Dataavlesning i forebyggende øyemed

Blir rettssikkerheten tilstrekkelig ivaretatt ved bruk av dataavlesning i forebyggende øyemed?

Kandidatnummer: 120

Antall ord: 14067

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

1 Juni 2018

INNHOLDSFORTEGNELSE

1. INNLEDNING

1.1 Tema og problemstilling

Temaet for oppgaven er om rettssikkerheten blir stilstrekkelig ivaretatt ved bruk av dataavlesning som tvangsmiddel i forebyggende øyemed.

I 2016 ble dataavlesning innført som selvstendig tvangsmiddel i norsk rett.[1] Dataavlesning er regulert i straffeprosessloven kap. 16 d,[2] og hjemmel for bruk av dataavlesning i forebyggende øyemed er inntatt i politiloven § 17 d.[3]

Endringen i kriminalitetsbildet har ført til et sterkere behov for vern mot kriminalitet enn tidligere. Hensynet til samfunnssikkerhet og kriminalitetsbekjempelse kan tilsi at samfunnet bør gå lenger i å tillate bruk av virkemidler for å bekjempe kriminalitet. Tillatelse til å anvende tvangsmidler, før en kriminell handling er begått, øker sjansen for at uskyldige personer rammes av bruken. Hensynet til rettssikkerhet og personvern taler derfor for å begrense bruk av tvangsmidler.

Det er nær sammenheng mellom begrepene rettssikkerhet og personvern. Personvern kan defineres som «ivaretakelsen av personlig integritet; ivaretakelsen av enkeltindividers mulighet til privatliv, selvbestemmelse (autonomi) og selvutfoldelse».[4] Begrunnelsen for prinsippet er blant annet behovet for en privat sfære og rett til å ha kontroll over opplysninger om seg selv.[5] Rettsikkerhet er ikke et entydig begrep. Metodekontrollutvalget definerer kjernen i begrepet som «krav om at enkeltindividet skal være beskyttet mot overgrep og vilkårlighet fra myndighetenes side, samtidig som vedkommende skal ha mulighet til å forutberegne sin rettsstilling og forsvare sine rettslige interesser».[6]

Sett i sammenheng skal hensynene «verne mot vilkårlige inngrep i personvernet fra statens side, og mot fare for misbruk og overgrep som følge av at opplysninger om borgerens

[1] Tilføyd ved lov 17. juni 2016 nr. 54.
[2] Lov av 22. mai 1981 nr. 25.
[3] Lov av 4. august 1995 nr. 53.
[4] NOU 2009: 15 *Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandlingen av informasjon i straffesaker,* s. 32.
[5] NOU 2009: 15 s. 49.
[6] NOU 2009: 15 s. 60.

personlige forhold samles inn, systematiseres og sammenstilles, og brukes uten dennes samtykke».[7]

Personvern er nært knyttet til retten til privatliv. Retten til privatliv er nedfelt som en menneskerettighet i den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8.[8] Det følger av menneskerettighetsloven § 3,[9] jf. Grunnloven § 92,[10] at EMK skal gjelde som norsk rett.

Både Grunnloven § 102 og EMK artikkel 8 verner om retten til privatliv. Grunnloven skal forstås i lys av EMK, med en reservasjon om at Høyesterett har et selvstendig ansvar for å tolke, avklare og utvikle Grunnloven.[11] Bestemmelsene skal derfor i utgangspunktet tolkes likt.

Oppgaven vil ta utgangspunkt i EMK artikkel 8 ved vurderingen av om dataavlesning i forebyggende øyemed skjer i samsvar med de rettssikkerhetsgarantier som er oppstilt for å verne om retten til privatliv.

Ifølge EMK artikkel 8 nr. 2 må inngrep i retten til privatliv skje «in accordance with the law» og være «necessary in a democratic society». Dataavlesning utgjør utvilsomt et inngrep etter artikkel 8 nr. 1,[12] og det kreves derfor at dataavlesning gjennomføres innenfor rammen av de rettssikkerhetsgarantier som oppstilles i EMK artikkel 8 nr. 2. Vilkårene i EMK artikkel 8 nr. 2 inneholder blant annet krav til lovhjemmelens tilgjengelighet og presisjon, formålet med inngrepet, forholdsmessighet og kontrollmekanismene.[13] EMD sin praksis viser at det er summen av rettssikkerhetsgarantiene som avgjør om inngrep i privatlivet kan aksepteres.[14] Krav til lovhjemmel, formål og kontrollen med inngrepet må derfor ses i sammenheng.

---

[7] NOU 2009: 15 s. 60.
[8] Europarådets konvensjon av 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter.
[9] Lov av 21. mai 1999 nr. 30.
[10] Lov av 17. mai 1814.
[11] Rt. 2015 s. 93 premiss 57 og Rt. 2015 s. 155 premiss 40.
[12] *Klass m.fl. mot Tyskland*, 6. september 1978 (saksnr. 5029/71) se særlig avsn. 36.
[13] Se Prop. 68 L (2015-2016) *Endringer i straffeprosessloven mv. (skjulte tvangsmidler)* s. 38-41 og Erling Johannes Husabø, *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og etterretningstjenestens inngrep i menneskerettigheter?*, Vedlegg 4 til Dokument 16 (2015) s. 247-260.
[14] J.P. Loof mfl., *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen - en veiligheidsdiensten: Afdeling staats- en bestuursrecht (Norsk oversettelse: Menneskerettighetsrammen for det nederlandske systemet for tilsyn med etterretnings- og sikkerhetstjenestene: delstatistikk og administrativ rett),* (Universitetet i Leiden 2015).

Nærmere drøftelser av kravene etter artikkel 8 nr. 2 vil bli tatt etter hvert som de gjør seg gjeldende i oppgaven.

Lovfestingen av dataavlesning i forebyggende øyemed er et utslag av at lovgiver har forsøkt å finne en balansegang mellom de hensynene som gjør seg gjeldende. Et effektivt vern mot kriminalitet er ønskelig, samtidig som ønsket om et lavt overvåkningsnivå står sentralt.

1.2 Bakgrunn og aktualitet

De siste tiårene har det skjedd en stor endring i måten mennesker kommuniserer på. Den teknologiske utviklingen har resultert i økt bruk av internett, smarttelefoner og sosiale medier. Utviklingen har også ført til at det har oppstått en rekke plattformer for kommunikasjon, som har gjort det enkelt og billig å kommunisere med andre individer uavhengig av geografisk avstand. I en undersøkelse fra 2017 fremgår det at 91 % av deltakerne hadde smarttelefon og 98 % internett hjemme.[15] Den teknologiske utviklingen har resultert i at mennesker i dag legger igjen store mengder digitale spor.

Økende bruk av internett og datasystemer er også blitt et viktig verktøy for å planlegge og gjennomføre tradisjonelle former for kriminalitet.[16] En del av begrunnelsen for å innføre regler om dataavlesning var å fange opp de digitale sporene som oppstår ved planlegging og gjennomføring av lovbrudd.

Det var først ved endringen av politiloven i 2005 at tvangsmidler ble tillatt brukt i forebyggende øyemed.[17] Begrepet «tvangsmiddel» kan defineres som «politimetoder som har det felles at de er så integritetskrenkende at politiet utvilsomt trenger hjemmel i lov for å ta metoden i bruk».[18] At bruken er skjult innebærer at det gjøres unntak fra utgangspunktet om krav til underretning.[19] Grunnlaget for å åpne opp for bruk av tvangsmidler i forebyggende øyemed var særlig de kvalitative endringene i kriminalitetsbildet. Politimetodeutvalget

[15] SSB.no, «Norsk mediebarometer 2017», https://www.ssb.no/kultur-og-fritid/artikler-og-publikasjoner/norsk-mediebarometer-2017 (Hentet: 11. april 2018).
[16] Prop. 68 L (2015-2016).
[17] Tilføyd ved lov 17 juni 2005 nr. 87.
[18] NOU 2004: 6 *Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed*, s. 55.
[19] Ingvild Bruce og Geir Sunde Haugland, *Skjulte tvangsmidler*, (Oslo 2014) s. 16.

påpekte at de kriminelle miljøene ble bedre organisert, med et større samarbeid mellom ulike kriminelle nettverk. Samtidig økte internasjonaliseringen, spesialiseringen og bruken av avansert teknologi. Disse endringene medførte et behov for å hindre utførelsen av visse typer kriminalitet på et tidligere stadium enn forsøksstadiet.[20]

Endringen i organiseringen av de kriminelle miljøene førte i hovedsak til at miljøene ble mer lukkede. Det ble registrert bruk av vold og trusler for å holde virksomheten lukket, noe som medførte at politiet i mindre grad fikk informasjon utenifra, og derfor hadde et større behov for å selv kunne gå aktivt inn å hente informasjonen. Uten tilgang til informasjonen var muligheten for å hindre lovbruddene lav.[21]

I Politiets sikkerhetstjeneste sin trusselvurdering av 2018 blir det fremhevet at det er «mulig» at det vil forekomme forsøk på terrorangrep i Norge.[22] At det er «mulig» betyr at det er like usannsynlig som det er sannsynlig at det vil skje. Dersom et angrep skulle skje vurderer Politiets sikkerhetstjeneste det som sannsynlig at angrepet vil bli utført av et fåtall personer, ved anvendelse av stikk- eller skytevåpen, kjøretøy eller enkle, eksplosive innretninger.[23]

De siste årene er det begått en rekke terrorangrep rundt om i Europa. Flere av angrepene er blitt utført ved bruk av kjøretøy som våpen, og av enkeltmennesker uten en konkret tilknytning til en spesiell terrorgruppe.[24] Trenden med å bruke kjøretøy som våpen gjør det vanskelig å oppdage angrepet i forkant. Det er ikke uvanlig at mennesker leier eller eier større kjøretøy i forbindelse med jobb, flytting eller andre sammenhenger hvor dette er praktisk. Denne type angrep har stort skadepotensial, og kan utføres på kort tid. Det korte tidsrommet kan gjøre det vanskelig av avverge slike angrep.

I trusselvurdering 2018 blir også etterretningsvirksomhet trukket frem som en sannsynlig trussel mot Norge i 2018.[25] I januar ble Helse Sør-Øst utsatt for et nettverksangrep, som etterforskes som et mulig brudd på straffeloven § 121 *Etterretningsvirksomhet mot*

[20] Ot.prp. nr. 60 (2004-2005) *Om lov om endringer til straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)* s. 9.
[21] Ot.prp. nr. 60 (2004-2005) s. 25.
[22] PST.no, *Trusselvurdering 2018*, https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2018/ (30 januar 2018).
[23] Trusselvurdering 2018.
[24] VG.no, *I disse angrepene brukte de bil som terrorvåpen*, https://www.vg.no/nyheter/utenriks/i/d3lPJ/i-disse-angrepene-brukte-de-bil-som-terrorvaapen.
[25] Trusselvurdering 2018.

statshemmeligheter.[26] Ved nettverksangrep er det vanskelig å avgjøre hvilke datasystemer som er rammet, og derfor også hvor stor skade som har skjedd. De store mengdene av informasjon som er digitalisert i dag medfører at slike angrep har et enormt skadepotensial. PST omtaler virksomheter innen norsk forsvars- og beredskapssektor, statsforvaltning, forskning og utvikling, samt virksomheter innen kritisk infrastruktur, som særskilt utsatte etterretningsmål.[27] Etterretningsvirksomhet ender sjelden med straffeforfølgelse, og behovet for å forebygge handlingene står derfor sentralt.[28]

1.3 Avgrensninger

Bruk av dataavlesning i forebyggende øyemed, jf. politiloven § 17 d, har likhetstrekk med dataavlesning i avvergende øyemed, jf. straffeprosessloven § 222 d. Oppgaven er avgrenset til å omhandle dataavlesning i forebyggende øyemed, men straffeprosessloven § 222 d vil i noen tilfeller være et relevant sammenlikningsgrunnlag. Straffeprosessloven § 222 d vil av den grunn behandles der den har betydning for tolkningen av bestemmelsene som gjør seg gjeldende for den forebyggende bruken.

Dataavlesning medfører at det blir samlet inn store mengder informasjon. Dette aktualiserer problemstillinger vedrørende oppbevaring, håndtering og sletting av denne informasjonen. Det er ikke til å unngå at dataavlesning fanger opp informasjon som ikke er relevant for forebyggingen, ett spørsmål blir da hvilke regler som gjelder for behandlingen av denne overskuddsinformasjonen.[29] Av hensyn til oppgavens omfang har jeg valgt å avgrense mot behandlingen av opplysningene som blir samlet inn.

Fokuset i oppgaven vil i hovedsak være rettet mot de nasjonale rettssikkerhetsgarantiene som gjør seg gjeldende for bruk av dataavlesning i forebyggende øyemed. Internasjonale skranker vil i noen tilfeller bli trukket inn for å belyse hvorvidt de nasjonale rettssikkerhetsgarantiene i tilstrekkelig grad ivaretar rettsikkerheten til individer som rammes av overvåkningen.

[26] Lov av 20. mai 2005 nr. 28.
[27] Trusselvurdering 2018.
[28] Bruce og Haugland (2014) s. 75.
[29] Se Dokument 7:1 (2017-2018), *Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget),* s. 21-23 for ytterligere redegjørelse av problemstillingen.

1.4 Rettskildebilde og metode

Oppgaven er av rettsdogmatisk art, da den foretar en kritisk analyse av om det foreligger tilstrekkelige rettssikkerhetsgarantier til å forsvare bruk av dataavlesning i forebyggende øyemed. Analysen baserer seg på vilkårene som stilles for dataavlesning i forebyggende øyemed, og de forutgående og etterfølgende kontrollmekanismene.

Kildeomfanget om dataavlesning i forebyggende øyemed er begrenset som følge av at dataavlesning er et forholdsvis nytt tvangsmiddel, og informasjon om bruken er gradert. Analysen vil i stor grad bygge på lovforarbeidene og den tilhørende litteraturen, men suppleres av rettspraksis om de øvrige tvangsmidlene, der denne kan belyse oppgavens problemstilling. Også EMD praksis utgjør en sentral kilde der den gir retningslinjer for bruk av skjulte tvangsmidler.

1.5 Den videre fremstillingen

Dataavlesning i forebyggende øyemed er en del av Politiets sikkerhetstjeneste sin forebyggende virksomhet. I kapittel 2 vil jeg kort redegjøre for skillet mellom Politiets sikkerhetstjeneste sin forebyggende virksomhet og etterforskning. I lys av at dataavlesning er en forholdsvis ny metode, finner jeg det nødvendig med en nærmere beskrivelse av tvangsmiddelet. I kapittel 3 vil jeg redegjøre for behovet for å innføre dataavlesning, den lovtekniske gjennomføring, og hvordan dataavlesning utføres. Jeg vil også komme med noen kritiske betraktninger vedrørende metoden.

I kapittel 4 vil jeg foreta en gjennomgang av de ulike materielle rettsikkerhetsgarantiene som er oppstilt for dataavlesning i forebyggende øyemed. Deretter vil jeg ta for meg de prosessuelle rettssikkerhetsgarantiene. I kapittel 6 vil jeg redegjøre for kontrollsystemet for dataavlesning i forebyggende øyemed. Flere av de prosessuelle rettsikkerhetsgarantiene er også en del av kontrollsystemet. Disse vil jeg behandle under kapittel 6.

Avslutningsvis vil jeg oppsummere funnene som er gjort i oppgavens forutgående kapitler.

2. POLITIETS SIKKERHETSTJENESTE

Politiets sikkerhetstjeneste, PST, er en særskilt polititjeneste som er organisert parallelt med politiet, men som rapporterer direkte til Justisdepartementet.[30]

Videre i oppgaven vil jeg referere til «PST» der det gjelder oppgaver som særskilt er tillagt PST, mens jeg vil bruke omtalen «politiet» der det gjelder oppgaver som er felles for politiet og PST.

PST sitt primære ansvar er, jf. politiloven § 17 b, å «forebygge og etterforske» straffbare handlinger mot rikets sikkerhet. Et viktig skille går mellom etterforskning og den forebyggende virksomheten. Skillet avgjør hvilke regler som skal legges til grunn for iverksettelse, og hvilke rettslige konsekvenser og rettigheter som gjør seg gjeldende.[31]

Formålet med virksomheten er et moment som har betydning for å avgjøre om det i det konkrete tilfellet dreier seg om etterforskning eller forebyggende virksomhet. Ved etterforskning er formålet å avdekke om et straffbart forhold er begått, eller er i ferd med å bli begått.[32] Målet med forebyggende virksomhet er å sørge for at det ikke blir grunnlag for å iverksette etterforskning.[33] Forebyggende virksomhet er aktuelt der handlingene har et stort skadepotensial, og konsekvensene av handlingene er så alvorlige, at hensynet til å forebygge handlingen veier tyngre enn hensynet til straffereaksjon.[34]

PST er det eneste politiorganet i Norge som kan anvende tvangsmidler utenfor etterforskning.[35] Hjemmelsgrunnlaget for å utføre det forebyggende arbeidet følger av politiets grunnleggende plikt til å forebygge lovbrudd jf. politiloven § 2 nr. 2 og politiinstruksen § 3-1 tredje ledd. Rammene for bruk av tvangsmiddel i forebyggende øyemed følger av politiloven § 17 d og instruks for politiets sikkerhetstjeneste § 5.[36]

[30] EOS-utvalget.no, *Politiets sikkerhetstjeneste (PST*), https://eos-utvalget.no/norsk/tjenester/eos_tjenestene/politiets_sikkerhetstjeneste_pst_/.
[31]Tor-Geir Myhrer, *Lov om politiet (politiloven)*, Gyldendal Rettsdata (1 november 2013), note 81.
[32] Ot.prp. nr. 60 (2004-2005) s. 42.
[33] Ot.prp. nr. 60 (2004-2005) s. 112.
[34] PST.no, *Oppgaver*, https://www.pst.no/temasider/oppgaver/#Forebyggje,.
[35] Ot.prp. nr. 60 (2004-2005) s. 112.
[36] Instruks for Politiets sikkerhetstjeneste 19. august 2005 nr. 920.

Bruk av tvangsmidler i forebyggende virksomhet blir utført der vilkårene for å igangsette etterforskning ikke er tilstede,[37] dvs. der det ikke foreligger «rimelig grunn til å undersøke om det foreligger et straffbart forhold» jf. straffeprosessloven § 224 første ledd. Dersom vilkårene for å bruke tvangsmidler i avvergende øyemed er oppfylt, jf. straffeprosessloven § 222 d, plikter PST å velge det avvergende sporet fremfor det forebyggende.[38]

Begrunnelsen for å gi PST adgang til tvangsmiddelbruk i forebyggende øyemed er for å fange opp enkelte typer straffri forberedelse.[39] Departementet understreker at slik bruk av tvangsmidler er «en sikkerhetsventil, som bare kan bli brukt når reglene om avverging som ledd i etterforskning ikke er anvendbare».[40] Den utvidede adgangen til tvangsmiddelbruk var en konsekvens av at de kvalitative endringene i kriminalitetsbildet medførte et misforhold mellom de forventningene som ble stilt til PST sitt forebyggende arbeid, og de virkemidlene som PST hadde til rådighet i den forebyggende virksomheten.[41]

[37] Ot.prp. nr. 60 (2004-2005) s. 112.
[38] NOU 2009: 15 s. 229.
[39] NOU 2009: 15 s. 230.
[40] 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)* s. 35.
[41] Ot.prp. nr. 60 (2004-2005) s. 112.

3. DATAAVLESNING

3.1 Behovet

Dataavlesning er ikke et entydig juridisk eller teknologisk begrep.[42] Metodekontrollutvalget definerer metoden som «avlesning av opplysninger i et ikke offentlig tilgjengelig informasjonssystem ved hjelp av programmer eller annet utstyr».[43] Definisjonen av dataavlesning åpner for at en rekke metoder kan anvendes for å innhente opplysninger.

Ifølge straffeprosessloven § 216 o er det kun «datasystem[er]» som kan avleses. Departementet uttaler at «datasystem» skal forstås på samme måte som «computer system» i Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi artikkel 1 bokstav a:[44]

> ««computer system» means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data».

Definisjonen innebærer at bestemmelsen favner vidt. Den omfatter smarttelefoner, datamaskiner og alle andre innretninger bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer.[45]

Dataavlesning ble først vurdert av Politimetodeutvalget i NOU 2004: 6 *Mellom effektivitet og personvern.* Flertallet la til grunn at det på tidspunktet for utredningen var et sterkt behov for å innføre regler om dataavlesning. Bakgrunnen for standpunktet var at krypteringsprogrammer hadde svekket effektiviteten av flere av de øvrige tvangsmidlene, særlig kommunikasjonskontroll og hemmelig ransaking og beslag. Utvalget påpekte at det var uheldig at politiet ikke lenger kunne hente ut den type informasjon som de tidligere hadde tilgang til. De redegjorde videre for behovet for nye regler, uten å foreta en nærmere utredning av hvordan eventuelle regler om dataavlesning skulle innføres.[46] Departementet la til grunn at det var behov for å vurdere metoden nærmere.

---

[42] NOU 2009: 15 s. 240.
[43] NOU 2009: 15 s. 17.
[44] Prop. 68 L (2015-2016) s. 270.
[45] Ot.prp. nr. 22 (2008-2009) *Om lov om endringer i straffeloven 20. mai 2005 nr. 28* s. 400.
[46] NOU 2004: 6 s. 25-26.

Den 15 februar 2008 ble Metodekontrollutvalget oppnevnt for å «etterkontrollere lovgivningen om inngripende etterforskningsmetoder mv.».[47] Utvalget evaluerte den daværende lovgivningen om politiets bruk av skjulte tvangsmidler, og gikk nærmere inn på behovet for å innføre regler om dataavlesning og hva dette ville innebære. Utredningen ble fulgt opp av justis- og beredskapsdepartementet i Prop. 68 L (2015-2016).

Innføringen av reglene som tillater bruk av dataavlesning er begrunnet i den teknologiske utviklingen. Samtidig som en stor del av de kriminelle handlingene planlegges og gjennomføres ved bruk av internett og datasystemer, har fokus på personvern medført et stort antall nye sikkerhetstiltak for å hindre at informasjon som lagres i et datasystem gjøres tilgjengelig for uvedkommende. Blant disse sikkerhetstiltakene er kryptering og andre former for informasjonsbeskyttelse.[48] Kryptering er en «matematisk metode som sørger for konfidensialitet ved at informasjonen ikke kan leses av uvedkommende».[49]

Krypteringen medfører at informasjon som politiet tidligere hadde tilgang til ved bruk av andre tvangsmidler, ikke lenger er leselig for politiet i sin opprinnelige form. Politiet er avhengig av å knekke krypteringen, eller ha tilgang til krypteringsnøkkelen, for å lese informasjonen.

Krypteringsprogrammer er nå så avanserte at politiet ofte ikke har evne til å omgå krypteringen. I de tilfeller krypteringen kan omgås, tar det ofte så lang tid, at informasjonen ikke lenger har betydning for politiet når den er blitt leselig.[50] Den økte bevisstheten på behovet for å beskytte den digitale informasjonen har medført at det i dag er enkelt og billig å skaffe seg avanserte krypteringsprogrammer. Utviklingen har også ført til at det ikke bare er kriminelle enkeltpersoner som ser et behov for å beskytte sin informasjon. Det er i dag vanlig at bedrifter sikrer den digitale informasjonen ved kryptering, for å hindre at uvedkommende skal få tilgang til sensitiv informasjon om bedriften. Det blir også mer vanlig at digitale plattformer krypterer informasjonen som er lagret, uten at brukerne er klar over dette. Et eksempel på dette er den digitale kommunikasjonstjenesten WhatsApp. Tjenesten lar

[47] NOU 2009: 15.
[48] Prop. 68 L (2015-2016) s. 249.
[49] Datatilsynet, *Kryptering*, https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/kryptering/.
[50] NOU 2009: 15 s. 241.

brukerne sende meldinger og gjennomføre taleanrop gratis via internett, og blir ofte brukt til å kommunisere på tvers av landegrenser. WhatsApp har kryptert all data som brukerne kommuniserer i tjenesten.[51] Nasjonal sikkerhetsmyndighet (NSM), avdeling NorCert har bekreftet at bruken av krypteringsprogrammer og andre lignende sikkerhetstiltak vil øke i fremtiden.[52]

Den økte bevisstheten på sikkerhetstiltak for å beskytte digital informasjon er positiv i den forstand at den bidrar til å hindre at kriminelle utfører dataangrep. Den negative siden ved krypteringen er at den fører til at politiets bruk av skjulte tvangsmidler gir betydelig mindre informasjonsutbytte enn tidligere.[53] Det er ikke politiets tilgang til beviset som er problematisk, tilgangen er den samme uavhengig av kryptering eller ikke, men det problematiske er at politiet blir hindret fra å fremkalle innholdet av beviset. Ifølge Kripos har bruken av krypterte nettforbindelser og krypterte autentiseringsdata, i saker hvor kommunikasjonskontroll har vært benyttet, ført til at politiet ikke har fått tilgang til informasjonen i lesbar form.[54] Politiet sin manglende mulighet til å fremkalle bevis, som er lovlig innhentet, er problematisk. Krypteringen gjør det også vanskelig for politiet å ha en begrunnet oppfatning av hvilken informasjon de ikke har fått tilgang til.[55]

De overnevnte problemstillingene dannet bakgrunnen for at dataavlesning i 2016 ble innført som et selvstendig tvangsmiddel. Behovet for å innføre regler som tillater dataavlesning ble bekreftet av blant annet Riksadvokaten, Politiets sikkerhetstjeneste, Økokrim og Det nasjonale statsadvokatembetet for bekjempelse av organisert og annen alvorlig kriminalitet (NAST).[56] Økokrim uttalte at dataavlesning er «en svært effektiv måte å få tilgang til informasjon uten hinder av krypteringen».[57]

[51] WhatsApp*, Sikkerhet*, https://www.whatsapp.com/security/?l=nb.
[52] NOU 2009: 15 s. 241.
[53] Prop. 68 L (2015-2016) s. 249.
[54] Prop. 68 L (2015-2016) s. 249.
[55] Prop. 68 L (2015-2016) s. 249.
[56] Prop. 68 L (2015-2016) s. 249-250.
[57] Prop. 68 L (2015-2016) s. 250.

3.2 Den lovtekniske gjennomføringen

Det var delte meninger om hvordan reglene om dataavlesning skulle innføres. I NOU 2009: 15 ble det redegjort for to mulige løsninger. Den første var å innføre dataavlesning som en gjennomføringsmåte til kommunikasjonskontroll, hemmelig ransaking og beslag. Den andre var å innføre dataavlesning som et selvstendig tvangsmiddel.

Metodekontrollutvalget konkluderte med at det ikke var «dokumentert et tilstrekkelig behov for å innføre dataavlesning som nytt selvstendig tvangsmiddel»,[58] og foreslo å innføre dataavlesning som en gjennomføringsmetode i forbindelse med de eksisterende tvangsmidlene kommunikasjonskontroll og hemmelig ransaking og beslag.[59]

Departementet stilte seg kritisk til metodekontrollutvalget sitt forslag om å innføre dataavlesning som en gjennomføringsmåte, og la vekt på at en slik innføring ikke ville gi politiet en tilfredsstillende tilgang til informasjonen i datasystemet. I straffeprosessloven er det trukket opp et skille mellom lagret informasjon og informasjon som er under overføring. Dersom dataavlesning hadde blitt innført som en gjennomføringsmåte ville dette skillet blitt enda tydeligere.[60]

Forslaget gikk ut på å innføre «et nytt fjerde ledd i straffeprosessloven § 216 a som gir retten adgang til å gi politiet tillatelse til å foreta innbrudd i et datasystem for å kunne gjennomføre kommunikasjonsavlyttingen, dersom avlyttingen er vanskeliggjort på grunn av teknologiske eller andre innretninger».[61]

Hovedproblemet knyttet til denne løsningen er at straffeprosessloven § 216 a kun gir politiet tilgang til å innhente informasjon som er under overføring. Teknologiske løsninger gjør det nå mulig å kommunisere uten at informasjon overføres fra et kommunikasjonsanlegg til et annet.[62] Et eksempel på dette er der flere personer deler tilgang til internettsbaserte e-post og fildelingskontoer. Alle med brukernavn og passord til en slik konto kan opprette, lese og

[58] NOU 2009: 15 s. 244.
[59] NOU 2009: 15 s. 246.
[60] Prop. 68 L (2015-2016) s. 260.
[61] NOU 2009: 15 s. 245.
[62] Prop. 68 L (2015-2016) s. 260.

redigere filer som lagres, uten at informasjonen overføres. Det er ikke gitt at straffeprosessloven § 216 a gir tilgang til slik informasjon.[63]

Metodekontrollutvalget sitt forslag møtte kritikk også i forhold til å innføre dataavlesning som en gjennomføringsmåte for ransaking. Utvalget foreslo en tilføyelse i straffeprosessloven § 200 a første ledd om at «retten kan gi politiet tillatelse til å foreta innbrudd i et datasystem for å kunne gjennomføre ransaking etter denne bestemmelsen».[64] Denne løsningen ville ikke gitt politiet tilgang til å fange opp data som ikke lagres i datasystemet, slik som krypteringsnøkler, passord og annen informasjon som kan brukes til å bryte krypteringen.[65]

Ettersom den teknologiske utviklingen har medført at flere typer data verken lagres eller blir overført, blir det kunstig å trekke et skille mellom informasjonstypene. Ved å innføre dataavlesning som et selvstendig tvangsmiddel blir ikke denne problemstillingen aktuell.[66]

3.3 Den tekniske gjennomføringen

Straffeprosessloven § 216 p angir de nærmere rammene for hvilke fremgangsmåter politiet kan benytte for å foreta avlesning etter straffeprosessloven § 216 o.

Ifølge bestemmelsen kan politiet foreta avlesning «ved hjelp av tekniske innretninger, dataprogram eller på annen måte». Bestemmelsens teknologinøytrale utforming er et virkemiddel som skal sikre at tvangsmiddelet ikke skal bli utdatert som følge av den teknologiske utviklingen, og åpner for at politiet kan anvende en rekke forskjellige fremgangsmåter. [67]

Av taktiske årsaker er det også ønskelig at kriminelle ikke innehar detaljert informasjon om hvordan politiet går frem for å gjennomføre dataavlesningen. Mangelen på detaljer om mulige fremgangsmåter bidrar til at politiet kan benytte fremgangsmåter som ikke er kjent for de

[63] Prop. 68 L (2015-2016) s. 260.
[64] NOU 2009: 15 s. 246.
[65] Prop. 68 L (2015-2016) s. 255.
[66] Prop. 68 L (2015-2016) s. 256-257.
[67] Prop. 68 L (2015-2016) s. 270.

kriminelle. Dette bidrar til at de kriminelle ikke like effektivt kan utvikle sikkerhetstiltak som hindrer politiet tilgang til deres systemer.[68]

De metodene politiet benytter kan deles inn i utstyrs - og informasjonsbaserte fremgangsmåter. Betegnelsene er ikke rettslige, men gir en oversiktlig fremstilling.[69]

De utstyrsbaserte metodene kan igjen deles inn i to hovedkategorier; hardware og softwarebaserte fremgangsmåter.

Hardwarebaserte fremgangsmåter innebærer at det ved et fysisk innbrudd monteres komponenter på datasystemet som skal avleses, eller på annen maskinvare som kan knyttes til datasystemet.[70] Det kan for eksempel monteres utstyr i tastaturet, eller i overgangen mellom tastaturet og datamaskinen, som leser av tastetrykkene. På denne måten får politiet tilgang til all informasjon som går fra tastaturet til datamaskinen. Fremgangsmåten kalles «key-logging». En annen mulighet er å montere utstyr i headsett eller mikrofon som gjør det mulig å fange opp lydsignaler ved kommunikasjon.[71]

For å gjennomføre dataavlesningen ved bruk av hardwarebaserte fremgangsmåter må politiet ved fysisk innbrudd både installere og avinstallere komponentene. Dette er ofte operativt vanskelig. Det er derfor lite sannsynlig at denne fremgangsmåten vil bli benyttet der det finnes andre mulige løsninger, som ikke krever fysisk innbrudd.[72]

Softwarebasert fremgangsmåte går ut på at politiet installerer en programvare i et datasystem eller brukerkonto, som gir de tilgang til å hente ut informasjon.[73] For å få tilgang til systemet kan politiet for eksempel utnytte et sikkerhetshull eller en sårbarhet i systemet. En annen mulighet er å sende en e-post til datasystemet med et skjult vedlegg som inneholder programvaren.[74]

---

[68] Prop. 68 L (2015-2016) s. 264.
[69] Inger Marie Sunde, *Dataavlesning som etterforskningsmetode*, tidsskrift for retfærd, årgang 35 nr. 1/136 2012 s. 3-25 (s. 9).
[70] NOU 2009: 15 s. 248.
[71] NOU 2009: 15 s. 248.
[72] Prop. 68 L (2015-2016) s. 258.
[73] Prop. 68 L (2015-2016) s. 271.
[74] NOU 2009: 15 s. 247.

Informasjonsbaserte fremgangsmåter innebærer at politiet skaffer seg tilgang til datasystemet ved å utnytte brukernavn og passord, uten bruk av teknisk utstyr.[75] Tilgang til brukernavn og passord kan oppnås på flere måter, for eksempel ved at politiet blir kjent med opplysningene og kan benytte seg av ordinær påloggingsprosedyre. En annen måte er at politiet bruker «hackerkompetanse» til å utnytte sårbarheter i programvaren for å trenge seg inn i systemet.[76]

Det finnes også en rekke andre muligheter og kombinasjoner av muligheter, som kan gi politiet tilgang til et datasystem, jf. «på annen måte».

EMK artikkel 8 nr. 2 stiller krav til at inngrepet er «in accordance with the law». Begrunnelsen for vilkåret er at den enkelte skal ha mulighet til å forutse sin rettsstilling og vernes mot vilkårlige myndighetsinngrep. For å oppnå formålet kreves det at inngrepsregler er tilgjengelige og tilstrekkelig presise.[77] Bestemmelsene som hjemler og regulerer dataavlesning fremgår av politiloven og straffeprosessloven, hvilket tilfredsstiller EMD sitt krav til tilgjengelighet.[78] Det er imidlertid nødvendig med en nærmere vurdering av hvorvidt kravet til presisjon er oppfylt.

Ifølge EMD stilles det strengere krav til presisjon jo større inngrepet er. Domstolen la til grunn at det kreves «particularly precise» lovhjemmel for telefonavlytting og romavlytting.[79] Kravet er begrunnet i inngrepets størrelse.[80] Dette taler for at det samme kravet bør gjelde for dataavlesning, da dataavlesning anses for å utgjøre et stort inngrep i personvernet.

EMD har oppstilt visse minstekrav for hva som må være nedfelt i lovhjemmelen.[81] Det kreves blant annet at lovhjemmelen angir karakteren av de forbrytelsene som kan gi grunnlag for overvåkning,[82] hvem som kan bli gjenstand for overvåkningen,[83] og at det foreligger en grense for varigheten av overvåkningen.[84]

[75] Sunde (2012) s. 11.
[76] Sunde (2012) s. 11.
[77] Husabø (2015) s. 247-248.
[78] Husabø (2015) s. 247-248.
[79] Kruslin mot Frankrike avsn. 33.
[80] Husabø (2015) s. 248.
[81] Weber og Savaria mot Tyskland avsn. 95.
[82] Se punkt 4.1.2.
[83] Se punkt 4.1.1.
[84] Se punkt 5.1.

Kravet til presisjon innebærer også at «the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity».[85] Formuleringen stiller krav til at lovhjemmelen angir hvordan myndighetene gjennomfører dataavlesningen, og hvilken informasjon avlesningen omfatter.

Straffeprosessloven § 216 p gir en indikasjon på at det er ulike teknologiske fremgangsmåter som vil benyttes ved dataavlesning, men det kan stilles spørsmål ved om formuleringen «på annen måte» møter de krav som EMD oppstiller.

I 2015, da arbeidet med å utforme regler for dataavlesning pågikk i Norge, påpekte EMD at klare og detaljerte regler var særlig viktig for kommunikasjonsavlytting. Dette nettopp fordi teknologien stadig blir mer avansert.[86] At den nøytrale utformingen av straffeprosessloven § 216 p blant annet er begrunnet i den teknologiske utviklingen er betenkelig sett i lys av uttalelsen fra EMD.

Departementet uttalte at «fravær av detaljerte beskrivelser må imidlertid ledsages av tydelige ytre grenser for hva politiet skal ha anledning til å foreta seg med grunnlag i en tillatelse til dataavlesning».[87]

Straffeprosessloven § 216 o fjerde ledd annet punktum angir grensene for hvilken informasjon som kan avleses. Ifølge bestemmelsen kan avlesningen omfatte «kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen».

Ordlyden er forholdsvis åpen, og det kan være uklart hvilken informasjon som omfattes av avlesningen.

Det fremgår av forarbeidene at informasjonen som kan avleses bare begrenses av «hva slags informasjonssystem det dreier seg om og funksjonaliteten til program- eller maskinvaren som benyttes».[88] Dataavlesning kan for eksempel innebære avlesning av lydstrøm som sendes fra en tilknyttet mikrofon, videostrøm som sendes fra et tilknyttet webkamera og geografiske

[85] Roman Zakharov mot Russland avsn. 231.
[86] Roman Zakharov mot Russland avsn. 229.
[87] Prop. 68 L (2015-2016) s. 264.
[88] Prop. 68 L (2015-2016) s. 224.

koordinatinformasjon fra en tilknyttet GPS-enhet.[89] Dette viser at avlesningen kan omfatte mer enn hva som fremgår av ordlyden.

Det blir imidlertid presisert at dataavlesning skal kompensere for effekttapet kommunikasjonsavlytting og hemmelig ransaking har hatt som følge av den teknologiske utviklingen. Dataavlesning er ment å omfatte tilgang til «samme type elektronisk informasjon som politiet ellers har rettslig adgang til» gjennom disse tvangsmidlene.[90]

En begrensning av hva som kan avleses følger av at det kun er informasjon «om bruk» av datasystemet eller brukerkontoen som kan avleses. Dette innebærer at avlesningen «ikke skal gi politiet adgang til å manipulere datasystemet for å drive andre former for skjult overvåkning. Politiet kan for eksempel ikke selv aktivere mikrofoner tilknyttet datasystemet for å fange opp lyd i et rom, eller slå på et tilknyttet kamera for å skaffe seg stillbilder eller levende bilder fra stedet der datasystemet befinner seg».[91]

Utformingen av bestemmelsen er vag, sett i lys av at metoden kan innebære avlesning av mer informasjon enn den forarbeidene presiserer at det tas sikte på å avlese. Dette kan være problematisk i forhold til de krav som EMD stiller til lovhjemmelens presisjon.

3.4 Kritiske betraktninger

Ved innføringen av dataavlesning stilte flere av høringsinstansene, deriblant datatilsynet, seg kritisk til å åpne opp for en metode som innebærer at «tanker, assosiasjoner og ønsker som kanskje engang aldri var tenkt kommunisert til noen andre blir gjenstand for politiets behandling».[92]

Det var særlig metoden «key-logging» som dannet grunnlaget for kritikken. Metoden gir politiet mulighet til å fange opp alle tastetrykk mellom datasystemet og tastaturet, også informasjon som verken blir lagret eller kommunisert. Dette kan illustreres ved at dataavlesning for eksempel fanger opp tastetrykk der brukeren av datasystemet anvender et

[89] Prop. 68 L (2015-2016) s. 224.
[90] Prop. 68 L (2015-2016) s. 264-265.
[91] Prop. 68 L (2015-2016) s. 264.
[92] Prop. 68 L (2015-2016) s. 252.

tekstbehandlingsprogram til å formulere tanker eller betraktninger, som vedkommende ikke har til hensikt å lagre.[93] Tilgang til slik informasjon gjør at dataavlesning fremstår som meget integritetskrenkende.

Metoden fører likevel ikke til en vesentlig utvidelse, sett i forhold til den informasjonen politiet hadde tilgang til før dataavlesning ble innført som et selvstendig tvangsmiddel. Bestemmelsene om ransaking og beslag gir politiet tilgang til personlige notater, slik som dagbøker.[94] Det legges også til grunn at det ikke kan anses som vanlig at datasystemer blir brukt til å formulere betraktninger som det ikke er meningen at skal lagres.[95]

PST uttaler at dataavlesning vil medføre at politiet «ved mindre integritetskrenkelser settes i stand til bedre å bekjempe de alvorligste straffbare handlingene».[96] Synspunktet deles av departementet, som vektlegger at dataavlesning innebærer mer målrettet informasjonsinnhenting enn de øvrige tvangsmidlene.[97] Begrunnelsen er at tradisjonell kommunikasjonsavlytting ofte innebærer at avlyttingspunktet er en internettforbindelse, og at politiet kontrollerer all kommunikasjon over internettforbindelsen. Ved dataavlesning har politiet mulighet til å begrense avlesningen til for eksempel å gjelde en bestemt brukerkonto eller en bestemt smarttelefon, som i hovedsak bare brukes av det individet som avlesningen retter seg mot. [98]

[93] Prop. 68 L (2015-2016) s. 265-266.
[94] Prop. 68 L (2015-2016) s. 265.
[95] Prop. 68 L (2015-2016) s. 266.
[96] Prop. 68 L (2015-2016) s. 250.
[97] Prop. 68 L (2015-2016) s. 265.
[98] Prop. 68 L (2015-2016) s. 265.

4. MATERIELLE RETTSSIKKERHETSGARANTIER

4.1 Vilkår for tvangsmiddelbruk i forebyggende øyemed

4.1.1 Mistankekravet

For å iverksette bruk av tvangsmidler i forebyggende øyemed kreves det at det er «grunn til å undersøke om noen forbereder» den aktuelle straffbare handlingen, jf. politiloven § 17 d første ledd.

Ordlyden av «om noen forbereder» tilsier at det stilles krav om formålsbestemthet.

Kravet medfører at det bare er undersøkelser som er saklig begrunnet i PST sin forebyggende virksomhet, slik den kommer til uttrykk i politiloven § 17 b, som kan danne grunnlag for undersøkelse.[99] Dette innebærer at PST ikke har anledning til å anvende tvangsmidler for å innhente opplysninger som ikke har relevans for den forebyggende virksomheten. Dersom PST sitt formål med tvangsmiddelbruken for eksempel er å anvende de innhentede opplysningene som ledd i etterforskning, kan ikke tillatelse gis etter politiloven § 17 d.[100]

Uttrykket «dersom det er grunn til å undersøke» tilsier at det stilles konkrete krav til de faktiske opplysningene som ligger til grunn for å anvende tvangsmidlene.

I innstillingen fra justiskomiteen ble departementet sitt forslag til ny § 17 d i politiloven endret. Departementets forslag til grunnvilkåret var «for å undersøke om noen forbereder en handling». Flertallet i justiskomiteen vektla at bruk av tvangsmidler i forebyggende øyemed medfører en større risiko for at uskyldige rammes av tvangsmiddelbruken, og fremmet derfor forslag om å erstatte vilkåret med «dersom det er grunn til å undersøke om noen forbereder en handling».[101] Begrunnelsen for å endre ordlyden var for å tydeliggjøre at PST må «godtgjøre overfor domstolen at opplysningene i det konkrete saksforholdet gir grunn til å gjennomføre nærmere undersøkelser» for å få tillatelse til å ta i bruk metoden.[102] Slik flertallet så det ville endringen være viktig for befolkningens tillit til PST og det arbeidet de utfører.

[99] Ragnar L. Auglend og Henry John Mæland, *Politirett,* (Oslo 2016) s. 390-391.
[100] Ot.prp. nr. 60 (2004-2005) s. 151.
[101] Innst. O. nr. 113 (2004-2005) s. 34.
[102] Innst. O. nr. 113 (2004-2005) s. 34.

Ved tvangsmiddelbruk i forebyggende øyemed blir personvernet og rettsikkerheten til de individer som rammes av bruken utfordret. Tillit til at PST utfører sitt arbeid i tråd med de rammer som er oppstilt er derfor viktig. En slik tillit vil hindre mistanke om politisk motivert overvåkning, og skape trygghet om at det er handlinger, ikke holdninger, som danner grunnlag for at det tillates bruk av tvangsmidler i forebyggende øyemed.[103]

Uttrykket «grunn til å undersøke om noen forbereder» innebærer at det må godtgjøres «ytre konstaterbare og etterprøvbare opplysninger eller forhold som gir grunn til å gjennomføre nærmere undersøkelser».[104] Slike objektive holdepunkter kan være saksopplysninger i form av spanings- eller infiltrasjonsopplysninger, tips, dokumentfunn eller andre bevis som indikerer at noen kan være i ferd med å forberede bestemte straffbare handlinger, som for eksempel en terrorhandling.[105]

Vurderingstemaene for grunnvilkåret ble ytterligere klargjort da flertallet i justiskomiteen påpekte at vilkåret har klare likhetstrekk med mistankekravet for å iverksette etterforskning etter straffeprosessloven § 224 første ledd. Ifølge flertallet gir uttrykket «rimelig grunn til å undersøke» i straffeprosessloven § 224 første ledd veiledning for forståelsen av grunnvilkåret i politiloven § 17 d.[106] På bakgrunn av dette ligger det tre krav innbakt i vilkåret; et saklighetskrav, krav om en viss sannsynlighet for at noe er under forberedelse, og et krav om forholdsmessighet mellom det som skal undersøkes og de virkemidler som tas i bruk.[107] Kravene innebærer at PST ikke kan foreta nærmere undersøkelser basert på utsagn som det åpenbart ikke er hold i. Dersom det er hold i utsagnene kan bruk av tvangsmidler være nødvendig, men slik bruk må avsluttes dersom det ikke fremkommer ytterligere opplysninger som underbygger at en handling som rammes av kriminalitetskravet er i ferd med å bli forberedt. Forholdsmessighetskravet medfører også at «grunn til å undersøke» er relativt i forhold til handlingens alvor. Kravet oppfylles derfor lettere dersom det for eksempel er snakk om en terrorhandling, enn om det gjelder forebygging av trusler mot politikere.[108]

[103] Innst. O. nr. 113 (2004-2005) s. 34.
[104] Auglend og Mæland (2016) s. 391.
[105] Auglend og Mæland (2016) s. 391.
[106] Innst. O. nr. 113 (2004-2005) s. 35.
[107] Innst. O. nr. 113 (2004-2005) s. 35.
[108] Innst. O. nr. 113 (2004-2005) s. 35.

Ved å oppstille klare vurderingstemaer for mistankekravet foreligger det et bedre grunnlag for å sikre en reel og grundig domstolsbehandling. Klare vurderingstemaer hindrer også at bruk av tvangsmidler i forebyggende øyemed blir benyttet i større grad enn hva formålet tilsier.[109]

4.1.2 Kriminalitetskravet

Det er kun utvalgte handlinger kan danne grunnlag for å anvende dataavlesning i forebyggende øyemed, jf. politiloven § 17 d bokstav a-d. Den forebyggende virksomheten er begrenset til å gjelde terrorhandlinger etter straffeloven §§ 131, 133 og 134, ulovlig etterretningsvirksomhet etter straffeloven §§ 121 til 126, og vold eller trusler rettet mot representanter for Norges øverste statsmyndighet eller tilsvarende organer i andre stater etter straffeloven §§ 251, 254, 256, 263, 273 eller 275.

Hvilke handlinger som skulle rammes av den forebyggende virksomheten ble diskutert i flere sammenhenger forut for innføringen av politiloven § 17 d. I NOU 2003: 18 *Rikets sikkerhet* viser Lund-utvalget til at inngripende tvangsmidler bare skal kunne brukes dersom det anses som nødvendig etter en avveining av hensynet til samfunnsvern mot hensynet til rettssikkerhet og personvern.[110] PST sitt forslag var å tillate bruk av tvangsmidler i forebyggende øyemed for de straffebud som kvalifiserer til tvangsmiddelbruk i avvergende øyemed etter straffeprosessloven § 222 d.[111]

Departementet la til grunn at lovgiver ønsket en snever adgang til å benytte tvangsmidler i forebyggende øyemed, og fant det ikke hensiktsmessig at det skulle være samsvar mellom kriminalitetskravet ved forebyggende og avvergende virksomhet.[112] Ved bruk av tvangsmidler i forebyggende øyemed er risikoen for at uskyldige tredjepersoner rammes høyere, og hensynet til rettssikkerhet veier derfor tungt. Dette er bakgrunnen for at tvangsmiddelbruk i forebyggende øyemed i dag er en sikkerhetsventil som bare kan benyttes for de mest alvorlige lovbruddene, som ligger i kjernen av PST sin oppgave om å beskytte rikets sikkerhet.[113]

[109] Innst. O. nr. 113 (2004-2005) s. 35.
[110] NOU 2003: 18 *Rikets sikkerhet. Straffekommisjonens delutredning VIII,* s. 17-18.
[111] Prop. 68 L (2015-2016) s. 205-206.
[112] Prop. 68 L (2015-2016) s. 208.
[113] Prop. 68 L (2015-2016) s. 205 og 208.

Det strenge kriminalitetskravet taler for at tvangsmiddelbruken i forebyggende øyemed faller innenfor hva som kan anses som et legitimt formål jf. EMK artikkel 8 nr. 2.[114]

4.1.3 Indikasjonskrav og subsidiaritetskrav

Ytterligere vilkår for bruk av tvangsmidler i forebyggende øyemed oppstilles i politiloven § 17 d annet ledd. Det følger av bestemmelsen at tillatelse bare kan gis dersom det «er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge saken» og «forebygging ellers i vesentlig grad vil bli vanskeliggjort».

Det oppstilles her et indikasjonskrav og et subsidiaritetskrav. Formuleringen i politiloven § 17 d annet ledd har på dette punkt store likheter med formuleringen i straffeprosessloven § 222 d, og skal ifølge motivene forstås på samme måte.[115]

Indikasjonskravet fremgår av at det kreves «grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge saken». Ifølge motivene innebærer dette at det kreves «en viss grad av sannsynlighet for at metodebruken vil bidra med opplysninger av betydning for det formål som ligger til grunn for metodebruken».[116] Opplysninger som er mer perifere for formålet med metodebruken kan således ikke begrunne bruk av tvangsmidler. Graden av sannsynlighet som kreves er relativt. Dette innebærer at det i noen tilfeller kreves sannsynlighetsovervekt for at metoden vil bidra til å forebygge handlingen, mens det i andre tilfeller vil være tilstrekkelig at det er en realistisk mulighet for det. Hvor vesentlig bidrag opplysningene kan antas å gi for å forebygge handlingen vil her være av betydning.[117]

Kravet om at «forebygging ellers i vesentlig grad vil bli vanskeliggjort» blir omtalt som subsidiaritetskravet. Ifølge motivene innebærer kravet at «metodebruk bare skal finne sted når mindre inngripende metoder ikke anses anvendelige».[118] Dette er likevel ikke til hinder for at det kan tas hensyn til fornuftig ressursanvendelse, og andre mulige ulemper knyttet til alternativ innhenting av opplysningene. Dersom en mindre inngripende metodebruk vil medføre at polititjenestemenn eller andre utsettes for farlige situasjoner, kan dette tale for å

[114] Husabø (2015) s. 249.
[115] Ot.prp. nr. 60 (2005-2005) s. 152.
[116] Ot.prp. nr. 60 (2005-2005) s. 70.
[117] Ot.prp. nr. 60 (2005-2005) s. 71.
[118] Ot.prp. nr. 60 (2005-2005) s. 71.

anvende det tvangsmiddelet som hindrer at slike situasjoner oppstår.[119] Det skal også tas hensyn til om det er begrenset tid til rådighet for å forebygge handlingen. Dersom handlingen fryktes å være nært forestående kan det for eksempel ikke kreves at opplysningene forsøkes innhentes ved spaning, da dette vil ta for lang tid.[120]

4.1.4 Krav om forholdsmessighet

I politiloven § 17 d annet ledd oppstilles det et forholdsmessighetskrav. Det følger av bestemmelsen at tillatelse til bruk av tvangsmidler bare kan gis dersom «inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig».

Kravet til forholdsmessighet ble oppstilt fordi politiloven ikke har en generell forholdsmessighetsregel tilsvarende straffeprosessloven § 170 a. Departementet la til grunn at forholdsmessighetskravet ved bruk av tvangsmidler i forebyggende øyemed skal forstås på samme måte som forholdsmessighetskravet ved bruk av tvangsmidler under etterforskning i § 170 a.[121] Dette innebærer at «nytten eller fordelen [ved tvangsmiddelbruken] må være større enn ulempene eller skaden».[122] Selv om forholdsmessighetskravet skal forstås på samme måte ved bruk av tvangsmidler i etterforskning og forebyggende virksomhet, medfører det senkede mistankekravet i politiloven § 17 d at forholdsmessighetsvurderingen etter politiloven § 17 d vil være strengere.[123]

Forholdsmessighetsvurderingen grenser mot vurderingen av indikasjons- og subsidiaritetskravet. Forskjellen i vurderingene er hvem fokuset retter seg mot. Mens forholdsmessighetsvurderingen skal avgjøre om tvangsmiddelbruken er forholdsmessig for den eller de som utsettes for den, er det politiets behov for tvangsmiddelbruk som er i fokus ved om indikasjons- og subsidiaritetskravet er oppfylt.[124] Selv om fokuset er rettet forskjellig i vurderingene, medfører den nære sammenhengen at forholdsmessighetsvurderingen gir en «anvisning på en interesseavveining der enkeltindividets interesse i ikke å bli utsatt for kontroll, skal veies opp mot politiets interesse i at metoden brukes».[125] Behovet for

[119] Ot.prp. nr. 60 (2005-2005) s. 71.
[120] Ot.prp. nr. 60 (2005-2005) s. 71.
[121] Ot.prp. nr. 60 (2005-2005) s. 152.
[122] NOU 2004: 6 s. 52.
[123] NOU 2009: 15 s. 247.
[124] Ot.prp. nr. 60 (2005-2005) s. 72.
[125] NOU 2004: 6 s. 192.

tvangsmiddelbruken vil således være moment som også vil ha betydning i forholdsmessighetsvurderingen.

Sentralt ved vurderingen av om tvangsmiddelbruken er forholdsmessig er mistankens styrke. Dersom politiet vurderer det som svært sannsynlig at vedkommende forbereder en handling som nevnt i politiloven § 17 d første ledd bokstav a-d, vil det sjelden være uforholdsmessig å gi tillatelse til å bruke tvangsmidler.

Alvoret i den forbrytelse som det er grunn til å undersøke om noen forbereder, har også betydning for forholdsmessighetsvurderingen. De straffbare handlingene som kan gi grunnlag for bruk av tvangsmiddel i forebyggende øyemed er alle alvorlige forbrytelser som kan gi store skadevirkninger.[126] Likevel vil en mulig forberedelse av en terrorhandling lettere kunne begrunne bruk av inngripende tvangsmidler enn for eksempel trusler mot myndighetspersoner. Dette på grunn av det potensielt store materielle og personelle skadeomfanget en terrorhandling kan ha.

Ved bruk av dataavlesning foreligger det ingen garanti for at utenforstående ikke vil rammes av tvangsmiddelbruken. Sannsynligheten for at utenforstående rammes av tvangsmiddelbruken må derfor inngå som et moment i forholdsmessighetsvurderingen.[127]

Politiloven § 17 d gir hjemmel for bruk av en rekke tvangsmidler. Et relevant moment i forholdsmessighetsvurderingen er hvor inngripende det aktuelle tvangsmiddelet er.[128] Dataavlesning anses som et meget inngripende tvangsmiddel, noe som taler for at bruken lettere anses som uforholdsmessig.

4.2 Særvilkår for dataavlesning i forebyggende øyemed

4.2.1 Skjerpet forholdsmessighetskrav

Politiloven § 17 d annet ledd annet punktum oppstiller et skjerpet forholdsmessighetskrav for utvalgte tvangsmidler, deriblant dataavlesning. Ifølge bestemmelsen kreves det «særlige

[126] Ot.prp. nr. 60 (2004-2005) s. 73.
[127] NOU 2004: 6 s. 192.
[128] Ot.prp. nr. 60 (2004-2005) s. 72.

grunner» for å gi tillatelse til å ta i bruk disse tvangsmidlene. Bakgrunnen for kravet er tvangsmiddelets inngripende karakter.

Ordlyden «særlige grunner» tilsier at det skal mye til for å gi tillatelse til å anvende dataavlesning i forebyggende øyemed. Uttrykket skal forstås på samme måte som i straffeprosessloven § 222 d tredje ledd.[129] Departementet uttaler at vurderingen «ikke [skal] være vesensforskjellig fra den som må foretas der begjæringen knytter seg til andre og mindre inngripende tvangsmidler, men kravet om særlige grunner er ment å markere at det skal mer til enn ellers for å tillate bruk av tvangsmidler».[130]

4.2.2 Dataavlesning ved innbrudd i private hjem

Politiloven § 17 d annet ledd tredje og fjerde punktum oppstiller ytterligere begrensninger i retten til å anvende tvangsmidler i «noens private hjem».

Tredje punktum oppstiller et absolutt forbud mot romavlytting i forebyggende øyemed i noens private hjem. Begrunnelsen for forbudet er et ønske om å «ikke trå grunnloven for nær»,[131] da Grunnloven § 102 setter skranker for husinkvisisjoner. Departementet understreker at «romavlytting representerer et av de aller mest inngripende virkemidler norsk politi har til rådighet, og utgjør et betydelig inngrep i personvernet. Dette skyldes ikke minst at det ved bruk av metoden er nær sagt uunngåelig at uskyldige tredjepersoner kan bli gjenstand for overvåkning».[132] Tredje punktum er således et utslag av at personvernet her veier tyngre enn hensynet til samfunnssikkerhet.

Fjerde punktum åpner for at det kan gis tillatelse til å «ransake eller ved dataavlesning å gjøre innbrudd i noens private hjem». Det kreves at de øvrige vilkårene i politiloven § 17 d er oppfylt, samtidig som fjerde punktum er begrenset til gjelde terrorrelaterte handlinger jf. første ledd bokstav a.

Ved innføringen av fjerde punktum la departementet vekt på at grunnloven ikke oppstiller en absolutt skranke mot husinkvisisjoner, og at en utvidelse i forhold til skranken i tredje

[129] Ot.prp. nr. 60 (2004-2005) s. 152.
[130] Ot.prp. nr. 60 (2004-2005) s. 73.
[131] Ot.prp. nr. 60 (2004-2005) s. 132.
[132] Prop. 68 L (2015-2016) s. 217.

punktum derfor ikke ville være i strid med loven.[133] Det er flere grunner til at det ble åpnet for ransaking og innbrudd ved dataavlesning. Metodene anses som mindre inngripende enn romavlytting. Romavlytting medfører en kontinuerlig overvåkning over tid, mens ransaking og innbrudd innebærer av overvåkningen skjer gjennom mer målrettede prosesser. Sannsynligheten for at tvangsmiddelbruken rammer utenforstående er begrenset i forhold til romavlytting. Nytteverdien av metodene var også et argument for tilføyelsen av fjerde punktum. Ved å ransake noens bolig kan politiet raskt avsløre om det oppbevares materiale som kan anvendes ved terrorhandlinger, slik som for eksempel våpen eller sprengstoff.[134]

Departementet fant det også hensiktsmessig å differensiere mellom lovbrudd. Fjerde punktum åpner for at det kun er handlinger knyttet til terror som kan begrunne bruk av tvangsmidler i noens private hjem. Terroraksjoner har et meget stort skadepotensial, både når det kommer til tap av menneskeliv, og materielle ødeleggelser. Sett i sammenheng med at utviklingen i samfunnet går i retning av at forberedelsestiden på terroraksjoner er blitt kortere,[135] er det viktig at politiet har mulighet til å komme inn på et stadium i hendelsesforløpet hvor det fremdeles er mulig å forhindre den straffbare handlingen.

4.2.3 Spesifisering av avlesningsobjektet

Straffeprosessloven § 216 o fjerde ledd oppstiller begrensninger til hvilke datasystemer og brukerkontoer det kan gis tillatelse til å avlese. Ifølge bestemmelsen kan det bare gis tillatelse til å avlese «bestemte» datasystemer eller brukerkontoer som den mistenkte «besitter eller kan antas å ville bruke». Kravet skal forstås på samme måte som tilsvarende uttrykk i straffeprosessloven § 216 a tredje ledd.[136]

Kravet om «bestemte» datasystemer eller brukerkontoer innebærer at objektet for dataavlesningen må identifiseres i politiets begjæring og rettens kjennelse.[137] Ifølge departementet innebærer kravet at «angivelsen må være så spesifikk som mulig for å unngå tvil om hvilke objekter som tillates avlest».[138] For eksempel kan brukerkontoer identifiseres med brukernavn eller e-postadresse, mens utstyr kan identifiseres ved at utstyrets fabrikant

[133] Prop. 68 L (2015-2016) s. 215.
[134] Prop. 68 L (2015-2016) s. 217.
[135] Prop. 68 L (2015-2016) s. 215.
[136] Prop. 68 L (2015-2016) s. 270.
[137] Prop. 68 L (2015-2016) s. 270.
[138] Prop. 68 L (2015-2016) s. 270.

opplyses, eller ved å angi det geografiske stedet utstyret befinner seg på og hvem som har rådighet over det.[139]

Bakgrunnen for å tillate overvåkning av brukerkontoer er at denne type overvåkning er mer målrettet og effektiv enn å overvåke hele datasystemer. En brukerkonto kan være knyttet til en rekke datasystemer gjennom brukernavn og passord. Tilgang til brukerkontoer gir politiet mulighet til å avlese den ønskede informasjonen, uten at de gis tilgang til all informasjon som befinner seg i datasystemene knyttet til brukerkontoen. Et datasystem kan for eksempel være en datamaskin som flere har tilgang til.[140] En brukerkonto bærer et mer personlig preg, og slik avlesning medfører at det er mindre sannsynlighet for at utenforstående rammes. Fremgangsmåten bidrar til bedre rettsikkerhet.

Bestemmelsen oppstiller også et krav om at det kun er datasystemer eller brukerkontoer som den mistenkte «besitter eller kan antas å ville bruke» som kan avleses. Med «bruke» siktes det til den «direkte bruken av for eksempel en datamaskin, smarttelefon eller andre typer terminaler.»[141] Dette innebærer at en tillatelse til å avlese for eksempel en smarttelefon gir tilgang til å avlese all informasjon som er tilgjengelig fra telefonen, uavhengig av om informasjonen er lagret lokalt på telefonen eller på en internettserver. Kravet innebærer en begrensning ved at det ikke gis adgang til å direkte avlese servere hos tjenesteleverandøren som mistenkte bare indirekte gjør bruk av.[142]

Ordlyden «kan antas å ville bruke» tilsier at det må foreligge konkrete holdepunkter for at slik bruk vil skje. Kravet innebærer at det ved «objektive kriterier kan konstateres en viss sannsynlighet for at mistenkte vil bruke det datasystem eller den brukerkonto som ønskes avlest.»[143] Videre presiserer departementet at «det ikke kreves sannsynlighetsovervekt, men det må være objektive holdepunkter for at mistenkte vil bruke det aktuelle datasystemet. Rene formodninger er altså ikke tilstrekkelig».[144]

[139] Prop. 68 L (2015-2016) s. 270.
[140] Prop. 68 L (2015-2016) s. 270.
[141] Prop. 68 L (2015-2016) s. 270-271.
[142] Prop. 68 L (2015-2016) s. 271.
[143] Prop. 68 L (2015-2016) s. 271.
[144] Prop. 68 L (2015-2016) s. 271.

Høyesterett har slått fast at selv om et datasystem, for eksempel en telefon, blir brukt gjennom en tredjemann avskjærer det ikke avlesning.[145]

[145] Rt. 2006 s. 1546.

5. PROSESSUELLE RETTSSIKKERHETSGARANTIER

5.1 Tidsbegrensing

Dataavlesning kan bare foretas innenfor fastsatte tidsbegrensinger. Det følger av politiloven § 17 e første ledd at tillatelse kan gis for inntil 6 måneder av gangen «dersom særlige omstendigheter tilsier at en fornyet prøving etter 4 til 8 uker vil være uten betydning».

Ordlyden tilsier at tillatelse som hovedregel kun skal gis for 4 til 8 uker av gangen. Dette bekreftes av departementet.[146] Muligheten for å gi tillatelse for 6 måneder er begrunnet i at et særtrekk ved det forebyggende arbeidet er at det ofte har et lenger tidsperspektiv enn tilsvarende bruk i etterforskning. Ved bruk av inngripende tvangsmidler skal muligheten til å gi langvarige tillatelser «nyttes med varsomhet».[147] Ettersom dataavlesning anses som et meget inngripende tvangsmiddel taler dette for at det skal mye til for å gi langvarig tillatelse.

Ytterligere krav følger av bestemmelsens tredje punktum. Tvangsmiddelbruken skal avsluttes før fristens utløp dersom «vilkårene ikke lenger er oppfylt» eller tvangsmiddelbruken «ikke lenger anses som hensiktsmessig». Vilkåret henger nært sammen med kravet om forholdsmessighet,[148] og innebærer at tvangsmiddelbruken «kontinuerlig [må] være forholdsmessig».[149]

5.2 Gjennomføringen av avlesningen

Straffeprosessloven § 216 p stiller krav til gjennomføringen av dataavlesningen. Kravene skal sikre at dataavlesning innebærer så liten sikkerhetsrisiko for mistenktes datasystem som mulig.[150]

Første ledd første punktum stiller krav til hvem som kan utføre dataavlesning. Det følger av bestemmelsen at dataavlesning kun kan utføres av «personell som er skikket til det». Kravet må ses i sammenheng med annet ledd annet og tredje punktum som stiller krav til at

[146] Ot.prp. nr. 60 s. 153.
[147] Ot.prp. nr. 60 s. 153.
[148] Se punkt 4.1.4.
[149] NOU 2004: 6 s. 52.
[150] NOU 2009: 15 s. 248.

avlesningen skal «utføres slik at det ikke unødig voldes fare for driftshindring eller for skade på utrustning eller data» og at «politiet skal så vidt mulig avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger».

Dataavlesning kan blant annet foregå ved at politiet installerer en programvare som gir de tilgang til datasystemet.[151] Det er viktig å sørge for at gjennomføringen og avinstalleringen foregår så effektivt som mulig, uten at det fører til sikkerhetshull som gjør det mulig for andre enn politiet å overta eller utnytte programvaren.[152] Personell med tilstrekkelig høy informasjonsteknologisk kompetanse er et sentralt virkemiddel for å oppfylle kravene som stilles til gjennomføringen etter annet ledd.

Metodekontrollutvalget påpeker at det også vil være i politiets interesse å utvikle sikre programvareløsninger. Dersom avlesningen ødelegger eller forstyrrer elementer i brukerens datasystem, øker faren for at avlesningen blir oppdaget. Dette kan føre til at metodebruken avsløres og etterforskningen spoleres. Utvalget påpeker også at politiet vil være erstatningsansvarlig dersom datasystemet blir ødelagt.[153]

På bakgrunn av disse forholdene uttaler Metodekontrollutvalget at sikkerhetsrisikoen i forbindelse med avlesningen er «liten og innenfor et akseptabelt nivå».[154] Sikkerhetsrisikoen i det enkelte tilfellet vil være et moment i forholdsmessighetsvurderingen jf. politiloven § 17 d annet ledd. Det er derfor opp til retten å vurdere om sikkerhetsrisikoen i det enkelte tilfellet er akseptabel.

[151] Se punkt 3.3.
[152] NOU 2009: 15 s. 248.
[153] NOU 2009: 15 s. 248.
[154] NOU 2009: 15 s. 248.

6. KONTROLLSYSTEMET

6.1 Generelt

Bruk av dataavlesning som et skjult tvangsmiddel i forebyggende øyemed innebærer et stort inngrep i den private sfæren til de som rammes av bruken. For å ivareta hensynet til personvern og rettssikkerhet er det viktig å ha på plass kontrollmekanismer som kan sikre notoritet rundt bruken. Kontrollen med bruken av skjulte tvangsmidler består av en rekke enkeltmomenter, som til sammen utgjør er «kontrollsystem».[155]

På 1990-tallet ble det fremmet en rekke påstander om at norske borgere hadde vært gjenstand for omfattende ulovlig overvåkning. Lund-utvalget ble i 1994 opprettet for å granske disse påstandene.[156] Resultatet av utvalgets granskning viste blant annet at PST fra 1940 til 1960-tallet drev omfattende ulovlig romavlytting. Det ble blant annet avslørt at en enkeltperson hadde blitt overvåket 14 år i strekk, på bakgrunn av mistanke om å ha begått en forbrytelse som kunne gi ett års fengsel.[157] Lund-utvalget påpekte at den manglende kontrollen av tvangsmiddelbruken, både fra domstolen og fra kontrollutvalgets side, hadde vært med på å muliggjøre den ulovlige overvåkningen. Både den rettslige reguleringen av og kontrollen med PSTs tvangsmiddelbruk er i årene etter disse avsløringene blitt betydelig utbedret.[158]

Bruk av dataavlesning i forebyggende øyemed innebærer at PST avleser informasjonen uten at vedkommende som utsettes for tvangsmiddelbruken blir informert om det.[159] Hemmelighold rundt tvangsmiddelbruken svekker flere av rettssikkerhetsgarantiene til de som rammes. Målet er derfor å opparbeide et effektivt kontrollsystem som stryker befolkningens tillitt til at PST kun anvender tvangsmidler innenfor lovens rammer. Et effektivt kontrollsystem er av Metodekontrollutvalget sin oppfatning et system som «beskytter mot, fanger opp og sikrer mot svikt eller mangler på et så tidlig tidspunkt og på et så lavt nivå som mulig».[160]

[155] NOU 2009: 15 s. 130.
[156] Bruce og Haugland (2014) s. 117.
[157] Dokument 15 (1995-1996), *Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåkning av norske borgere (Lund-rapporten),* s. 340-341.
[158] Bruce og Haugland (2014) s. 118.
[159] NOU 2009: 15 s. 130.
[160] NOU 2009: 15 s. 131.

For at et inngrep i privatlivet skal være i samsvar med de rettssikkerhetsgarantier som oppstilles i EMK artikkel 8 nr. 2 kreves det at inngrepet er «necessary». Vilkåret innebærer at inngrepet må være nødvendig for å ivareta det legitime formålet inngrepet har, og at disse interessene i en samlet vurdering anses som mer tungtveiende enn de interessene som krenkes.[161] Staten har ifølge EMD en viss skjønnsmargin i vurderingen. Ved inngrep som er begrunnet i hensynet til nasjonal sikkerhet har denne skjønnsmarginen blitt ansett for å være vid.[162] EMD har samtidig påpekt at vilkårlighet og myndighetsmisbruk på dette området kan få alvorlige konsekvenser, og føre utviklingen i retning av en politistat som undergraver og ødelegger demokratiet.[163] For å hindre at overvåkningen går utover demokratiet legger EMD til grunn at overvåkning bare kan godtas der det er «strictly necessary for safeguarding democratic institutions».[164] Et sentralt moment i forholdsmessighetsvurderingen er om det er etablert kontrollmekanismer som ivaretar hensynet til demokratiet. EMD stiller derfor krav til at det eksisterer adekvate og effektive kontrollmekanismer mot myndighetsmisbruk, både forut for inngrepet og i etterkant.[165]

6.2 Forutgående kontroll

6.2.1 Domstolskontroll

En viktig del av kontrollsystemet er domstolens forhåndskontroll. Forhåndskontrollen kommer til uttrykk i politiloven § 17 d ved at retten som hovedregel må gi PST tillatelse før bruk av tvangsmidler kan iverksettes.

Departementet uttalte følgende om hvorfor forhåndkompetansen burde legges til retten:[166]

> «at avgjørelsen fattes av en nøytral instans med høy kompetanse, er viktig for å sikre at mothensynene som gjør seg gjeldende mot bruk av tvangsmidler i en konkret sak, tillegges den vekt de fortjener. Det er også viktig for å sikre at folk skal ha tillit til at misbruk ikke skjer.»

[161] Husabø (2015) s. 249.
[162] Leander mot Sverige avsn. 59.
[163] Klass m.fl. mot Tyskland avsn. 42 og 49.
[164] Kennedy mot Storbritannia avsn. 153.
[165] Husabø (2015) s. 250 og 251.
[166] Ot.prp. nr. 60 (2004-2005) s. 76.

Kravet til forutgående domstolskontroll sikrer kravet til uavhengighet, objektivitet og saklighet. Dette fører til at rettsikkerheten på best mulig måte blir ivaretatt.[167] Departementet viser til at domstolskontrollen også har en disiplinerende effekt på PST, og dermed styrker rettsikkerheten og personvernet.[168]

Kravet til uavhengighet blir også sett på som en viktig rettssikkerhetsgaranti av EMD. Ifølge EMD stilles det ikke krav til at det er en domstol som fatter avgjørelsen om å tillate bruk av tvangsmidler, selv om dette blir ansett som det mest betryggende.[169]

Domstolskontrollen innebærer at retten ved kjennelse skal vurdere om vilkårene for å iverksette tvangsmiddelbruken er til stede. At tillatelsen skal avsies ved kjennelse medfører at tillatelsen må begrunnes, jf. straffeprosessloven § 52. Begrunnelse er viktig for å «sikre en reell og samvittighetsfull vurdering, etterprøvbarhet og en effektiv rett til overprøving».[170] Metodekontrollutvalget uttaler at det er en alminnelig oppfatning at «rettens begrunnelse i seg selv virker skjerpende og begrenser muligheten for urettmessige avgjørelser. Begrunnelseskravet utgjør dermed i seg selv en rettssikkerhetsgaranti».[171] Om begrunnelsens betydning ved kjennelser om skjult tvangsmiddelbruk er det blitt uttalt at:[172]

> «For at [den offentlige advokatens] ankerett ikke skal bli illusorisk, må rettens begrunnelse være slik at det er mulig å etterprøve om vilkårene for tvangsmiddelet er oppfylt. Dermed kan den ikke være for kortfattet. Dette er også viktig for at kontrollutvalgene skal kunne utføre en betryggende kontroll i henholdsvis saker om kommunikasjonskontroll og i saker om rikets sikkerhet.»

Retten står forholdsvis fritt til begrunnelsens omfang, men det er et krav at det fremgår hvilket faktum avgjørelsen bygger på, hvilken rettsanvendelse som er lagt til grunn,[173] og at de spørsmål som saken reiser har vært vurdert.[174] En gjennomgang av begrunnelser for kommunikasjonskontroll ved Oslo tingrett viser at begrunnelsene ofte er knappe og ikke

[167] NOU 2009: 15 s. 165.
[168] Ot.prp. nr. 60 (2004-2005) s. 133.
[169] Klass m.fl. mot Tyskland avsn. 56.
[170] Rt. 2009 s. 750 avsn. 35.
[171] NOU 2009: 15 s. 172.
[172] Ot.prp. nr. 64 (1998-1999) *Om lov om endringer i straffeprosessloven og straffeloven mv. (etterforskningsmetoder mv)*, s. 145.
[173] Bruce og Haugland (2014) s. 130.
[174] Rt. 1999 s. 475.

sjelden anvender standardformuleringer.[175] Dette kan svekke muligheten til ankerett og etterfølgende kontroll, og dermed også rettsikkerheten.

Det fremgår av politiloven § 17 d annet ledd at tillatelse til tvangsmiddelbruk bare kan gis dersom «det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen» og «at forebygging ellers i vesentlig grad vil bli vanskeliggjort». For å vurdere om tillatelse til tvangsmiddelbruk skal gis må domstolen ha et tilstrekkelig grunnlag til å prøve om disse vilkårene er oppfylt. I en undersøkelse som omhandler erfaring med kommunikasjonskontroll og betydningen av personvern og rettssikkerhet, svarte hele 14,3 % av dommerne at begjæringene om kommunikasjonskontroll var mindre enn tilstrekkelig grundig.[176] Dommerne ga også uttrykk for at det er vanskelig å foreta en reell prøving av de påstander som blir lagt ned der begjæringene ikke er tilstrekkelig grundige.[177]

Det er betenkelig at 14,3 % av dommerne mener at det ikke foretas tilstrekkelig vurdering av om vilkårene er oppfylt. Domstolskontrollen anses som den viktigste rettssikkerhetsgarantien for at bruk av tvangsmidler i forebyggende øyemed ikke blir misbrukt.

Undersøkelsen skiller ikke mellom begjæringer fra politiet og PST, men flere dommere gir uttrykk for at begjæringene fra PST er svært grundige sammenlignet med de fra politiet.[178] Dette kan tale for at rettsikkerheten står sterkere ved tvangsmiddelbruk i forebyggende øyemed enn ved tvangsmiddelbruk i etterforskning. Undersøkelsen gjelder ikke dataavlesning, men belyser hvordan tillatelser om skjult tvangsmiddelbruk blir behandlet.

En annen problemstilling vedrørende forhåndskontrollen er at den åpner for at dommeren blir satt i en tvangssituasjon. Det kan for eksempel være spørsmål om tillatelse til å avlese en brukerkonto i forbindelse med å undersøke om det forberedes et terrorangrep. Departementet vedkjenner seg at domstolen reelt sett har begrensede muligheter til å etterprøve det faktiske grunnlaget som PST baserer sin begjæring på.[179] Dette kan medføre at dommeren lett kan

[175] NOU 2009: 15 s. 172.
[176] Forsker Gunnar Thomassen og professor dr. juris Tor-Geir Myhrer, *Kommunikasjonskontroll og betydningen for etterforskning, personvern og rettssikkerhet: En studie av erfaringene med bruk av metoden,* Vedlegg 1 til NOU 2009: 15 (Oslo 2009).
[177] Thomassen og Myhrer (2009) s. 399.
[178] Thomassen og Myhrer (2009) s. 399.
[179] Ot.prp. nr. 60 (2004-2005) s. 133.

mene at han, i forhold til politiet, har for liten kunnskap til å sette spørsmålstegn ved politiets vurderinger. Dersom dommeren avviser begjæringen, og et terrorangrep blir utført, vil dommeren ofte bli tillagt et ansvar.[180] Det kan derfor være fristende for dommeren å tillate tvangsmiddelbruken uten at en reell prøving av vilkårene foreligger.

Forhåndskontrollens viktigste funksjon er ifølge departementet å hindre bruk av tvangsmidler der kravet til forholdsmessighet og særlige grunner ikke er til stede.[181] Det er lettere for domstolen å foreta en grundig vurdering av forholdsmessighetskravene. Det er oppstilt nærmere retningslinjer for vurderingene, slik at domstolen har flere holdepunkter enn bare PST sine vurderinger å ta utgangspunkt i.[182]

Departementet advarer mot at man ikke må ha «urealistiske forestillinger om hvor høy rettssikkerhet og hvor godt personvern som kan oppnås ved å kreve at domstolene på forhånd må gi tillatelse til å bruke tvangsmidler i forebyggende øyemed».[183] Til tross for at det finnes svakheter ved forhåndskontrollen mener departementet at dagens kontrollsystem bør opprettholdes.[184] Der forhåndskontrollen ikke tilstrekkelig sikrer et ønsket krav til rettssikkerhet og personvern vil de øvrige kontrollmekanismene være desto viktigere.[185] Et slikt synspunkt er også lagt til grunn av EMD.[186]

6.2.2 Hastekompetanse

Politiloven § 17 d tredje ledd oppstiller unntak fra kravet om forhåndsgodkjennelse fra domstolen. Unntaket kommer til anvendelse dersom «det ved opphold er stor fare for at muligheten til å forebygge et forhold som nevnt i første ledd bokstav a eller d vil gå tapt».

Regelen kan sammenlignes med tilsvarende regler som gjelder for tvangsmiddelbruk i etterforskning, blant annet straffeprosessloven § 216 d. Vilkårene for å anvende hastekompetansen utenfor etterforskning er imidlertid vesentlig strengere.[187]

[180] Prop. 68 L (2015-2016) s. 204.
[181] Ot.prp. nr. 60 (2004-2005) s. 133.
[182] Se punkt 4.1.4 og 4.2.1.
[183] Ot.prp. nr. 60 (2004-2005) s. 134.
[184] Prop. 68 L (2015-2016) s. 220.
[185] Ot.prp. nr. 60 (2004-2005) s. 134.
[186] Leiden-rapport (2015) s. 19.
[187] Ot.prp. nr. 60 (2004-2005) s. 134.

Ordlyden «stor fare» og «vil gå tapt» viser til at det er høy terskel for å anvende hastekompetansen. Ifølge departementet er hastekompetansen ment som en meget snever unntaksregel.[188]

I vurderingen av om vilkårene er oppfylt forutsettes det at det utøves skjønn basert på rettssikkerhet og personvern. Bestemmelsen kan ikke anvendes dersom det bare anses som mest praktisk for PST å igangsette tvangsmiddelbruken uten rettens kjennelse. Det kreves antakeligvis sannsynlighetsovervekt både for at det er «stor fare» og for at «muligheten til å forebygge (…) vil gå tapt».[189]

Hastekompetansen gjelder kun for handlinger etter politiloven § 17 d første ledd bokstav a og d. I utgangspunktet var det bare handlinger etter politiloven § 17 d bokstav d som kunne gi grunnlag for anvendelse, og kjerneområdet ble ansett for å være forebyggelse av attentat mot myndighetspersoner.[190] Begrunnelsen for å utvide anvendelsesområdet var endringer i trusselbildet:[191]

> «Dagens trusselbilde er forskjellig fra 2005, og det forebyggende arbeidet er blitt langt mer fremtredende siden den gang. Det må også tas i betraktning at de handlinger som omfattes av straffeloven § 131-134 (…) er meget alvorlige, og i dag kan det synes inkonsekvent å la PST ha hastekompetanse i attentatsaker, men ikke i terrorsaker».

Utenom kontortid, i helger og høytider, kan det oppstå situasjoner hvor det ikke er mulig å få forhåndstillatelse fra retten. Felles for de handlingene som tillater bruk av hastekompetanse er at de har et stort skadepotensial. For terrorhandlinger har tendensen de siste årene vært at forberedelsestiden generelt er blitt kortere,[192] hvilket medfører at PST er avhengig av å handle raskt for å ha mulighet til å forebygge slike handlinger.

Metodekontrollutvalget viste i 2009 til at hastekompetansen ble brukt i ca. en tredjedel av beslutningene om kommunikasjonskontroll. I lys av de strenge vilkårene kan det virke som at hastekompetansen ble brukt i overkant mye, men konklusjonen til utvalget var at

[188] Ot.prp. nr. 60 (2004-2005) s. 134.
[189] Bruce og Haugland (2014) s. 195-196.
[190] Innst. O. nr. 113 (2004-2005) s. 35.
[191] Prop. 68 L (2015-2016) s. 212.
[192] Prop. 68 L (2015-2016) s. 215.

kompetansen ikke ble brukt ugrunnet, og at bruken ikke ble oppfattet som problematisk. Årlig var det bare ca. en prosent av tilfellene som ikke ble godkjent av domstolens etterkontroll.[193]

Der det ikke blir utført en forutgående domstolskontroll av tvangsmiddelbruken stiller EMD krav til at det oppstilles «sufficient safeguards to ensure that it is used sparingly and only in duly justified cases».[194]

Ved bruk av hastekompetansen kreves det at beslutningen «snarest mulig» og «senest 24 timer etter at tvangsmiddelet ble tatt i bruk» legges frem for retten for godkjennelse, jf. politiloven § 17 d tredje ledd annet punktum. Beslutningen skal «så vidt mulig være skriftlig» og «opplyse om hva saken gjelder» og om «formålet med bruken av tvangsmiddelet». Det kreves også at en muntlig beslutning «snarest mulig nedtegnes». Kravene som stilles til beslutningen er ment å sikre notoritet og etterprøvbarhet av tvangsmiddelbruken,[195] og virker skjerpende på PSTs anvendelse av hastekompetansen.

EMD praksis viser at dersom hastekompetansen er begrenset til kun å gjelde de mest alvorlige lovbruddene, samt at retten kan vurdere lovligheten av tvangsmiddelbruken i etterkant, er kravet til «sufficient safeguards» oppfylt.[196] Ettersom hastekompetansen er innenfor de krav som stilles av EMD taler det for at rettsikkerheten er tilstrekkelig ivaretatt.

6.2.3 Offentlig advokat

Den som blir utsatt for tvangsmiddelbruk i forebyggende øyemed har etter politiloven § 17 e annet ledd annet punktum rett til offentlig oppnevnt forsvarer jf. straffeprosessloven § 100 a. Regelen er et utslag av at den tvangsmiddelbruken retter seg mot ikke har anledning til å uttale seg om og, forsvare seg mot tvangsmiddelbruken, jf. politiloven § 17 e annet ledd første punktum.

Kontradiksjon er en viktig rettssikkerhetsgaranti som også bidrar til sakens opplysning. Manglende underretning svekker mistenktes mulighet for kontradiksjon, hvilket taler for at det bør stilles strengere krav til de øvrige rettsikkerhetsgarantiene.

[193] NOU 2009: 15 s. 167.
[194] Roman Zakharov mot Russland avsn. 266.
[195] Ot.prp. nr. 60 (2004-2005) s. 152.
[196] Roman Zakharov mot Russland avsn. 266.

Departementet viser til at reglene om underretning kun er en del av et større regelsett som skal sikre at bruk av tvangsmidler ikke anvendes i større grad enn hva loven tillater, og at rettsikkerheten derfor kan sikres ved hjelp av de øvrige virkemidlene.[197] Begrunnelsen for at hensynet til kontradiksjon må vike er at «et særtrekk ved den forebyggende virksomheten gjør at det vil være behov for skjult bruk av tvangsmidler i forebyggende øyemed, dvs. uten at den som inngrepet retter seg mot, blir varslet om det».[198] Formålet med den forebyggende virksomheten faller således bort dersom den inngrepet retter seg mot er klar over tvangsmiddelbruken.

Offentlig oppnevnt forsvarer er ment å kompensere for unnlatt underretning ved at advokaten fremsetter motargumenter og sørger for at saken best mulig opplyst før retten fatter en avgjørelse.[199] Advokaten har, etter straffeprosessloven § 100 a tredje ledd første punktum, ikke adgang til å «sette seg i forbindelse med den mistenkte», og har taushetsplikt vedrørende de opplysninger som kommer frem i forbindelse med begjæringen og behandlingen av saken. Forbudet mot å kontakte den som rammes av tvangsmiddelbruken medfører at advokaten kun har politiets syn av saken for hånd ved vurderingen av om innsigelse mot tvangsmiddelbruken skal fremmes.[200] Dette kan føre til et manglende grunnlag for å vurdere begjæringen,[201] hvilket gjør det vanskelig å fremme konkrete innsigelser. Det kan derfor settes spørsmålstegn ved om ordningen utgjør en reell rettsikkerhetsgaranti.

En undesøkelse utført av EOS-utvalget i 2005 viste at advokatene fremmet innsigelser i 65 % av tilfellene. Det ble ikke påvist noen tilfeller hvor domstolen avslo en begjæring uten innsigelse fra advokat. I omtrent en tredjedel av de tilfellene hvor advokaten fremmet innsigelser fikk advokaten helt eller delvis medhold.[202] Undersøkelsen viser at dommere regelmessig stiller seg mer kritisk til begjæringer der det er fremmet innsigelse fra advokaten. Dette viser at innsigelser kan ha en opplysende og skjerpende effekt på domstolskontrollen.[203]

[197] Innst. O. nr. 113 (2004-2005) s. 19.
[198] Innst. O. nr. 113 (2004-2005) s. 33.
[199] NOU 2009: 15 (2004-2005) s. 134.
[200] Bruce og Haugland (2014) s. 124.
[201] NOU 2009: 15 (2004-2005) s. 134.
[202] Bruce og Haugland (2014) s. 124.
[203] Bruce og Haugland (2014) s. 125.

Ordningen inneholder mangler som gjør at det er vanskelig for advokaten å ivareta hensynet til kontradiksjon, likevel må man kunne si at forsvareren medvirker til å gjøre domstolskontrollen mer effektiv. Det er derfor grunnlag for å si at ordningen er med på å ivareta rettssikkerheten til de som rammes av inngrepet.

6.2 Etterfølgende kontroll

6.2.1 Stortingets kontrollutvalg for etterretnings-, overvåknings-, og sikkerhetstjenestene (EOS-utvalget)

EOS-utvalget ble opprettet i 1996, i kjølvannet av Lund-utvalgets avsløringer om ulovlig overvåkning.[204] EOS-utvalget er underlagt Stortinget, men er et selvstendig organ. Dette følger av EOS-kontrolloven § 1, hvor det fremgår at utvalget skal utføre sitt verv «selvstendig og uavhengig av Stortinget».

Reguleringen av utvalget sikrer en uavhengighet fra myndighetene som beslutter og gjennomfører overvåkningen, hvilket er viktig for å sikre en reell kontroll av overvåkningen. Kravet til uavhengighet er presisert av EMD.[205]

Formålet med utvalget er å kontrollere og forebygge at EOS-tjenestene, deriblant PST, ikke krenker noens rettigheter, ikke bruker mer inngripende midler enn hva som er nødvendig, ikke utilbørlig skader samfunnets interesser og påse at tjenestene opererer innenfor loven, jf. EOS-kontrolloven § 2 første ledd.[206] Formålet illustrerer at utvalget er et viktig virkemiddel for å sikre at rettsikkerheten blir ivaretatt. Utvalgets kontroll overfor PST er:[207]

> «å føre kontroll med at tjenestens behandling av forebyggende saker og etterforskningssaker, dens bruk av skjulte tvangsmidler, behandling av personopplysninger og utveksling av informasjon med innenlandske og utenlandske samarbeidspartnere, skjer etter det gjeldende regelverk og tilfredsstiller krav til gode rutiner, alt innen rammen av formålet i lovens § 2».

[204] Se punkt 6.1.
[205] Husabø (2015) s. 251-252.
[206] Lov av 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåking- og sikkerhetstjeneste (EOS-kontrolloven).
[207] Dokument 16 (2015-2016), *Rapport til stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget),* s. 64.

Ifølge EOS-kontrolloven § 8 har utvalget rett til innsyn og adgang til «arkiver og registre, lokaler, installasjoner og anlegg av enhver art». I 2016 og 2017 var det likevel uenighet mellom PST og utvalget angående omfanget av utvalgets innsynsrett i PST sitt kildearbeid, men PST anerkjente i januar 2018 utvalgets innsynsrett. Utvalget har rett til fullt innsyn i alle opplysninger, foruten kildens navn og personnummer.[208]

Innsynsretten er det viktigste virkemiddelet EOS-utvalgt har for å gjennomføre den etterfølgende kontrollen.[209] Fullt innsyn har for det første en preventiv og disiplinerende effekt på EOS-tjenestene. EOS-tjenestene er klar over at utvalget til enhver tid kan foreta kontroll av ethvert register. For det andre gir innsynsretten utvalget mulighet til å sette seg inn i, og vurdere, alle sider av en sak. Dette bidrar til økt legitimitet av tjenestene,[210] og sikrer at utvalget møter de krav EMD stiller til kompetanse til å foreta en reell kontroll av overvåkningen. [211]

Etter at PST i 2005 fikk adgang til å anvende tvangsmidler i forebyggende øyemed, intensiverte utvalget kontrollen av PST sin tvangsmiddelbruk. Dagens kontroll innebærer at utvalget hvert halvår gjennomgår alle saker der tvangsmiddelbruk har vært anvendt. Kontrollen har særlig fokus på om PST sine begjæringer til retten samsvarer med informasjonsgrunnlaget som ligger til grunn for begjæringen. Utvalget har fullt innsyn i etterretningsinformasjon mottatt fra samarbeidende parter, både nasjonalt og internasjonalt, og derfor mer informasjon enn hva retten har tilgang til. Kontrollen innebærer også gjennomgang av om PST overholder de forutsetninger som er satt for tvangsmiddelbruken.[212]

Det totale omfanget av PST sin bruk av skjulte tvangsmidler i forebyggende øyemed er unntatt offentligheten. EOS-utvalget uttalte i 2006 og 2007 at bruken var økende, men fremdeles beskjeden.[213] Den gradvise økningen omtales som naturlig sett i sammenheng med de forventninger som stilles til PST og endringene i kriminalitetsbildet.[214] EOS-utvalgets

[208] Dokument 7:1 (2017-2018) s. 17-18.
[209] Dokument 7:1 (2017-2018) s. 18.
[210] Dokument 7:1 (2017-2018) s. 18.
[211] Husabø (2015) s. 252.
[212] Dokument 16 (2015-2016) s. 65.
[213] Dokument nr. 20 (2006-2007), *Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget),* s. 7 og Dokument nr. 9 (2007-2008), *Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget),* s. 14.
[214] Dokument 16 (2015-2016) s. 65.

årsmelding for 2018 gir ingen indikasjon på at er grunn til bekymring vedrørende dagens omfang av tvangsmiddelbruk.

I 2017 ble det påvist flere avvik ved PST sin tvangsmiddelbruk. Ved ett tilfelle avlyttet PST en telefon to dager lenger enn hva de hadde tillatelse til, og fikk tilgang til tolv telefonsamtaler uten rettslig grunnlag. Ved ett annet tilfelle pågikk skjult kameraovervåking nesten en måned lenger enn hva retten hadde godkjent. PST varslet selv utvalget om feilen som medførte at kameraovervåkingen ikke ble avsluttet til rett tid.[215] Om varslingen blir det uttalt at:[216]

> «Utvalget ser positivt på at tjenesten selv avdekker og rapporterer avvik til utvalget under inspeksjoner i tjenesten. Utvalget legger til grunn at tjenesten tar slike feil og avvik alvorlig, og at tjenesten har oppmerksomhet rettet mot kvalitetssikring og rutiner for å minimere mulighetene for at slike feil skal oppstå igjen».

Det er uheldig at det påvises avvik i etterkant av tvangsmiddelbruk, til tross for de rettssikkerhetsgarantier som er oppstilt for å på forhånd forhindre dette. På den annen side er det positivt at kontrollen fanger opp avvik, dette tyder på at kontrollen er effektiv, og dermed ivaretar rettssikkerheten. At PST selv varsler om avvik de oppdager er et tegn på samarbeidsvilje og at avvik ikke skjer med hensikt.

EOS-utvalget har tre forskjellige kontrollformer: inspeksjoner, klagesaker og saker som utvalget av eget tiltak tar opp.[217] En evaluering av utvalget viste at inspeksjonene er en viktig kilde til kunnskap om tjenestenes virksomhet, og at det er inspeksjonene som ofte danner bakgrunnen for sakene som utvalget tar opp av eget tiltak.[218]

I 2017 gjennomførte utvalget 7 inspeksjoner av PST.[219] Inspeksjonene ble varslet på forhånd, men inneholdt fremdeles betydelige uanmeldte elementer.[220] Det foretas både søk i arkiver og registre i form av stikkprøver og mer systematiske søk.[221]

[215] Dokument 7:1 (2017-2018) s. 9.
[216] Dokument 7:1 (2017-2018) s. 17.
[217] Dokument 16 (2015-2016) s. 12.
[218] Dokument 16 (2015-2016) s. 12.
[219] Dokument 7:1 (2017-2018) s. 9.
[220] Dokument 7:1 (2017-2018) 2017 s. 17.
[221] EOS-utvalget.no, *kontrollvirksomheten*, https://eos-utvalget.no/norsk/tjenester/hva_kontrollerer_eos_utvalget_/kontrollvirksomheten/.

Klagesakene som EOS-utvalget behandler har stor betydning for befolkningens tillit til EOS-tjenestene og kontrollen av dem. Klageadgangen kan også utledes som et krav av EMD praksis.[222]

I 2017 mottok utvalget 12 klager, hvorav en ga grunnlag for kritikk av PST. Klagen omhandlet ransakelse av bolig uten tillatelse fra retten. PST mente det forelå «fare for opphold», mens utvalget konkluderte med at det ikke var grunnlag for å si at vilkåret var oppfylt.[223]

Evalueringen av EOS-utvalget viser at tekselen for å få en klage behandlet av utvalget er lav.[224] Den lave terskelen styrker rettssikkerheten, da klagesakene gir flere muligheter til å oppdage eller avkrefte kritikkverdige forhold.

Foruten å kontrollere og avdekke kritikkverdige forhold, har også den etterfølgende kontrollen en forebyggende effekt. I forbindelse med opprettelsen av EOS-utvalget uttalte Skauge-utvalget at:[225]

> «tilsyn kan aldri avdekke enhver tenkelig uregelmessighet eller ethvert tvilsomt spørsmål straks etter at de har oppstått. Verdien ligger i at det i det lange løp er påreknelig at slike forhold kommer fram i dagen og i den forebyggende virkning som følger av det».

Uttalelsen reflekterer at det ved opprettelsen av EOS-utvalget var annen holdning med mer mistro til kontrollen enn hva situasjonen er i dag. Forholdet mellom EOS-tjenestene og EOS-utvalget blir i dag gjerne omtalt som et konstruktivt forhold, hvor tjenestene i stor grad er villig til å forbedre seg og lære av de feil som blir begått.[226] EOS-utvalget har verken instruksjons- eller vedtaksmyndighet overfor EOS-tjenestene, hvilket medfører at utvalget kun kan komme med anbefalinger og uttalelser.[227] Det konstruktive forholdet er derfor viktig for å sikre at anbefalingene fra utvalget følges opp.

---

[222] I.R og G.T mot Storbritannia avsn. 62.
[223] Dokument 7:1 (2017-2018) s. 26.
[224] Dokument 16 (2015-2016) s. 12.
[225] NOU 1994: 4 *Kontrollen med «de hemmelige tjenester»* s. 39.
[226] Dokument 16 (2015-2016) s. 112.
[227] EOS-utvalget, *Kontrollområdet*, https://eos-utvalget.no/norsk/tjenester/hva_kontrollerer_eos_utvalget_/kontrollomradet/.

En undersøkelse av klagesaker fra 2010-2014 viste at 7 av14 klagesaker som endte med kritikk fra utvalget fikk konsekvenser utover den aktuelle saken klagen gjaldt. Tre av disse sakene var rettet mot PST og gjaldt ulovlig overvåkning.[228] Dette viser at den etterfølgende kontrollen ikke bare får betydning for enkeltsaker, men også for systemet generelt. Eksempler på tiltak som blir iverksatt er omdisponering av personell kompetanse, opprettelse av nye stillinger, gjennomgang av rutiner, endringer i saksbehandlingssystemer, økt fokus på bestemte problemområder og intern opplæring.[229] Rettsikkerheten ved bruk av tvangsmidler i forebyggende øyemed blir bedre og bedre etter hvert som tjenestene utbedrer de mangler som EOS-utvalget påpeker.

Selv om statistikkene tilsier at PST i praksis ofte etterlever anbefalingene fra utvalget, er rettsikkerheten svekket ved at utvalget ikke kan garantere etterlevelse ved juridisk bindende avgjørelser, kun «uttale sin mening», jf. EOS-kontrolloven § 14.

Muligheten for å behandle klager henger nært sammen med kravet EMK artikkel 13 stiller til effektivt rettsmiddel. EMD uttaler at:[230]

> «Further, given the overlap between the procedural safeguards under Article 8 and the right to an effective remedy under Article 13, the former should be interpreted in a manner consistent with the latter.»

Etter artikkel 13 kreves det ikke bare at klageorganet har kompetanse til å prøve klagens materielle innhold,[231] men også at organet har kompetanse «to grant appropriate relief».[232] Dette innebærer at organet må kunne hindre videre krenkelse, eller gjenopprette eller kompensere for krenkelsen.[233]

Rettsutviklingen i EMD og litteratur tyder på at det sistnevnte kravet også innebærer at det må være mulighet for å fatte juridisk bindende vedtak i klagesaker.[234] EOS-utvalgets

[228] Dokument 16 (2015-2016) s. 207-208.
[229] Dokument 16 (2015-2016) s. 112.
[230] I.R. og G.T. mot Storbritannia avsn. 62.
[231] Husabø (2015) s. 253.
[232] Savovi mot Bulgaria avsn. 63.
[233] Husbø (2015) s. 253.
[234] Segerstedt-Wiberg og andre mot Sverige avsn. 120-122 og Leiden-rapport (2015) s. 7.

klagebehandling oppfyller ikke et slikt krav. Dette taler for at dataavlesning, slik det er innført i norsk rett, ikke oppfyller forholdsmessighetskravet etter EMK artikkel 8 og kravet til «appropriate relief» etter artikkel 13.

6.2.2 Domstolsbehandling

Tvisteloven § 1-3[235] åpner for å få rettmessigheten av overvåkningen avgjort av domstolen. Den som er utsatt for ulovlig overvåkning kan reise fastsettelsessøksmål med krav på dom for brudd på menneskerettighetene, eller fullbyrdelsessøksmål med krav om at opplysninger skal slettes eller at staten skal utbetale erstatning for krenkelsen.[236]

Domstolsbehandlingen kan, sammen med klagebehandlingen, oppfylle kravet til effektivt rettsmiddel jf. EMK artikkel 13.

En forutsetning for å oppfylle retten til effektivt rettsmiddel etter EMK artikkel 13 er at muligheten til effektivt rettsmiddel er «reell».[237] Den som klager til EOS-utvalget har krav på uttalelse fra utvalget dersom klagen har gitt grunnlag for kritikk, jf. EOS-kontrolloven § 15. En slik uttalelse gir et konkret grunnlag for å reise sak for domstolene.

En «reell» domstolsprøving innebærer imidlertid også at retten har kompetanse til å foreta materiell prøving av kravet.[238]

Tvisteloven § 22-1 første ledd oppstiller bevisforbud for opplysninger «som holdes hemmelig av hensyn til rikets sikkerhet eller forholdet til fremmed stat». Forbudet rammer bevis tilknyttet saker om forebyggende overvåkning, og hindrer en reell prøving av rettmessigheten av tvangsmiddelbruken.

I Lysebøl-saken fra 1987,[239] som omhandlet lovligheten av en eventuell telefonkrontoll, tillot ikke staten at det ble utført avhør av en tjenestemann i Televerket. Høyesterett uttalte at «en reell prøving av lovligheten av en eventuell telefonkontroll er under disse omstendighetene

[235] Lov av 17. juni 2005 nr. 90.
[236] Husabø (2015) s. 256.
[237] Husabø (2015) s. 256.
[238] Husabø (2015) s. 256.
[239] Rt. 1987 s. 612

ikke mulig».[240] Klagen ble vurdert som «indamissible» av menneskerettskommisjonen.[241] Nyere EMD praksis stiller imidlertid strengere krav til statene. I Al-Nashif-saken fra 2002 uttalte EMD følgende om inngrep som er begrunnet i nasjonal sikkerhet:[242]

> «(…) measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence, if need be with appropriate procedural limitations on the use of classified information (…)».

Selv om det blir lagt til grunn at det kan foreligge hensiktsmessige begrensinger vedrørende bruken av klassifisert informasjon, blir det også presisert at dette «by no means justify doing away with remedies altogether», og at organet som avgjør saken må ha innsyn i grunnlaget for utvisningsvedtaket.[243] Høyesterett uttalte i Krekar-dommen, med henvisning til denne saken, at det «ikke uten videre [er] innlysende at det norske regelverket innfrir de krav som følger av menneskerettskonvensjonen».[244] De to dommene omhandler bevisforbudets betydning for overprøving av utvisningsvedtak, men har overføringsverdi til saker om dataavlesning.

Uttalelsen i Krekar-dommen var medvirkende til at det ble foretatt endringer i utlendingsloven.[245] Endringene gikk ut på at en særskilt oppnevnt advokat får tilgang til graderte opplysninger, uten at disse kan formidles videre til klienten.

Endringene i utlendingsloven illustrerer at det er mulig å utforme prosessreglene for bruk av dataavlesning i forebyggende øyemed på en måte som i større grad enn de nåværende reglene verner rettsikkerheten, og møter de krav som stilles til reell domstolsprøving jf. EMK artikkel 13. Endringene kan enten være av en slik karakter at EOS-utvalget alene vil tilfredsstille kravet til effektivt rettsmiddel, eller slik at utvalget og domstolen til sammen tilfredsstiller kravene. Uavhengig av hvordan endringene utføres taler hensynet til rettsikkerhet for at kravene etter EMK artikkel 13 bør være oppfylt.

---

[240] Rt. 1987 s. 612 (s. 618).
[241] L. mot Norge.
[242] Al-Nashif m.fl. mot Bulgaria avsn. 123.
[243] Al-Nashif m.fl. mot Bulgaria avsn. 137.
[244] Rt. 2007 s. 1573.
[245] Lov av 15. mai 2008 nr. 35 kap 14 II (§§ 131-138).

7. AVSLUTTENDE BEMERKNINGER

Oppgaven viser at det er oppstilt en rekke rettssikkerhetsgarantier for bruk av dataavlesning i forebyggende øyemed. De strenge materielle vilkårene fører til at det er høy terskel for å gi tillatelse til å anvende dataavlsening i forebyggende øyemed. Dette er med på å forhindre at dataavlesning blir brukt utenfor de fullmakter PST er gitt.

Den vage utformingen av fremgangsmåten for avlesningen, og hvilken informasjon som kan avleses, fører til svekket forutberegnelighet for de som rammes av tvangsmiddelbruken. Forutberegnelighet anses som en viktig rettsikkerhetsgaranti for vern mot vilkårlige myndighetsinngrep, og mangler ved lovhjemmelen innebærer at det stilles strengere krav til de øvrige rettssikkerhetsgarantiene. Det foreligger imidlertid flere svakheter ved disse.

Den forutgående domstolskontrollen sikrer at tillatelse til bruk av dataavlesning i forebyggende øyemed fattes av et uavhengig organ. En svakhet ved domstolskontrollen er at dommere opplever det som vanskelig å foreta en reell prøving av påstandene som politiet legger ned. Uten en reell prøving av vilkårene blir forhåndskontrollen mangelfull, og rettssikkerheten svekkes. Svakhetene ved forhåndskontrollen taler for at det stilles strenge krav til den etterfølgende kontrollen.

Verken EOS-utvalgets klageadgang, eller domstolsbehandlingen etter tvisteloven § 1-3, tilfredsstiller de krav som EMD stiller til effektiv domstolsbehandling. Selv om forholdet mellom EOS-utvalget og PST medfører at PST i praksis retter seg etter utvalgets anbefalinger, veier det ikke opp for at retten til et effektivt rettsmiddel ikke formelt er til stede. Ettersom EOS-utvalget har klarlagt at det forekommer ulovlig overvåkning, er det betenkelig at en så sentral rettsikkerhetsgaranti ikke foreligger.

Summen av manglene ved kontrollsystemet, sett i lys av at dataavlesning innebærer et stort inngrep, taler for at rettsikkerheten ikke er tilstrekkelig ivaretatt ved bruk av dataavlesning i forebyggende øyemed. For å gi individet et større vern mot ulovlig overvåkning, og forsbedre rettsikkerheten, bør lovgiver foreta endringer som sikrer at retten til effektivt rettsmiddel er tilstrekkelig ivaretatt.

8. KILDEREGISTER

LOVER, FORSKRIFTER, KONVENSJONER OL.

Norske lover

Grunnloven	Lov 17. mai 1981, Kongerikets Norges Grunnlov.
Straffeprosessloven	Lov 22. mai 1981 nr. 30 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.
Tvisteloven	Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister.
Straffeloven	Lov 20. mai 2005 nr. 28 om straff.
Utlendingsloven	Lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her.

Instrukser

Instruks for Politiets sikkerhetstjeneste 19. august 2005 nr. 920.

Internasjonale konvensjoner

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

Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

STORTINGSDOKUMENTER, FORARBEIDER OL.

Lovforarbeid

NOU 1994: 4	Kontrollen med «de hemmelige tjenester».
Ot.prp. nr. 64 (1998-1999)	Om lov om endringer i straffeprosessloven og straffeloven mv. (etterforskningsmetoder mv.).
NOU 2003: 18	Rikets sikkerhet. Straffekommisjonens delutredning VIII.
NOU 2004: 6	Mellom effektivitet og personvern. Politimetoder i forebyggende øyemed.
Ot.prp. nr. 60 (2004-2005)	Om lov om endringer til straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet).
Ot.prp. nr. 22 (2008-2009)	Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon – sluttføring av spesiell del og tilpasning av annen lovgivning).
NOU 2009: 15	Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.

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

Rapporter, årsmeldinger mv.

Dokument 15 (1998-1999)	Rapport til Stortinget fra kommisjonen som ble opprettet av Stortinget for å granske påstander om ulovlig overvåkning av Norske borgere («Lund-rapporten»).
Dokument nr. 20 (2006-2007)	Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).
Dokument nr. 9 (2007-2008)	Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).
Dokument 16 (2015-2016)	En evaluering av EOS-utvalgets kontroll med etterretnings-, overvåkning- og sikkerhetstjeneste.
Dokument 7:1 (2017-2018)	Årsmelding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).

RETTSPRAKSIS

Høyesterettspraksis

Rt. 1987 s. 612

Rt. 1999 s. 475

Rt. 2006 s. 1546

Rt. 2007 s. 1573

Rt. 2009 s. 750

Rt. 2015 s. 93

Rt. 2015 s. 155

Praksis fra Den europeiske menneskerettighetsdomstolen

Klass m.fl. mot Tyskland, saksnr. 5029/71, 6. september 1978.

Leander mot Sverige, saksnr. 9248/81, 26. mars 1987.

Kruslin mot Frankrike, saksnr. 11801/85, 24. april 1990.

L. mot Norge, saksnr. 13564/88, 8. juni 1990.

Al-Nashif m.fl. mot Bulgaria, saksnr. 50963/99, 20. juni 2002.

Weber og Savaria mot Tyskland, saksnr. 54934/00, avvisningsavgjørelse 29. juni 2006

Segerstedt Wiberg og andre mot Sverige, saksnr. 62332/00, 6. juni 2007.

Kennedy mot Storbritannia, saksnr. 26839/05, 18. mai 2010.

Savovi mot Bulgaria, saksnr. 7222/05, 27. november 2012.

I.R. og G.T. mot Storbritannia, saksnr. 14876/12 og 63339/12, avvisningsavgjørelse 28. januar 2014.

Roman Zakharov mot Russland, saksnr. 47143/06, 4. desember 2015.

LITTERATUR, FORSKNING MV.

Thomassen og Myhrer (2009)	Thomassen, Gunnar og Myhrer, Tor-Geir, *Kommunikasjonskontroll og betydningen for etterforskning, personvern og rettsikkerhet: En studie av erfaringene med bruk av metoden*, Vedlegg 1 til NOU 2009: 15 (Oslo 2009).
Sunde (2012)	Sunde, Inger Marie, *Dataavlesing som etterforskningsmetode*, tidsskrift for retfærd, årgang 35 nr. 1/136 side 3-35 (2012).
Bruce og Haugland (2014)	Bruce, Ingvild og Haugland, Geir Sunde, *Skjulte tvangsmidler* (Oslo 2014).
Leiden-rapport (2015)	Loof, J.P. mfl., *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen - en veiligheidsdiensten: Afdeling staats- en bestuursrecht* (Universitetet i Leiden 2015).
Husabø (2015)	Husabø, Erling Johannes, *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og*

etterretningstjenestenes inngrep i menneskerettigheter?, Vedlegg 4 til Dokument 16 (2015-2016).

Auglend og Mæland (2016) Auglend, Ragnar L. og Mæland, Henry John, *Politirett*, 3. utgave (Oslo 2016).

NETTBASERTE KILDER

Datatilsynet, *Kryptering*, https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/kryptering/ (Hentet: 6. februar 2018).

EOS-utvalget, *Kontrollområdet*, https://eos-utvalget.no/norsk/tjenester/hva_kontrollerer_eos_utvalget_/kontrollomradet/ (Hentet 11. mai 2018).

EOS-utvalget.no, *Politiets sikkerhetstjeneste (PST*), https://eos-utvalget.no/norsk/tjenester/eos_tjenestene/politiets_sikkerhetstjeneste_pst_/ (Hentet: 9. April 2018).

Gyldendal rettsdata, Myhrer, Tor-Geir, *Lov om politiet (politiloven)*, www.rettsdata.no, (1 november 2013).

PST.no, *Oppgaver*, https://www.pst.no/temasider/oppgaver/#Forebyggje, (10. oktober 2017).

PST.no, *Trusselvurdering 2018*, https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2018/ (30 januar 2018).

SSB.no, «Norsk mediebarometer 2017», https://www.ssb.no/kultur-og-fritid/artikler-og-publikasjoner/norsk-mediebarometer-2017 (Hentet: 11. april 2018).

VG.no, *I disse angrepene brukte de bil som terrorvåpen*, https://www.vg.no/nyheter/utenriks/i/d3lPJ/i-disse-angrepene-brukte-de-bil-som-terrorvaapen (19 august 2017).

WhatsApp*, Sikkerhet*, https://www.whatsapp.com/security/?l=nb, (Hentet: 19. februar 2018).