholdet mellom politilovens og straffeprosesslovens virkefelt, se Auglend & Mæland (2016) s. 98 flg.
[9] Se Sunde (2012) s. 3-35 og Bruce & Haugland (2014) s. 253-271

og adgangen til å gjøre inngrep i nevnte rettigheter. Avhandlingen reiser ingen særlige metodespørsmål som må skilles ut til egen behandling ettersom det er alminnelig norsk rettskildelære som kommer til anvendelse. Enkelte metodespørsmål knyttet opp mot forholdet mellom Grunnloven og internasjonale menneskerettighetskonvensjoner, samt konvensjonsrettighetenes betydning for tolkningen av Grunnloven, vil behandles i pkt. 4.1.

1.5 Fremstillingen videre

Først vil «dataavlesing» som fenomen undersøkes nærmere i kapittel 2. Her vil det gis en deskriptiv fremstilling av metodens karakter, herunder foretas en gjennomgang av metodens bakgrunn i norsk rett, de ulike lovforslagene om dataavlesing og endelig hvordan dataavlesing teknisk kan gjennomføres. I kapittel 3 vil det gjøres en rettsdogmatisk analyse av dataavlesing i forebyggende øyemed *de lege lata*. Gjenstand for analyse vil her være den formelle hjemmelsloven for dataavlesing i forebyggende øyemed i pl. § 17d, de materielle inngrepsvilkårene, og de prosessuelle rettssikkerhetsgarantiene og kontrollmekanismene.

I kapittel 4 vil dataavlesing i forebyggende øyemed konfronteres med retten til privatliv etter Grl. § 102. Innledningsvis i delkapittel 4.1 vil grunnrettigheten i Grl. § 102 analyseres der formålet er å gi en deskriptiv fremstilling adgangen til å gjøre inngrep i rettighetsvernet etter Grl. § 102. Under analysen i delkapittel 4.1 vil det være nødvendig å avklare forholdet mellom Grl. § 102 og internasjonale menneskerettighetskonvensjoner Norge er bundet av. Avhandlingen vil på dette punktet begrense seg til forholdet mellom Grunnloven og EMK. Videre i delkapittel 4.2 og 4.3 vil avhandlingen drøfte hvorvidt det innførte tvangsmiddelet dataavlesing i forebyggende øyemed etter pl. § 17d er i samsvar med retten til privatliv etter Grl. § 102. Her vil det være hensiktsmessig å drøfte bestemmelsen opp mot henholdsvis Grl. § 102 første ledd første og annet punktum. Avslutningsvis i kapittel 5 vil funnene som er gjort i avhandlingens foregående kapitler oppsummeres.

2 Hva er «dataavlesing»?

2.1 Bakgrunn for «dataavlesing» i norsk rett

Spørsmålet om å innføre dataavlesing som politimetode i norsk rett har vært omtalt av flere lovutvalg siden starten av 2000-tallet.[10]

[10] Bruce & Haugland (2014) s. 253.

Lund-utvalget tok opp problemstillingen, men viste til at det var mer naturlig å overlate spørsmålet til Datakrimutvalget, som var sammensatt til å ta stilling til de kompliserte, tekniske spørsmålene som metoden reiser.[11] I *Politimetodeutvalget* foreslo flertallet i utvalget å lovfeste dataavlesing som en ny selvstendig forebyggende politimetode, på linje med andre tvangsmidler.[12] Høringen av Politimetodeutvalgets forslag ga, etter departementets oppfatning, et inntrykk av at metoden burde vurderes nærmere, og sa seg enig i at spørsmålet burde behandles av Datakrimutvalget.[13] Imidlertid var Datakrimutvalget av den oppfatning at det måtte utredes nærmere hva metoden bestod i.[14]

Spørsmålet ble deretter inntatt i Metodekontrollutvalgets mandat, der utvalget blant annet ble bedt om «å utrede og foreslå regler som tillater at politiet tar i bruk dataavlesing som metode i etterforskningen».[15]

2.2 De ulike forslagene til lovfesting av dataavlesing

2.2.1 Metodekontrollutvalgets lovforslag

Metodekontrollutvalget presiserte at «dataavlesing» ikke var et entydig juridisk eller teknologisk begrep, men la til grunn at dataavlesing kunne innebære å «skaffe seg tilgang til opplysninger i et elektronisk datasystem ved hjelp av dataprogrammer eller på annen måte».[16] Utvalget viste til at begrepet («dataavlesing») refererte seg dermed til en fremgangsmåte, og ikke nødvendigvis til en selvstendig etterforskningsmetode. I hvilken grad politiet ville kunne benytte seg av dataavlesing ville avhenge av hvilke omstendigheter lovgiver åpnet opp for bruken. I utredningen er det presisert at utvalget var særlig opptatt av «å kartlegge behovet for metoden og dens antatte effektivitet».[17]

Dataavlesing kunne enten innføres som en ny selvstendig metode slik som Politimetodeutvalget hadde foreslått,[18] og som var løsningen valgt i Danmark og foreslått i Sverige. Å innføre dataavlesing som selvstendig metode ville gitt tilgang til informasjon som politiet kunne fått tilgang til ved bruk av eksisterende metoder, og til informasjon som politiet

---

[11] NOU 2003:18 Rikets sikkerhet s. 126-127.
[12] NOU 2004:6 Mellom effektivitet og personvern s. 207-208 og s. 250-251.
[13] Ot.prp.nr.60 (2004-2005) s. 141.
[14] NOU 2007:2 s. 47
[15] NOU 2009:15 s. 17-18. Mandatet ble forstått slik at utvalget også skulle ta stilling til dataavlesing i forebyggende øyemed.
[16] NOU 2009:15 s. 237.
[17] NOU 2009:15 s. 236.
[18] NOU 2004:6 s. 250-251.

etter gjeldende rett ikke har mulighet til å innhente, altså den løpende informasjonen om den bruken av informasjonssystemet som ikke kommuniseres eller lagres i datasystemet.[19] Alternativt kunne dataavlesing målrettes slik at politiet kunne benytte seg av dataavlesing som fremgangsmåte som politiet allerede hadde tilgang til, men på en måte som ikke hindres av tekniske beskyttelsesinnretninger som kryptering. En slik tilnærming ville innebære en videreføring av den mulighet allerede eksisterende metoder gir til å fremskaffe informasjon, f. eks. gjennom kommunikasjonsavlytting.

Metodekontrollutvalget viste til at den teknologiske utviklingen hadde gjort det mulig å sørge for at informasjon ikke lengre var forståelig eller leselig innen politiet fikk tilgang til den.[20] Utvalget viste videre til at tendensen gikk mot økt kryptering. Dette skyldtes blant annet økt bevissthet rundt kryptering, enkle og billige krypteringsløsninger som var allment tilgjengelig, samt at kryptering ofte inngikk som «standardløsninger». Gjennom kryptering hadde politiets eksisterende metoder mistet mye av dets effektivitet, både når det kom til å fange opp kommunikasjon og beslag av lagret data gjennom de eksisterende hjemlene om kommunikasjonsavlytting og hemmelig ransaking og beslag.

Utvalget var av den oppfatning at innføring av nye tvangsmidler, eller utvidelse av eksisterende tvangsmidler, måtte bygge på solid dokumentasjon av behovet, og understrekte at det kreves tungtveiende grunner for å innføre nye metoder eller gjennomføringsmåter.[21] Utvalget fant det ikke tilstrekkelig bevist at et slikt behov forelå, men at det likevel var «gode grunner for at dataavlesing burde innføres som en nødvendig teknologisk tilpassing for å kunne opprettholde effektiviteten av enkelte allerede eksisterende metoder».[22] Utvalget foreslo å innføre dataavlesing som ledd i gjennomføring av kommunikasjonskontroll etter strpl. § 216a og i forbindelse med hemmelig ransaking og beslag etter strpl. § 200a, slik at politiet settes i stand til å sikre informasjon som er kryptert eller på annen måte gjort utilgjengelig.[23]

Dataavlesing for å muliggjøre kommunikasjonsavlytting etter strpl. § 216a måtte etter utvalgets oppfatning begrense seg til ikke å fremskaffe andre opplysninger enn dem som

[19] NOU 2009:15 s. 237. Se også Bruce & Haugland (2014) s. 255-256.
[20] NOU 2009:15 s. 240 flg.
[21] NOU 2009:15 s. 240-244.
[22] NOU 2009:15 s. 244.
[23] NOU 2009:15 s. 237 og s. 244-247.

relaterer seg til vanskeliggjøringen av kommunikasjonsavlytting. Det var heller ikke adgang til å manipulere datasystemet til å fange opp annen informasjon enn den mistenkte sendte eller mottok i kommunikasjonen, f. eks ved å skru på kamera, mikrofon eller lignende i tilknytning til datasystemet. Også informasjon som var lagret i datasystemet falt utenfor, inkludert opplysninger fra tidligere kommunikasjon eller lignende.

Dataavlesing som gjennomføringsmåte for hemmelig ransaking og beslag, jfr. strpl. § 200a, ville gi adgang til *lagret* informasjon på mistenktes datasystem. Utvalget mente det både var hensiktsmessig og mindre integritetskrenkende å tillate hemmelig ransaking og beslag uten politiets fysiske tilstedeværelse, som gjerne krevde at politiet tok seg inn i mistenktes private bolig. Utvalget mente imidlertid at det ikke var grunn til å foreslå adgang til fortsatt eller gjentatt ransaking. Det ble vist til at det ville gitt politiet anledning til å kartlegge mistenktes bruk av et datasystem over tid, noe som etter utvalgets syn ville innebære en for stor integritetskrenkelse i forhold til det anførte behovet. En slik adgang ville i praksis innebære at dataavlesing ble innført som en selvstendig metode ved at en kunne kontinuerlig overvåke et datasystem og på den måte registrere enhver endring som brukeren gjør. Utvalget viste til at det ikke var i veien for at politiet kunne begjøre flere hemmelige ransakinger i løpet av en periode, slik at det ville være opp til retten å avgjøre når en ny ransaking innebar et uforholdsmessig inngrep.

Det man kan utlede fra Metodekontrollutvalgets forslag, og som utvalget uttrykkelig presiserer, er at de *ikke* foreslår å innføre dataavlesing som metode «med det formål å gi politiet mulighet til fortløpende å overvåke all aktivitet i et datasystem».[24] Innføring av dataavlesing som selvstendig metode ville innebære nettopp dette.

2.2.2 Departementets lovforslag

I Prop. 68 L (2015-206) ble det foreslått en rekke lovendringer for å gi politiet utvidet adgang til å benytte seg av skjulte tvangsmidler, inkludert ved å lovfeste dataavlesing. I motsetning til lovforslaget som ble fremmet av Metodekontrollutvalget, foreslo departementet å innføre dataavlesing som et selvstendig tvangsmiddel.[25] Som grunnleggende forutsetninger for departementets vurderinger ble det vist til at politiets adgang til skjult tvangsmiddelbruk ikke skulle være videre enn nødvendig for å møte behovet for effektiv kriminalitetsbekjempelse,

[24] NOU 2009:15 s. 26-27 og s. 237.
[25] Prop. 68 L (2015-2016) s. 264 flg.

samt at det var avgjørende at eventuelle utvidelser ble innrettet slik at den enkeltes krav på materiell og prosessuell rettssikkerhet ble ivaretatt.[26]

Departementet fremhevet at utvalgets forslag ikke synes å ta høyde for utfordringene politiet hadde med hensyn til effektiv avlytting av kommunikasjon etter de gjeldende metoder.[27] Det ble vist til at både Metodekontrollutvalget og flere av høringsinstansene hadde pekt på den teknologiske utviklingen i samfunnet. Etter departementets vurdering viste utredningen og høringen at de eksisterende metodene hadde tapt mye av sin effektivitet. Videre ble det vist til at det i større utstrekning brukes kommunikasjonstjenester som ikke er bundet til et bestemt kommunikasjonsanlegg eller nettverksforbindelse, men til en virtuell brukerkonto knyttet til innehaveren. Departementet hadde, i likhet med Metodekontrollutvalget, ikke klart «å tallfeste behovet for dataavlesing», men mente at utredningen og høringen viste at det forelå et klart behov.[28] Dette behovet var etter departementets oppfatning større per 2016 enn da Metodekontrollutvalget presenterte sin utredning i 2009.

Det tilspissede behovet kunne etter departementets oppfatning dekkes ved å innføre dataavlesing som selvstendig metode. Departementets forslag gir politiet muligheten til å skaffe seg tilgang til opplysningene i et datasystem, herunder opplysninger om bruken av datasystemet over tid.[29] Forslaget gir dermed politiet anledning til fortløpende å overvåke bruken av datasystemet i sanntid. Forslaget står i klar motsetning til den forutsetningen som Metodekontrollutvalget hadde om at dataavlesing ikke skulle innføres med det formål å gi politiet mulighet til å fortløpende overvåke bruken av et datasystem, jfr. tidl. redegjørelse. Departementet mente at en slik fortløpende overvåking av bruken av datasystemet var nødvendig for å kunne møte utfordringene knyttet til kryptering og moderne kommunikasjonstjenester på en effektiv måte. I motsetning til Metodekontrollutvalget var departementet av den oppfatningen at en slik overvåking *ikke* vil innebære en større integritetskrenkelse enn tradisjonell kommunikasjonskontroll allerede utgjør.[30] Den risikoen som fortløpende overvåking medførte for å gi et visst rom for innsyn i personlige

[26] Prop. 68 L (2015-2016) s. 258-259.
[27] Prop. 68 L (2015-2016) s. 264, jfr. 259-264
[28] Prop. 68 L (2015-2016) s. 261, cfr. NOU 2009:15 s. 240 flg.
[29] Prop. 68 L (2015-2016) s. 264-265
[30] Prop. 68 L (2015-2016) s. 265-266.

betraktninger eller liknende, og virke vesentlig integritetskrenkende, kunne etter departementets syn ikke veie tyngre enn de viktige samfunnsinteressene som søktes vernet.

Dette illustrerer at de to lovforslagene ikke bare hadde et grunnleggende ulikt syn på metoden, men også på selve *vurderingen* av metoden. Lovforslagene viser at departementet vurderer både behovet og nødvendigheten av metoden annerledes enn Metodekontrollutvalget. Lovforslagenes anførte behov og vurdering av nødvendigheten av å innføre dataavlesing vil således være viktige momenter for den videre drøftelsen.

Dataavlesing ble innført som selvstendig metode ved lov 17. juni 2016 nr. 54, i all hovedsak i samsvar med departementets lovforslag.[31]

2.2.3 Nærmere om den tekniske gjennomføringen av dataavlesing

Som antydet i de overnevnte lovutvalgene er ikke «dataavlesing» et entydig juridisk begrep, og betegner heller ikke noe klart avgrenset teknologisk fremgangsmåte.[32] Det kan derfor fremstå som uklart hva metodens karakter i realiteten innebærer. På bakgrunn av dette er det nødvendig å undersøke nærmere hva «dataavlesing» er, og hvordan metoden teknisk kan gjennomføres av politiet. Videre vil metodens karakter og inngrepets art være av betydning ved konfrontasjonen med Grl. § 102 senere i avhandlingen.

Ordet «dataavlesing» er sammensatt av ordet «data» og «avlesing». Begrepet «data» (lat. *datum* 'noe som er gitt') er et mangfoldig begrep, men i forbindelse med databehandling referer det seg til enhver faktisk representasjon av opplysninger, viten, meninger etc. i motsetning til innholdet, som kalles informasjon.[33] Dataavlesing kan således være en «avlesing» av enhver form for opplysning, viten, mening osv. uavhengig av innholdet.

Helt generelt kan dataavlesing defineres som en fremgangsmåte som gir tilgang til opplysninger i et *datasystem*[34] ved hjelp av dataprogrammer eller andre teknologiske hjelpemidler.[35] Departementet har lagt til grunn at termen «datasystem» passer godt til det

---

[31] Komiteen viste til at departementets lovforslag hadde satt terskelen for lavt for enkelte forbrytelser der dataavlesing kunne benyttes, b.la. simpel narkotikaovertredelse, simpelt narkotikaheleri og uaktsom narkotikaheleri, se Innst. 343 L (2015-2016) s. 6-11.
[32] Prop. 68 L (2015-2016) s. 224.
[33] https://snl.no/data - definisjon av «data», sist besøkt 13. mars 2017.
[34] Til sammenligning benytter den danske bestemmelsen om 'dataaflæsning' i retsplejeloven § 791 b betegnelsen 'informasjonssystem', og det var også den samme betegnelse som ble bruk av Politimetodeutvalget og i mandatet til Metodekontrollutvalget, se henholdsvis NOU 2004:6 s. 233 forslaget til § 8-1 nr. 9 og NOU 2009:15 s. 17-18.
[35]Prop. 68 L (2015-2016) s. 224 og 269-270 og NOU 2009:15 s. 237, se også Bruce & Haugland (2014) s. 254.

tilsiktede virkeområdet for dataavlesing, og blant annet vil omfatte smarttelefoner, datamaskiner, og andre anlegg for elektronisk kommunikasjon som foretar behandling av data ved hjelp av dataprogrammer. Departementet påpeker at også innretninger som ikke brukes til kommunikasjon omfattes. Ved at departementets forslag åpnet for dataavlesing av «datasystemer eller *brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester*» fanget man også opp virtuelle brukerkontoer som ikke var bundet til et bestemt datasystem eller ulike enheter.[36]

Selve gjennomføringen av dataavlesing kan inndeles i ulike faser.[37] Først en innledende fase der det teknologiske virkemiddelet som skal forestå avlesingen installeres eller monteres. Deretter en avlesingsfase, hvor datasystemet avleses og tilgjengeliggjøres for politiet. Til slutt en avslutningsfase der avlesningsmiddelet avinstalleres eller fjernes. For den videre fremstillingen vil jeg først presentere hvordan politiet kan få tilgang til datasystemet for å foreta avlesingen. Deretter vil jeg behandle hvilke opplysninger som kan avleses.

Verken Metodekontrollutvalget eller departementet mente det var mulig eller hensiktsmessig å gi en uttømmende beskrivelse på hvordan dataavlesing kunne gjennomføres.[38] Det ble vist til at de tekniske alternativene var mangfoldig og ulikartet, og dessuten ville utvikle seg i takt med den teknologiske utviklingen. Videre måtte politiet ut fra en taktisk og teknologiske vurdering kunne avgjøre hvilken gjennomføringsmåte som var mest hensiktsmessig i det enkelte tilfellet. Det kan problematiseres om lovgivers begrunnelse på dette punktet kan forsvares opp mot kravet om at inngrepet må ha tilstrekkelig presis lovhjemmel og være forholdsmessig.

En sammenfatning av lovens forarbeider og juridisk teori gir uttrykk for tre ulike gjennomføringsmåter for dataavlesing.[39] Det kan skilles mellom utstyrsbasert og informasjonsbasert dataavlesing, og en mellomform.[40]

En *utstyrsbasert* dataavlesing går ut på at man fanger opp eller avleser data fra et datasystem ved hjelp av tekniske hjelpemidler eller programvare. Innhentingen av informasjon gjennom

---

[36] Se strpl. § 216o fjerde ledd.
[37] NOU 2009:15 s. 247.
[38] NOU 2009:15 s. 248-249 og Prop. 68 L (2015-2016) s. 271, jfr. også s. 264 flg.
[39] NOU 2009: 15 s. 247 flg. og Prop. 68 L (2015-2016) s. 247-248 og 261 flg. Se også Bruce & Haugland (2014) s. 254-256, samt Sunde (2012) s. 14 flg.
[40] Betegnelsene på de ulike fremgangsmåten er ikke rettslige, men bidrar til en systematisk og pedagogisk fremstilling, jfr. Sunde (2012) s. 14.

dataavlesing kan gjennomføres ved ulike former for signaletterretning,[41] eller ved installasjon av *maskinvare* (hardware) eller *programvare* (software) på eller i et datasystem.[42]

Med en *softwarebasert løsning* kan installasjon av programvaren skje ved å modifisere filer som datasystemets bruker laster ned, eller ved å sende programvare som vedlegg (eller skjult vedlegg) til brukeren, og få vedkommende til å åpne vedlegget. Videre kan installasjon skje ved fysisk eller elektronisk innbrudd. Programmet kan kopiere og sende data til politiet, og vil, avhengig av programmering, forholde seg til et logisk avgrenset område i datasystemet.[43] På teknisk fagspråk kalles en slik programvare for «trojaner», eller «politiprogram/polititrojaner» for å markere at det er et verktøy som anvendes av politiet.[44] Når trojaneren infiserer datasystemet, åpner den for tilgang til systemet gjennom en såkalt «bakdør».[45] Politiet benytter deretter denne bakdøren ved at trojaneren kopierer og sender data tilbake til politiet.

Med en *hardwarebasert løsning* installeres komponenter i informasjonssystemet som gjør politiet i stand til å skaffe seg tilgang til informasjonen, f. eks ved plassering av utstyr på tastatur, mikrofon, USB-port el. Plassering av maskinvare krever, i motsetning til programvare, fysisk tilgang til datasystemet, og vil avgrense seg til det enkelte datasystemet. Funksjonaliteten til komponenten som installeres vil kunne variere etter omfang.[46] På den ene siden kan komponenten avlese og kopiere lagrede data og tappe trafikk ut/inn av datasystemet, altså fungere som en 'kopieringsinnretning'. På den andre siden kan funksjonaliteten begrenses til å fange opp særlig angitt data, f. eks tastetrykk på et tastatur (keylogger). På denne måten vil politiet kunne få tilgang til f. eks passord eller krypteringsnøkler som skrives inn, i tillegg til andre inntastinger som brukeren eventuelt måtte foreta.

---

[41] «SIGINT» - innhenting av informasjon manuelt, analogt og digitalt, eller fra elektroniske kilder, se Auglend & Mæland (2016) s. 382-383. Teknologi og kompetanse for bearbeidelse av signaletterretning er i stor grad utviklet for militære formål, og er i liten grad tilgjengeliggjort for politiet, se Sunde (2012) s. 14. Nærmere om norsk militær signaletterretning, se Riste & Moland (1997) kpt. 6-11 s. 129-270.
[42] Prop. 68 L (2015-2016) s. 224 og NOU 2009:15 s. 247 flg.
[43] Sunde (2012) s. 15.
[44] NOU 2007:2 s. 24 og Sunde (2012) s. 15-16.
[45] NOU 2007:2 s. 24 og Sunde (2012) s. 19.
[46] Sunde (2012) s. 15.

For å få tilgang til data som avleses må programvaren enten lagre den, eller sende den via internett eller annet tilknyttet nettverks- eller radioutstyr.[47] Dersom de avleste dataene lagres må politiet hente dem ut av datasystemet med fysisk tilstedeværelse (ransaking og beslag), mens dersom dataen sendes så kan politiet hente dem ut f. eks via en bakdør i programvaren via internett, eller ved et nytt innbrudd i datasystemet. Når dataavlesingen avsluttes må maskinvaren eller programvaren som muliggjør dataavlesing fjernes.[48] For den maskinvarebasert avlesing må politiet fysisk fjerne komponenten fra datasystemet. Avinstallering av programvare kan skje på samme måte som installeringen, eller ved at programmet tilintetgjør seg selv på kommando eller etter en forhåndsprogrammert tidsfrist.[49]

Ved *informasjonsbasert* dataavlesing skaffer politiet seg adgang til datasystemet gjennom utnyttelse av brukernavn og passord (tilgangsdata) og teknisk «know-how»/kompetanse, altså uten bruk av teknisk utstyr (annet enn tilgang til datasystem).[50] Politiet får f. eks tilgang til datasystemet gjennom ordinær påloggingsprosedyre, annet enn at politiet ikke er rett innehaver av tilgangsdataene. Videre kan politiet få tilgang til datasystemet ved å utnytte teknisk know-how om sårbarheter i programvaren til å trenge seg inn via en «bakdør».

Til slutt er det tenkelig med visse *mellomformer* mellom utstyrs- og informasjonsbaserte fremgangsmåter for dataavlesing.[51] Her utnytter politiet sårbarheter som er forårsaket av andre enn politiet selv. For eksempel kan politiet utnytte sin kompetanse til å trenge seg inn i datasystemet via en sårbarhet i programutrustningen, for så å installere en polititrojaner. Her vil fremgangsmåten være kombinert informasjons- og utstyrsbasert. Et annet eksempel er at politiet utnytter seg av skadelig programvare som er plassert i datasystemet av noen andre. Dersom politiet benytter seg av teknisk kunnskap for å bruke den fremmede trojaneren for å få tilgang til datasystemet så vil fremgangsmåten være kombinert informasjons- og utstyrsbasert.

Den vedtatte bestemmelsen i strpl. § 216p angir rammene for hvordan politiet kan gå frem ved gjennomføringen av dataavlesing etter strpl. § 216o. Det følger av § 216p første ledd annet til femte punktum at:

---

[47] Prop. 68 L (2015-2016) s. 224 og Bruce & Haugland (2014) s. 255.
[48] Se note 46.
[49] Bruce & Haugland (2014) s. 255.
[50] NOU 2007:2 s. 22-23, jfr. også Sunde (2012) s. 16.
[51] Sunde (2012) s. 16-17.

> «Avlesingen kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. § 199a 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.»

Ordlyden «tekniske innretninger» og «dataprogram» synes å ta særlig sikte på utstyrsbasert dataavlesing, herunder bruk av software- og hardwarebaserte løsninger.[52] Imidlertid åpner betegnelsen «eller på annen måte» for at også andre løsninger kan være aktuelle.[53] Det kan være problematisk opp mot kravet om lovhjemmel at lovgiver har valgt en løsning der gjennomføringsmåten, og dermed også metodens karakter, vil kunne utvikle seg i tråd med den teknologiske utviklingen.[54]

Med hensyn til hvilken type informasjon som kan avleses, følger begrensningene teknisk sett bare av hva slags informasjonssystem det dreier seg om og funksjonaliteten til program- eller maskinvaren som benyttes.[55] Dataavlesing kan i prinsippet innebære avlesing av blant annet; sending av lyd- og/eller bildestrømmen fra en tilknyttet mikrofon, høyttaler eller kamera til operasjonssystemets drivere, tastetrykk fra et tastatur til operasjonssystemets drivere, innholdet på harddisk eller annet lagringsmedium, data i fysisk og virtuelle minneområder, data som hentes inn fra eller sendes ut på internett eller andre nettverk osv.

I sin videste forstand vil dataavlesing innebære at politiet får tilgang til alle opplysninger som, i perioden avlesingen foregår, er lagret i eller passerer gjennom det aktuelle datasystem. Det vil med andre ord være snakk om en vedvarende overvåking i sanntid av enhver bruk av det aktuelle datasystemet. Dataavlesing kan også fange opp opplysninger i datasystemet som verken lagres eller kommuniseres.[56] Denne informasjonen kan ikke fanges opp ved bruk av andre av dagens tvangsmidler. Det kan for det første være snakk om inntastinger, tekst eller

---

[52] Dette synes også å være gjennomgående i lovforarbeidene, se NOU 2009:15 s. 247 flg. og Prop. 68 L (2015-2016) s. 224.
[53] Som tidligere nevnt har verken Metodekontrollutvalget eller departementet sett det som mulig eller hensiktsmessig å beskrive mulige gjennomføringsmåter uttømmende. Begge lovforarbeidene synes å gi politiet et romslig handlingsrom ift. hvordan avlesingen gjennomføres se NOU 2009:15 s. 248-249 og Prop. 68 L (2015-2016) s. 271, jfr. også s. 264 flg.
[54] Jfr. Grl. § 113 og EMK art. 8 nr. 2.
[55] Prop. 68 L (2015-2016) s. 224.
[56] Se Bruce & Haugland (2014) s. 255. Se for øvrig Prop. 68 L (2015-2016) s. 265-266 med videre henvisning til *Forsvarergruppen av 1977* sin høringsuttalelse under proposisjonens pkt. 14.7.4 på s. 257-258.

filer som brukeren oppretter, uten å lagre i ettertid. Videre kan politiet på denne måten fange opp passord og krypteringsnøkler som tastes inn, uten å lagres på datasystemet, og på denne måten få tilgang til passordbeskyttede deler av datasystemet eller eventuell kryptert informasjon. Som avhandlingen vil komme tilbake til i kapittel 4 er det særlig metodens vedvarende karakter som gjør dataavlesing problematisk opp mot kravet om tilstrekkelig presis lovhjemmel og at inngrepet skal være forholdsmessig.

3 Dataavlesing i forebyggende øyemed *de lege lata*

3.1 Generelt om PSTs forebyggende virksomhet

Politiets sikkerhetstjeneste (PST) skal – i likhet med det alminnelige politiet – forebygge og etterforske straffbare handlinger.[57] Adgang til å benytte tvangsmidler i forebyggende øyemed er imidlertid forbeholdt PST. Begrunnelsen er at lovgiver har forutsatt at det stilles særlige forventninger til at PST skal oppdage og forhindre trusler mot samfunnssikkerheten før de realiseres.[58] PST har andre oppgaver enn det alminnelige politiet, og vil ha større behov for å gripe inn uten at vilkårene for etterforskning er oppfylt. PSTs virksomhet skal i stor grad være forebyggende, der målet vil være å sørge for at det ikke blir grunnlag for etterforskning.[59] I tillegg ble det vist til at det forelå et misforhold mellom de forventningene som stilles til PST sin forebyggende virksomhet og de virkemidlene som tjenesten lovlig hadde tilgang til.

Som forebyggende virksomhet regnes «den informasjonsinnhenting PST driver uten at vilkårene for å igangsette etterforskning er oppfylt».[60] Det vil si når PST foretar undersøkelser uten at det foreligger rimelig mistanke rettet mot vedkommende om et straffbart forhold, jfr. strpl. § 224. Med hensyn til sporvalg la departementet til grunn at PST lojalt skiller mellom etterforskning og forebygging, og at dersom det er grunnlag for etterforskning, bør etterforskningssporet velges.[61] Det forebyggende aspektet må ses i sammenheng med at de straffbare handlinger som er underlagt PSTs funksjonsområde[62] er handlinger som i særlig grad truer sikkerheten i samfunnet eller grunnleggende samfunnsinstitusjoner, og begås ofte

[57] Pl. § 17b, jfr. pl. § 2 nr. 2 og 3.
[58] Ot.prp.nr.60 (2004-2005) s. 112, jfr. også Innst. O. nr. 113 (2004-2005) s. 33.
[59] Ot.prp.nr. 60 (2004-2005) s. 112, se også Auglend & Mæland (2016) s. 350 flg.
[60] Se Prop. 68 L (2015-2016) s. 202. Om grensen mellom etterforskning og forebygging, se NOU 2004:6 s. 171 flg. og Riksadvokatens rundskriv nr.3/1999 (RA-1999-3).
[61] Prop. 68 L (2015-2016) s. 202-203. Dette samsvarer også med den forutsetningen som er trukket opp i RA-1999-3 pkt. II.
[62] Se pl. § 17b.

av profesjonelle og lukkede miljøer. Videre vil skadeomfanget gjerne være dyptgripende og av irreversibel virkning.[63]

Adgang til å anvende skjulte tvangsmidler i forebyggende øyemed ble innført i 2005 ved tilføyelse av ny § 17d i politiloven. Flertallet i justiskomiteen (med unntak av medlemmet i SV) uttalte at:

> «Flertallet vil understreke at PSTs adgang til å bruke benytte tvangsmidler i forebyggende virksomhet er et begrenset supplement til den anledningen PST har, i likhet med politiet, til å bruke tvangsmidler for å avverge som ledd i etterforskning. Flertallet mener risikoen for at uskyldige skal rammes av tvangsmidler er større i slike saker, og vil derfor presisere at dette skal være et siste virkemiddel i forebyggingen av svært alvorlige forbrytelser som begås av lukkede og profesjonelle miljøer.»[64]

Uttalelsen gir inntrykk av at det skal være en høy terskel for at PST skal ha anledning til å benytte seg av tvangsmidler i sin forebyggende virksomhet.

Etter pl. § 17d kan retten gi PST tillatelse til å benytte bestemte tvangsmidler i sin forebyggende virksomhet.[65] Blant de oppregnede tvangsmidlene vises det til dataavlesing etter strpl. § 216o.

3.2 Materielle vilkår for dataavlesing i forebyggende øyemed

3.2.1 Grunnvilkåret «grunn til å undersøke om noen forbereder en handling»

Grunnvilkåret etter bestemmelsens første ledd er at det er «grunn til å undersøke om noen forbereder en handling» som rammes av nærmere angitte bestemmelser i straffelovgivningen. Det kan innfortolkes tre elementer i grunnvilkåret.[66]

For det første ligger det i «grunn til å undersøke» et *mistankekrav*. Det følger av dette at det må foreligge visse forhold som berettiger å undersøke om noen forbereder en nærmere angitt straffbar handling. I forarbeidene er det understreket at PST, for å få tillatelse til å benytte forebyggende tvangsmidler, må godtgjøre overfor domstolen at opplysninger i det konkrete saksforholdet gir grunn til å gjennomføre nærmere undersøkelser.[67] Grunnen til å undersøke

[63] NOU 2004:6 s. 177 flg.
[64] Innst.O.nr.113 (2004-2005) s. 34.
[65] Jfr. Innst.O.nr.113 (2004-2005) s. 34.
[66] Ot.prp.nr. 60 (2004-2005) s. 151-152. Se også Auglend & Mæland (2016) s. 390-391.
[67] Se Innst.O.nr.113 (2004-2005) s. 34 og Auglend & Mæland (2016) s. 391.

må være forankret i objektive og ytre konstaterbare holdepunkter, som f. eks infiltrasjons- eller spaningsopplysninger, tips, dokumentfunn eller andre beviser som indikerer at noen kan være i ferd med å forberede en nærmere bestemt straffbar handling.

For det andre er det et krav om *formålsbestemthet*, som setter grenser for hvilke formål som kan begrunne bruk av tvangsmidler.[68] I dette ligger det at anvendelsen av tvangsmidler må være saklig begrunnet i PSTs forebyggende virksomhet slik den kommer til uttrykk i pl. § 17b. Konsekvensen er at man ikke kan benytte forebyggende tvangsmidler dersom formålet er at det skal brukes som ledd i etterforskning.

For det tredje er det et *kriminalitetskrav*, som begrenser adgangen til å bruke forebyggende tvangsmidler til særskilt oppgitte og alvorlige straffbare handlinger, hvor det forebyggende aspektet gjør seg særlig gjeldende.[69] De særskilt opplistede straffebudene omfatter terrorhandlinger, jfr. bokstav a, ulovlig etterretningsvirksomhet, jfr. bokstav b, befatning med farlig materiale mv., jfr. bokstav c, og vold eller trusler mot de øverste statsmyndighetene, jfr. bokstav d. Forarbeidene viser til at «fordi det reiser særlige rettssikkerhetsmessige og personvernsmessige betenkeligheter å tillate tvangsmidler [når vilkårene for å sette i gang etterforskning ikke er oppfylt], går departementet inn for at hjemmelen kun skal gjelde for tre typer saker der behovet for slike virkemidler er størst …».[70]

3.2.2 Tilleggsvilkår

I tillegg til grunnvilkåret etter første ledd, oppstilles det tre *tilleggsvilkår* etter pl. § 17d annet ledd; et indikasjonskrav, et subsidiaritetskrav og et krav om forholdsmessighet. Det følger av bestemmelsens annet ledd at tillatelsen «bare kan gis» dersom «det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen, at forebygging ellers i vesentlig grad vil bli vanskeliggjort og at inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig». Ordlyden «grunn til å tro» tilsier at det må være konkrete objektive holdepunkter for at inngrepet vil være av betydning for å forebygge handlingen og ikke fremstå som uforholdsmessig.[71] Det må være en viss

[68] Se Ot.prp.nr.60 (2004-2005) s. 151.
[69] Se Ot.prp.nr.60 (2004-2005) s. 151 med videre henvisning til proposisjonens kpt. 9. Se for øvrig pl. § 17d første ledd bokstav a til d.
[70] Ot.prp.nr.60 (2004-2005) s. 127 flg. I Prop. 68 L (2015-2016) foreslo departementet innføring av ny bokstav c i bestemmelsen som tar for seg strl. § 142 om ulovlig befatning med farlig materiale mv.
[71] Ot.prp.nr.60 (2004-2005) s. 152 med videre henvisning til tilsvarende vilkår i utkast til strpl. § 222d på s. 148-151.

sannsynlighet for at handlingen vil bli begått, men det er ikke et krav om sannsynlighetsovervekt. Likevel må det være mer enn en teoretisk risiko.

For det første må det være grunn til å tro at inngrepet vil gi «opplysninger av vesentlig betydning for å kunne forebygge handlingen». For det andre må det være grunn til å tro at forebygging «ellers i vesentlig grad vil bli vanskeliggjort». I dette ligger det at inngrepet ikke kan begrunnes ut ifra at det er praktisk eller av bekvemmelighetshensyn. Forarbeidene gir uttrykk for at: «Kjernen i disse vurderingstemaene – som til en viss grad glir inn i hverandre – er at tvangsmidler bare skal kunne anvendes hvor det er en viss sannsynlighet at tvangsmiddelbruken vil gi opplysninger som kan bidra til å [forebygge en handling som nevnt i første ledd], og hvor det må antas at mindre inngripende etterforskningsmetoder vil komme til kort».[72] Indikasjons- og subsidiaritetskravet må ses i sammenheng med lovgivers forutsetning om at tvangsmidler i forebyggende øyemed skulle være 'et siste virkemiddel' i forebygging av svært alvorlig kriminalitet.

Til slutt må inngrepet «etter sakens art og forholdene ellers» ikke fremstå som uforholdsmessig. Vilkåret må leses på lik måte som den alminnelige forholdsmessighetsvurderingen i strpl. § 170a[73], og fungere som en sikkerhetsventil mot uforholdsmessige inngrep. Ordlyden tilsier at det må tas en bred skjønnsmessig vurdering der en må avveie de tungtveiende rettssikkerhets- og personverninteressene man griper inn i, mot de samfunnsmessige interessene man søker å verne gjennom å forebygge en handling i det konkrete tilfellet. I forarbeidene er det gitt uttrykk for at forholdsmessighetsvurderingen i det forebyggende sporet vil være strengere enn ved bruk av tvangsmidler under etterforskningen.[74]

3.2.3 Særvilkår for dataavlesing

I pl. § 17d annet ledd annet punktum er det inntatt et særlig tilleggsvilkår for enkelte tvangsmidler, herunder dataavlesing i forebyggende øyemed. Det følger av annet ledd andre setning at tillatelse til å bruke dataavlesing i forebyggende øyemed bare kan gis når «særlige grunner» tilsier det. Ordlyden «særlige grunner» må forstås som en hevet terskel for bruk av de mest inngripende tvangsmidlene i forebyggende øyemed. Forarbeidene gir uttrykk for at bestemmelsen tar sikte på en skjerpet forholdsmessighetsvurdering, og skal forstås på lik måte

[72] Se note 71.
[73] Se Ot.prp.nr.60 (2004-2005) s. 152.
[74] NOU 2009:15 s. 247.

som i strpl. § 222d om bruk av tvangsmidler i avvergende øyemed.[75] Tidsmessig vil gjennomføringstidspunktet stå mye lengre frem i tid i forebygging enn i avvergingssituasjoner. Dette kan tas til inntekt for at kravet om skjerpet forholdsmessighet gjør seg særlig gjeldende når det er snakk om å bruke tvangsmidler i forebyggende øyemed, enn i avvergende øyemed.

I pl. § 17d annet ledd tredje og fjerde punktum er det inntatt restriksjoner for når det kan gjøres inngrep «i noens private hjem». Etter tredje punktum settes det et absolutt forbud mot romavlytting i forebyggende øyemed i noens private hjem. På den annen side åpnes det for at det bare kan gis tillatelse til ransaking eller ved dataavlesing å gjøre innbrudd i noens private hjem når det er grunn til å undersøke om noen forbereder en handling som nevnt i første ledd bokstav a (terrorhandlinger).

Tredje og fjerde punktum innebærer en endring fra den vedtatte bestemmelsen fra 2005, der det kun var oppstilt et forbud i tredje punktum mot ransaking i forebyggende øyemed. Metodekontrollutvalgets flertall foreslo å utvide forbudet til å omfatte romavlytting, mens mindretallet foreslo å innskrenke forbudet ved å fjerne tredje punktum.[76] Departementets anbefalte en mellomløsning der en differensierte mellom de ulike tvangsmidlene som kunne benyttes og mellom ulike lovbrudd som gir grunnlag for bruk av tvangsmidlene.[77] Det ble lagt avgjørende vekt på at romavlytting representerte et så inngripende tvangsmiddel at det ikke rettferdiggjorde inngrep i forebyggende øyemed. Videre tilsa det behovet for inngrep størst i terrorsaker, noe som tilsa at det burde åpnes for ransaking eller ved dataavlesing å gjøre innbrudd 'i noens hjem'.
På dette punktet kommenterte ikke departementet differensieringen som dataavlesing som selvstendig metode og Metodekontrollutvalgets forslag om dataavlesing for å muliggjøre kommunikasjonskontroll innebærer i forhold til graden av inngripen.

3.3 Prosessuelle rettssikkerhetsgarantier og kontrollmekanismer

3.3.1 Generelt om kontrollen ved bruk av skjulte tvangsmidler

Det ligger i sakens natur at det er behov for hemmelighold ved politiets bruk av skjulte tvangsmidler. Uten hemmelighold ville de skjulte tvangsmidlene mistet deres effektivitet, og

[75] Ot.prp.nr.60 (2004-2005) s. 152 mvh. til s. 60-61 og s. 149-150, jfr. også tidl. note 60 om grensen mellom forebygging og etterforskning. Se også Auglend & Mæland (2016) s. 392.
[76] NOU 2009:15 s. 233-234 og s. 247.
[77] Prop. 68 L (2015-2016) s. 212 flg.

tvangsmiddelbruken ville ikke oppnådd dets tilsiktede resultat. Ulempen med behovet for hemmelighold er at det gjør unntak for flere sentrale rettssikkerhetsgarantier, som siktedes egenkontroll, rett til kontradiksjon og kontroll gjennom offentlighet. En forutsetning for å tillate bruk av skjulte tvangsmidler er at bruken underlegges prosessuelle rettssikkerhetsgarantier[78] og et effektivt kontrollregime.[79] Både Metodekontrollutvalget og departementet la til grunn en forutsetning om at dataavlesing ble underlagt et tilsvarende kontrollregime som de øvrige skjulte tvangsmidlene.[80] Kontrollmekanismer som gjør seg særlig gjeldende for skjulte tvangsmidler er forutgående kontroll (kontroll *ex ante*), løpende kontroll og etterfølgende kontroll (kontroll *ex post*).

3.3.2 Hovedregelen om domstolskontroll etter norsk rett

I likhet de skjulte tvangsmidlene ellers i norsk rett, er hovedregelen at bruk av skjulte tvangsmidler i forebyggende øyemed skjer med grunnlag i forutgående tillatelse fra retten. Domstolens forutgående kontroll ved politiets bruk av skjulte tvangsmidler regnes som en av de viktigste rettssikkerhetsgarantiene for rettmessigheten av tvangsmiddelbruken[81], og departementet har uttalt at det er en grunnleggende rettssikkerhetsgaranti at bruk av tvangsmidler som hovedregel må tillates av domstolen ved kjennelse.[82] Dels kan dette begrunnes i domstolens rolle som uavhengig statsmakt, og dels kan det begrunnes i at politiet (PST i forebyggende tilfeller) ikke selv bør avgjøre om det skal benyttes såpass inngripende tvangsmidler.

For forebyggende tvangsmidler sitt vedkommende følger dette direkte av ordlyden «Retten kan ved kjennelse gi (…) tillatelse» i pl. § 17d første ledd. Ved at tillatelsen skjer ved kjennelse, innebærer det også at tillatelsen må begrunnes, jfr. strpl. § 52. Dette bidrar for det første til å ivareta rettmessigheten rundt tvangsmiddelbruken ved at det skapes notoritet rundt grunnlaget for inngrepet i lys av vilkårene som stilles opp i pl. § 17d. Videre bidrar en begrunnet kjennelse også til at den etterfølgende kontrollen av tvangsmiddelbruken blir mer effektiv.

---

[78] NOU 2009:15 s. 60 flg.
[79] NOU 2009:15 s. 130 flg. for en generell gjennomgang av kontrollen med politiets bruk av skjulte tvangsmidler. For en generell gjennomgang av kontrollmekanismer for politiet i Norge, se NOU 2009:12 s. 44 flg., se også Auglend & Mæland (2016) kpt. 25 s. 1341 flg.
[80] NOU 2009:15 s. 249 og Prop. 68 L (2015-2016) s. 274, jfr. s. 259.
[81] NOU 2009:15 s. 137-138.
[82] Ot.prp.nr.60 (2004-2005) s. 133-134 og Prop. 68 L (2015-2016) s. 211.

I pl. § 17d tredje ledd er det gjort unntak fra utgangspunktet om forutgående domstolskontroll – dette omtales om PSTs hastekompetanse. Det følger av tredje ledd første punktum at ordre fra Sjef-PST eller Ass. Sjef-PST kan tre i stedet for kjennelse for retten dersom det «ved opphold er stor fare for at muligheten til å forebygge en handling som nevnt i første ledd bokstav a eller d vil gå tapt».

Ettersom forspillelsesrisikoen for å forebygge handlingen må være høy, tilsier ordlyden at hastekompetansen må anses som en snever unntaksregel. Forarbeidene gir uttrykk for at PSTs hastekompetanse gir en «meget snever adgang» til å gjøre unntak fra hovedregelen om forutgående tillatelse fra retten.[83] Videre begrenses PSTs hastekompetanse ved at den bare kan gis for å forebygge en handling etter pl. § 17d første ledd bokstav a (terrorhandlinger) eller d (vold eller trusler mot statsmyndighetene), samt at det, ved hastekompetanse, ikke kan gis tillatelse til romavlytting etter strpl. § 216m. Dette begrunnes med at romavlytting er et så inngripende tvangsmiddel at det alltid må tillates av retten.[84] Beslutningen skal snarest mulig, og senest innen 24 timer etter tvangsmiddelet ble tatt i bruk, legges frem for retten for godkjennelse, jfr. tredje ledd annet punktum. Etter tredje ledd tredje og fjerde punktum fremgår det at beslutningen skal så vidt mulig være skriftlig og opplyse om hva saken gjelder og om formålet med bruk av tvangsmiddelet, og en muntlig beslutning skal snarest nedtegnes skriftlig. Bestemmelsen skal sikre notoritet og etterprøvbarhet ved tvangsmiddelbruken, samt at muliggjøre etterfølgende kontroll.[85]

Behandlingen av begjæring om tvangsmiddelbruk etter pl. § 17d er regulert i pl. § 17e. Begjæringen fremsettes for tingretten på det sted det mest praktisk mulig kan skje, jfr. første ledd første punktum. Etter første ledd annet punktum at tillatelse kan gis for «inntil 6 måneder av gangen dersom særlige omstendigheter tilsier at en fornyet prøving etter 4 eller 8 uker vil være uten betydning». Bestemmelsen må forstås slik at det unntaksvis kan gis tillatelse utover utgangspunktet om 4 eller 8 uker, som gjelder etter tilsvarende bestemmelse etter straffeprosessloven.[86] Grunnen til at det kan gis tillatelse utover 4 eller 8 uker er at forebyggende arbeid ofte har lengre tidsperspektiv enn tilsvarende tvangsmiddelbruk under etterforskning.[87] Forarbeidene understreker videre at langvarige tillatelser bør brukes med

[83] Ot.prp.nr. 60 (2004-2005) s. 152.
[84] Se note 82.
[85] Se note 83.
[86] Sml. Strpl. § 216f, jfr. strpl. § 216o.
[87] Ot.prp.nr. 60 (2004-2005) s. 153.

varsomhet ettersom det dreier seg om inngripende tvangsmidler. Samtidig følger det av strpl. § 216o om dataavlesing at rettens tillatelse ikke kan gis for mer enn to uker om gangen. Det fremstår som noe uklart om rettens tillatelse om bruk av dataavlesing i forebyggende øyemed kan overstige to uker.

Etter pl. § 17e første ledd tredje punktum skal bruken av tvangsmidler stanses før utløpet av fristen som retten har satt dersom vilkårene for bruk av forebyggende tvangsmidler er bortfalt, eller tvangsmiddelbruken ikke lenger anses hensiktsmessig. Bestemmelsen må leses i samsvar med kravet om inngrepets forholdsmessighet. Det er et grunnleggende krav at tvangsmidler ikke brukes utover det som er nødvendig, og bestemmelsen etablerer en positiv plikt for PST å påse at noen ikke utsettes for tvangsmidler utover det som er nødvendig.[88] Et eksempel kan være at overvåkingen før fristen løper ut har skaffet til veie nok opplysninger til å forebygge handlingen uten ytterligere bruk av tvangsmiddelet.

Behandling av begjæring om tvangsmiddelbruk etter pl. § 17d skjer uten at den inngrepet retter seg mot gis adgang til å uttale seg, og at kjennelsen blir meddelt dem, jfr. pl. § 17e andre ledd første punktum. Dette innebærer et inngrep i en grunnleggende rettssikkerhetsgaranti om kontradiksjon, og tilsier at de øvrige rettssikkerhetsgarantiene må styrkes.[89] En nødvendig rettssikkerhetsgaranti er derfor sikret ved at strpl. § 100a om hemmelig advokat gjelder tilsvarende for forebyggingssaker, jfr. pl. § 17e annet ledd annet punktum, likevel slik at innsynsretten begrenses til de dokumenter som legges frem for retten.

Hensikten er at forsvareren skal vareta den inngrepet retter seg mot sine interesser under behandlingen av begjæringen, jfr. strpl. § 100a annet ledd første punktum.[90] Advokaten skal, så langt det er mulig, settes i den samme prosessuelle stillingen som om den inngrepet retter seg mot var klar over tvangsmiddelet. Advokaten skal dermed gjøres kjent med begjæringen og grunnlaget for det, og ha adgang til å fremme argumenter for om de materielle og prosessuelle vilkårene for tvangsmidlet er oppfylt. Som ledd i dette har advokaten adgang til å påanke rettens kjennelse, jfr. strpl. § 100a annet ledd sjette punktum. Ved at den inngrep etter § 17d retter seg mot ikke har krav på underretning, eller krav på innsyn i opplysningene som ble innhentet ved tvangsmiddelbruken, i etterkant av inngrepet, gjør ordningen om hemmelig

[88] Ot.prp.nr. 60 (2004-2005) s. 153.
[89] NOU 2009:15 s. 66-67.
[90] Nærmere om dette, se Ot.prp.nr.64 (1998-1999) s. 144-145.

advokat seg særlig gjeldende i forebyggingssaker. Rett til hemmelig advokat utgjør således en sentral rolle i å ivareta rettssikkerheten til den som inngrepet retter seg mot, og er således en viktig del av den forutgående kontrollen.

3.3.3 EOS-utvalgets kontroll

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenesten (EOS-utvalget) ble opprettet i 1996 for å føre kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene).[91] EOS-utvalgets virksomhet er regulert i egen lov og instruks.[92] Bakgrunnen for opprettelsen var den offentlige debatten om virksomheten til de hemmelige tjenestene, og nedsettelsen av Lund-kommisjonen, som konkluderte med at det særlig på 60- og 70-tallet hadde pågått omfattende ulovlig politisk overvåking av de hemmelige tjenestene.[93] Den 27. mars 2014 ble det oppnevnt et Evalueringsutvalg for å evaluere EOS-utvalgets kontrollvirksomhet, og den 23. februar 2016 avla Evalueringsutvalget sin rapport til Stortinget. Evalueringsutvalget konkluderte med at «EOS-utvalgets kontroll hadde fungert godt etter sin opprinnelige intensjon. Over tid er det utviklet gjensidig respekt mellom utvalget og tjenestene. Utvalget nyter allmenn tillit og bidrar således til samfunnets aksept av EOS-tjenestene. Tiden er likevel moden for enkelte endringer og justeringer i EOS-utvalgets arbeid og rammebetingelser.».[94] For øvrig bekreftet evalueringen at PST var den EOS-tjenesten som var grundigst kontrollert, og at EOS-utvalget i særlig grad hadde fokusert på blant annet PSTs bruk av skjulte tvangsmidler.[95]

For avhandlingens del er det EOS-utvalgets kontroll med PSTs forebyggende virksomhet som er av interesse, og da særlig PSTs bruk av skjulte tvangsmidler i forebyggende øyemed.

Sammenfatningsvis er formålet med EOS-utvalgets kontroll å drive en formell og materiell (lovlighets)kontroll av PSTs forebyggende virksomhet, samt verne om samfunnets interesser og den enkeltes rettssikkerhet og menneskerettigheter, jfr. EOS-loven § 2 første ledd nr. 1-3.[96]

---

[91] EOS-tjenestene består av: Etterretningstjenesten, Politiets sikkerhetstjeneste, Nasjonal Sikkerhetsmyndighet og Forsvarets sikkerhetstjeneste.
[92] Lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven) og Instruks 30. mai 1995 nr. 4295 om kontroll med EOS-tjenestene (EOS-kontrollinstruksen).
[93] https://eos-utvalget.no/norsk/tjenester/om_eos_utvalget/historikk/ - sist besøkt 02.02.2017. For nærmere redegjørelse av ulovlig politisk overvåking under den kalde krigen, se Dokument nr. 15 (1995-1996) Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»).
[94] Dok.nr.16 (2015-2016) s. 9.
[95] Dok.nr.16 (2015-2016) s. 10 og 64 flg.
[96] Ot.prp.nr.83 (1993-1994) s. 21.

EOS-utvalget har en rent kontrollerende funksjon, og har ikke adgang til å instruere de kontrollerte organene, jfr. EOS-loven § 2 tredje ledd.

EOS-utvalgets kontroll med PST skjer gjennom regelmessig tilsyn (inspeksjoner) med PST, behandling av klager fra enkeltpersoner og organisasjoner mot PST, og utvalget kan av eget tiltak ta opp saker i lys av lovens formål, jfr. EOS-loven § 3.[97] EOS-utvalgets kontroll er i utgangspunktet en etterfølgende kontroll, men kan «likevel kreve innsyn i og uttale seg om løpende saker», jfr. EOS-kontrollinstruksen § 7 første ledd. De viktigste virkemidlene for å utøve sin kontrollvirksomhet ligger i EOS-utvalgets innsynsrett, jfr. lovens § 4, og forklarings- og møteplikt for utvalget, jfr. lovens § 5.

Kontrollen gjennomføres blant annet ved at EOS-utvalget utfører stikkprøver, f. eks ved fritekstsøk i PSTs arkiver og systemer, og ved at EOS-utvalget får en orientering om PSTs løpende virksomhet.[98] For eksempel kan EOS-utvalget be om å bli forelagt PSTs avsluttede og pågående saker. Gjennom den vidtgående innsynsretten vil EOS-utvalget kunne kontrollere at det er samsvar mellom det informasjonsgrunnlaget PST har og innholdet i tjenestens begjæringer til retten. Videre vil utvalget kunne påse at PST overholder de rammene retten har satt i kjennelsene, samt kontrollere tjenestens behandling av informasjonen som samles inn.[99] Loven oppstiller ingen øvrige regler knyttet til EOS-utvalgets kontroll av PSTs bruk av dataavlesing i forebyggende øyemed.

Til sammenligning er det av interesse å se hen til kontrollen med politiets bruk av dataavlesing i straffesporet. I *etterforskning* av straffesaker er det opprettet et eget kontrollutvalg for kommunikasjonskontroll (KK-utvalget) som fører kontroll med politiets bruk av skjulte tvangsmidler.[100] Etter kommunikasjonskontrollforskriften § 7 skal det føres en protokoll som oppgir opplysninger om tvangsmiddelbruken. Ved bruk av dataavlesing stilles det også særlige krav til opplysningene som skal fremgå av protokollen, herunder; hvilke data som er avlest, hvorvidt det er benyttet utstyr eller programvare for avlesingen, om det er foretatt et fysisk innbrudd eller et innbrudd i datasystemet for å gjennomføre avlesingen, risiko og tiltak for å hindre skade eller uberettiget adgang til datasystemet, og hvilke personell

---

[97] Se også EOS-kontrollinstruksen § 11 nr. 1 bokstav c og nr. 2. For en nærmere redegjørelse av EOS-utvalgets kontroll med PST, se Bruce & Haugland (2014) s. 135-137.
[98] Bruce & Haugland (2014) s. 135-136 og EOS-utvalgets årsmelding til Stortinget 2015 s. 8 og 15 flg.
[99] Se politiregisterloven § 68 første ledd.
[100] Se Straffeprosessloven § 216h, jfr. også Forskrift av 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing (Kommunikasjonskontrollforskriften) – heretter KK-forskriften.

som har utført avlesingen. Hensikten bak protokolleringen er å skape notoritet rundt politiets metodebruk som en forutsetning for tilfredsstillende etterkontroll. KK-utvalgets kontrollvirksomhet omfatter ikke saker som faller inn under EOS-loven, og dermed EOS-utvalgets kontrollvirksomhet.[101] Således gjelder ikke reglene om protokollering etter KK-forskriften § 7 for dataavlesing i forebyggende øyemed. Det kan dermed problematiseres om hvorvidt reglene for etterfølgende kontroll for dataavlesing i forebyggende øyemed er tilfredsstillende. Dette vil bli behandlet senere i avhandlingen.

4 Konfrontasjon mellom dataavlesing i forebyggende øyemed og retten til privatliv etter Grunnloven § 102

4.1 Innledning – forholdet mellom Grunnloven § 102 og EMK

Alle mennesker har i utgangspunktet et behov for en privat sfære der en kan være i fred fra innblanding fra utenforstående.[102] Retten til privatliv er derfor ansett å være en sentral forutsetning for menneskets dannelsesprosess, og et grunnleggende prinsipp i en demokratisk rettsstat.[103] Ved grunnlovsrevisjonen av 2014 ble retten til privatliv konstitusjonelt forankret i Grunnloven § 102. I tillegg til grunnlovsforankringen er retten til privatliv forankret Den europeiske menneskerettighetskonvensjonen (EMK) art. 8, som er inkorporert i norsk rett ved menneskerettighetsloven § 2, og skal etter bestemmelsen gjelde som norsk lov.

I den nye bestemmelsen i Grunnloven § 92 følger det at statens myndigheter plikter å respektere og sikre menneskerettighetene slik de er nedfelt i Grunnloven og i for Norge bindende traktater om menneskerettigheter.[104] Ved at bestemmelsen både viser til menneskerettighetene slik det er nedfelt i Grunnloven og til de folkerettslige menneskerettighetskonvensjonene som Norge er bundet av, oppstår spørsmål om hvilken trinnhøyde menneskerettighetskonvensjonene får i norsk rett. Ordlyden gir liten veiledning på dette punktet, og gir ikke holdepunkter for å skille mellom de grunnlovfestede og konvensjonsfestede rettighetene. Den signaliserer heller at rettighetene skal sikres og respekteres på lik linje.[105] Enkelte uttalelser i Innst. 186 S (2013-2014) på s. 22 har reist

[101] Jfr. Strpl. § 216h første ledd annet punktum og KK-forskriften § 12.
[102] NOU 2009:15 s. 47 flg. og Prop. 68 L (2015-2016) s. 19 flg.
[103] NOU 2009:1 s. 209 flg. jfr. s. 32 og Prop. 68 L (2015-2016) s. 19 flg. Jfr. også Smith (2015) s. 426 flg.
[104] Bestemmelsen viderefører den tidligere Grl. § 110c intensjon om å gi et generelt uttrykk for menneskerettighetenes sentrale plass i norsk rett, se Innst.186 S (2013-2014) s. 22.
[105] Se Anine Kierulf, Rettsdata Norsk lovkommentar til Grl. § 92 note (197A5) – sist endret 15.11.2016.

spørsmålet om bestemmelsen skulle forstås slik at de gjeldende konvensjonene på området pr. 13. mai 2014 hadde grunnlovs rang.[106]

I HR-2016-2554-P (*Holship*) vurderte Høyesterett spørsmålet om forholdet mellom Grunnloven og internasjonale menneskerettighetskonvensjoner, og kom til at det var klart at Grl. § 92 ikke kunne tolkes som en inkorporasjonsbestemmelse, men må forstås som et pålegg til domstolene og andre myndigheter om å håndheve menneskerettighetene på det nivå de er gjennomført i norsk rett.[107] Dommen er avsagt i plenum under dissens 10 mot 7, men mindretallet var ikke uenig med flertallet i tolkningen av Grl. § 92.[108] Rettstilstanden i spørsmålet må anses som endelig avklart. Bestemmelsen i Grl. § 92 kan ikke tas til inntekt for at internasjonale menneskerettskonvensjoner som Norge er bundet til får grunnlovs trinnhøyde. Man kan dermed slå fast at Grunnlovens rettighetsbestemmelser etter *lex superior*-prinsippet har høyere rang enn menneskerettighetskonvensjonene i norsk rett.

Spørsmålet videre er hvordan man skal tolke rettighetsbestemmelsen i Grl. § 102, og hvilken betydning internasjonale menneskerettighetskonvensjoner har ved tolkningen av Grl. § 102.

Grunnloven § 102 første ledd slår fast at: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.»

Bestemmelsen i første punktum er ny ved grunnlovsrevisjonen av 2014, og har en tilnærmet identisk ordlyd som EMK art. 8 nr. 1. Bestemmelsen i annet punktum er en språklig fornyelse av tidligere Grl. § 102, som har stått i Grunnloven siden 1814. Formålet ved grunnlovfestingen av retten til privatliv var å gi prinsippet en generell forankring i Grunnloven.[109] Samtidig fremhevet Lønning-utvalget at grunnlovfestelsen av retten til privatliv og personvern ikke var ment å endre på rettstilstanden, men å heve det allerede eksisterende vernet som fulgte av Grl. § 102, ulovfestet rett, menneskerettighetsloven og annen ordinær lovgivning, til et konstitusjonelt nivå.[110]

---

[106] Se Aall (2015) s. 98-99 og Skoghøy (2015) s. 195-196.
[107] HR-2016-2554-P avsnitt 64-70.
[108] Se dommens avsnitt 140.
[109] Dok.nr.16 (2011-2012) s. 175 flg.
[110] Dok.nr.16 (2011-2012) s. 178 jfr. s. 175.

Etter ordlyden fremstår retten til privatliv etter Grl. § 102 som absolutt. Samtidig presiseres det i forarbeidene at formuleringen om rett til «respekt for» privatlivet ble valgt for å gjøre det klart for at bestemmelsen ikke var til hinder for bl.a. lovlig etterretning.[111] Bestemmelsen kan dermed ikke forstås som en ubetinget rett til privatliv. Grunnloven § 102 skiller seg dermed ut fra den parallelle rettighetsbestemmelsen i EMK art. 8 der det gis en anvisning på en fireleddet vurdering for å gjøre inngrep i retten til privatliv; det må være tale om et inngrep i rettigheten, inngrepet må være i samsvar med lov («in accordance with the law»), ivareta et legitimt formål og være «necessary in a democratic society».[112]

Ifølge Lønning-utvalget var ikke intensjonen at retten til privatliv etter Grl. § 102 skulle være absolutt, og det var foreslått en generell begrensningshjemmel i ny Grl. § 115.[113] Begrensningshjemmelen hentet inspirasjon fra tilsvarende hjemler i internasjonale menneskerettighetskonvensjon og andre lands konstitusjoner. Under stortingsbehandlingen våren 2014 ble behandlingen av den foreslåtte begrensningshjemmelen utsatt, og per våren 2017 har det vist seg vanskeligheter med å vedta bestemmelsen.[114]

Høyesterett har her måtte lede an rettsutviklingen. I en rekke høyesterettsdommer i etterkant av grunnlovsrevisjonen av 2014 har Høyesterett uttalt seg om tolkningen av Grunnlovens nye rettighetsbestemmelser, og hvilken betydning internasjonale menneskerettigheter har ved tolkningen av de parallelle rettighetsbestemmelsene i Grunnloven.

I Rt. 2014 s. 1105 (*Acta*) fremholdt Høyesterett som et alminnelig prinsipp om hvorvidt et inngrep i Grunnlovens menneskerettigheter var rettmessig beror på at det har *hjemmel i lov*, ivaretar et *legitimt formål* og er *forholdsmessig*.[115] Dette ble fulgt opp i Rt. 2015 s. 93 (*Maria*) der Høyesterett på avsnitt 60 la til grunn at grunnlovsvernet etter Grl. § 102 ikke var absolutt, og det ville være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom inngrepet «(…) har tilstrekkelig *hjemmel*, forfølger et *legitimt formål* og er *forholdsmessig*». Videre uttalte Høyesterett i *Maria*-saken at; «[Grl.] § 102 skal tolkes i lys av sine folkerettslige forbilder (…)», men med forbehold at «Det er etter vår forfatning Høyesterett (…) som har ansvaret for å tolke, avklare og utvikle Grunnlovens

[111] Innst. 186 S (2013-2014) s. 27.
[112] Se EMK art. 8 nr. 2, jfr. nr. 1.
[113] Dok.nr.16 (2011-2012) s. 72 flg. og s. 260.
[114] Innst. 165 S (2015-2016) s. 1-13.
[115] Rt. 2014 s. 1105 avsnitt 24-28.

menneskerettighetsbestemmelser.»[116] Dette synet på grunnlovstolkning er siden fulgt opp i Høyesteretts praksis, og må anses som sikker rett.[117]

De nevnte avgjørelsene har to implikasjoner ved tolkningen av Grunnloven § 102. For det første viser de at Høyesterett legger til grunn den samme vurderingen for å gjøre inngrep i menneskerettighetene etter Grunnloven, som foretas i EMD når det gjøres inngrep i EMK. For det andre ved at menneskerettighetene i Grunnloven skal «tolkes i lys av» sine folkerettslige forbilder i de tilsvarende konvensjonsbestemmelsene, vil de internasjonale menneskerettighetskonvensjonene ha betydning for klarleggingen av det materielle innholdet i Grl. § 102. Følgelig vil EMK være relevant og ha stor vekt, og vil kunne danne et utgangspunkt ved tolkningen av Grunnlovens rettighetsbestemmelser. Ved at Grunnloven § 102 skal «tolkes i lys av sine folkerettslige forbilder» gis det en indikasjon på at det i stor grad er harmoni mellom regelsettene. Det må da være en sterk generell presumsjon om at Grunnloven § 102 i hvert fall gir det *samme materielle minstevernet* som EMK art. 8, med mindre tolkningspraksis gir holdepunkter for noe annet.[118] Det kan dermed oppstå situasjoner i fremtiden hvor rettighetsvernet etter Grunnloven går lengre eller kortere enn vernet etter EMK.

Per våren 2017 er det ikke mulig å identifisere så klare tolkningsforskjeller at det er hensiktsmessig å drøfte vernet etter Grunnloven og EMK separat. For avhandlingens del vil det derfor være hensiktsmessig å kun foreta en drøftelse opp mot Grunnloven § 102. Samtidig er det lite praksis fra Høyesterett om retten til privatliv etter Grl. § 102, mens det er rikelig med praksis fra EMD om den tilsvarende bestemmelsen i art. 8. I mangel av praksis fra Høyesterett om retten til privatliv etter Grl. § 102 vil det derfor være nødvendig å se hen til EMDs praksis ved klarlegging av rettsregelen etter Grl. § 102, med forbehold om at det kan forekomme avvikende tolkningspraksis.

Ettersom de overnevnte observasjonene viser at Høyesterett i sin praksis legger til grunn den samme struktur og systematikk for tolkningen av Grl. § 102 som for tolkning av EMK art. 8, anses det hensiktsmessig å anvende tilsvarende struktur og systematikk i den videre

---

[116] Rt. 2015 s. 93 avsnitt 56-57.
[117] Se særlig Rt. 2015 s. 155 (*Rwanda*) avsnitt 40 og 52 som var enstemmig, og i plenumsdommen i HR-2016-2554-P som var enstemmig på dette punktet, se avsnitt 81-82 og 140.
[118] Se Bårdsen (2017) s. 9-12. Lønning-utvalget la til grunn at eventuelle avvik fra internasjonal tolkningspraksis burde begrunnes, se Dok.nr.16 (2011-2012) s. 89-90.

fremstillingen av avhandlingen. Følgelig vil det ved konfrontasjon mellom Grl. § 102 og dataavlesing i forebyggende øyemed bli vurdert om; (i) dataavlesing i forebyggende øyemed utgjør et inngrep i retten til privatliv, (ii) om dataavlesing i forebyggende øyemed tilfredsstiller kravet om hjemmel i lov, (iii) om dataavlesing i forebyggende øyemed ivaretar et legitimt formål, og (iv) om dataavlesing i forebyggende øyemed er forholdsmessig.[119]

4.2 Er dataavlesing i forebyggende øyemed et rettmessig inngrep i retten til privatliv etter Grunnloven § 102 første ledd første punktum

4.2.1 Utgjør dataavlesing i forebyggende øyemed et inngrep i retten til privatliv?

Den første vurderingen etter Grl. § 102 er om dataavlesing i forebyggende øyemed utgjør et inngrep i retten til privatliv. Den samme vurderingen følger av EMK art 8 nr. 2.

Det kan ikke være tvil om at å bli utsatt for den overvåking av myndighetene som dataavlesing innebærer er å anses som et inngrep hos den enkelte i norsk rett.[120] I EMD følger det videre av fast konvensjonspraksis om hemmelige etterretnings- og etterforskningsmetoder at kommunikasjonsavlytting innebærer et inngrep i privatlivet.[121] Det må være på det rene at dataavlesing utgjør en form for kommunikasjonskontroll som må likestilles med annen kommunikasjonsavlytting.

EMD har presisert at «secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions».[122] Uttalelsen må tas til inntekt for at bruken av skjulte tvangsmidler innebærer et *sterkt* inngrep i privatlivet. EMDs praksis viser at inngrepets styrke har stor betydning for lovs- og nødvendighetsvurderingen i saker om hemmelig overvåking.[123] Som drøftelsen under pkt. 2.2 viser, går dataavlesing slik det er innført i Norge lengre enn tradisjonell kommunikasjonskontroll. Dette tilsier at dataavlesing er et særlig sterkt inngrep i retten til privatliv. Betydningen er at det må stilles et strengt krav til klar

[119] Se for øvrig foredrag ved Høyesterettsdommer dr. juris Arnfinn Bårdsen, Oslo 21. april 2017: «*Grunnloven, overvåking og domstolenes rolle*», Høyesteretts nettsider 2017 nr. 4 (HOY-2017-4). Foredraget ble avholdt kort tid før innlevering av denne avhandlingen, men Bårdsen viser til den samme vurderingen som jeg benytter i den videre fremstillingen.
[120] Jfr. Rt. 2014 s. 1105 avsnitt 24. Se også NOU 2009:15 s. 130 flg.
[121] Se Klass and others v. Germany avsnitt 41.
[122] Klass and others v. Germany avsnitt 42 og Szabó and Vissy v. Hungary avsnitt 54-57.
[123] R.E. v. UK avsnitt 126-131 og Uzun v. Germany avsnitt 66 og Bykov v. Russia avsnitt 78-79.

lovhjemmel, samt til krav om nødvendighet og proporsjonalitet. Inngrepets styrke vil således være av betydning for den videre drøftelsen.

Vurderingen videre er hvorvidt dataavlesing i forebyggende øyemed er å anses som et rettmessig inngrep i privatlivet.

4.2.2 Kravet om lovhjemmel

4.2.2.1 Hva ligger i kravet om *tilstrekkelig hjemmel*?

For å gjøre inngrep i Grl. § 102 forutsettes det at det er *tilstrekkelig hjemmel*. I norsk rett er det et alminnelig prinsipp om at myndighetenes inngrep overfor den enkelte må ha grunnlag i lov, jfr. legalitetsprinsippet i Grl. § 113. Det er også lagt til grunn i Høyesteretts praksis at inngrep i Grl. § 102 må ha hjemmel i lov.[124] Tilsvarende følger det av EMK art. 8 nr. 2 at inngrep forutsetter at det «…in accordance with the law(…)». Grunnlovens krav til lovhjemmel er imidlertid strengere enn kravet etter EMK ved at bare formell lov aksepteres som grunnlag for inngrep etter norsk rett. Høyesteretts praksis viser at det skjerpede lovkravet er et uttrykk for at man i norsk rett ikke bare har vektlagt hensynet til forutberegnelighet ved inngrep, men også til maktfordelingen og demokrati.[125] Konvensjonens lovbegrep har imidlertid vært tolket autonomt, pga. tradisjonene på området har variert blant konvensjonsstatene, og lovkravet i EMK synes å være begrunnet i hensynet til forutberegnelighet og motgå vilkårlig maktmisbruk.[126]

I EMDs praksis har det blitt oppstilt visse kvalitetskrav om at lovhjemmelen må være tilgjengelig («accessable») og forutberegnelig («forseeable»).[127] Ved tolkningen av Grl. § 102 har også Høyesterett lagt til grunn at det må stilles kvalitative krav til lovgivningen. I Rt. 2014 s. 1105 på avsnitt 30 uttalte førstevoterende at;

> «For å gi en slik hjemmel som Grunnloven og menneskerettskonvensjonene krever, holder det ikke at loven er formelt sett i orden (…). Det gjelder også *kvalitative* krav: Loven må være tilgjengelig og så presis som forholdene tillater. Den må dessuten - i lys av den forhøyede risikoen for misbruk og vilkårlighet som erfaringsmessig kan

[124] Rt. 2014 s. 1105 avsnitt 28, Rt. 2015 s. 93 avsnitt 60 og Rt. 2015 s. 155 avsnitt 52.
[125] Se Rt. 2014 s. 1105 avsnitt 24-26 med videre henvisning til Dok.nr.16 (2011-2012) kpt. 41 på s. 246 flg. om Lønning-utvalgets redegjørelse for forslaget til grunnlovfesting av legalitetsprinsippet. Se også Bårdsen (2017) s. 14 flg. og Aall (2015) s. 118.
[126] Aall (2015) s. 118-119.
[127] Roman Zakharov v. Russia avsnitt 228 mvh.

> foreligge når myndigheter tillates å operere i hemmelighet - gi rimelige garantier knyttet til blant annet formen for lagring, bruken av materialet, mulighetene for innsyn, sikkerhet og sletting. For så vidt gjelder tolkningen av EMK artikkel 8 på dette punktet, viser jeg til EMDs [praksis]».[128]

Dette viser at de kvalitative kravene som stilles til lovgivningen etter Grl. § 102 er tilnærmet lik kravene som stilles etter EMDs praksis knyttet opp mot EMK art. 8 hva gjelder krav om tilgjengelighet og forutberegnelighet.

Om kravet til tilgjengelighet følger det av EMDs praksis at det må være mulig for allmennheten å få kjennskap til loven. I avgjørende grad synes det som EMD har lagt vekt på om loven er kunngjort eller publisert, og dermed gjort tilgjengelig for allmennheten i større eller mindre grad.[129] Ikke-publiserte instrukser og regelverk som ikke er blitt gjort tilgengelig vil således ikke oppfylle lovkravet.

Etter fast konvensjonspraksis følger det at kravet til forutberegnelighet knyttet opp mot myndighetenes bruk av overvåkingsmetoder står i en særstilling.[130] Dette begrunnes i at det gjør seg særlig gjeldende et behov for hemmelighold for at metodene skal være formålstjenlig. På den annen siden fremheves det at risikoen for vilkårlighet øker når slik maktbruk, som overvåkingsmetodene innebærer, utøves i hemmelighet. Dette medfører igjen til at det må stilles strenge krav for metodebruken.[131]

I den nye og ledende storkammerdommen *Roman Zakharov* fra 2015 oppsummerte EMD kravet om forutberegnelighet knyttet opp til myndighetenes bruk av overvåkingsmetoder slik; «The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures».[132] Videre må loven, i mangel av innsyn fra den tiltaket retter seg mot og fra offentligheten; «…indicate the scope of any such discretion conferred on the

---

[128] Dommen ble avsagt under dissens 3 mot 2, hvor mindretallet var uenig i at Grunnloven stilte opp andre kvalitetskrav «enn det som ellers gjelder for regler som gir adgang til å foreta inngrep overfor enkeltpersoner», se dommens avsnitt 68 flg. Flertallets vurdering ble imidlertid fulgt opp enstemmig i HR-2016-1833-A.
[129] Korbely v. Hungary avsnitt 74-75, Silver and others v. UK avsnitt 86-89, Roman Zakharov v. Russia avsnitt 239-242. Se også Aall (2015) s. 133-135.
[130] Roman Zakharov v. Russia avsnitt 229 mvh. og Szabó and Vissy v. Hungary avsnitt 62.
[131] Se note 130.
[132] Roman Zakharov v. Russia avsnitt 229 mvh.

competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference».[133]

Praksis fra EMD viser at det essensielle når det gjelder hemmelig overvåking er at borgerne gis en adekvat indikasjon på i hvilke omstendigheter og på hvilke vilkår myndighetene kan benytte seg av slike metoder, der det bærende hensynet er å gi en tilfredsstillende beskyttelse mot vilkårlige inngrep. Følgelig stilles det et strengt presisjonskrav til lovgivningen om overvåking, særlig på grunn av den teknologiske utviklingen gjør metodebruken mer inngripende. Ut fra dette presisjonskravet kan man utlede at hjemmelsloven må være tilstrekkelig klar både i relasjon til når og på hvilke vilkår overvåking kan skje, og hvordan overvåkingen teknisk gjennomføres. Det må være på det rene at prinsippene som EMD har trukket opp når det gjelder hemmelig overvåking også må legges til grunn ved bruk av dataavlesing.[134] Som selvstendig metode innebærer dataavlesing at det er den *kontinuerlige bruken* som overvåkes, og begrenser seg dermed ikke kun til kommunikasjon. En slik overvåking av *enhver* aktivitet i et datasystem tilsier at inngrepets styrke intensiveres, jfr. tidligere drøftelse i pkt. 2.2.3 og 4.2.1. Når dataavlesing innebærer et intensivert inngrep i retten til privatliv, tilsier de overnevnte prinsippene som EMD har trukket opp knyttet til hemmelig overvåking, at presisjonskravet i lovgivningen skjerpes ytterligere.

I EMDs praksis om hemmelige overvåkingsmetoder har domstolen stilt opp visse minimumskriterier («minimum safeguards») som lovgivningen må tilfredsstille;

> «In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of offences which may give rise to an interception order; the 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 the 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»[135]

---

[133] Roman Zakharov v. Russia avsnitt 230 mvh.
[134] Se Bykov v. Russia avsnitt 79.
[135] Roman Zakharov v. Russia avsnitt 231 mvh. og Szabó and Vissy v. Hungary avsnitt 56, sml. Høyesteretts uttalelse i note 128 ovenfor.

Uttalelsen viser at lovgivningen, i tillegg til å inneha et visst presisjonsnivå knyttet opp mot de materielle vilkårene, også må inneha visse prosessuelle rettssikkerhetsgarantier for å sikre mot vilkårlig overvåking. Loven må gi uttrykk for varigheten til overvåkingen, regler for bruk, lagring og utlevering av de registrerte opplysningene, samt regler for når de innhentede opplysningene bør og skal slettes. Videre har EMD fremholdt at når det gjelder hemmelig overvåking, er det nær sammenheng mellom presisjonskravet som stilles til lovgivningen og vurderingen av om inngrepet er nødvendig i et demokratisk samfunn, noe som medfører at lovkravet og nødvendighetsvurderingen etter omstendighetene kan vurderes under ett.[136]

Hvorvidt dataavlesing i forebyggende øyemed tilfredsstiller kravet om tilstrekkelig hjemmel, beror etter dette på om inngrepet har hjemmel i lov og om loven i så fall tilfredsstiller de kvalitetskravene som kreves.

4.2.2.2 Tilfredsstiller den norske lovgivningen kravet om tilstrekkelig hjemmel?

Adgangen til å benytte dataavlesing i forebyggende øyemed følger av pl. § 17d med videre henvisning til bestemmelsen i strpl. § 216o om dataavlesing. Lovbestemmelsene er formelt vedtatt av Stortinget, og offentlig tilgjengelig for allmennheten. Bestemmelsene fyller dermed i utgangspunktet kravet om *formell lov* og tilgjengelighet. Som det følger av avhandlingen ovenfor stiller det norske legalitetsprinsippet, jfr. Grl. § 102, jfr. § 113, og EMDs praksis, videre et krav om at loven er tilstrekkelig klar og presis.

Vurderingstemaet er om dataavlesing i forebyggende øyemed, jfr. pl. § 17d, jfr. strpl. § 216o, gir en tilstrekkelig klar og presis lovhjemmel slik at borgerne kan forutberegne sin rettsstilling.[137] Av relevans for vurderingen vil være om loven gir borgeren en tilstrekkelig indikasjon på når og på hvilke vilkår PST kan benytte seg av dataavlesing i forebyggende øyemed. Avgjørende for vurderingen er om hjemmelsloven er utformet tilstrekkelig presist hva gjelder materielle vilkår, metodens karakter og gjennomføringsmåte, samt prosessuelle rettssikkerhetsgarantier. Det vises her til om loven tilfredsstiller de minimumskriteriene som er oppstilt i EMDs praksis knyttet opp mot hemmelige overvåkingsmetoder, jfr. drøftelsen ovenfor.

Dataavlesing i forebyggende øyemed kan etter pl. § 17d kun benyttes når det er «grunn til å undersøke om noen forbereder en handling» som rammes av en nærmere bestemt katalog av

[136] R.E v. UK avsnitt 122. I samme retning, se Szabó and Vissy v. Hungary avsnitt 58.
[137] Jfr. Roman Zakharov v. Russia avsnitt 228-230, jfr. tidl. drøftelse.

straffbare handlinger. Som det fremgår av pkt. 3.2.1 kan det innfortolkes tre elementer i dette grunnvilkåret; et mistankekrav, krav om formålsbestemthet og et kriminalitetskrav. Ordlyden i bestemmelsen gir etter dette en klar indikasjon på hvem dataavlesing kan anvendes ovenfor.

EMD har fremholdt at lovgivningen ikke må gi en uttømmende oppregning av de straffbare handlingene som kan gi grunn til inngrep, men at «sufficient detail should be provided on the nature of the offences in question».[138] Det avgjørende er om lovgivningen gir en tilstrekkelig indikasjon på hvilke omstendigheter som kan gi grunnlag for dataavlesing. Videre stilles ikke et uttrykkelig krav om formålsbestemthet, men når det gjelder inngrep på grunnlag av «national security» må loven angi rekkevidden av inngrepet slik at borgerne får en tilstrekkelig beskyttelse mot vilkårlige inngrep.[139] Lovgivningen må altså gi uttrykk for hvilke straffbare handlinger og til hvilket formål som kan gi grunnlag for dataavlesingen.

Dataavlesing kan kun benyttes i forebyggende øyemed dersom det foreligger objektive og ytre konstaterbare holdepunkter som gir grunn til å undersøke om noen forbereder visse særskilt oppgitte og alvorlige straffbare handlinger. Handlingene som rammes av bestemmelsen er konkretisert gjennom henvisning til straffeloven, og fremgår uttrykkelig av bestemmelsen i pl. § 17d. Videre må undersøkelsen være saklig begrunnet i PSTs forebyggende virksomhet. Samlet sett gir den norske lovgivningen borgerne tilstrekkelig indikasjon på hvilke handlinger som kan begrunne dataavlesing i forebyggende øyemed, og hvilke omstendigheter som må være til stede for at dataavlesing skal kunne bli anvendt. Den norske lovgivningen må følgelig anses å oppfylle klarhetskravet på dette punktet.

Videre må lovgivningen gi borgerne en tilstrekkelig indikasjon på hva inngrepet kan innebære, herunder hvordan inngrepet gjennomføres.[140] Dette er nødvendig for at borgeren skal kunne forutse hvilke inngrep som han kan utsettes for, og at inngrepet ikke skal virke vilkårlig.

Etter strpl. § 216o første ledd kan politiet foreta en «avlesing av ikke offentlige tilgjengelige opplysninger i et datasystem». Bestemmelsen i første ledd må leses sammen med fjerde ledd hvor det fremgår at: «Det kan bare gis tillatelse til å avlese bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- eller lagringstjenester som den mistenkte

[138] Roman Zakharov v. Russia avsnitt 243-244. Se også Szabó and Vissy v. Hungary avsnitt 64.
[139] Roman Zakharov v. Russia avsnitt 247 og Szabó and Vissy v. Hungary avsnitt 65.
[140] Roman Zakharov v. Russia avsnitt 230-231.

besitter eller kan antas å ville bruke. Avlesingen *kan* omfatte kommunikasjon, elektronisk lagrede data eller andre opplysninger om bruk av datasystemet eller brukerkontoen.» (min utheving). Ordlyden i seg selv gir liten veiledning på hva som menes med en «avlesing» og hva som nærmere ligger i definisjonen av et «datasystem». Ordlyden fremstår heller ikke som uttømmende når det kommer til hva som kan avleses.

Når det gjelder hva som kan avleses viser forarbeidene til at valget av betegnelsen «datasystem» var begrunnet i at begrepet var forholdsvis teknologinøytralt, og passet godt til det tilsiktede virkeområdet for dataavlesing.[141] Departementet har ikke begrunnet hvorfor de valgte betegnelsen «datasystem» fremfor den videre betegnelsen «informasjonssystem» som var foreslått av både Politimetodeutvalget og Metodekontrollutvalget, samt anvendt i den danske bestemmelsen om dataavlesning.[142] Dette kan lede til usikkerhet om hvilke systemer som rent faktisk faller innenfor bestemmelsens anvendelsesområde.

I forarbeidene fremgår det at begrensningene til hvilken informasjon som kan avleses teknisk sett bare følger av hva slags informasjonssystem det dreier seg om og funksjonaliteten til program- eller maskinvaren som benyttes.[143] I prinsippet vil dataavlesing kunne være enhver registrering av data i datasystemet, alt fra lydstrøm, tastetrykk, videostrøm, til lagrede data, GPS-koordinater, kommunikasjon osv. Dette illustrerer at det er et misforhold mellom bestemmelsens ordlyd og forarbeidene på hva dataavlesing i realiteten kan innebære. Slik dataavlesing er innført vil det være mer eller mindre mulig å kontinuerlig overvåke bruken av et datasystem i sanntid. Det må dermed anses som problematisk at ordlyden ikke er mer utførlig når det kommer til hva som rent faktisk omfattes av overvåkingen.

Departementet åpnet for at politiet fortløpende kunne gjøre seg kjent med bruken av et datasystem, og begrenset seg dermed ikke kun til å muliggjøre kommunikasjonsavlytting og hemmelig ransakelse slik som Metodekontrollutvalget gjorde.[144] Etter departementets vurdering var en slik utvidelse nødvendig for å kunne møte utfordringen knyttet til kryptering og moderne kommunikasjonstjenester på en effektiv måte, og dermed dekke det anførte

---

[141] Prop. 68 L (2015-2016) s. 270, se for øvrig tidl. redegjørelse ovenfor under pkt. 2.2.2.
[142] Se note 34. Departementet berører ikke spørsmålet annet enn å nevne at «*informasjonssystem* som begrep sies å favne videre enn *kommunikasjonsanlegg*» og departementet «bruker … betegnelsen «*datasystem*» synonymt med informasjonssystem», se Prop. 68 L (2015-2016) s. 224. Det er usikkert hvilken betydning dette har for metodens karakter når det gjelder hva som avleses og hvordan avlesingen kan gjennomføres, men det kan være et uheldig valg fra departementets side mht. kravet om lovhjemmel.
[143] Prop. 68 L (2015-2016) s. 224.
[144] Prop. 68 L (2015-2016) s. 264-265.

behovet. Det er dermed oppsiktsvekkende at når departementet på den ene siden uttrykkelig åpner for at metoden skal gå ut på å overvåke bruken av et datasystem i sanntid, samtidig begrenser ordlyden til kun å nevne «kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen». Den kontinuerlige overvåkingen av et datasystem i sanntid må dermed innfortolkes i passusen om at dataavlesing *kan* omfatte «andre opplysninger om bruk». Det må anses uheldig at ordlyden er såpass snever og uklar på dette punktet.

Om den nærmere gjennomføringen presiserer strpl. § 216p første ledd at dataavlesing «*kan* foretas ved hjelp av tekniske innretninger, dataprogram *eller på annen måte*» (min utheving). Ved at ordlyden viser til «tekniske innretninger» og «dataprogram» er det tydelig at bestemmelsen viser til den hardware- og software-baserte fremgangsmåten som kommer til uttrykk i forarbeidene. Imidlertid er det en kuriositet at departementet valgte ordet «kan» fremfor en direkte anvisning til hvordan dataavlesing skal skje. Videre ved å innta passusen «eller på annen måte» åpner ordlyden for at dataavlesing kan skje på en ikke nærmere angitt måte. Ordlyden fremstår dermed som noe uklar når det kommer til hvordan dataavlesing vil gjennomføres.[145]

I forarbeidene ga departementet uttrykk for at politiet burde ha stor valgfrihet når det kommer til valg av fremgangsmåte, samt at det var ansett uhensiktsmessig å komme med en uttømmende beskrivelse av gjennomføringsmåten for dataavlesing.[146] Det er dermed et bevisst valg å gi politiet et vidt skjønn i valg av gjennomføringsmåte. Departementets valg om å gi politiet et vidt skjønn i valg av gjennomføringsmåte står i et motsetningsforhold til EMDs praksis knyttet opp mot hemmelige overvåkingsmetoder. I EMDs storkammerdom *Roman Zakharov v. Russia* viste EMD til at det var særlig den teknologiske utviklingen som gjorde det nødvendig med et presist regelverk knyttet til overvåkingsmetoder.[147] Det er dermed betenkelig at lovgiver rettferdiggjør et lite presisjonsnivå i lovgivningen under henvisning til at det er hensiktsmessig med hensyn til den teknologiske utviklingen. Forarbeidene gir uttrykk for at ordlyden i strpl. § 216p første ledd må forstås slik at politiet skal kunne benytte tekniske hjelpemidler, programvare og kunnskap for å gjennomføre avlesingen.[148] Det er

[145] Til sammenligning se den danske bestemmelsen om «dataaflæsning» i retsplejeloven § 791 b som anviser at avlesingen kan skje «ved hjælp av programmer eller andet udstyr».
[146] Prop. 68 L (2015-2016) s. 264.
[147] Roman Zakharov v. Russia avsnitt 229-231.
[148] Prop. 68 L (2015-2016) s. 271.

dermed den utstyrs- og informasjonsbaserte varianten av dataavlesing som er aktuelle gjennomføringsmåter, jfr. drøftelsen ovenfor i pkt. 2.2.3. Ordlyden, sammenholdt med forarbeidene gir dermed en noenlunde klarere indikasjon på hvordan dataavlesing nærmere kan gjennomføres.

På den ene siden kan det aksepteres at politiet ut fra et taktisk perspektiv har et visst behov for hemmelighold rundt de tekniske detaljene for metodebruken. På den annen side er det et viktig hensyn borgerne er klar over hvilke overvåkingsmetoder staten bruker for å forhindre vilkårlighet og ivareta den enkeltes rettssikkerhet. I EMD har domstolen flere ganger idømt brudd på konvensjonen som følge av manglende detaljert regelverk.[149] Dette tilsier at hjemmelen er for upresis i det henseende at kun en anvisning til utstyrs- og informasjonsbasert dataavlesing åpner for et udefinert spektrum av gjennomføringsmåter med tilhørende problemstillinger. Blant annet gir ikke lovgivningen noen indikasjon på opprinnelsen til den programvaren eller utstyret som benyttes. Dersom f. eks polititrojaneren som benyttes, er et alminnelig og kommersielt tilgjengelig produkt foreligger det et viss misbrukspotensiale hos tredjepersoner. På bakgrunn av dette ville det vært ønskelig om lovgivningen stilte nærmere krav til hvilke utstyr og programvare som skulle benyttes, herunder krav om at teknologien som anvendes er produsert nasjonalt og jevnlig oppdatert for å sikre mot misbruk.[150]

Videre oppstiller § 216p kvalitative krav til gjennomføringen av dataavlesingen. Etter strpl. § 216p første ledd første punktum kreves det at avlesingen kun skal utføres av særskilt skikket personell utpekt av Sjef-PST. Videre i annet ledd følger det at avlesingen skal innrettes slik at det ikke unødig fanges opp opplysninger om andre enn den avlesingen retter seg mot, og at datasystemet ikke unødig kompromitteres. Bestemmelsen må forstås slik at politiet plikter å påse at utstyret eller programvaren som brukes ikke har nevneverdige svakheter, herunder utsetter datasystemet for unødig fare for misbruk. Bestemmelsen i § 216p om gjennomføringen av dataavlesing viser at den norske lovgivningen har visse svakheter med hensyn til presisjonsnivået, samtidig som at det oppstilles prosessuelle rettssikkerhetsgarantier gjennom kvalitative krav til metodebruken. Det kan dermed være vanskelig å gi en

[149] Se bl.a. Bykov v. Russia avsnitt 76-83 og Huvig v. France avsnitt 32-35
[150] Se Sunde (2012) s. 30 flg.

konklusjon på om hvorvidt den norske lovgivningen tilfredsstiller det presisjonsnivået som kreves for hemmelige overvåkingsmetoder.

Videre må lovgivningen angi en «limit on the duration» av inngrepet.[151] Etter pl. § 17e første ledd kan det unntaksvis gis tillatelse til å bruke tvangsmidler i forebyggende øyemed inntil 6 måneder dersom det foreligger «særlige grunner». Utgangspunktet er dermed 4 eller 8 uker med fornyet prøving. Grunnen til at det gis en lengre adgang for bruk av tvangsmidler i forebyggende øyemed er at det forebyggende arbeidet gjerne har et lengre tidsperspektiv enn tilsvarende bruk under etterforskning.[152] Etter strpl. § 216o femte ledd gjelder strpl. §§ 216d til 216k tilsvarende slik at det ikke kan gis tillatelse for avlesing i mer enn to uker om gangen. Dette begrunnes i at dataavlesing etter omstendighetene kan fremstå som et større integritetsinngrep enn kommunikasjonsavlytting, noe som tilsier hyppigere prøving av om det er grunnlag for inngrep.[153] Forarbeidene gir imidlertid ikke uttrykk for om den samme regelen gjelder for bruk av dataavlesing i forebyggende øyemed. Ut fra et lex specialis-prinsipp må man anta at det er regelen i pl. § 17e som gjelder for bruk av dataavlesing i forebyggende øyemed. Det er uheldig at forarbeidene ikke gir en avklaring på spørsmålet.

Til slutt stilles det krav til tilstrekkelige regler og retningslinjer for bruk, lagring og utlevering av de registrerte opplysningene, samt regler for når de innhentede opplysningene bør og skal slettes.[154]

I pl. § 17f er det gitt en særlig bestemmelse om bruk av opplysninger som er innhentet med forebyggende tvangsmidler. Bestemmelsen har to sider. For det første er det underlagt taushetsplikt at det er begjært eller besluttet bruk av tvangsmidler i forebyggende øyemed, samt om opplysningene som fremkommer av tvangsmiddelbruken, jfr. første ledd. For det andre lister bestemmelsen opp en rekke tilfeller hvor taushetsplikten ikke er til hinder for at opplysningene brukes, jfr. annet ledd bokstav a til e. Bestemmelsen sier imidlertid ingenting om når materialet fra overvåkingen kan eller må slettes eller tilintetgjøres.[155] Bestemmelsen i

[151] Roman Zakharov v. Russia avsnitt 231.
[152] Ot.prp.nr.60 (2004-2005) s. 153.
[153] Prop. 68 L (2015-2016) s. 272-273.
[154] Roman Zakharov v. Russia avsnitt 231 mvh.
[155] Cfr. Strpl. § 216g som gir en regel om sletteplikt i etterforskningssaker.

pl. § 17f må leses i sammenheng med politiregisterloven kpt. 11 og politiregisterforskriften del 6 hvor det gis særregler for PSTs behandling av registrerte opplysninger.[156]

Etter pregl. § 64 og politiregisterforskriften § 21-1, jfr. § 20-2 stilles det krav om nødvendighet og formålsbestemthet for PSTs behandling av opplysninger. I forbindelse med opprettelse av forebyggende sak eller første gangs behandling av opplysningen skal formålet med behandlingen angis konkret, jfr. § 20-2 tredje ledd. Bestemmelsen sikrer at det er notoritet rundt PSTs behandling av opplysninger.[157] Utover dette sier lovgivningen lite om hvordan det sikres notoritet rundt bruken av opplysningene.

Når det gjelder sletting av opplysninger, følger det av pregl. § 50 og politiregisterforskriften § 22-3 første ledd første punktum at opplysningene ikke skal lagres lengre enn formålet med behandlingen. Etter forarbeidene må bestemmelsen forstås slik at opplysningene skal slettes når formålet er bortfalt.[158] Etter politiregisterforskriften § 22-3 første ledd annet punktum skal opplysninger som kan ha betydning som dokumentasjon av notoritetshensyn sperres. De samme gjelder ved avslutning av forebyggende sak, jfr. fjerde ledd Ved at opplysningene sperres, sikrer man at det kan skje en faktisk etterfølgende kontroll av EOS-utvalget, samtidig som man hindrer videre behandling av opplysningene.

Reglene for bruk, lagring og utlevering av opplysninger, samt om sletting og sperring, er dermed utførlig regulert i politiregisterloven og politiregisterforskriften. Det kunne vært hensiktsmessig om reglene i politiregisterloven og politiregisterforskriften var tydeligere henvist til i pl. § 17f. Videre er det uheldig at lovgiver ikke vurderte problematikken rundt sletting av opplysninger som stammer fra skjult tvangsmiddelbruk ytterligere i lovforarbeidet. Som lovverket er utformet i dag er det noe uklart når endelig sletting av opplysningene må finne sted. Dette kan tale for regelverket ikke utgjør en tilstrekkelig prosessuell rettssikkerhetsgaranti, til tross for å være tilsynelatende utførlig regulert.

---

[156] Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (pregl.) og Forskrift av 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten.
[157] I 2015 fant EOS-utvalget flere kritikkverdige forhold hos PST når det gjaldt oppbevaring, bruk og sletting av opplysninger, til tross for et utførlig regelverk, se EOS-utvalgets årsmelding 2015 s. 15-20. I årsmeldingen for 2016 fant utvalget kritikkverdig lagring og behandling av opplysninger utenfor det ordinære etterretningssystemet, se EOS-utvalgets årsmelding 2016 s. 19-20. Se også NOU 2009:15 s. 253 flg. om tilsvarende problem når det gjaldt opplysninger som stammet fra kommunikasjonskontroll i etterforskningssaker.
[158] Ot.prp.nr. 108 (2008-2009) s. 317-318.

Samlet sett er det usikkert om den norske lovgivningen om dataavlesing i forebyggende øyemed tilfredsstiller kravet til lovhjemmel.

4.2.3 Inngrepet må ivareta et legitimt formål

Videre må inngrepet i privatlivet etter Grl. § 102 være begrunnet i et legitimt formål for å anses som rettmessig.[159] Etter EMK art. 8 nr. 2 kan et inngrep begrunnes bl.a. i: «the interests of national security, (…) the prevention of crime and disorder, (…) or for the protection of the rights and freedoms of others». Når Lønning-utvalget vurderte å lovfeste en begrensningshjemmel ved grunnlovsrevisjonen av 2014, ble det videre vist til de samme formålene som kunne begrunne et inngrep etter EMK art. 8 nr. 2.[160] Dette må tas til inntekt for at de samme formålene kan begrunne et inngrep etter Grl. § 102.[161]

Dataavlesing i forebyggende øyemed har som formål å forebygge alvorlige straffbare handlinger som kan utgjøre en fare for rikets sikkerhet og borgernes liv og helse. Ved at lovgiver har vedtatt pl. § 17d som tillater bruk av dataavlesing i forebyggende øyemed ligger det implisitt at inngrep i Grl. § 102 tillates under henvisning til «national security».[162] Dette vil følgelig bli godtatt av domstolene om at inngrepet skal ivareta et legitimt formål. Kravet om å ivareta et legitimt formål må derfor anses oppfylt.

4.2.4 Inngrepet må være forholdsmessig

4.2.4.1 Hva ligger i kravet om forholdsmessighet?

I tillegg til at et rettmessig inngrep må tilfredsstille kravet om hjemmel i lov og ivareta et legitimt formål, stilles det også et krav om at inngrepet må være forholdsmessig.[163] En naturlig forståelse av «forholdsmessig» er at de interessene som inngrepet søker å verne må stå i et rimelig forhold til de interessene som inngrepet griper inn i. Høyesterett har lagt til grunn at forholdsmessighetsvurderingen «må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre».[164] Sett i sammenheng med uttalelsen om at Grunnloven skal tolkes «i

---

[159] Rt. 2015 s. 93 avsnitt 60.
[160] Se Dok.nr.16 (2011-2012) s. 74.
[161] Se Rt. 2015 s. 1456 avsnitt 22 hvor Høyesterett anså kravet om legitimt formål som oppfylt der kommunikasjonsavlytting var motivert bl.a. kriminalitetsbekjempelse. Se også Prop. 68 L (2015-2016) s. 172 og s. 185, jfr. s. 214.
[162] Se Auglend & Mæland (2016) s. 314 flg. om forebyggende virksomhet, cfr. s. 347 flg. om PST.
[163] Rt. 2014 s. 1105 avsnitt 28, Rt. 2015 s. 93 avsnitt 60 og Rt. 2015 s. 155 avsnitt 52. Se tidligere drøftelse i pkt. 4.1.
[164] Rt. 2015 s. 93 avsnitt 60. Se også Høyesteretts formulering i HR-2016-2554-P på avsnitt 82.

lys av de folkerettslige forbildene», ser man at forholdsmessighetsvurderingen som skal foretas etter Grunnloven § 102 er nokså sammenfallende med vurderingen om at inngrepet må være «necessary in a democratic society» etter bl.a. den tilsvarende bestemmelsen i EMK art. 8.[165]

Etter fast konvensjonspraksis skal kravet om nødvendighet («necessary») forstås som at et rettmessig inngrep korresponderer til «a pressing social need» og at det er «proportionate to the legitimate aim pursued».[166]

I spørsmålet om hva som er «nødvendig» har EMD uttrykt at medlemsstatene står nærmere til å foreta den konkrete vurderingen, og domstolen har innrømmet medlemsstatene en skjønnsmargin («margin of appreciation») i vurderingen.[167] Hvor vid skjønnsmarginen er vil kunne variere avhengig av hvilken rett det er tale om, rettens betydning for individet, inngrepets art og formålet bak inngrepet.[168] EMD presiserer likevel at skjønnsmarginen ikke gir statene fritt spillerom, og at EMD kan foreta den endelige vurderingen av om inngrepet er i tråd med konvensjonen.[169] Skjønnsmarginen innebærer med andre ord at EMD tillegger statenes egne vurderinger mer eller mindre vekt, og er tilbakeholden med å overprøve de nasjonale vurderingene.[170] Ved valg av hemmelige etterretnings-/etterforskningsmetoder som griper inn i individets rett til privatliv ved beskyttelse av rikets sikkerhet eller kriminalitetsbekjempelse, har EMD innrømmet nasjonale myndigheter en viss skjønnsmargin («a certain margin of appreciation»).[171] Begrunnelsen er at de nasjonale myndigheter står nærmere til å vurdere hvilke tiltak som er nødvendig for å beskytte nasjonal sikkerhet.[172]

Det første elementet i nødvendighetsvurderingen er om inngrepet korresponderer til et pressende samfunnsbehov. På grunn av skjønnsmarginen i saker om «national security» har EMD vært tilbakeholden med å overprøve behovet, og har istedenfor nøyd seg med å vurdere de nasjonale myndigheters begrunnelse for inngrepet. Avgjørende er ofte hvorvidt

---

[165] Keegan v. Ireland avsnitt 30 og Lindheim and others v. Norway avsnitt 119. Se også Prop. 68 L (2015-2016) s. 37-38.
[166] Olsson v. Sweden avsnitt 67 og Paradiso and Campanelli v. Italy avsnitt 181.
[167] Se bl.a. Handyside v. UK avsnitt 48 og Klass and others v. Germany avsnitt 49.
[168] S. and Marper v. UK avsnitt 102. Se også Kjølbro (2017) s. 768-769
[169] Se de to forrige notene.
[170] Aall (2015) s. 158 flg.
[171] Klass and others v. Germany avsnitt 48-49 og Roman Zakharov v. Russia avsnitt 232 mvh.
[172] Harris mfl. s. 14 flg. og s. 510 flg, se også Schabas (2015) s. 78-83 og Kjølbro (2017) s. 767.

myndighetenes begrunnelse for inngrep fremstår som «relevant and sufficient».[173] I vurderingen av om lovgivers begrunnelse for inngrep er «relevant and sufficient» har EMD vist til at inngrepet må ha en tilknytning til det legitime formålet som begrunner inngrepet.[174]

Dersom det kan påvises et pressende samfunnsbehov, og myndighetenes begrunnelse anses som 'relevant and sufficient', vil det andre elementet i nødvendighetsvurderingen være om inngrepet er proporsjonalt i forhold til det legitime formålet. Denne delen av nødvendighetsvurderingen knytter seg til forsvarligheten av inngrepet, hvor vurderingstemaet er om det etter omstendighetene var nødvendig å gå frem på en så inngripende måte.[175] Kjernen i vurderingen er at;

> «(…) there must also be a reasonable relation of proportionality between the means employed and the aim sought to be realised by any measures applied by the State (…). That requirement is expressed by the notion of a 'fair balance' that must be struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights.»[176]

I at det må være en 'fair balance' tilsier at desto viktigere den enkeltes rettighet som det gripes inn i står seg, desto sterkere grunner kreves for at inngrepet skal anses proporsjonalt. Det er ulike momenter som kan inngå i denne vurderingen, blant annet om inngrepet er egnet til å oppnå formålet og om formålet kan oppnås ved lempeligere midler.[177] Avgjørende for vurderingen er at inngrepet ikke går lengre enn nødvendig.
EMD har, i lys av fremveksten av alvorlige trusler mot nasjonal sikkerhet, slått fast at det kan være nødvendig i et demokratisk samfunn å tillate inngripende hemmelige overvåkingsmetoder i lovgivningen for å imøtegå truslene mot nasjonal sikkerhet.[178]
Imidlertid har det i EMDs praksis om hemmelige overvåkingsmetoder blitt presisert 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,

[173] Se bl.a. S. and Marper v. UK avsnitt 101, Paradiso and Campanelli v. Italy avsnitt 179 og Handyside v. UK avsnitt 50.
[174] Se bl.a. Paradiso and Campanelli v. Italy avsnitt 197 og Szabó and Vissy v. Hungary avsnitt 54-57 og 72-73.
[175] Aall (2015) s. 156 og Harris m.fl. s. 519 flg.
[176] Lindheim and others v. Norway avsnitt 119.
[177] Aall (2015) s. 156-157, Kjølbro (2017) s. 768 og Harris m.fl. (2014) s. 519-520.
[178] Klass and others v. Germany avsnitt 48.

> the Court must be satisfied that there are adequate and effective guarantees against abuse.»[179]

Uttalelsen, som gjentas i EMDs praksis om hemmelige overvåkingsmetoder, illustrerer poenget om den nære sammenhengen mellom lovkravet og om inngrepet anses 'necessary in a democratic society'. Som tidligere nevnt i pkt. 4.2.2 kreves det at de prosessuelle rettssikkerhetsgarantiene kommer tilstrekkelig klart frem i lovgivningen slik at borgerne kan forutberegne rettsstillingen sin. Videre vil det ha betydning i relasjon til om inngrepet anses å være 'necessary'. Dersom det ikke foreligger tilstrekkelige og effektive rettssikkerhetsgarantier vil ikke lovgivningen om inngripende overvåking kunne anses å være nødvendig og proporsjonal. Avgjørende i den relasjon er om hvorvidt de rettssikkerhetsgarantiene som er oppstilt i lovgivningen begrenser inngrepet til det som er forholdsmessig ('necessary in a democratic society').[180]

De siste årene har det skjedd en endring i EMDs konvensjonspraksis når det kommer til prøving av påståtte konvensjonsbrudd.[181] Istedenfor å foreta en indre materiell prøving av om det foreligger et konvensjonsbrudd, har EMD i flere tilfeller nøyd seg med å foreta en såkalt 'ytre prosessuell' kontroll av om inngrepet fremstår som nødvendig.[182]

Et nyere eksempel på denne utviklingen er i EMDs storkammerdom *Perinçek v. Switzerland*. Saken gjaldt anført brudd på EMK art. 10 ved ileggelse av straff for offentlige uttalelser som fornektet Det armenske folkemordet i 1915. Om avveiningen mellom klagerens rett til ytringsfrihet og armenernes rett til respekt for privatlivet uttalte EMD følgende;

> «(…) [T]he High contracting parties are afforded a margin of appreciation in that respect, but only if their authorities have undertaken the balancing exercise in conformity with the criteria laid down in the Court's case law and have duly considered the importance and scope of the rights at stake.»[183]

---

[179] Klass and others v. Germany avsnitt 49-50, Roman Zakharov avsnitt 232 og Szabó and Vissy v. Hungary avsnitt 57.
[180] Roman Zakharov v. Russia avsnitt 232 mvh. og Dragojević v. Croatia avsnitt 83-84.
[181] Se bl.a. Austin and others v. UK, Lillo-Stenberg and Sæther v. Norway, Mouvement Raélien Suisse v. Switzerland og Animal Defender International v. UK.
[182] For nærmere redegjørelse av denne trenden i EMDs praksis, se Spano (2014), Rui (2013) og Sørensen (2014).
[183] Perinçek v. Switzerland avsnitt 274, jfr. avsnitt 198-199.

Videre når det gjaldt nasjonale myndigheter vurdering uttalte EMD at;

> «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.»[184]

I mangel av en avveining av de motstående rettighetene i spørsmålet om inngrepet var å anse som 'necessary in a democratic society' gikk EMD videre i avsnitt 279-281 for å selv foreta en avveining der de konkluderte med at inngrepet ikke kunne anses nødvendig. Dommen illustrerer at lovgiver må foreta en kartlegging og avveining av de motstående interessene eller rettighetene, og i mangel av en slik avveining vil myndighetenes skjønnsmargin tillegges mindre vekt.[185] Selv om saken *Perinçek v. Switzerland* gjaldt en avveining mellom EMK art. 8 og art. 10 så har uttalelsene en generell overføringsverdi når det kommer til avveiningen av motstående interesser som må foretas etter EMK art. 8.

I HR-2016-304-S viste Høyesterett, under henvisning til EMD praksis, at statens skjønnsmargin får «begrenset betydning for den konvensjonsrettslige bedømmelsen dersom lovgiver *ikke* har foretatt en kartlegging og avveining av de motstridene interessene».[186] Saken gjaldt tomtefeste, men illustrerer poenget om at en forutsetning for at EMD viker tilbake for å overprøve den nasjonale lovgivningen under henvisning til statenes skjønnmargin, er at lovgiver faktisk har foretatt en kartlegging og avveining av de motstridende interessene. Når spørsmålet om tomtefestelovens innløsningsregler var forholdsmessig etter EMK P1-1 skulle vurderes så Høyesterett hen til lovgivers begrunnelse for reglene om innløsningssum og de avveiningene som var gjort fra lovgivers side.[187] Etter inngående å ha sett på lovgivers vurderinger kom Høyesterett til at Stortinget hadde vært oppmerksom på og vektlagt bortfesteres interesser i lovforarbeidet.[188]

Dommen viser at også Høyesterett legger vekt på om hvorvidt lovgiver har foretatt en forholdsmessighetsvurdering etter EMK. Dommen kan tas til inntekt for at Høyesterett vil kunne vektlegge om hvorvidt lovgiver har foretatt en 'kartlegging og avveining av motstående

---

[184] Perinçek v. Switzerland avsnitt 278, jfr. avsnitt 274-277.
[185] I samme retning, se Lindheim and others v. Norway avsnitt 128, jfr. avsnitt 119 flg.
[186] HR-2016-304-S avsnitt 50-51.
[187] HR-2016-304-S avsnitt 60.
[188] HR-2016-304-S avsnitt 61-70, jfr. avsnitt 60.

interesser' i relasjon til forholdsmessighetsvurderingen etter Grl. § 102. For avhandlingens del betyr det at lovgiver må ha vurdert nødvendigheten med å innføre dataavlesing i forebyggende øyemed, samt foretatt en 'kartlegging og avveining av motstående interesser'. Dersom lovgiver ikke har foretatt en slik avveining vil det kunne tas til inntekt for at det foreligger en «prosessuell» krenkelse av Grl. § 102.

I norsk rett har norske domstoler en rett og plikt til å prøve om lovgivningen strider mot Grunnloven.[189] I Høyesteretts praksis har det utviklet seg visse trekk knyttet til domstolens prøvingsintensitet av grunnlovmessigheten. Høyesterett uttalte i *Kløfta*-dommen at prøvingsintensiteten «(…) vil avhenge av hvilke grunnlovsbestemmelser det er tale om. Gjelder det bestemmelser til vern om enkeltmenneskets personlige frihet eller sikkerhet, antar jeg at grunnlovens gjennomslagskraft må være betydelig.».[190] Videre uttalte Høyesterett at: «(…) Stortingets forståelse av lovens forhold til slike grunnlovsbestemmelser må spille en betydelig rolle når domstolene skal avgjøre grunnlovmessigheten, og domstolene må vise varsomhet med å sette sin vurdering over lovgiverens», og at Høyesterett vil «(…) vike tilbake for å konstatere grunnlovsstrid i tilfelle hvor det foreligger rimelig tvil, og hvor Stortinget klart har vurdert og bygd på at loven ikke kommer i strid med grunnloven». Dommen er fulgt opp i en rekke senere dommer i Høyesterett.[191]

Høyesteretts praksis viser at Høyesterett tillegger Stortingets vurdering liten vekt i vurderingen av lovgivningens grunnlovmessighet når det gjelder grunnrettigheter som verner «enkeltmenneskers frihet og sikkerhet». Det må kunne antas at retten til privatliv etter Grl. § 102 faller inn i denne kategorien, og at Høyesterett ikke nødvendigvis vil tillegge lovgivers vurdering av grunnlovmessigheten særlig stor vekt. Høyesteretts praksis om prøvingsintensiteten av norsk lovgivnings grunnlovmessighet, sett i sammenheng med EMDs praksis om en 'ytre prosessuell kontroll' og HR-2016-304-S, jfr. drøftelsen ovenfor, kan dermed tyde på at Høyesterett vil kunne tillegge lovgivers vurdering mindre vekt i vurderingen av om dataavlesing i forebyggende øyemed er i strid med Grl. § 102, til tross for at lovgiver har foretatt en 'kartlegging og avveining av de motstridende interessende'.

[189] Jfr. Grl. § 89.
[190] Rt. 1976 s. 1 på s. 5-6.
[191] Rt. 1996 s. 1415 på s. 1429, Rt. 1997 s. 1821 på s. 1831 og Rt. 2007 s. 1281 avsnitt 72-76.

Det er ikke nødvendigvis slik at Høyesterett vil legge til grunn en tilsvarende forholdsmessighetsvurdering etter Grl. § 102 som etter EMK. Likevel ettersom Høyesterett har lagt til grunn en lik struktur og systematikk i forholdsmessighetsvurderingen som EMD, jfr. drøftelsen over i pkt. 4.1, er formodningen at Høyesterett minst vil legge de samme prosessuelle og materielle kravene til grunn i vurderingen etter Grl. § 102 som etter EMK art. 8.

4.2.4.2 Tilfredsstiller den norske lovgivningen kravet om forholdsmessighet?

Spørsmålet om dataavlesing i forebyggende øyemed er et forholdsmessig inngrep etter Grl. § 102 baserer seg som sagt på en sammensatt vurdering av om det foreligger et pressende samfunnsbehov og om inngrepet kan anses å være proporsjonalt. Vurderingstemaet er om lovgiver har vurdert nødvendigheten med å innføre dataavlesing i forebyggende øyemed, samt foretatt en kartlegging og avveining av de motstående interessene. Videre må inngrepet være nødvendig og proporsjonalt i forhold til det legitime formålet som ønskes oppnådd. Det avgjørende er om lovgiver har gitt en relevant og tilstrekkelig begrunnelse for å innføre dataavlesing i forebyggende øyemed, og at lovgivningen ikke går lengre enn det som er nødvendig, jfr. tidligere drøftelse.

Utgangspunktet for vurderingen må være at dataavlesing er en overvåkingsmetode som griper sterkt inn i den enkeltes rett til privatliv, og kan kun tillates i den grad det er nødvendig.[192]

Innføring av dataavlesing er hovedsakelig begrunnet i den teknologiske utviklingen, særlig fremveksten av avanserte krypteringsløsninger og nye former for elektroniske kommunikasjonstjenester.[193] Departementets oppfatning er at utredningen og høringen viser at de eksisterende skjulte tvangsmidlene har tapt mye av sin effekt som følge av den teknologiske utviklingen, og politiet står i større grad uten faktisk adgang til informasjonen til tross for at den rettslige adgangen er den samme. På grunn av dette mener departementet at det foreligger et behov for nye politimetoder for å kunne imøtegå utfordringene knyttet til den teknologiske utviklingen. Departementet har lagt til grunn at krypteringsproblematikken også gjør dataavlesing nødvendig i forebyggende øyemed.[194] Det må her tas i betraktning at PSTs virksomhet i stor grad skal være forebyggende, og at PSTs adgang til å benytte dataavlesing i forebyggende øyemed etter pl. § 17d er begrenset til å forebygge særlig alvorlige straffbare

[192] Klass and others v. Germany avsnitt 42, Roman Zakharov v. Russia avsnitt 232.
[193] Prop. 68 L (2015-2016) s. 12, jfr. s. 259 flg.
[194] Prop. 68 L (2015-2016) s. 259, s. 274 og s. 214-218 med videre henvisning til s. 184-189.

handlinger der det er et stort skadepotensiale.[195] I den henseende kan man si at behovet for inngrep gjør seg særlig gjeldende ettersom at inngrepets formål er å forebygge at svært alvorlige straffbare handlinger blir realisert.

Dataavlesing kan etter dette fremstå som nødvendig for å kunne imøtegå den teknologiske utfordringen da nye politimetoder vil sette politiet i stand til å omgå problematikken knyttet til kryptering. Således må dataavlesing også anses å være egnet til å oppnå formålet ved at PST settes i stand til å kunne forebygge alvorlige straffbare handlinger. Dette taler for at lovgivers begrunnelse for inngrep må anses som 'relevant'.

Den største motforestillingen mot å innføre dataavlesing som selvstendig metode er at det gjør det mulig å kunne overvåke bruken av datasystemet i sanntid. Spørsmålet er dermed om lovgiver har begrunnet nødvendigheten for en slik utvidelse, og at begrunnelsen er tilstrekkelig.

Metodekontrollutvalget pekte på at dataavlesing som selvstendig metode ville innebære en utvidelse av de eksisterende hjemlene, og mente at det ikke var dokumentert et tilstrekkelig behov for en slik utvidelse.[196] I motsetning var departementet av den oppfatning at Metodekontrollutvalgets forslag bare syntes å ta sikte på å overvinne krypteringsproblematikken, men ikke syntes å ta høyde for de teknologiske utfordringene mht. effektiv avlytting av kommunikasjon.[197] Departementet viste blant annet til problemer knyttet opp mot flyktige data og krypteringsnøkler, mistenktes sletting av informasjon og kommunikasjonsformer som ikke fanges opp gjennom kommunikasjonsavlytting.[198] Departementet var derfor av den oppfatning at dataavlesing som metode burde gi politiet anledning til å skaffe seg tilgang til opplysninger i et datasystem, herunder opplysninger om bruken av datasystemet over tid. Dette viser på den ene siden at departementets begrunnelse for å innføre dataavlesing som selvstendig metode er relevant. På den andre siden gir ikke departementets begrunnelse nødvendigvis uttrykk for hvorfor behovet er *annerledes* enn det som ble lagt til grunn i Metodekontrollutvalgets utredning. Dette kan tale imot innføringen av

[195] Prop. 68 L (2015-2016) s. 202.
[196] NOU 2009:15 s. 244.
[197] Prop. 68 L (2015-2016) s. 264.
[198] Prop. 68 L (2015-2016) s. 263-264, jfr. også s. 260-261.

dataavlesing som selvstendig metode i forebyggende øyemed er tilstrekkelig velbegrunnet, og kan anses som nødvendig.

Innføring av dataavlesing som metode kan medføre at kriminelle ved å tilpasse sin atferd gjør at metoden blir mindre egnet og effektiv enn ønsket. Den som dataavlesing retter seg mot kan f. eks benytte seg av stjålne datasystemer eller offentlig tilgjengelige datasystemer, og dermed i stor grad omgå politiet, til tross for at metoden imøtegår krypteringsproblematikken. Departementet synes ikke å ha vurdert problemstillingen opp mot metodens effektivitet, og kan tale mot at lovgivers begrunnelse er tilstrekkelig.

Departementet trekker frem at dataavlesing vil åpne for en mer målrettet og skånsom informasjonsinnhenting.[199] Tanken er at når avlesingen knytter seg opp til et spesifikt datasystem og behovet for et fysisk innbrudd blir mindre, vil færre tredjepersoner rammes av inngrepet. På den annen side vurderer ikke departementet om en kontinuerlig overvåking av et datasystem i sanntid vil kunne generere store mengder overskuddsinformasjon som potensielt kan ramme langt flere enn alminnelig kommunikasjonsavlytting vil, herunder uskyldige tredjepersoner som indirekte vil omfattes av overvåkingen.

Forarbeidene synes heller ikke å ha foretatt en kartlegging av risikoen for at dataavlesing vil åpne for misbruk av tredjepersoner, annet enn å vise til at det eksisterer en viss risiko for misbruk.[200] Det kan blant annet vises til at når politiet lager eller utnytter en bakdør i et datasystem så muliggjør det at også andre uvedkommende benytter seg av 'bakdøren' inn i datasystemet. Det foreligger også en fare for at politiets metoder selv kan bli kompromittert, som f. eks i dokumentsamlingen 'Vault 7', som ble lekket av WikiLeaks 7. og 23. mars 2017, ble store deler av CIAs verktøy for elektronisk overvåking gjort kjent for allmenheten.[201] Dette taler mot at departementets begrunnelse for å innføre dataavlesing er tilstrekkelig velbegrunnet, samtidig som det kan tilsi at metoden utgjør et uproporsjonalt inngrep i privatlivet.[202] På den andre siden oppstiller loven nærmere bestemmelser om gjennomføringen av dataavlesing der det stilles kvalitative krav til politiets fremgangsmåte

[199] Prop. 68 L (2015-2016) s. 265.
[200] Prop. 68 L (2015-2016) s. 266-267.
[201] https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?hpid=hp_hp-top-table-main_wikileaks-11a%3Ahomepage%2Fstory&utm_term=.434ed5d88d99 – sist besøkt 13. mars 2017.
[202] I samme retning, se Sunde (2012) s. 30 flg.

for å minimere faren for misbruk.[203] Dette taler for at loven oppstiller tilstrekkelige rettssikkerhetsgarantier for å beskytte borgerne mot misbruk ved at nasjonale myndigheter pålegges en plikt å påse at metodene ivaretar den enkeltes rettssikkerhet på en tilfredsstillende måte. Samtidig kan det knyttes tvil til om lovens klarhetskrav er oppfylt med hensyn til å oppstille tilfredsstillende rettssikkerhetsgarantier knyttet opp mot gjennomføringen av dataavlesing, jfr. tidligere drøftelse under punkt 4.2.2.2.

Vedvarende overvåking av et datasystem i sanntid reiser særlige problemstillinger da inngrepet fremstår som svært inngripende. Ved å overvåke et datasystem i sanntid vil dataavlesing kunne fange opp opplysninger som ikke var ment kommunisert til noen, og ikke var ment å skulle lagres. På denne måten flyttes overvåkingen tettere innpå sfæren for privatliv til personen som er underlagt overvåking, og nærmere 'tankesettet' til vedkommende. Flere av høringsinstansene hadde sterke innvendinger mot dette.[204] Departementet mente på sin side at den beskjedne risikoen ikke kunne overveie de viktige samfunnsinteressene som søktes vernet.[205] Her illustrerer forarbeidene at departementet verken har kartlagt eller avveid behovet for å innføre dataavlesing som selvstendig metode mot det utvidede inngrepet som overvåking i sanntid utgjør i borgernes privatliv. I relasjon til at metoden må være nødvendig er også inngrepets styrke fraværende i departementets vurdering av behovet for dataavlesing i forebyggende øyemed.[206] Det er tvilsomt om departementets begrunnelse på dette punktet er tilstrekkelig, og taler for at dataavlesing som selvstendig metode går lengre enn nødvendig.

Det må også tas i betraktning at dataavlesing ikke nødvendigvis fanger opp opplysninger som individuelt er av inngripende natur. Imidlertid er det muligheten for systematisk å kunne kartlegge og sammenstille de enkelte opplysningene som innhentes gjennom vedvarende overvåking som gjør at inngrepet fremstår som særlig intenst og inngripende. I en nylig avsagt dom fra den tyske forfatningsdomstolen kom domstolen til at en rekke av de tyske overvåkingsbestemmelsene stred med den tyske forfatningen, blant annet bestemmelsen i BKAG § 20k, som åpnet for en tilsvarende overvåking som den norske bestemmelsen om dataavlesing.[207] Domstolen viste til at overvåking av bruken av informasjonssystemer, særlig

[203] Se Strpl. § 216p første og annet ledd, jfr. Prop. 68 L (2015-2016) s. 271-272.
[204] Prop. 68 L (2015-2016) s. 265, jfr. s. 249-257.
[205] Prop. 68 L (2015-2016) s. 266.
[206] Se Prop. 68 L (2015-2016) s. 214-218 og s. 264-267.
[207] BVerfG, Urteil des Ersten Senat vom 20. April 2016 – 1 BvR 966/09 – Rn. (1-29).

tatt i sin helhet, innebær et særlig intenst inngrep i retten til privatliv, som var sammenlignbart med inngrep i hjemmet.[208] Videre mente domstolen at når overvåkingen ga tilgang til 'alt eller ingenting' av opplysninger, måtte det stilles særlige krav til behandlingen av de innsamlede opplysningene.[209] Selv om dommen ikke har selvstendig rettskildeverdi ved fortolkningen av norsk rett, har begrunnelsen en generell overføringsverdi til vårt tilfelle.

Både Metodekontrollutvalget og departementet har lagt til grunn at dataavlesing innebærer et inngrep i enkeltmenneskers privatliv, og bare kan aksepteres dersom det underlegges forsvarlig kontroll.[210] Domstolens og EOS-utvalgets kontroll, og ordningen med hemmelig advokat, utgjør her en sentral rettssikkerhetsgaranti ved bruk av dataavlesing i forebyggende øyemed, jfr. drøftelsen i pkt. 3.3. I dette henseende er det et viktig poeng at departementet presiserte at en grunnleggende forutsetning for innføring av dataavlesing var at metoden *ikke gikk lengre enn nødvendig*, og underlegges *effektiv og reell* kontroll.[211]

Metodekontrollutvalget presiserte at det ved dataavlesing eksisterte en misbruksfare som tilsa skjerpet kontroll med og dokumentasjon av bruken av dataavlesing. Utvalget foreslo innføring av et loggsystem (protokoll) etter lignende modell som KK-forskriften § 7 som et minimumsbehov for å sikre notoritet. Når det gjaldt kontrollregime la departementet til grunn at notoritet mht. hvilke skritt politiet har foretatt var en forutsetning for å sikre tilfredsstillende kontroll.[212] Det ble vist til at det kunne være nødvendig å gi særskilte regler om kontroll i saker om dataavlesing som tilpasses metodens særpreg. Det måtte legges til rette for at kontrollutvalget kunne utføre en effektiv og reell kontroll, og metodens karakter tilsa at utvalget var avhengig av å ha høy teknologisk kompetanse tilgjengelig.[213]

Det må bemerkes at det kontrollregime som departementet viser til i hovedsak sammenfaller med det kontrollregimet som ble foreslått i Metodekontrollutvalgets forslag om dataavlesing som fremgangsmåte ved kommunikasjonsavlytting og hemmelig ransaking. Når departementets forslag til dataavlesing reelt sett innebærer en vesentlig utvidelse i forhold til eksisterende hjemler er det bemerkelsesverdig at kontrollregimet ikke foreslås utvidet

---

[208] Se dommens avsnitt 210.
[209] Se dommens avsnitt 218.
[210] NOU 2009:15 s. 249, jfr. også kpt. 11 hvor utvalget redegjør for kontrollen med politiets bruk av skjulte tvangsmidler, og Prop. 68 L (2015-2016) s. 258-259.
[211] Prop. 68 L (2015-2016) s. 258-259, s. 272 og s. 273-274.
[212] Prop. 68 L (2015-2016) s. 272 og s. 273-274.
[213] Departementet viser til Metodekontrollutvalgets utredning pkt. 11.10.2 s. 140.

tilsvarende i lovforslaget. Dataavlesing som selvstendig metode vil gi adgang til betydelige mengder med data sammenlignet med Metodekontrollutvalgets forslag. Det er tvilsomt om protokollering vil sørge for en tilfredsstillende notoritet rundt behandlingen av de innsamlede opplysningene ved bruk av dataavlesing, og således være egnet til å sikre en reell kontroll ved metodebruken.[214] Det kommenteres heller ikke at protokollen etter KK-forskriften § 7 ikke gjelder for saker som faller inn under EOS-kontrollutvalgets virksomhet.[215] Om kontrollen med dataavlesing i forebyggende øyemed sier departementet ikke annet enn at det vil reguleres av EOS-loven og EOS-instruksen. Det må anses som svært problematisk at lovgiver ikke har gått nærmere inn på spørsmålet. Departementets manglende vurdering og oppretting av et kontrollregime for dataavlesing i forebyggende øyemed tilsier at kontrollmekanismene ikke er tilpasset den utvidelsen som dataavlesing representerer. Slik regelverket i EOS-kontrolloven og EOS-kontrollinstruksen er utformet i dag er det tvilsomt at lovgivningen gir en effektiv og reell kontroll med bruken av dataavlesing i forebyggende øyemed, og dermed tilfredsstiller kravene til rettssikkerhetsgarantier som kreves etter EMDs praksis.[216] Dette må tas til inntekt for at dataavlesing i forebyggende øyemed ikke er proporsjonalt.

Samlet sett er det tvilsomt om dataavlesing i forebyggende øyemed kan anses å være forholdsmessig slik det er innført i dag. Av særlig betydning er det at lovgiver ikke har foretatt en tilstrekkelig kartlegging og avveining av de ulike interessene. Det kan stilles tvil til om inngrepet går lengre enn nødvendig, og om det foreligger tilstrekkelige rettssikkerhetsgarantier, herunder om bruk av dataavlesing i forebyggende øyemed er underlagt et effektivt og reelt kontrollregime.

4.3 Er dataavlesing i forebyggende øyemed forenelig med Grunnloven § 102 første ledd annet punktum?

I Grl. § 102 første ledd annet punktum fastslås det at «[h]usransakelse må ikke finne sted, unntatt i kriminelle tilfeller».

[214] Jfr. Roman Zakharov v. Russia avsnitt 272, se også Kjølbro (2017) s. 881.
[215] Se KK-forskriften § 12, jfr. strpl. § 216h, jfr. redegjørelsen ovenfor i pkt. 3.3.3.
[216] Se Roman Zakharov v. Russia avsnitt 232-234 og 272. Se for øvrig Evalueringsutvalgets konklusjoner i Dok.nr.16 (2015-2016) s. 11 mvh. og Husabø (2015), inntatt som Vedlegg 4 i Evalueringsutvalgets rapport på s. 245 flg.

Bestemmelsen er utformet som et forbud, og gir etter sin ordlyd en anvisning på et vern mot inngrep som anses som «husransakelse», unntatt når dette gjøres «i kriminelle tilfeller». En isolert tolkning av ordlyden tilsier at bestemmelsen må forstås som et absolutt forbud.

I forslag til lovfesting av dataavlesing ble det lagt til grunn at bestemmelsen trolig ga et absolutt forbud.[217] Departementet går verken nærmere inn på spørsmålet eller begrunner sitt standpunkt. I Lønning-utvalget var bestemmelsen i Grl. § 102 første ledd annet punktum foreslått opphevet.[218] Det ble vist til at bestemmelsen hadde hatt liten praktisk verdi, og først var «vekket til live» etter inkorporeringen av EMK art. 8 i menneskerettighetsloven. En opphevelse av bestemmelsen ville dermed «gi større rom for avveininger og skjønn enn hva tilfellet er for husinkvisisjoner i dag». Til tross for forslaget valgte lovgiver å videreføre bestemmelsen, uten nærmere begrunnelse eller kommentar til Lønning-utvalgets forslag.[219] Det må etter dette anses å være noe usikkert hvorvidt lovgiver er av den oppfatning et bestemmelsen i annet punktum oppstiller et absolutt forbud. Lovgivers vurdering vil således være et moment i vurderingen av spørsmålet.

Heller ikke referatene til grunnlovsforsamlingen eller konstitusjonskomiteen fra Eidsvoll i 1814 gir noen særlig veiledning i spørsmålet.[220] Trolig må bestemmelsen leses i lys av det historiske bakteppet med omfattende husundersøkelses knyttet opp mot tollbeskatning, samt inspirasjon fra andre lands konstitusjoner som en del av idégrunnlaget for Grunnloven.

Bestemmelsen i Grl. § 102 første ledd annet punktum har hatt begrenset praktisk betydning inntil nyere tid, og er nokså lite behandlet i rettspraksis. En rettsavgjørelse av relevans for spørsmålet er inntatt i Rt. 1871 s. 221. Saken gjaldt forståelsen av Grl. § 102 etter at politiet hadde gjennomført en ransaking på grunnlag av mistanke om ulovlig brennevinssalg. Førstvoterende ga til uttrykk at man ved vurderingen av Grl. § 102 verken kunne legge avgjørende vekt på om den straffbare handlingen kunne straffes med bøter eller fengsel, eller trekke grensen ved det prosessuelle skillet mellom justisforbrytelser eller politiforseelser (tidl. forbrytelse/forseelse i strl. 1902). Deretter uttalte førstvoterende på vegne av flertallet følgende:

---

[217] Prop. 68 L (2015-2016) s. 34 flg.
[218] Dok.nr.16 (2011-2012) s. 176.
[219] Innst. 186 S (2013-2014) s. 27-29.
[220] Høgberg & Stub (2009) s. 425-431 mvh. og Andenæs & Fliflet (2006) s. 407-409, jfr. s. 66-67.

> «Jeg antager derfor, at man ikke kan opstille nogen saadan absolut almindelig Regel, men at man maa tage Hensyn til hvorvidt Omstændighederne i det enkelte konkrete Tilfælde er af den Beskaffenhed, at det Offentliges Interesse i om muligt at saa Forbrydelsen opdaget og bevist er saa stor, at det er rimeligt, at den Privates Interesse, som bestaar deri ikke uden rimelig Grund at skulle taale Indtrængen i sit Hus, maa staa tilside. Jeg er saaledes med de foregaaende Retter af den Mening, at Grundlovsbestemmelsen maa ansees mere som en Veiledning end som et positivt absolut Bud.»[221]

Høyesterett la her til grunn at Grl. § 102 ikke kunne anses som et absolutt forbud, men ga en anvisning på at det måtte foretas en interesseavveining mellom myndighetenes *behov* for inngrep på den ene siden og borgernes rett til privatliv på den andre siden. Interessant nok er denne vurderingen tilsynelatende lik den forholdsmessighetsvurderingen som Høyesterett har lagt til grunn etter nytt første ledd første punktum i Grl. § 102, jfr. de overnevnte avgjørelsene fra 2014 og 2015.[222] Dommen taler dermed i retning av at forbudet i Grl. § 102 første ledd annet punktum ikke kan anses å være absolutt, og bestemmelsen gir anvisning på at det må foretas en konkret helhetsvurdering av om inngrepet er i strid med forbudet.[223] På den annen side er dommen avsagt under dissens, og er om lag 150 år gammel. Det er dermed usikkert hvor stor rettskildemessig vekt dommen kan tillegges, og om den gir uttrykk for gjeldende rett i dag. Husabø gir uttrykk for at dersom utsagnet fra dommen var ment som et generelt utsagn om Grl. § 102, må det vike for det generelle synet som Høyesterett har lagt til grunn i dag.[224]

Husabøs vurdering av dommens aktualitet kan ikke stå seg i dag. Tvert imot viser rettspraksis at Høyesterett i mindre grad tillegger den historiske konteksten rundt tilblivelsen av Grunnloven vekt. Praksis viser at Høyesterett i stor grad har relativisert grunnlovsvernet ved prøvingen av lovers grunnlovmessighet, og har lagt til grunn en dynamisk fortolkning av Grunnloven, der Grunnloven tolkes i lys av dagens samfunnsforhold, verdisyn, rettsoppfatninger og behov.[225] Et eksempel er Rt. 2014 s. 620, som gjaldt om ileggelse av

---

[221] Rt. 1871 s. 221 på s. 223.
[222] Rt. 2014 s. 1105, Rt. 2015 s. 93 og Rt. 2015 s. 155, jfr. tidligere drøftelse i pkt. 4.1.
[223] Se Rui (2016) s. 100 flg. som tar til ordet for en «relativisert tolkning» av Grl. § 102 første ledd annet punktum.
[224] Husabø (2009) s. 407 flg. I motsatt retning, se Rui (2016), jfr. forrige note.
[225] Bårdsen skriver treffende at: «Skal Grunnloven over tid fungere, må man søke etter balanse mellom stabilitet og fleksibilitet, med utgangspunkt i en *samtidsorientert* grunnlovstolkning.», se Bårdsen (2017) s. 8. Se også Bårdsen, Arnfinn, «*Norges Høyesterett som konstitusjonsdomstol*» i Øie, Schei & Skoghøy (red.), *Lov, sannhet, rett: Norges Høyesterett 200 år* (Oslo 2015) s. 291-316 på s. 307 flg.

overtredelsesgebyr etter akvakulturloven var å regnes som straff etter det materielle straffebegrepet i Grl. § 96, og dermed var ilagt i strid med bestemmelsens domskrav.[226] Høyesteretts argumentasjon viser at Høyesterett vurderte spørsmålet ut fra en interesseavveining med bakgrunn i grunnlovsbestemmelsens formål der det foretas en avveining mellom statens og individets behov, og ikke ut ifra tolkning av det materielle straffebegrepet i bestemmelsen.[227] Høyesterettspraksis forut av grunnlovsrevisjonen av 2014 viser at Høyesterett har relativisert Grunnlovens bestemmelser, bl.a. i saker om tilbakevirkning etter Grl. § 97 og ytringsfrihet etter Grl. § 100.[228] Også lovgiver synes å ha lagt til grunn at det er den historiske konteksten som Grunnloven inngår i til enhver tid som må legges til grunn ved forståelsen av Grunnlovens bestemmelser.[229]

Ved tolkningen av Grl. § 102 første ledd annet punktum må det også tas i betraktning at Høyesterett har slått fast at rettigheten etter første punktum er relativ. Videre er det av betydning at de aller fleste menneskerettighetene er relative.[230] I Lønning-utvalgets forslag til en generell begrensningshjemmel ble det uttrykkelig opplistet hvilke rettigheter som skulle anses å være absolutte.[231] At lovgiver videreførte den tidligere Grl. § 102 i nytt annet punktum, og ikke har tatt stilling til forståelsen av bestemmelsen, kan ikke tas til inntekt at bestemmelsen skal forstås som et absolutt forbud. Det kan etter dette ikke tas for gitt at forbudet etter Grl. § 102 første ledd annet punktum er absolutt.

Dersom forbudet etter annet punktum anses som et absolutt forbud ville spørsmålet vært om dataavlesing i forebyggende øyemed gikk klar av forbudet. Det problematiske med en slik tolkning er at det i stor grad vil avhenge av om man anser inngrepet for å være en 'husransakelse' og om det skjer 'i kriminelle tilfeller', noe som uten tvil vil være gjenstand for uenighet.[232] Det vil derfor ha gode grunner for seg å legge til grunn at forbudet i Grl. §

---

[226] Det følger av bestemmelsen i Grl. § 96 at: «Ingen kan (…) straffes uten etter dom», hvilket betyr at dersom overtredelsesgebyret var å anse som straff måtte den ilegges av domstolen. Virkningssiden ved at overtredelsesgebyret var ilagt av forvaltningen ville i så fall vært at det var i strid med Grl. § 96.
[227] Dommens avsnitt 46, 48, 50-53, 78 og 80-83. Se Rui (2016) s. 103 flg.
[228] Se Dok.nr.16 (2011-2012) s. 73 med videre henvisning til bl.a. Rt. 1996 s. 1415, Rt. 1997 s. 1812, Rt. 2006 s. 293 og Rt. 2007 s. 1807. I HR-2016-389-A uttalte Høyesterett at det «måtte skje en interesseavveining mellom de vernede interesser på en side, og de samfunnsmessige hensynene på den annen [side]», se dommens avsnitt 77, jfr. avsnitt 61-76 mvh.
[229] Dok.nr.16 (2011-2012) s. 86-87. Se også Innst. 186 S (2013-2014) s. 20 flg. der stortingskomiteen blant annet uttaler at Grunnloven er et 'tilpasningsdyktig og levende dokument'.
[230] I EMK oppstilles et absolutt forbud mot tortur og slavearbeid, jfr. henholdsvis EMK art. 3 og 4.
[231] Dok.nr.16 (2011-2012) s. 76, jfr. s. 69-76.
[232] Se NOU 2009:15 kpt. 13 152 flg., jfr. også de to betenkningene i Metodekontrollutvalgets vedlegg 2 og 3. I motsatt retning se Prop. 68 L (2015-2016) s. 32-38. I Årsmelding fra Nasjonal institusjon for

102 første ledd annet punktum er relativt. Som det fremgår av drøftelsen over er det overordnede formålet til menneskerettighetsbestemmelsen i både Grl. § 102 og EMK art. 8 å beskytte den enkelte mot *vilkårlig* og *uforholdsmessige* inngrep. Det overordnede formålet til Grl. § 102 første ledd annet punktum kan også sies å skulle beskytte borgeren mot vilkårlige husransakelser.[233] En relativisering vil legge rette for et større rom for avveininger og skjønn, slik som Lønning-utvalget la opp til.[234] En slik tolkning vil derfor også harmonere best med Grunnlovens formål.[235]

Spørsmålet om forståelsen av Grl. § 102 første ledd annet punktum må per i dag anses uavklart. Ettersom lovgiver ikke synes å ha tatt et uttrykkelig standpunkt i spørsmålet[236] tilsier Høyesteretts praksis og formålsbetraktninger at forbudet i annet punktum er relativt. Dette standpunktet har dessuten støtte i Lønning-utvalgets rapport, samtidig som et relativt forbud i Grl. § 102 først ledd annet punktum harmonerer best med rettighetsbestemmelsen i første punktum. Bestemmelsen i annet punktum må etter dette forstås som et relativt forbud.

Virkningen av å relativisere Grl. § 102 første ledd annet punktum er at det ikke blir noen realitetsforskjell mellom den interesseavveiningen som må tas i annet punktum og den forholdsmessighetsvurderingen som er innfortolket i første punktum, jfr. tidligere drøftelse. Samtidig gir forbudet i annet punktum en særlig presisering av hva som utgjør et inngrep i privatlivet etter første punktum, og gir uttrykk for at et inngrep i hjemmet må anses som særlig inngripende. Forbudet i annet punktum sett i sammenheng med rettigheten i første punktum må etter dette forstås som en anvisning på ytterlig skjerpende krav til lovhjemmel og forholdsmessighet. Det må legges til grunn at Grl. § 102 første ledd annet punktum har en kjerne som må respekteres. I dette ligger det at en begrensning i retten til privatlivet ikke kan være så omfattende at det i realiteten ikke blir noe igjen av rettigheten.[237] Videre må det kunne antas at jo nærmere kjernen av privatlivet man befinner seg på, desto mer tungtveiende

---

menneskerettigheters (2016-2017) er det inntatt en temarapport «*Grunnloven § 102: Hva må ikke finne sted, unntatt i hvilke tilfeller?*» som i stor grad slutter seg til Metodekontrollutvalgets syn på forståelsen av forbudet.

[233] Se Rt. 2004 s. 1723 (*Våpenkontroll*) som omhandlet politiets kontroll med oppbevaring av skytevåpen. Høyesterett viste til at bakgrunnen for og den praktiske gjennomføringen av kontrollen sto sentralt i vurderingen, se avsnitt 34 og 42-53. Samtidig la de vekt på kjerneområdet for tidl. Grl. § 102 var å verne mot vilkårlige husundersøkelser på bakgrunn av en krenkende mistanke, se avsnitt 44, 45 og 49.

[234] Dok.nr.16 (2011-2012) s. 176.

[235] Det følger av Grl. § 2 annet punktum at: «Denne Grunnlov skal sikre demokratiet, rettsstaten og menneskerettighetene». Se også Dok.nr.16 (2011-2012) s. 51.

[236] Prop. 68 L (2015-2016) s. 34 flg., Innst. 186 S (2013-2014) s. 21-22 og s. 27 flg.

[237] Dok.nr.16 (2011-2012) s. 73.

grunner kreves for at inngrepet skal være forholdsmessig. Således vil det etter en forholdsmessighetsvurdering kreves mer for å kunne gjøre inngrep i den privates hjem eller andre steder hvor man har en berettiget forventning om å være i fred.[238]

Spørsmålet om dataavlesing er samsvar med annet punktum må etter dette løses ut fra en konkret interesseavveining. Vurderingstemaet er om de samfunnsmessige hensyn som begrunner inngrepet er så tungtveiende at hensynet til den enkelte må vike.[239] Momentene som inngår i vurderingen av inngrep i annet punktum vil være identisk med momentene som er relevant ved vurderingen etter første punktum, jfr. drøftelsen over i pkt. 4.2. Det vil her være av betydning hvor påtrengende myndighetenes behov er for å forebygge alvorlige forbrytelser, og om begrunnelsen for inngrepet er velbegrunnet. Videre vil inngrepets intensitet og hvilke rettssikkerhetsgarantier som er oppstilt ha stor betydning i vurderingen av om inngrepet tilfredsstiller et skjerpet kravet om klar lovhjemmel og forholdsmessighet.

Når departementet gikk inn for et absolutt forbud mot romavlytting av private hjem i forebyggende øyemed, var begrunnelsen at det var nært sagt uunngåelig at uskyldige tredjepersoner ble rammet og at inngrepet innebar en kontinuerlig overvåking over tid.[240] Likevel gikk departementet inn for å tillate dataavlesing i forebyggende øyemed i private hjem. Det kan stilles spørsmålstegn til hvorfor departementet har differensiert mellom disse tvangsmidlene når de samme hensynene i stor grad gjør seg gjeldende også for dataavlesing slik det er innført, jfr. drøftelsen i pkt. 4.2.4. Etter en skjerpet forholdsmessighetsvurdering er det derfor gode grunner som taler for å tolke pl. § 17d innskrenkende slik at også dataavlesing i forebyggende øyemed i private hjem forbys.

Dataavlesing i forebyggende øyemed står dermed ikke direkte i strid med Grl. § 102 første ledd annet punktum. Imidlertid er det nærliggende å tro at Høyesterett vil kunne føre en streng linje dersom spørsmålet ble satt på spissen. Det er gode grunner som taler for å tolke

---

[238] I juridisk litteratur er det argumentert for at tidligere Grl. § 102 ikke nødvendigvis begrenset seg til det privat hjem, se Høgberg & Stub (2009) s. 431-440 og Stub (2009) s. 410 flg. I HR-2016-471-U gjaldt saken Mattilsynets inspeksjon av et fjøs. Ankeutvalget gikk ikke nærmere inn på spørsmålet da inspeksjonen ikke ville gripe inn i privatlivsinteresser og det ikke forelå opplysninger som ga grunnlag for det motsatte, se avsnitt 15. Dommen viser at Høyesterett ikke utelukker at også andre lokaler kan ha et særskilt vern. I motsatt retning, se Aschehoug (1893) s. 12-13, Morgenstierne (1927) s. 359 og Husabø (2009) s. 409.
[239] Høgberg & Stub (2009) s. 442 og Rui (2016) s. 102. Se også Prop. 68 L (2015-2016) s. 36-38.
[240] Prop. 68 L (2015-2016) s. 216-217.

regelverket om dataavlesing i forebyggende øyemed innskrenkende når det er tale om å gjøre inngrep i kjernen av privatlivet, f. eks i private hjem.

5 Avsluttende bemerkninger

Avhandlingen viser at dataavlesing i forebyggende øyemed i seg selv, og *om* det skal innføres, ikke er i strid med Grl. § 102. Imidlertid er det måten som lovgiver har gått frem, og *hvordan* dataavlesing er innført, som ikke er i samsvar med Grl. § 102. Avhandlingen viser at det særlig er kravet om tilstrekkelig klar lovhjemmel og at inngrepet skal være forholdsmessig som er problematisk i relasjon til dataavlesing.

Et gjennomgående problem er at lovgiver ikke synes å ha foretatt en tilstrekkelig og velbegrunnet kartlegging og avveining av om hvorvidt dataavlesing i forebyggende øyemed er nødvendig og forholdsmessig. En svakhet er at lovgivers begrunnelse i stor grad fokuserer på å gi politiet effektive metoder, samt overvinne krypteringsproblematikken. Lovgiver har i mindre grad vurdert de diverse utfordringene som knytter seg til metoden, bl.a. faren for misbruk av tredjepersoner. Det må også anses som tvilsomt at loven slik den er utformet i dag oppstiller tilstrekkelige rettssikkerhetsgarantier. Det mest problematiske er den manglende vurdering av og oppretting av et kontrollregime til dataavlesing i forebyggende øyemed. Det etablerte kontrollregimet for forebyggende tvangsmidler er ikke tilpasset den utvidelsen som dataavlesing innebærer. Mye taler derfor for at dataavlesing i forebyggende øyemed må anses som et uforholdsmessig inngrep, og derfor er uforenelig med Grunnloven § 102 slik det er innført i dag.

Den uavklarte betydningen av Grl. § 102 første ledd annet punktum medfører også at det i høy grad er knyttet usikkerhet til grensene for bruk av dataavlesing i forebyggende øyemed. Samtidig skaper bestemmelsens fortsatte tilstedeværelse i Grunnloven et tankekors knyttet til hvor grensene for myndighetenes inngrep i privatlivet skal gå. I faren for å uthule retten til privatliv, og dermed undergrave demokratiet under påskuddet av å beskytte det, er det mulig at en nærmere grense for hvilke inngrep myndighetene kan gjøre i privatlivet i forebyggende øyemed er ønskelig. Det nærmere innholdet, rekkevidden og virkningen av Grl. § 102 første ledd annet punktum, samt grunnlovsmessigheten av lovgivningen om dataavlesing i forebyggende øyemed vil i siste instans måtte bli avgjort av Høyesterett.

Kilderegister

Lover, forskrifter, konvensjoner ol.

Norske lover

Grunnloven	Kongeriket Norges Grunnlov, gitt i riksforsamlingen på Eidsvoll 17. mai 1814.
Straffeprosessloven	Lov 22. mai 1981 om rettergangsmåten i straffesaker
EOS-kontrolloven	Lov 3. februar 1995 nr. 7 om kontroll med etterretnings- overvåkings- og sikkerhetstjeneste
Politiloven	Lov 4. august 1995 nr. 53 om politiet
Menneskerettighetsloven	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett
Politiregisterloven	Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten

Forskrifter

Politiregisterforskriften	Forskrift av 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten
Kommunikasjonskontrollforskriften	Forskrift av 9. september 2016 nr. 1047 om kommunikasjonskontroll, romavlytting og dataavlesing

Internasjonale konvensjoner

Europarådets konvensjon 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter (Den europeiske menneskerettighetskonvensjonen – EMK)

Stortingsdokumenter, forarbeider ol.

Lovforarbeid

Ot.prp.nr.83 (1993-1994) Om lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste

NOU 2003:18 Rikets sikkerhet. Straffelovkommisjonens delutredning del VIII

NOU 2004:6 Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed

Ot.prp.nr.60 (2004-2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)

Innst.O.nr.113 (2004-2005) Innstilling fra justiskomiteen om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre

alvorlig kriminalitet)

NOU 2007:2 Lovtiltak mot datakriminalitet. Delutredning II

NOU 2009:1 Individ og integritet. Personvern i det digitale samfunnet

NOU 2009:12 Et ansvarlig politi. Åpenhet, kontroll og læring

NOU 2009:15 Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker

Ot.prp.nr.108 (2008-2009) Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)

Dok. nr.16 (2011-2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven (Lønning-utvalget)

Innst.186 S (2013-2014) Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag fra Per-Kristian Foss, Martin Kolberg, Marit Nybakk, Jette F. Christensen, Anders Anundsen, Hallgeir H Langeland, Per Olaf Lundteigen, Geir Jørgen Bekkevold og Trine Skei Grande om grunnlovfesting av sivile og politiske menneskerettigheter, med unntak av romertall X og romertall XXIV

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

Innst.165 S (2015-2016) Innstilling fra kontroll- og konstitusjonskomiteen om Grunnlovsforslag fra Per-Kristian Foss, Martin Kolberg, Marit Nybakk, Jette F. Christensen, Hallgeir H Langeland, Per Olaf Lundteigen, Geir Jørgen Bekkevold og Trine Skei Grande om grunnlovfesting av økonomiske, sosiale og kulturelle menneskerettigheter (romertall IX - begrensninger i de grunnlovfestede rettigheter)

Innst. 343 L (2015-2016) Innstilling fra justiskomiteen om Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Rapporter

Dokument nr. 15 (1995-1996) Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»)

Dok.nr.16 (2015-2016) En evaluering av EOS-utvalgets kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste

Temarapport 2016: «*Grunnloven § 102: Hva må ikke finne sted, unntatt i hvilke tilfeller*?», utgitt som vedlegg til Årsmelding 2016 – Norges nasjonale institusjon for menneskerettigheter, dokument 6 (2016-2017) - http://www.nhri.no/getfile.php/131701/nim/Nyhet/Temarapport%202016%20-%20Grunnloven%20§%20102.%20Hva%20må%20ikke%20finne%20sted%20unntatt%20i%20hvilke%20tilfeller.pdf – sist besøkt 22. april 2017.

Årsmeldinger

EOS-utvalgets årsmelding til Stortinget for 2015 – Dokument 7:1 (2015-2016)

Rundskriv

RA-1993-3: Riksadvokatens rundskriv nr.3/1999, Etterforskning

Instrukser

EOS-kontrollinstruksen	Instruks 30. mai 1995 nr. 4295 om kontroll med EOS-tjenestene

Rettspraksis

Høyesteretts praksis

Rt. 1871 s. 221 (*brennevinssalg*)

Rt. 1976 s. 1 (*Kløfta*)

Rt. 1996 s. 1415 (*Borthen*)

Rt. 1997 s. 1821 (*Kjuus*)

Rt. 2004 s. 1723 (*Våpenkontroll*)

Rt. 2006 s. 293 (*Arves trafikkskole*)

Rt. 2007 s. 1281 (*Øvre Ullern*)

Rt. 2007 s. 1807 (*Vigrid*)

Rt. 2014 s. 620 (*Selsøyvik*)

Rt. 2014 s. 1105 (*Acta*)

Rt. 2015 s. 93 (*Maria*)

Rt. 2015 s. 155 (*Rwanda*)

Rt. 2015 s. 1456

HR-2016-304-S

HR-2016-389-A

HR-2016-471-U

HR-2016-1833-A

HR-2016-2554-P (*Holship*)

Praksis fra Den europeiske menneskerettighetsdomstolen

Handyside v. United Kingdom, saksnr. 5493/72, plenumsdom av 7. desember 1976

Klass and others v. Germany, saksnr. 5029/71, plenumsdom av 6. september 1978

Silver and others v. United Kingdom, saksnr. 7136/75, dom av 25. mars 1983

Olsson v. Sweden, saksnr. 10465/83, plenumsdom av 24. mars 1988

Huvig v. France, saksnr. 11105/84, dom av 24. april 1990

Keegan v. Ireland, saksnr. 28867/03, dom av 18. juli 2006

Korbely v. Hungary, saksnr. 9174/02, storkammerdom av 19. september 2008

S. and Marper v. United Kingdom, saksnr. 30562/04, storkammerdom av 4. desember 2008

Bykov v. Russia, saksnr. 4378/02, storkammerdom av 12. mars 2009

Uzun v. Germany, saksnr. 35623/05, dom av 2. september 2010

Austin and others v. United Kingdom, saksnr. 39692/09, storkammerdom av 15. mars 2012

Lindheim and others v. Norway, saksnr. 13221/08, dom av 12. juni 2012

Mouvement Raélien Suisse v. Switzerland, saksnr. 16354/06, storkammerdom av 13. juli 2012

Animal Defenders International v. United Kingdom, saksnr. 48876/08, storkammerdom av 22. april 2013

Lillo-Stenberg and Sæther v. Norway, saksnr. 13258/09, dom av 16. januar 2014

Dragojević v. Croatia, saksnr. 68955/11, dom av 15. januar 2015

Perinçek v. Switzerland, saksnr. 27510/08, storkammerdom av 15. oktober 2015

R.E v. United Kingdom, saksnr. 62498/11, dom av 27. oktober 2015

Roman Zakharov v. Russia, saksnr. 47143/06, storkammerdom av 4. desember 2015

Szabó and Vissy v. Hungary, saksnr. 37138/14, dom av 12. januar 2016

Paradiso and Campanelli v. Italy, saksnr. 25358/12, storkammerdom av 24. januar 2017

Tysk rett

BVerfG, Urteil des Ersten Senat vom 20. April 2016 – 1 BvR 966/09 – Rn. (1-29)

(http://www.bverfg.de/e/rs20160420_1bvr096609.html) - sist besøkt 2. mai 2017.

Engelsk versjon er også tilgjengelig på nettsiden.

Juridisk litteratur, forskningsartikler ol.

Aall (2015)	Aall, Jørgen, *Rettsstat og menneskerettigheter*, 4. utg. (Bergen 2015)
Andenæs & Fliflet (2006)	Andenæs, Johs. & Fliflet, Arne, *Statsforfatningen i Norge*, 10. utg. (Oslo 2006).

Aschehoug (1893)	Aschehoug, T.H., *Norges nuværende Statsforfatning*, 3. bind 2. utgave (Christiania: Malling 1893)
Auglend & Mæland (2016)	Auglend, Ragnar L. & Mæland, John Henry, *Politirett*, 3. utg. (Oslo 2016)
Bruce & Haugland (2014)	Bruce, Ingvild & Haugland, Geir Sunde, *Skjulte tvangsmidler* (Oslo 2014)
Bårdsen (2017)	Bårdsen, Arnfinn, *Grunnloven, straffeprosessen og strafferetten – Noen linjer i Høyesteretts praksis etter grunnlovsreformen 2014*, Jussens venner vol. 52 nr. 1 (2017) s. 1-44
Harris m.fl. (2014)	David, D.J, O'Boyle, M., Bates, E.P. & Buckley, C.M., *Law of the European Convention on Human Rights*, 3. utg. (Oxford 2014)
Husabø (2009)	Husabø, Erling J., *Grunnlova § 102 og bruk av enkelte tvangsmidlar for å førebyggja eller avverja straffbare handlinger* – Vedlegg 2 til NOU 2009:15. Avgitt Metodekontrollutvalget 9. april 2009.
Husabø (2015)	Husabø, Erling J., *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og etterretningstjenestenes inngrep i menneskerettigheter?* – Vedlegg 4 til Dok.nr.16 (2015-2016). Utarbeidet 11. desember 2015.
Høgberg & Stub (2009)	Høgberg, Alf P. & Stub, Marius, *Er reglene om bruk av tvangsmidler i avvergende og forebyggende øyemed forenelige med forbudet mot husinkvisisjoner i Grunnloven § 102?* – Vedlegg 3 til NOU 2009:15. Avgitt Metodekontrollutvalget 13. mars 2009.
Kjølbro (2017	Kjølbro, Jon F., *Den Europæiske Menneskerettighedskonvention: For praktikere*, 4. utg. (København 2017)
Morgenstierne (1927)	Morgenstierne, Bredo, *Lærebok i den norske statsforfatningsret*, 2. bind 3. utgave (Oslo: O. Christiansen 1927)
Olsen, Schneier & Zittrain m.fl.	Olsen, M., Schneier, B. & Zittrain, J. m.fl., *Don't Panic: Making progress on the "Going Dark" Debate*, Berkman Center Research Publication 2016-1 (https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf) – sist nedlastet 29. april 2017.
Schabas (2015)	Schabas, William A., *The European Convention on Human Rights* (Oxford 2015)

Skoghøy (2015)	Skoghøy, Jens Edvin A., *Menneskerettighetenes stilling etter Grunnloven*, Lov og Rett 2015 s. 195-196
Smith (2015)	Smith, Eivind, *Konstitusjonelt demokrati*, 3. utg. (Oslo 2015)
Spano (2014)	Spano, Robert, *Universality or Diversity of Human Rights?: Strasbourg in the Age of Subsidiarity*, Human Rights Law Review, Volume 14, Issue 3 s. 487-502
Stub (2009)	Stub, Marius, *Om forbudet mot husinkvisisjoner i Grunnloven § 102*, Tidsskrift for rettsvitenskap 2009 s. 388-442 (TFR-2009-388)
Sunde (2012)	Sunde, Inger Marie, *Dataavlesing som etterforskningsmetode*, tidsskriftet *Retfærd* (2012) årgang 35, nr. 1/136 s. 3-35 (RETF-2012-136-3)
Sørensen (2014)	Sørensen, Christian Børge, *Nasjonale proporsjonalitetsvurderinger etter EMK – prosessuell rasjonalitet*, Tidsskrift for rettsvitenskap 2014 s. 348-383 (TFR-2014-348)
Riste & Moland (1997)	Riste, Olav & Moland, Arnfinn, *«Strengt hemmelig»: Norsk etterretningsteneste 1945-1970* (Oslo 1997)
Rui (2013)	Rui, Jon Petter, *The Interlaken, Izmir and Brighton Declarations: Towards a Paradigm Shift in the Strasbourg Court's Interpretation of The European Convention of Human Rights?*, Nordic Journal of Human Rights No. 1/2013, vol. 31, s. 28-54 (NMR-2013-28)
Rui (2016)	Rui, Jon Petter, *Betenkning: Sivilrettslig inndragning rettet direkte mot formuesgoder*, (https://www.regjeringen.no/contentassets/563c5153753e41438ec0b6d047f3ab20/betenkning_sivilrettslig-inndragning.pdf - sist lastet ned 10. mars 2017)
Øie, Schei & Skoghøy (2015)	Øie, Toril M., Schei, Tore & Skoghøy, Jens Edvin A. (red.), *Lov, sannhet, rett: Norges Høyesterett 200 år* (Oslo 2015)

Nettbaserte kilder

Foredrag ved Høyesterettsdommer dr. juris Arnfinn Bårdsen, Oslo 21. april 2017: «*Grunnloven, overvåking og domstolenes rolle*», Høyesteretts nettsider 2017 nr. 4 (HOY-2017-4) - http://www.domstol.no/no/Enkelt-domstol/-Norges-Hoyesterett/Artikler-med-mer/samerett-i-hoyesterett/grunnloven-og-overvakning/ - sist besøkt 29. april 2017

Gyldendals Rettsdata - https://www.rettsdata.no/

EOS-utvalgets hjemmesider - https://eos-utvalget.no/norsk/tjenester/om_eos_utvalget/historikk/ - sist besøkt 2. februar 2017

Statistisk sentralbyrå, Bruk av IKT i husholdningene, 2. kvartal 2016 - https://www.ssb.no/teknologi-og-innovasjon/statistikker/ikthus - sist besøkt 29. april 2017

Store norske leksikon, definisjon av «data» - https://snl.no/data - sist besøkt 13. mars 2017

Washington Post - https://www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?hpid=hp_hp-top-table-main_wikileaks-11a%3Ahomepage%2Fstory&utm_term=.434ed5d88d99 (7. mars 2017) - sist besøkt 29. april 2017