DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 68 L

(2015–2016)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Innhold

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 68 L

(2015–2016)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i straffeprosessloven mv. (skjulte tvangsmidler)

Tilråding fra Justis- og beredskapsdepartementet 11. mars 2016, godkjent i statsråd samme dag.
(Regjeringen Solberg)

1 Proposisjonens hovedinnhold

1.1 Innledning

Justis- og beredskapsdepartementet legger i denne proposisjonen frem forslag om lovendringer som vil gi politiet en utvidet adgang til å benytte skjulte tvangsmidler ved etterforskning, avverging og forebygging av alvorlige lovbrudd. Straffeprosesslovens regler om skjulte tvangsmidler bygger på vanskelige vurderinger hvor hensynet til effektiv kriminalitetsbekjempelse må avveies mot hensynet til personvern og rettssikkerhet. Ubegrunnede inngrep i den enkeltes rettigheter og private sfære må unngås. Et endret kriminalitets- og trusselbilde kan imidlertid tilsi at adgangen til å benytte skjulte politimetoder utvides.

Proposisjonen følger opp deler av Metodekontrollutvalgets utredning NOU 2009: 15 Skjult informasjon – åpen kontroll. Utredningen har to overordnede temaer; behandling og beskyttelse av informasjon i straffesaker og politiets bruk av skjulte tvangsmidler. Departementet fant det hensiktsmessig å dele dette store lovarbeidet i to delproposisjoner. Første delproposisjon – Prop. 147 L (2012–2013) om endringer i straffeprosessloven mv. (behandling og beskyttelse av informasjon) – ble fremmet våren 2013 og vedtatt av Stortinget ved lov 21. juni 2013 nr. 86. Den foreliggende proposisjonen omhandler behovet for endringer i reglene om politiets bruk av skjulte tvangsmidler, som er behandlet i utredningen del IV.

Det fremmes blant annet forslag om utvidet adgang til bruk av kommunikasjonskontroll, ransaking, romavlytting, teknisk sporing, kameraovervåking og tvangsmiddelbruk i avvergende og forebyggende øyemed. Videre foreslås det at det åpnes for bruk av et nytt skjult tvangsmiddel, dataavlesing. Nedenfor i punkt 1.2 til 1.10 oppsummeres de viktigste endringsforslagene nærmere.

Den nye straffeloven trådte i kraft 1. oktober 2015. Dette innebærer at mens Metodekontrollutvalget og høringsinstansene refererer til straffeloven 1902, må departementet forholde seg til gjeldende rett på tidspunktet for fremleggelse av proposisjonen for Stortinget. Departementet har funnet det nødvendig å innta henvisninger til begge lovene i proposisjonsteksten, slik at det

henvises til de speilede bestemmelser i enten 1902- eller 2005-loven i parentes.

1.2 Fellesspørsmål

Fellesspørsmål om tvangsmiddeladgang behandles i kapittel 6.

Departementet foreslår at strafferammekrav skal beholdes som grunnvilkår for å ta i bruk skjulte tvangsmidler. Departementet finner ikke grunn til å foreslå at det stilles lempeligere krav for å anvende straffeloven § 79 bokstav c (straffeloven 1902 § 60 a), hvoretter strafferammen forhøyes dersom en straffbar handling er utøvet som ledd i aktivitetene til en organisert kriminell gruppe. Siden metodetilgangen er knyttet til et strafferammekrav, har regelen betydning for det saklige virkeområdet for de skjulte metodene. Departementet mener at en riktigere tilnærming er å utvide metodetilgangen ved at det åpnes for bruk av skjulte metoder ved enkelte alvorlige lovbrudd med strafferamme under ti år, der det påvises et behov for dette og der utvidelsen er forholdsmessig.

Departementet støtter utvalget i at en ordning hvor det kreves samtykke fra domstolen for å ta i bruk skjulte tvangsmidler, alt i alt gir best rettssikkerhet, og går ikke inn for endringer her. Videre mener departementet at det mest forsvarlige er at disse sakene fortsatt fordeles blant dommerne etter et tilfeldighetsprinsipp. Det foreslås heller ikke endringer i dommerfullmektigenes kompetanse, ettersom det i alminnelighet ikke kan legges til grunn at de er mindre egnet enn embetsdommere til å behandle slike saker.

Departementet ser en klar fordel i at samme offentlig oppnevnte advokat gjør tjeneste ved rettens behandling av alle begjæringer om skjulte tvangsmidler mot samme mistenkte i en sak, siden dette vil gi advokaten en totaloversikt over tvangsmiddelbruken i saken. Det foreslås derfor at samme advokat «så langt det er mulig» oppnevnes for samtlige begjæringer om bruk av skjulte tvangsmidler mot mistenkte i samme sak. Reservasjonen vil ta høyde for at regelen ikke skal medføre forsinkelser hos domstolene. Departementet går ikke inn for å utvide advokatens oppdrag ved at det lovfestes en rolle for denne under gjennomføringen av tvangsmiddelet eller etter at tvangsbruken er opphørt. Det vises til at utredningen er uklar med tanke på hva oppdraget mer konkret ville bestått i. Den offentlig oppnevnte advokaten bør også vareta tredjepersoners interesser.

Departementet ser et klart behov for at påtalemyndigheten beholder den hastekompetansen den har under etterforskningen, og foreslår ikke endringer i dagens regler. Når det gjelder Sjef PSTs hastekompetanse i forebyggingssaker, foreslås det at denne utvides til å omfatte forebygging av terrorhandlinger.

Departementet går ikke inn for utvalgets forslag om at det skal gjennomføres muntlige forhandlinger ved begjæringer om tillatelse til bruk av skjulte tvangsmidler. Det fremheves at dagens ordning i stor grad legger til rette for at saker om skjulte tvangsmidler blir tilstrekkelig belyst. Dommeren kan innkalle til muntlige forhandlinger ved behov. Dessuten forutsettes den offentlig oppnevnte advokaten å begjære muntlige forhandlinger dersom det synes nødvendig av hensyn til sakens opplysning. En viktig innvending mot forslaget er at muntlige forhandlinger kan forsinke gjennomføringen av tvangsmidlene og svekke metodenes effektivitet.

Departementet mener at det også ved kommunikasjonskontroll og romavlytting bør gjelde en *hovedregel* om underretningsplikt. Disse metodene er inngripende, og personvernhensyn gjør seg i minst like stor grad gjeldende her som ved de metodene en i dag har plikt til å underrette om. På bakgrunn av innvendinger fra høringsinstanser foreslår imidlertid departementet at det etter henleggelse – på nærmere bestemte vilkår – gis adgang til å unnlate underretning. Det foreslås dessuten å videreføre PSTs adgang til ikke å underrette om bruk av skjulte metoder i forebyggende øyemed.

Departementet er enig med utvalget i at myndigheten til å beslutte utsatt underretning bør ligge hos retten, og det foreslås at dette også skal gjelde i saker om rikets sikkerhet. Grunnen er at en domstolsbehandling synes best egnet til å avveie behovet for hemmelighold mot hensynet til mistenktes personvern. Siden beslag og utleveringspålegg er mindre inngripende metoder, går departementet imidlertid inn for at påtalemyndigheten her kan beslutte utsatt underretning i inntil åtte uker. Det foreslås dessuten at retten gis en viss mulighet til å utsette underretning for lengre tid enn åtte uker, i inntil fire måneder. Disse tiltakene vil gjøre metodebruken noe mindre ressurskrevende, samtidig som mistenktes og tredjepersoners interesser og rettssikkerhet synes tilstrekkelig varetatt.

Departementet ser at en underretningsplikt kan skape særlige utfordringer hvor skjulte tvangsmidler gjennomføres på anmodning fra utenlandske myndigheter. Norske myndigheter

kan ha vanskelig for å begrunne utsatt underretning dersom etterforskningen for øvrig gjennomføres av utenlandske myndigheter, og vil kunne trenge bistand fra utlandet både for å få kjennskap til om mistenkte bør underrettes, og for å gjennomføre selve underretningen. Det er videre grunn til å spørre om det i slike saker er rimelig at byrden med å underrette påhviler norske myndigheter. Det foreslås derfor at Kongen gis hjemmel til å gi særregler om underretning ved gjennomføring av tvangsmidler på begjæring fra utenlandske myndigheter.

1.3 Kommunikasjonskontroll

Departementet foreslår i kapittel 7 en viss utvidelse av politiets adgang til å iverksette kommunikasjonsavlytting og annen kommunikasjonskontroll, jf. straffeprosessloven § 216 a og b, i etterforskningsøyemed. Det foreslås å åpne for kommunikasjonsavlytting i saker som gjelder grov menneskesmugling, menneskehandel, frihetsberøvelse og overgrepsbilder av barn. Disse lovbruddene representerer alvorlige integritetskrenkelser, og de er i tillegg kjennetegnet av særlige etterforskningsmessige utfordringer. Departementet finner derfor at det er behov for å utvide politiets etterforskningsmessige verktøy i bekjempelsen av disse kriminalitetsformene.

Departementet har i tillegg vurdert om det bør åpnes for bruk av kommunikasjonsavlytting i saker om hallikvirksomhet, grooming og ransforbund, men finner ikke å kunne fremme forslag om dette. Bakgrunnen er at de nevnte kriminalitetsformene ikke anses tilstrekkelig alvorlige til å begrunne et så inngripende virkemiddel som kommunikasjonsavlytting. Til det er de personvernmessige konsekvenser ved bruk av metoden for store.

På bakgrunn av høringsnotat 12. juli 2012 om kriminalisering av forberedelse til terror mv. har departementet vurdert om det bør åpnes for bruk av kommunikasjonsavlytting i saker om oppfordring, rekruttering og opplæring til terror. På grunn av vansker med å skaffe bevis i slike saker, samt alvorligheten av de handlinger oppfordringen, rekrutteringen eller opplæringen kan lede til, finner departementet at det bør gis adgang til slik metodebruk. Det samme foreslås for hemmelig ransaking, skjult kameraovervåking på privat sted, personnær teknisk sporing og dataavlesing.

Videre vurderes hvorvidt det bør være adgang til å knytte en tillatelse til kommunikasjonskontroll til en bestemt person (den mistenkte) og ikke bare et bestemt kommunikasjonsanlegg, som er regelen i dag. Selv om en slik mulighet kan medføre tids- og ressursmessige besparelser hos både påtalemyndigheten og domstolene, mener departementet at hensynet til en grundig rettslig kontroll taler mot dette. Departementet er derfor enig med Metodekontrollutvalget i at det ikke bør åpnes for kommunikasjonskontroll knyttet til person.

Departementet slutter seg til utvalgets forslag om å åpne for kommunikasjonskontroll ved at politiet bruker eget teknisk utstyr for å lokalisere kommunikasjonsanlegg. I dag kan metoden benyttes for å identifisere et anlegg, for dermed å kunne bestemme *hvilket* kommunikasjonsanlegg den mistenkte benytter. Departementet kan ikke se at personvernmessige eller andre hensyn taler mot at det samme bør gjelde når man vil bringe på det rene *hvor* det aktuelle kommunikasjonsanlegget befinner seg. Videre foreslår departementet at det ikke lenger skal være noen forutsetning for å kunne kreve utlevert lokaliseringsopplysninger fra nett- eller tjenestetilbyder, at kommunikasjonsanlegget er i bruk. En mistenkt i en straffesak kan neppe sies å ha en mer berettiget interesse i at politiet ikke vet hvor han befinner seg når han ikke kommuniserer via et mobilanlegg, enn når han bruker anlegget til kommunikasjon. Av hensyn til legalitetsprinsippet foreslås det også at politiets bruk av såkalt stille SMS gis en klar lovhjemmel. Dette innebærer at politiet kan sende en melding over mobilnettet som ikke er synlig på mottakerens mobilanlegg, men som likevel genererer trafikk – og dermed basestasjonsopplysninger – som igjen kan brukes til å lokalisere det aktuelle anlegget.

1.4 Romavlytting

I proposisjonen kapittel 8 foreslår departementet å fjerne kravet om tilknytning til organisert kriminalitet ved bruk av romavlytting i drapssaker. Selv om det er grunn til å utvise stor varsomhet med å utvide anvendelsesområdet for romavlytting, er forsettlig eller overlagt drap etter departementets syn en så alvorlig forbrytelse at manglende metodetilgang ikke bør stå i veien for oppklaring. Hva gjelder grovt ran og særlig grov narkotikaforbrytelse, finner departementet ikke at det er grunnlag for å fjerne kravet om tilknytning til organisert kriminalitet.

For øvrig foreslås ingen endringer i reglene om romavlytting i straffeprosessloven § 216 m.

1.5 Teknisk sporing

Departementet foreslår i proposisjonen kapittel 9 at personnær teknisk sporing – i likhet med hemmelig ransaking, skjult kameraovervåking på privat sted og kommunikasjonsavlytting – skal kunne benyttes ved mistanke om frihetsberøvelse og om oppfordring, rekruttering og opplæring til terror.

1.6 Skjult ransaking, postbeslag, postkontroll og utleveringspålegg mv.

I kapittel 10 foreslår departementet å åpne for hemmelig ransaking etter straffeprosessloven § 200 a i saker om frihetsberøvelse, grov menneskesmugling, menneskehandel, overgrepsbilder av barn og offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, med tilsvarende begrunnelse som for kommunikasjonskontroll, jf. punkt 1.3 ovenfor.

Straffeprosessloven §§ 211 og 212 har særregler om postbeslag, det vil si beslag av sending som besittes av postoperatør eller tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste. Departementet støtter Metodekontrollutvalget i at særreglene om postbeslag i straffeprosessloven §§ 211 og 212 kan oppheves. Departementet støtter videre at opphevelsen av postkontrolloven ikraftsettes. Behovet for postbeslag og postkontroll i saker om rikets sikkerhet må søkes dekket gjennom de ordinære bestemmelsene om beslag, utleveringspålegg og utleveringspålegg fremover i tid.

Departementet går inn for å åpne for utleveringspålegg fremover i tid i forebyggende øyemed med hjemmel i politiloven § 17 d, i tråd med Metodekontrollutvalgets forslag.

1.7 Innhenting av trafikkdata

Metodekontrollutvalgets forslag knyttet til innhenting av trafikkdata er i all hovedsak fulgt opp ved vedtakelsen av lov 15. april 2011 nr. 11 om gjennomføring av datalagringsdirektivet. Departementet finner på det nåværende tidspunkt ikke grunn til å foreta endringer i reglene om utlevering av trafikk- og lokaliseringsdata, jf. proposisjonen kapittel 11. Bestemmelsene må vurderes samlet med øvrige lovendringer knyttet til datalagringsdirektivet, herunder lagringsplikten, i lys av EU-domstolens avgjørelse 8. april 2014.

1.8 Skjult kameraovervåking

Departementet foreslår i proposisjonen kapittel 12 å presisere at politiets adgang til å iverksette skjult kameraovervåking på offentlig sted, også gjelder overvåking som skjer fra offentlig mot privat sted. Dette kan for eksempel være et inngangsparti. Departementet kan ikke se at vektige hensyn taler mot en slik adgang, så lenge det er tale om sted som er synlig fra et offentlig sted. Forslaget er i tråd med Metodekontrollutvalgets forslag.

Departementet slutter seg videre til utvalgets forslag om å åpne for skjult kameraovervåking på privat sted, unntatt i private hjem. Kameraovervåking på privat sted må anses betraktelig mer inngripende enn overvåking som skjer på offentlig sted, slik at vilkårene for bruk av metoden bør være strenge. Departementet finner det riktig å legge inngangsvilkårene på samme nivå som det som gjelder for kommunikasjonsavlytting.

1.9 Tvangsmiddelbruk i avvergende og forebyggende øyemed

1.9.1 Avvergende tvangsmidler

Bruk av tvangsmidler i avvergende og forebyggende øyemed behandles i kapittel 13.

Departementet konkluderer med at det av formuleringen «kriminelle tilfeller» i Grunnloven § 102 første ledd annet punktum ikke kan utledes et krav om at det allerede må være begått en straffbar handling for at det skal være adgang til tvangsmiddelbruk i private hjem. Ved vurderingen av hvilken adgang det skal være til å benytte tvangsmidler for å avverge og forebygge kriminalitet, må det først og fremst tas stilling til om de lovhjemlede inngrep ivaretar legitime formål og er forholdsmessige.

Departementet mener at det ikke er hensiktsmessig å innskrenke adgangen til bruk av tvangsmidler i avvergende øyemed på en slik måte Metodekontrollutvalget foreslår. Det bemerkes at en slik innsnevring vil ha betydning for et stort antall saker der grunnlovsspørsmålet uansett ikke vil komme på spissen. Dette fordi innsnevringen vil gjelde generelt for all tvangsmiddelbruk i avvergende øyemed, og således også for andre tvangsmidler enn ransaking og romavlytting i private hjem.

Departementet mener at etterforskningsbegrepet i dag er tilstrekkelig klart og at det er pedagogisk gunstig å beholde dette i lovteksten. Slik tydeliggjøres det grunnleggende skillet mellom

bruk av tvangsmidler i avvergende øyemed under påtalemyndighetens og Riksadvokatens ledelse og ansvar, og bruk av forebyggende metoder undergitt Politidirektoratet og Justis- og beredskapsdepartementet. Departementet mener dessuten at det vil kunne gi svært uheldige utslag å begrense muligheten til å bruke tvangsmidler i avvergende øyemed til der det er sammenheng mellom en opprinnelig straffbar handling og den som søkes avverget.

Departementet støtter utvalget og høringsinstansene i at drap, uavhengig av hvilken sammenheng det inngår i, er en så alvorlig og uopprettelig krenkelse av menneskelivet at politiet bør ha anledning til å benytte tvangsmidler for å søke det avverget. Departementet mener at tilleggskriteriet om organisert kriminalitet derimot er berettiget og bør opprettholdes ved ran. Det bør fortsatt være adgang til å bruke tvangsmidler i avvergende øyemed der det er rimelig grunn til å tro at noen kommer til å begå grove narkotikaforbrytelser som ledd i organisert kriminalitet. Selv om de skadelige følgene av slikt lovbrudd er noe mer indirekte og langsiktige, er de av svært alvorlig karakter, og departementet mener det ikke er tilrådelig å svekke politiets evne til å bekjempe slikt narkotikalovbrudd.

Departementet støtter ikke utvalgets forslag om å fjerne forberedelseshandlinger til terror som grunnlag for å iverksette bruk av tvangsmidler i avvergende øyemed. Disse er i seg selv alvorlige lovbrudd og har dessuten et så omfattende avledet skadepotensiale at hensynet til kriminalitetsbekjempelse bør veie tyngre enn hensynet til personvernet. Departementet foreslår dessuten at også offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger bør inntas i listen over lovbrudd som gir adgang til avvergende bruk av tvangsmidler som ledd i etterforskning. Rekruttering eller opplæring til terrorhandlinger vil senere kunne avføde nettopp slike. Det anses nødvendig å kunne benytte tvangsmidler allerede for å avverge de opprinnelige, forberedende lovbruddene.

1.9.2 Forebyggende tvangsmidler

Departementet mener at det reiser særlige personvernmessige og rettssikkerhetsmessige spørsmål å tillate bruk av tvangsmidler i forebyggende øyemed, det vil si uten at det er grunnlag for å iverksette etterforskning, og dette tilsier at adgangen bør være snevrere i slike tilfelle. Det er således ikke et mål i seg selv å oppnå en parallellitet mellom PSTs adgang til tvangsmiddelbruk for å forebygge og for å avverge alvorlig kriminalitet. En avveining mellom hensynet til kriminalitetsbekjempelse og samfunnssikkerhet på den ene siden og rettssikkerhet og personvernhensyn på den andre siden, tilsier at tvangsmidler bare bør kunne nyttes for å forebygge de mest alvorlige straffbare handlingene som hører under PSTs ansvarsområde.

Enkelte at de lovbrudd der PST ber om utvidelser vil imidlertid kunne innebære store og uopprettelige skader, nærmere bestemt ulovlig omgang med masseødeleggelsesvåpen. Disse lovbruddene er likestilt med andre alvorlige lovbrudd når det gjelder adgangen til romavlytting i avvergende øyemed, som anses å være et svært inngripende tvangsmiddel. Her foreslår departementet at adgangen til å benytte tvangsmidler også i forebyggende øyemed utvides.

Departementet mener at det verken er hensiktsmessig med et generelt forbud mot, eller en ubetinget adgang til, tvangsmiddelbruk i private hjem i forebyggingsøyemed, slik henholdsvis Metodekontrollutvalgets flertall og mindretall mener. Etter departementets oppfatning bør lovgiver differensiere mellom de tre metodene – romavlytting, ransaking og innbrudd ved dataavlesing – og også mellom ulike lovbrudd – terrorhandlinger, spionasje og ulovlig etterretningsvirksomhet, attentat mot myndighetspersoner og ulovlig befatning med masseødeleggelsesvåpen. En vurdering av et inngreps forholdsmessighet vil måtte ta i betraktning alvorligheten av det lovbruddet som søkes avverget og hvor sikre holdepunkter en har for at en slik alvorlig straffbar handling vil bli begått. Departementet understreker videre at graden av inngripen for det enkelte tvangsmiddel vil være av stor betydning for vurderingen av hvorvidt det skal være adgang til å benytte det i forebyggende øyemed. Departementet konkluderer med at det under visse vilkår bør åpnes for skjult ransaking og innbrudd ved dataavlesing for å forebygge terrorhandlinger, i motsetning til øvrige lovbrudd angitt i politiloven § 17 d, samt at enhver romavlytting i private hjem i forebyggende øyemed bør forbys. Det understrekes at sjefen eller den assisterende sjefen for PST, som fremmer beslutning om å begjære bruk av tvangsmidler i forebyggingsøyemed, og domstolen i tillegg må foreta en forholdsmessighetsvurdering i den enkelte sak, og blant annet se hen til hvor sikre holdepunkter en har for at en terrorhandling vil kunne bli begått og hvor alvorlige konsekvensene vil kunne bli.

Departementet foreslår at sjef PSTs hastekompetanse utvides til å omfatte forebygging av

terrorhandlinger. Det er viktig at PST sikres tilstrekkelige virkemidler for å forebygge slik alvorlig kriminalitet. 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 om terror (straffeloven 1902 § 147 a) er meget alvorlige, og i dag kan det synes inkonsekvent å la PST ha hastekompetanse i forebygging av attentatsaker mot myndighetspersoner, men ikke i terrorsaker. Faren for misbruk må dessuten sies å være minimal, ettersom PSTs hastebeslutning vil overprøves av retten i etterkant og dessuten vil inngå i EOS-utvalgets kontrollarbeid.

Det foreslås å videreføre PSTs adgang til å unnlate underretting om bruk av skjulte tvangsmidler i forebyggende øyemed. Særtrekkene ved den forebyggende virksomheten vil som regel gjøre det nødvendig å holde opplysninger om bruken av tvangsmidlet og opplysningene som bruken resulterte i, hemmelig for den som ble utsatt for inngrepet.

1.10 Dataavlesing

I proposisjonen kapittel 14 foreslår departementet at dataavlesing innføres som nytt, skjult tvangsmiddel med hjemmel i straffeprosessloven nye §§ 216 o og 216 p.

«Dataavlesing» refererer ikke til noen klart avgrenset fremgangsmåte, men brukes som samlebetegnelse for flere utstyrs- og kunnskapsbaserte metoder for å skaffe tilgang til opplysninger i et datasystem som ikke er offentlig tilgjengelig. Blant de mange tenkelige variantene kan bruk av «trojanere» og annen tilsvarende programvare trekkes frem. Slik programvare kan plasseres i mistenktes datasystem for å gi politiet tilgang til mistenktes kommunikasjon, lagret informasjon og andre opplysninger om bruken av datasystemet. Departementet foreslår også at politiet skal ha tillatelse til å gjøre fysisk innbrudd for å plassere og fjerne utstyr som er nødvendig for å gjennomføre dataavlesingen.

Departementets forslag er i hovedsak begrunnet med at det er et stort og udekket behov for effektiv tilgang til elektronisk lagret og kommunisert informasjon. Informasjon produseres, bearbeides, kommuniseres og lagres i dag ofte elektronisk og ved bruk av mobile tjenester. Samtidig øker bruken av krypteringsløsninger og andre metoder for beskyttelse av slik informasjon. Informasjonsbeskyttelsen er ikke forbeholdt aktører med spesiell kunnskap og interesse, men tilbys i dag ofte som «standardløsning». Metodekontrollutvalget og sentrale høringsinstanser innen politiet og påtalemyndigheten påpeker at den teknologiske utviklingen og bruken av krypteringsløsninger har medført at politiet stadig oftere blir stående uten faktisk tilgang til informasjon som det rettslig sett ellers har adgang til i medhold av de eksisterende tvangsmiddelbestemmelsene om kommunikasjonsavlytting og hemmelig ransaking.

Departementets forslag til nytt tvangsmiddel gir mulighet til å oppfylle det ovennevnte behovet, ved at politiet gis adgang til å følge med på mistenktes bruk av et datasystem over tid, uavhengig av det tradisjonelle skillet mellom kommunikasjon og lagret informasjon. Dette gir rom for å avdekke informasjon som politiet i dag ikke får tilgang til gjennom kommunikasjonsavlytting og enkeltstående hemmelige ransakinger, enten på grunn av kryptering eller fordi informasjonen slettes fortløpende eller ikke blir lagret i det hele tatt.

Departementet har også vurdert Metodekontrollutvalgets forslag om å tillate dataavlesing i mer begrenset utstrekning, som gjennomføringsmåte for henholdsvis kommunikasjonsavlytting og hemmelig ransaking. Etter departementets vurdering er en slik løsning ikke godt nok egnet til å møte utfordringene som den teknologiske utviklingen har skapt. I tillegg utfordrer løsningen de alminnelige skrankene for henholdsvis kommunikasjonsavlytting etter straffeprosessloven § 216 a og hemmelig ransaking etter § 200 a. Dette kan unngås ved å innføre dataavlesing som selvstendig tvangsmiddel.

Tvangsmiddelet dataavlesing skal etter departementets forslag kunne benyttes i samme typer saker og på lignende vilkår som kommunikasjonsavlytting etter § 216 a. Det innebærer at metoden bare skal kunne benyttes i saker som gjelder alvorlig kriminalitet, og bare dersom strenge tilleggsvilkår er oppfylt.

Videre foreslår departementet at dataavlesing tilføyes i oppregningen av skjulte tvangsmidler som kan benyttes i avvergende øyemed etter straffeprosessloven § 222 d og som ledd i forebyggingen av alvorlig kriminalitet etter politiloven § 17 d – på nærmere angitte vilkår.

2 Bakgrunnen for lovforslaget

2.1 Historikk

Politiets adgang til skjult tvangsmiddelbruk har historisk vært, og er fortsatt, et omstridt tema. Dette skyldes den personverns- og rettssikkerhetsproblematikk som er knyttet til slik bruk.

Stortingets granskningskommisjon for de hemmelige tjenester (Lund-kommisjonen) ble oppnevnt 1. februar 1994 på bakgrunn av påstander om ulovlig eller irregulær overvåking av norske borgere etter 1945. Kommisjonen ble ledet av høyesterettsdommer Ketil Lund. De øvrige medlemmene var advokat Regine Ramm Bjerke, professor Berge Furre, generalmajor Torkel Hovland og likestillingsombud Ingse Stabel. Kommisjonens mandat gikk ut på å granske alle forhold i forbindelse med påstander om at politiets overvåkingstjeneste, Forsvarets sikkerhetstjeneste og Forsvarets etterretningstjeneste, eller personer knyttet til disse tjenester, hadde vært engasjert i ulovlig eller irregulær overvåking av norske borgere. Det ble vedtatt en særlov (lov 25. mars 1994 nr. 6) som ga granskningskommisjonen myndighet som en domstol til å avhøre vitner mv. direkte for kommisjonen. Lund-kommisjonens rapport ble presentert for Stortinget 28. mars 1996 (Dokument nr. 15 (1995–96) – Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere). Rapporten konkluderte med at det har foregått ulovlig politisk overvåking i Norge etter 1945, hovedsakelig av kommunister og sosialister, som ble ansett for å representere en trussel mot rikets sikkerhet under den kalde krigen.

Frem til 1999 kunne politiet bare bruke skjulte tvangsmidler i etterforskningen av narkotikaforbrytelser og saker om rikets sikkerhet. I narkotikasaker fulgte hjemmelen til å foreta telefonavlytting av midlertidig lov 17. desember 1976 nr. 99. Ved lov 5. juni 1992 nr. 52 ble denne ordningen gjort permanent og hjemlene flyttet til straffeprosessloven kapittel 16 a. I saker om rikets sikkerhet hadde sikkerhetstjenesten adgang til å anvende telefonavlytting og postkontroll i medhold av lov 24. juni 1915 nr. 5 om kontroll med post- og telegrafforsendelse og med telefonsamtaler. Ved lov 3. desember 1999 nr. 82 ble loven av 1915 opphevet og reglene om telefonkontroll i saker om rikets sikkerhet innarbeidet i straffeprosessloven kapittel 16 a.

Ved lovendringen i 1999 ble det også innført generelle regler som ga politiet hjemmel til å gjennomføre kommunikasjonskontroll (kommunikasjonsavlytting og annen kontroll av kommunikasjon) i en rekke sakstyper. Det ble videre åpnet for utsatt underretning om ransaking, beslag og utleveringspålegg, og politiets bruk av teknisk sporing ble lovfestet og utvidet. Ved samme lov ble det innført en ordning med oppnevning av forsvarer for den mistenkte ved bruk av tvangsmidler som den mistenkte ikke får kunnskap om, jf. straffeprosessloven § 100 a. Lovendringene ble utformet på bakgrunn av forslagene i Metodeutvalgets utredning NOU 1997: 15 Etterforskingsmetoder for bekjempelse av kriminalitet – Delinnstilling II, Ot.prp. nr. 64 (1998–99) og Innst. O. nr. 3 (1999–2000).

Ved lov 17. juni 2005 nr. 87 ble det åpnet for romavlytting som etterforskningsmetode, samt for tvangsmidler i avvergende og forebyggende øyemed. Videre ble politiet gitt adgang til å identifisere mobiltelefoner og andre kommunikasjonsanlegg. Det ble også gjort endringer i reglene om hemmelig ransaking, kommunikasjonskontroll, teknisk sporing, utleveringspålegg fremover i tid og avlytting eller opptak av samtale med samtykke fra en av samtalepartene. Lovendringen var basert på Politimetodeutvalgets utredning NOU 2004: 6 Mellom effektivitet og personvern – Politimetoder i forebyggende øyemed, Ot.prp. nr. 60 (2004–2005) og Innst. O. nr. 113 (2004–2005).

Et endret trusselbilde har ledet til at politiet og påtalemyndigheten ved ovennevnte lovendringer har fått adgang til å benytte flere og mer inngripende tvangsmidler i etterforskningen av terrorhandlinger og annen alvorlig kriminalitet. Det er stilt spørsmål om pendelen er i ferd med å snu, med det sterke fokuset på rettssikkerhet og personvern i Metodekontrollutvalgets utredning og motstanden mot datalagringsdirektivet, jf. Bjerke, Keiserud og Sæther: Straffeprosessloven kommentarutgave Bind I (4. utgave, Oslo 2011) side 17.

Det er verdt å påpeke at samtidig med utvidelsen av adgangen til å anvende skjulte tvangsmidler, har det skjedd en utvikling av kontrollmekanismer og rettssikkerhetsgarantier. Opprettelsen av Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) er et eksempel på dette. Om dette heter det i EOS-utvalgets *Årsmelding for 2011*, Dokument 7:1 (2011–2012) til Stortinget, del III nr. 1 side 10:

> «Utvalget har i 2011 lagt bak seg 15 år med kontroll av EOS-tjenestene – de hemmelige tjenestene. EOS-utvalget er et parlamentarisk forankret kontrollorgan som ble opprettet ved lov av Stortinget i 1995 og startet opp sin virksomhet året etter. Bakgrunnen for opprettelsen var omfattende offentlig oppmerksomhet og politisk debatt omkring virksomheten i de hemmelige tjenestene. Debatten førte til nedsettelsen av Lund-kommisjonen, samt etableringen av EOS-utvalget. Dette markerte et skille mellom gammel og ny tid hva angår tjenestenes virksomhet og kontrollen med dem.
>
> Formålet med utvalgets kontroll er å påse at det ikke øves urett mot enkeltpersoner. Som en konsekvens av at en i et demokratisk samfunn også har et legitimt behov for hemmelige tjenester, møter utvalget flere dilemmaer. Det er en stadig utfordring å skulle balansere hensynet til enkeltpersoners rett til privatliv mot statens behov for beskyttelse.[…]»

Vurderingen av balansepunktet mellom kriminalitetsbekjempelse, personvern og rettssikkerhet kan ikke være statisk, jf. Bruce og Haugland: Skjulte tvangsmidler (Oslo 2014) side 33. Både kriminalitetsbildet og personvernfeltet er i konstant utvikling. Dette tilsier at verken samfunnets behov for beskyttelse, omfanget av politiets lovpålagte oppgaver eller borgernes vurdering av hvilken kriminalitetstrussel og hvilket inngrepsnivå som er akseptabelt, vil være konstant. Det er lovgivers ansvar å finne balansepunktet mellom kriminalitetsbekjempelse, samfunnssikkerhet, personvern og rettssikkerhet.

2.2 Aktuelle dokumenter fra regjeringen

2.2.1 Metodekontrollutvalgets utredning NOU 2009: 15 Skjult informasjon – åpen kontroll

Ved lov 3. desember 1999 nr. 82 ble det som nevnt i punkt 2.1 vedtatt en rekke endringer i straffeprosessloven for å få bedre etterforskningsmetoder i kampen mot alvorlig kriminalitet. Slik lovgivning bygger på vanskelige vurderinger hvor hensynet til personvern og rettssikkerhet for mulig lovbryter og dennes omgangskrets må avveies med hensynet til effektiv kriminalitetsbekjempelse. Siden lovendringene berører tungtveiende motstridende hensyn, så departementet behov for en etterkontroll av lovgivningen om slik etterforskning, jf. Ot.prp. nr. 64 (1998–99) kapittel 22 side 141.

Metodekontrollutvalget, ledet av sorenskriver Nils Terje Dalseide, ble nedsatt ved kgl. res. 15. februar 2008 for å foreta etterkontrollen av straffeprosesslovens regler om skjulte etterforskningsmetoder og behandling av informasjon i straffesaker. Utvalget vurderte også effekten av lovendringer foretatt i 2005 som ledd i oppfølgingen av NOU 2004: 6 Mellom effektivitet og personvern. Metodekontrollutvalget leverte sin evaluering NOU 2009: 15 Skjult informasjon – åpen kontroll 26. juni 2009.

Metodekontrollutvalgets utredning har to overordnede temaer; behandling og beskyttelse av informasjon i straffesaker og politiets bruk av skjulte tvangsmidler. Denne proposisjonen inneholder lovforslag knyttet til sistnevnte tema.

2.2.2 Høringsnotat 12. juli 2012

Departementet sendte forslag til lovendringer om blant annet kriminalisering av forberedelse til terrorhandling og utvidet adgang til tvangsmiddelbruk på høring 12. juli 2012. Forslagene var basert på innspill fra PST i brev 1. november 2011. Høringsbrevet del II omhandler forslag fra PST om endringer i reglene om tvangsmiddelbruk og om anonym vitneførsel. Noen av forslagene var i en viss grad behandlet av Metodekontrollutvalget. Andre elementer av PSTs innspill var nye eller bare delvis berørt av Metodekontrollutvalget, og ble derfor sendt på høring. Det er kun ett av temaene i høringsnotatet del II som ble berørt i den første delproposisjonen, nærmere bestemt anonyme vitner. Øvrige temaer vil behandles i denne delproposisjonen.

2.3 Høringer

2.3.1 Høringen av Metodekontrollutvalgets utredning

Metodekontrollutvalgets utredning ble sendt på høring 15. desember 2009 med høringsfrist 1. mai 2010. Utredningen ble sendt til følgende høringsinstanser:

Departementene

Høyesterett
Lagmannsrettene
Oslo tingrett
Bergen tingrett
Trondheim tingrett
Nord-Troms tingrett
Kristiansand tingrett
Tønsberg tingrett
Domstoladministrasjonen

Riksadvokaten
Statsadvokatembetene
Politidirektoratet
Politiets sikkerhetstjeneste (PST)
Generaladvokaten
Spesialenheten for politisaker
Regjeringsadvokaten

Datatilsynet
Post- og teletilsynet (fra 1. januar 2015 Nasjonal kommunikasjonsmyndighet)
Stortingets kontrollutvalg for etterretnings-, overvåkings- og trygghetstjenester (EOS-utvalget)
Kontrollutvalget for kommunikasjonskontroll

Sivilombudsmannen

Det juridiske fakultet i Bergen
Det juridiske fakultet i Oslo
Det juridiske fakultet i Tromsø
Norsk Senter for Menneskerettigheter

Amnesty International Norge
Den Norske Advokatforening
Den norske Dommerforening
Forsvarergruppen av 1977
NGO-forum for menneskerettighetene
NetCom GSM AS
Norges forskningsråd
Norges Juristforbund
Norsk forening for kriminalreform (KROM)
Norsk Utenrikspolitisk Institutt
Næringslivets Sikkerhetsorganisasjon
Organisasjonen mot politisk overvåking (OPO)
Politiets Fellesforbund
Politijuristene
Rettspolitisk forening
Statsadvokatenes forening
TDC Norge AS
Tele2 Norge AS
Telenor AS
Teleplan AS
Teletopia AS

På den opprinnelige adressatlisten var det ikke oppført presseorganisasjoner. Fordi særlig utredningen kapittel 28 om skjult tvangsmiddelbruk og pressens rett til kildevern ble vurdert å være av interesse for denne gruppen, ble kopi av høringsbrev 15. desember 2009 med vedlegg sendt på høring til følgende adressater 19. april 2010:

Norsk Journalistlag
Norsk Presseforbund
Norsk Redaktørforening
Norsk Rikskringkasting
Norsk Telegrambyrå
TV2 AS

Instansene på den reviderte adressatlisten fikk høringsfrist 15. juni 2010.

Etter foreleggelsen har også Scandinavian Tv Organisations Against Piracy (STOP), Elektronisk Forpost Norge, Advokatfirmaet Elden, Kommisjonen for gjenopptakelse av straffesaker, Politihøgskolen, Hordaland politidistrikt og Norges Politilederlag avgitt høringssvar.

De siste uttalelsene kom inn sommeren 2010.

Departementet gjør oppmerksom på at det er politi- og påtalemyndigheten som har avgitt langt de fleste høringsuttalelsene, og at det dessverre har kommet få innspill fra forsvarerhold. En nærmere gjennomgåelse av høringsuttalelsene fremgår av kapittel 6 til 14 i tilknytning til de enkelte lovforslagene.

2.3.2 Høringsnotat 12. juli 2012

Forslag til lovendringer om kriminalisering av forberedelse til terrorhandling, organisert kriminalitet og utvidet adgang til tvangsmiddelbruk ble sendt på høring 12. juli 2012. Høringsfristen var 1. november 2012. Høringsnotatet ble sendt til følgende høringsinstanser:

Departementene
Høyesterett
Lagmannsrettene
Tingrettene
Domstoladministrasjonen
Riksadvokaten
Statsadvokatembetene
Politidirektoratet
ØKOKRIM

Datatilsynet
Generaladvokaten
Kontrollutvalget for kommunikasjonskontroll

Politiets sikkerhetstjeneste
Post- og teletilsynet (fra 1. januar 2015 Nasjonal kommunikasjonsmyndighet)
Regjeringsadvokaten
Sivilombudsmannen
Stortingets kontrollutvalg for etterretnings-, overvåkings- og trygghetstjenester (EOS-utvalget)

Advokatforeningen
Amnesty International Norge
Den norske Dommerforening

Den Norske Fagpresses Forening
Forsvarergruppen av 1977
Juridisk rådgivning for kvinner (JURK)
Jusshjelpa i Nord-Norge
Juss-Buss
Jussformidlinga i Bergen
Norges Juristforbund
Norsk presseforbund
Organisasjonen mot politisk overvåkning (OPO)
Politiets fellesforbund
Politijuristene
Rettspolitisk forening
Stine Sofies Stiftelse

Det juridiske fakultet ved Universitetet i Oslo
Det juridiske fakultet ved Universitetet i Bergen
Det juridiske fakultet ved Universitetet i Tromsø
Institutt for kriminologi og rettssosiologi, UiO
Norsk senter for menneskerettigheter
Politihøgskolen

Andre som har uttalt seg er Kriminalpolitisentralen (KRIPOS), Oslo politidistrikt, Hordaland politidistrikt, Nordre Buskerud politidistrikt, Vestfold politidistrikt, Etterretningstjenesten, Den norske Helsingforskomité, Den internasjonale juristkommisjon (ICJ-Norge) og Norsk forening for kriminalreform (KROM).

Høringsuttalelsene som knytter seg til forslagene som følges opp i denne proposisjonen, går frem av de enkelte kapitlene nedenfor.

2.4 Kontrollen med politiets bruk av skjulte tvangsmidler

2.4.1 Kort om bruken av skjulte tvangsmidler og kontrollen av denne

Politiets sikkerhetstjeneste (PST) er Norges sivile innenlands etterretnings- og sikkerhetstjeneste og har ansvar for nasjonens indre sikkerhet. PST er en del av politiet, men er direkte underlagt Justis- og beredskapsdepartementet. PSTs primære oppgave er å forebygge, avverge og etterforske straffbare handlinger mot nasjonens sikkerhet. Mer presist omfatter dette spionasje, terrorvirksomhet, politisk motivert vold, spredning av masseødeleggelsesvåpen og av utstyr, materiale og teknologi for produksjon av slike våpen samt trusler mot myndighetspersoner. Dette gjør tjenesten ved hjelp av ulike metoder og arbeidsmåter.

PST kan i dag på lik linje med det ordinære politiet inngi begjæring til retten om å få bruke skjulte tvangsmidler ved *etterforskning* av straffbare handlinger. Politiet, herunder PST, har videre hjemmel til å begjære bruk av skjulte tvangsmidler for å *avverge* straffbare handlinger. Som eneste politimyndighet kan PST også benytte skjulte tvangsmidler for å *forebygge* visse typer straffbare handlinger. I tillegg kan PST og det ordinære politiet benytte seg av ulovfestede metoder, såkalte *operative tiltak*, som ikke er så inngripende at lovhjemmel anses nødvendig.

Kontrollen med politiets bruk av skjulte tvangsmidler er nærmere beskrevet i Metodekontrollutvalgets rapport kapittel 11 side 130 flg. Slik kontroll består av en rekke elementer eller kontrollmekanismer. Utvalget peker særlig på advokaters kontrollfunksjon (både § 100 a-advokater og forsvarere), politiets internkontroll, påtalemyndighetens kontroll med politiet, Politidirektoratets instruksjonsmyndighet og ansvar for ledelse og oppfølging av politidistriktene, Justisdepartementets overordnede etatslederansvar og rolle i lovgivningsprosessen, domstolenes forhåndskontroll av begjæringer om bruk av tvangsmidler og etterkontroll av hastebeslutninger, Datatilsynets og medienes rolle, samt kontroll som utføres av Kontrollutvalget for kommunikasjonskontroll (KK-utvalget) og Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget).

2.4.2 Nærmere om KK-utvalget

KK-utvalget er oppnevnt med hjemmel i straffeprosessloven § 216 h og regulert nærmere i forskrift om kommunikasjonskontroll 31. mars 1995 nr. 281 (kommunikasjonskontrollforskriften) kapittel 2. Også romavlytting faller innenfor utvalgets virkeområde gjennom bestemmelsen i straffeprosessloven § 216 m siste ledd, jf. også Riksadvokatens retningslinjer 22. juli 2005. Kontrollutvalget skal kontrollere at politiets bruk av kommunikasjonskontroll og romavlytting skjer innenfor rammen av lov og instrukser. Det skal også sørge for at bruken av kommunikasjonskon-

troll begrenses mest mulig og ikke benyttes i andre saker enn dem som er nevnt i straffeprosessloven kapittel 16 a. Utvalget skal ikke behandle saker som hører inn under PST, jf. nedenfor.

KK-utvalget slår fast at politiets bruk av kommunikasjonskontroll gjennomgående er forsvarlig og godt begrunnet, jf. utvalgets Årsrapport 2014 punkt 4 side 4-5. Dette er den samme konklusjonen som i rapportene for de siste årene, og den er ytterligere forsterket gjennom utvalgets arbeid i første del av 2015. KK-utvalget peker på et samvirke av en rekke faktorer som bakgrunn for sin konklusjon: Norge har generelt en høy faglig og etisk standard i politiet, og arbeidet med den alvorligste kriminaliteten og bruk av kommunikasjonskontroll som arbeidsredskap tiltrekker seg mange av de dyktigste personene i politiet. Regelverket, saksbehandlingen og gjennomføringen er lagt opp slik at avgjørelsene om å begjære bruk av kommunikasjonskontroll blir behandlet og kvalitetssikret på flere nivåer i politiet. Etterforsker, etterforskningsleder, politijurist og politimester eller visepolitimester er direkte involvert i beslutningsprosessen. Den hierarkiske strukturen gjør at saken er bredt vurdert med nødvendig avstand før det begjæres kommunikasjonskontroll. Politiet ønsker å ha en godt underbygd sak når det ber om rettens tillatelse, og kommunikasjonskontroll iverksettes normalt bare i saker der politiet forventer et etterforskningsgjennombrudd med et resultat som kan forsvare ressursbruken. Høyeste påtalemyndighet fører en overordnet kontroll med kommunikasjonskontrollbruken i Norge. Alle kommunikasjonskontrollsaker knyttet til etterforskning behandles av domstol, og de skal innrapporteres til Riksadvokaten straks den finner sted og ved kvartalsrapporter. KK-utvalget foretar dessuten inspeksjoner i politidistriktene, og alle i politi og påtalemyndighet har forklaringsplikt for utvalget. Samlet sett innebærer dette et strengt tiltaks- og kontrollregime som bidrar til en høy grad av rettssikkerhet i denne type saker.

KK-utvalget bemerker at omfanget av hurtigkobling, det vil si at kommunikasjonskontroll blir iverksatt av politiet før det foreligger rettslig kjennelse, synes noe høyt (35 %). Men utvalget har ikke sett tilfeller av misbruk av ordningen, altså at det har vært iverksatt hurtigkobling der politiet måtte anta at retten ikke ville gi medhold.

Metodekontrollutvalgets vurdering er at tilretteleggingen for og gjennomføringen av KK-utvalgets kontroll kan forbedres, uten at dette innebærer noen kritikk av det arbeid som er utført så langt. Etter Metodekontrollutvalgets syn kan KK-utvalgets tilgjengelighet for omverden bedres dels gjennom økt ressurstilgang og dels gjennom administrative endringstiltak, uten at dette foranlediger noe lovendringsbehov. Metodekontrollutvalget finner det klart at kontrollorganet må ha tilgjengelig tilstrekkelig teknologisk kompetanse, og at uavhengighetshensyn og kontinuitetshensyn kan tilsi at slik kompetanse finnes blant utvalgsmedlemmene og ikke for eksempel innleies fra eksterne. Metodekontrollutvalget finner videre grunn til å peke på at en av de mest avgjørende faktorer for at kontrollen skal bli effektiv er at utvalget selv innehar høy og oppgaverelevant kompetanse og at de kontrollerte og omverdenen oppfatter det slik.

2.4.3 Nærmere om EOS-utvalget

EOS-utvalget er oppnevnt av Stortinget ved lov 3. februar 1995 nr. 7 for å føre kontroll med etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene) som utøves av eller på vegne av offentlige myndigheter til beskyttelse av nasjonale sikkerhetsinteresser. EOS-tjenestene består av Politiets sikkerhetstjeneste (PST), Etterretningstjenesten (E-tjenesten), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetstjeneste (FOST). Utvalget utfører sitt arbeid uavhengig av Stortinget, men rapporterer hvert år til Stortinget gjennom en årsmelding.

EOS-utvalget gir i sin *Årsmelding for 2012* punkt 4.2 side 6 uttrykk for at PST generelt synes å være bevisst de skrankene lovgivningen og legalitetsprinsippet setter for bruk av tvangsmidler og andre tiltak av inngripende karakter.

I *Årsmelding for 2013* fremgår det at kontrollen ikke har avdekket at PST har gjennomført skjult kameraovervåking eller romavlytting i strid med rettens kjennelser. Utvalget har imidlertid kritisert PST for feil i begjæringer til teletilbyderne om bistand til kommunikasjonskontroll, som har medført at tjenesten i enkelttilfeller har gått utover rettens tillatelser om bruk av tvangsmidler, jf. *Årsmelding for 2013* punkt 4.1 side 19, jf. punkt 4.2. I 2013 har utvalget også tatt opp flere saker der det er stilt skriftlige spørsmål til PST angående behandlingen av personopplysninger i tjenestens arkiver og registre. Utvalgets inntrykk er at PST i det alt vesentlige retter seg etter utvalgets merknader og er enig i utvalgets tolkning av regelverket, jf. *Årsmelding for 2013* punkt 2.1 side 13. Utvalgets kontroll har ført til at opplysninger om flere personer har blitt slettet fra tjenestens systemer. I *Årsmelding for 2014* fremgår det i

punkt 3.3.1 side 13 at utvalget ser positivt på at PST har funnet en teknisk løsning som ivaretar personvernhensyn på en tilfredsstillende måte.

EOS-utvalget mottok 21 klager fra enkeltpersoner og organisasjoner rettet mot PST i 2013, mot henholdsvis 14 klager i 2012 og 11 klager i 2011. De fleste av klagene omhandler påstander om ulovlig overvåking. Ingen av de avsluttede klagesakene har gitt grunnlag for kritikk av tjenesten for ulovlig overvåking. EOS-utvalget mottok 13 klager rettet mot PST i 2014, hvorav to saker ga grunn til merknader fra utvalget, jf. *Årsmelding for 2014* punkt 3.13 side 27.

Metodekontrollutvalget finner at EOS-utvalget innenfor sitt arbeidsfelt synes å ha etablert et forsvarlig kontrollregime samlet sett. Utvalget mener det er grunn til å anta at KK-utvalget kan ha nytte av faglig innflytelse fra EOS-utvalget eller samarbeid om kontrollsystem og kontrollmetodikk. Dette kan for eksempel oppnås gjennom samlokalisering og kontrollfaglig samarbeid. Dette har imidlertid en side til forholdet mellom statsmaktene, ved at EOS-utvalget er oppnevnt av Stortinget mens Kontrollutvalget for kommunikasjonskontroll er et forvaltningsorgan oppnevnt av Kongen. Metodekontrollutvalget har derfor ikke vurdert dette forholdet nærmere.

2.4.4 Vurdering av kontrollsystemet

Etter en samlet gjennomgåelse av kontrollsystemet er *Metodekontrollutvalget* av den klare oppfatning at volumet av kontroll og kontrollorganer fullt ut er tilstrekkelig, men at det er punkter hvor det etter utvalgets syn er grunn til å gjøre grep for å forbedre kontrollen. Det er videre utvalgets syn at blant de mange organ som bidrar til kontrollen er EOS-utvalget, KK-utvalget og domstolene de mest sentrale. EOS-utvalgets kontroll synes etter utvalgets oppfatning å fungere tilfredsstillende. KK-utvalgets kontroll i etterforskningssporet synes imidlertid både å ha rom og behov for betydelig styrking.

Departementet konstaterer at Metodekontrollutvalgets vurdering av kontrollsystemet i liten grad munner ut i konkrete lovforslag. Det er derfor ikke naturlig å behandle dette mer inngående i den foreliggende proposisjonen. Det understrekes imidlertid at enkeltelementer av kontrollsystemet, der lovforslag foreligger, for eksempel om bruk av § 100 a-advokat, vil behandles i kapitlet om fellesspørsmål nedenfor, jf. kapittel 6. Videre reflekteres utvalgets synspunkter i kapitlet om økonomiske og administrative kostnader, jf. kapittel 15.

3 Prinsipper og hensyn som ligger til grunn for departementets vurderinger

3.1 Innledning

Alle mennesker er i utgangspunktet frie individer som beskyttes av et sett med grunnleggende rettigheter. Blant disse er retten til personvern og rettssikkerhet. For at staten skal kunne gjøre inngrep i disse rettighetene, må den kunne vise til et legitimt behov og påvise at dette behovet er så tungtveiende at inngrepet kan rettferdiggjøres. Behovet for å bekjempe kriminalitet kan være et slikt legitimt hensyn.

I Metodekontrollutvalgets utredning del II redegjøres det grundig for de sentrale prinsipper som ligger til grunn for utvalgets vurderinger. Det vises til utredningen kapittel 6 om personvern, kapittel 7 om rettssikkerhet og kapittel 8 om behovet for effektiv kriminalitetsbekjempelse. Videre behandler utvalget de særlige hensyn som gjør seg gjeldende for de aktuelle inngrepene i de enkelte kapitlene om disse. For sammenhengens skyld vil departementet kort belyse de aktuelle kryssende hensyn her.

3.2 Personvern

Alle enkeltmennesker har i utgangspunktet behov for en privat sfære der man kan være i fred for innblanding fra utenforstående, det være seg myndighetene, næringsdrivende mv. eller andre enkeltmennesker. Metodekontrollutvalget slår fast at den private sfære er et sentralt element både i den personlige integritet og personvernet, og en forutsetning for menneskets dannelsesprosess og myndiggjøring, samt for demokratiet og maktbalansen, jf. utredningen punkt 6.2 side 51. Utvalget gir uttrykk for at denne sfæren derfor i utgangspunktet bør være fri både for regulering og innsyn fra det offentlige.

Personvernkommisjonen har foretatt en bred gjennomgåelse av hvordan enkeltmenneskets personvern ivaretas i samfunnet i dag, jf. NOU 2009: 1 Individ og integritet. Her definerer Personvernkommisjonen den enkeltes personvern som «[…] ivaretakelsen av personlig integritet; ivaretakelsen av enkeltindividers mulighet til privatliv, selvbestemmelse (autonomi) og selvutfoldelse», jf. utredningen punkt 4.1.5 side 32.

Det er vanlig å avgrense personvernet til de regler som har som formål å beskytte den *psykiske* integritet. Regler som skal verne individet mot fysisk ubehag eller skade faller således utenfor det tradisjonelle personvernbegrepet. Et vesentlig element i personvernet er at personer i utgangspunktet skal kunne bestemme hva andre skal få vite om hans eller hennes egne personlige forhold. Retten til kontroll over egne opplysninger omtales som et «personopplysningsvern».

Grunnloven § 102 ble endret 14. mai 2014 og etablerer nå et generelt grunnlovsvern for privatlivets fred og personlig integritet, jf. kapittel 5.1 nedenfor.

Personvernet som ideal reflekteres også ved at retten til respekt for privatlivet er en menneskerettighet etter Den europeiske menneskerettskonvensjonen (EMK) artikkel 8 og FNs konvensjon om sivile og politiske rettigheter artikkel 17. Personvernet og personopplysningsvernet er også gitt en sterk stilling i EU-retten, jf. EUs charter om fundamentale rettigheter artikkel 7.

Utgangspunktet etter EMK artikkel 8 nr. 1 er at «[e]nhver har rett til respekt for privatliv, sitt hjem og sin korrespondanse». Bestemmelsen åpner imidlertid for at inngrep kan rettferdiggjøres dersom det har hjemmel i lov og er nødvendig i et demokratisk samfunn for å oppfylle ett eller flere legitime formål, jf. artikkel 8 nr. 2 som lyder:

> «Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

Det følger av menneskerettsloven § 3 at konvensjonen ved motstrid skal gå foran bestemmelser i annen norsk lovgivning. Således markerer konvensjonen en ytre skranke for myndighetenes adgang til inngrep i individets rett til privatliv for å bekjempe kriminalitet og trygge samfunnet.

Av Norges menneskerettslige og EØS-rettslige forpliktelser er det utledet flere grunnleggende prinsipper omtalt som de europeiske personvernprinsippene. Til grunn for alle prinsippene ligger et krav om at personopplysninger skal behandles «fairly and lawfully». Dette innebærer for det første at behandling av personopplysninger skal ha *hjemmel i lov*, og at denne lovhjemmelen må være tilstrekkelig presis. Videre angir *formålsbestemthetsprinsippet* at personopplysninger skal behandles med spesifikke, uttrykkelig angitte og legitime formål, og kun brukes i samsvar med disse formålene. *Nødvendighetsprinsippet* medfører at mengden innsamlede opplysninger skal begrenses til det som er nødvendig for å realisere formålene med innsamlingen og den videre behandlingen av opplysningene. Videre tilsier *sensitivitetsprinsippet* at enkelte typer opplysninger som anses mer sensitive enn andre, skal underkastes en strengere regulering enn andre personopplysninger. Prinsippet om *informasjonssikkerhet* innebærer at det skal etableres tiltak for å sikre personopplysninger mot uautorisert eller utilsiktet tilgang, videreformidling, endring og sletting. Videre betyr prinsippet om *opplysningskvalitet* at personopplysninger skal ha den kvalitet som formålet med behandlingen av opplysningene tilsier, de skal være relevante, adekvate og fullstendige med hensyn til sine bruksformål. Til sist oppstilles krav om at behandlingen av personopplysninger er *forholdsmessig*.

I norsk rett finnes det både bestemmelser som gjelder behandling av personopplysninger og regler som skal ivareta personvernet i form av den personlige integritet. Personopplysningsloven, som trådte i kraft 1. januar 2001, er den generelle loven for behandling av personopplysninger i Norge og gjennomfører EUs personverndirektiv 24. oktober 1995 (95/46/EF). Loven utfylles og suppleres av særlover, for eksempel folkeregisterloven, helseregisterloven og politiregisterloven. Det finnes også en rekke regler i lovverket som skal verne konfidensialitet, det vil si motvirke at personopplysninger gjøres tilgjengelig for andre enn dem som har lovlig tilgang. Brudd på taushetsplikten for personer i tjeneste eller arbeid for offentlig virksomhet er straffbart, jf. Straffeloven § 209 (straffeloven 1902 § 121). Av regler som beskytter den personlige integritet kan nevnes åndsverksloven § 45 c, som beskytter retten til eget bilde. Straffeloven §§ 266–267 (straffeloven 1902 §§ 390 og 390 a) gjør det straffbart å krenke privatlivets fred, ved henholdsvis å gi offentlige meddelelser om personlige forhold og ved skremmende og plagsom opptreden eller annen hensynsløs atferd (for eksempel telefonsjikane). Også straffeloven §§ 204–205 (straffeloven 1902 § 145 om brevbrudd og § 145 a om blant annet telefonavlytting), beskytter privatlivets fred. Straffeprosessloven ivaretar dessuten personvernhensyn gjennom begrensninger i politiets adgang til å bruke etterforskningsmetoder som utgjør inngrep i privatlivet.

Privatlivets fred og den personlige integritet er også gitt et allment vern på ulovfestet grunnlag gjennom rettspraksis. I dommen inntatt i Rt. 1952 side 1217 («To mistenkelige personer») viste Høyesterett til det «alminnelige rettsvern for personligheten», som gir en viss beskyttelse mot at personer brukes som «levende modeller» i kunstneriske verk.

3.3 Rettssikkerhet

Kjernen i begrepet «rettssikkerhet» er knyttet til 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, jf. Metodekontrollutvalgets utredning punkt 7.1 side 60.

Rettssikkerhetskravene kan deles i to hovedkategorier; *materiell rettssikkerhet*, som stiller overordnede krav til en avgjørelses innhold, og *prosessuell rettssikkerhet*, som angir kravene til hvordan avgjørelsen blir truffet.

Sentrale elementer i det materielle rettssikkerhetsbegrepet er *hjemmelskravet* (legalitetsprinsippet) og *forholdsmessighetskravet*. Inngrep mot borgerne må ha hjemmel i lov, for å sikre mot overgrep og vilkårlighet og for å gjøre borgerne i stand til å forutberegne sin rettsstilling. Forholdsmessighetsprinsippet gir anvisning på en interesseavveining hvor nytten av å gjennomføre inngrepet må måles mot hvilken belastning det innebærer for borgeren. Negativt kan dette formuleres som et krav til at skaden eller uleiligheten forbundet med inngrepet ikke må stå i misforhold til det som søkes oppnådd. Nytten eller fordelen må være større enn ulempene eller skaden.

Prosessuell rettssikkerhet omfatter kravene til saksbehandling, herunder saksbehandlings-

reglene for iverksetting og kontroll av etterforskningsmetoder. Dette inkluderer regler som har som formål å forhindre at det benyttes tvangsmidler uten materielt grunnlag, slik som regler om rettens samtykke. I denne sammenheng er krav til *uavhengighet*, *objektivitet* og *saklighet* sentrale rettssikkerhetsgarantier. Kravene innebærer at den som treffer beslutninger må ha den tilstrekkelige distanse til saken til å kunne treffe avgjørelser uten at det tas utenforliggende eller usaklige hensyn.

Andre prosessuelle rettssikkerhetskrav er retten til *kontradiksjon*, *innsyn og underretning*, samt adgangen til *bistand og representasjon*. Borgernes mulighet til å forsvare sine rettslige interesser ivaretas gjennom det grunnleggende prinsippet om kontradiksjon, som innebærer et krav på å varsles til rettsmøter, rett til å være til stede under forhandlingene, til å gjøre seg kjent med materialet som brukes og å ta til motmæle mot det. Dersom kontradiksjon ikke kan gjøres gjeldende fullt ut, må de øvrige rettssikkerhetsgarantier styrkes. Særlig viktig blir mistenktes rett til å være representert ved advokat.

Videre er krav til *begrunnelse av avgjørelsen*, *overprøving*, *kontroll* og *offentlighet* viktige elementer under den prosessuelle rettssikkerhet.

Begrepet «rettssikkerhet» kan også brukes i en videre forståelse, som omfatter samfunnets rettssikkerhet eller kriminalitetsofrenes (fornærmedes og etterlattes) rettssikkerhet. Metodekontrollutvalget påpeker at det kan diskuteres om disse interessene skal omfattes av rettssikkerhetsbegrepet eller ses på som mothensyn til ivaretakelsen av rettssikkerhet for mistenkte. Den allmenne oppfatning synes å være at rettssikkerhetsbegrepet i straffeprosessen bør reserveres for mistenktes vern mot uriktige avgjørelser. I et lovgivningsperspektiv vil et realistisk rettssikkerhetsideal, slik utvalget ser det, bli å finne i et balansepunkt mellom hensynet til mistenktes rettssikkerhet og samfunnets/fornærmede/etterlattes interesser, innenfor rammen av en effektiv ressursutnyttelse.

Vernet mot overgrep og vilkårlighet er ikke først og fremst et vern mot inngrep i seg selv. Inngrep i enkeltpersoners rettssfære kan ha legitime begrunnelser og er i mange tilfeller nødvendige i et demokratisk samfunn. For eksempel vil hensynet til kriminalitetsbekjempelse kunne rettferdiggjøre inngrep i borgernes rettssfære. Vernet mot overgrep og vilkårlighet innebærer imidlertid at inngrepet må skje innenfor de rettslige rammene for inngrepet, slik de er fastsatt gjennom demokratiske prosesser.

3.4 Kriminalitetsbekjempelse

Utgangspunktet for vår samfunnsorden er at alle individer har en alminnelig handlefrihet. For at det moderne samfunn skal fungere, inneholder imidlertid lovgivningen en rekke normer som utgjør begrensninger i denne handlefriheten og som er ment å legge føringer for våre handlinger. Kriminalitetsbekjempelse er en samlebetegnelse på den virksomhet som drives for å hindre at samfunnet og borgerne utsettes for kriminelle handlinger.

Straffelovgivningen retter seg mot handlinger som fører til skade eller fare for skade på interesser som er ansett så viktige at de bør lede til straff. De mest sentrale av disse interessene er individers fysiske og psykiske integritet, økonomiske verdier og særskilte samfunnsinteresser. Straffbare handlinger vil imidlertid også kunne virke destabiliserende på samfunnet generelt. Opplever borgerne at trusselen om kriminalitet blir for stor, vil dette kunne skape en utrygghetsfølelse som igjen vil kunne true samfunnssikkerheten ved at borgerne tar oppgaven med å beskytte seg og sine i egne hender. En slik utrygghetsfølelse vil også kunne svekke borgernes tillit til staten, en tillit som er en forutsetning for vår samfunnsorden og vårt demokrati. Derfor utgjør kriminalitet en trussel mot stabiliteten i og kvaliteten på det samfunnet vi lever i.

Retten til liv blir ofte fremhevet som den mest grunnleggende av menneskerettighetene, og rettigheten er gitt en fremtredende plass i de internasjonale menneskerettighetskonvensjonene. Det følger av EMK artikkel 2 at staten har en positiv plikt til å beskytte borgernes liv mot alle former for trusler, herunder livstruende kriminelle handlinger. Norge har også gjennom ulike internasjonale konvensjoner forpliktet seg til å bekjempe særskilte former for kriminalitet. Det fremgår dessuten av Grunnloven §§ 93 og 102 annet ledd at statens myndigheter skal beskytte retten til liv og verne om ulike sider ved den enkeltes fysiske og psykiske integritet. I korte trekk innebærer retten til liv en plikt for myndighetene til å respektere den enkeltes rett til liv, dvs. at myndighetene ikke kan ta liv (med visse unntak) og til å beskytte den enkelte mot at andre tar deres liv. Statens plikt til å beskytte samfunnet mot kriminalitet kommer videre til uttrykk i politiloven § 1, der det heter at staten skal sørge for den polititjeneste samfunnet har behov for. Politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borger-

nes rettssikkerhet, trygghet og alminnelige velferd for øvrig. Omfanget av politiets oppgaver med å beskytte samfunnet mot kriminalitet, avhenger i stor grad av den til enhver tid gjeldende kriminalitetsutviklingen.

De senere år har det vokst frem former for kriminalitet som i seg selv er egnet til å true stabiliteten i samfunnet. Terrorisme er straffbare handlinger som har som formål nettopp å skape frykt og undergrave stabiliteten i samfunnet og grunnlaget for den demokratiske rettsstaten. Også enkelte andre kriminalitetsformer er i seg selv egnet til å svekke stabiliteten i samfunnet, som for eksempel organisert kriminalitet og korrupsjon. Det vises til utvalgets redegjørelse for kriminalitetsutviklingen i utredningen punkt 8.6 side 74 flg. samt til kapittel 4 nedenfor.

4 Kriminalitetsbildet – trender og utfordringer

4.1 Innledning

«Kriminalitetsbildet» er en samlebetegnelse på den kriminalitet som samfunnet til enhver tid står overfor. Samfunnets behov for beskyttelse defineres av risikoen for kriminalitet. Denne risikoen er et produkt av sannsynligheten for at kriminelle handlinger vil finne sted og konsekvensene av at slike handlinger inntreffer. Metodekontrollutvalget gir i utredningen punkt 8.6 side 74 til 100 en oversikt over kriminalitetsutviklingen og politiets utfordringer per 2009. Departementet har i tillegg sett hen til 22. juli-kommisjonens rapport (NOU 2012: 14 Rapport fra 22. juli-kommisjonen), Politianalysen (NOU 2013: 9 Ett politi – rustet til å møte fremtidens utfordringer) og trusselvurderinger og årsrapporter de siste årene fra blant annet PST, Kripos, Direktoratet for samfunnssikkerhet og beredskap, EOS-utvalget og KK-utvalget. Nedenfor gis en oversikt over noen utviklingstrekk i kriminalitetsbildet.

Innledningsvis kan det slås fast at utviklingen innen den organiserte kriminaliteten viser større mobilitet, mer komplekse lovbrudd, en profesjonalisering av utøverne og større grad av internasjonalisering og multikriminalitet. Politiets tilgang til skjulte etterforskningsmetoder er en forutsetning for effektiv kriminalitetsbekjempelse av de mest alvorlige og samfunnsskadelige forbrytelsene. Det er viktig at styrkeforholdet mellom politiet og den trusselen de kriminelle representer ikke forrykkes i negativ retning. Tvert imot bør politiet styrkes og gjøres bedre i stand til å bekjempe kriminalitet, gitt at rettsstatsprinsippene fortsatt ivaretas på en god måte.

4.2 Grenseoverskridende kriminalitet

Det fremgår av Politianalysen at den grenseoverskridende kriminaliteten gir politiet nye utfordringer, jf. NOU 2013: 9 punkt 3.1 side 18:

> «Flere utviklingstrekk i samfunnet utfordrer den norske politimodellen og stiller nye krav til hva som er en god polititjeneste. Selv om den registrerte kriminaliteten både i Norge og resten av Nord-Europa totalt sett er fallende, blir den stadig mer kompleks, grenseoverskridende og organisert. Informasjons- og kommunikasjonsteknologi danner stadig oftere en arena og et virkemiddel for å gjennomføre kriminalitet. Det er en sterk befolkningsvekst, konsentrasjon av bosettingsmønstrene og til dels markante endringer i befolkningssammensetningen. Disse utviklingstrekkene har allerede satt dagens politimodell under betydelig press når det gjelder krav til spesialisert kompetanse, nye arbeidsmetoder, systemer og responsevne. Dette er i seg selv en utfordrende situasjon å håndtere for enhver organisasjon. Med dagens organisering og struktur vil disse utfordringene forsterkes i årene som kommer.»

Når det gjelder kriminalitetens karakter, viser Metodekontrollutvalget på side 78 til de utviklingstrekk som Metodeutvalget og Politimetodeutvalget pekte på. Metodeutvalget la i NOU 1997: 15 punkt 2.2 side 8 til grunn at kriminaliteten hadde undergått kvalitative endringer og uttalte blant annet:

> «[..] kriminalitetsutviklingen har vist en fremvekst av alvorlig og brutal voldskriminalitet tilknyttet spesielle miljøer. Utviklingen [viser at] kriminelle i større grad sprer frykt, og bruker mer vold og våpen. Miljøene er ofte lukket, og det er en økt grad av profesjonalitet og hensynsløshet i forhold til omverdenen.»

Det ble også påpekt at den økte kontakten over landegrensene og økningen i innvandring til Norge hadde medført økning i kriminalitet begått av personer med utenlandsk opprinnelse og innenfor utenlandske miljøer. Det ble understreket at globaliseringen i verden for øvrig også hadde fått konsekvenser for kriminalitetsbildet. Et typisk trekk i de senere år – så vel internasjonalt som nasjonalt – er at det ikke lenger bare snakkes om internasjonal narkotikakriminalitet som et hovedproblem, men om organisert internasjonal kriminalitet, jf. NOU 1997: 15 punkt 3.1.3.4 side 28.

> «[…] Narkotikaorganisasjonene engasjerer seg i dag innenfor mange sider av kriminaliteten, som f eks våpenhandel, prostitusjon, ordinær vinningskriminalitet og økonomisk kriminalitet. En spesielt bekymringsfull side av dette er det som kalles hvitvasking. Penger fra kriminell virksomhet investeres i lovlig eller tilsynelatende lovlig virksomhet. På sikt kan dette bidra til undergraving av den lovlige virksomhet i offentlig og privat sektor, noe som vil kunne få alvorlige konsekvenser. Allerede i dag kan det i enkelte land være vanskelig å skille mellom de organiserte kriminelles virksomhet og myndighetsutøvelse. Også i Norge må vi være på vakt mot en slik utvikling. I sin ytterste konsekvens kan dette innebære en trussel mot demokratiet.»

Politimetodeutvalget la i NOU 2004: 6 punkt 9.1.3.4 side 163 til grunn at kriminalitetsbildet på det tidspunktet hadde enkelte kvalitative trekk som skilte det fra kriminaliteten ti år tidligere, og som måtte forventes å forsterke seg ytterligere i de kommende årene. Disse trekkene var bedre organisering, økt fleksibilitet hos de kriminelle, større grad av samarbeid mellom ulike kriminelle nettverk, økt internasjonalisering gjennom økt mobilitet, økt bruk av avansert teknologi, økt spesialisering og profesjonalisering, økt sammenblanding mellom illegal og legal virksomhet og fare for økt brutalitet. Disse tendensene har altså slått til, jf. ovenfor og nærmere nedenfor.

4.3 Organisert kriminalitet

I Kripos' rapport *Den organiserte kriminaliteten i Norge – trender og utfordringer 2013–2014* omtales kriminalitetstyper og aktører innen den organiserte kriminaliteten i Norge som utgjør en trussel mot det norske samfunnet. Det gis uttrykk for at den pågående utviklingen fortsetter, med stadig større mobilitet og tettere samarbeid mellom norske og internasjonale kriminelle, se side 4:

> «Organisert kriminalitet består i økende grad av uformelle og fleksible nettverk som samarbeider på tvers av nasjonalitet, etnisitet og annen kulturell tilhørighet. Større mobilitet og lettere tilgang til teknologi gjør det mindre viktig for kriminelle aktører å være tett organisert geografisk og hierarkisk.»

Av de kriminelle aktørene som opererer i Norge, er størst bekymring knyttet til litauiske kriminelle nettverk, 1 % MC-miljøene og gjengmiljøene i og rundt Oslo.

Litauiske kriminelle nettverk har stor utbredelse, både i Norge og internasjonalt. De samarbeider med mange kriminelle aktører og har en bred kontaktflate i Norge. Litauiske nettverk knyttes til organisert og alvorlig kriminalitet i Norge, blant annet mobil vinningskriminalitet, grove tyverier og annen organisert vinningskriminalitet. De fremstår også som hovedleverandør av metamfetaminer til Norge. Disse kriminelle miljøene har en lav terskel for bruk av vold, og det er flere eksempler på drap ved interne oppgjør, samt bruk av grov vold og trusler.

De såkalte 1 % MC-miljøene har ekspandert kraftig både nasjonalt og internasjonalt. Ekspansjonen utfordrer situasjonen mellom 1 % MC-klubbene i Norge. Hells Angels (inkludert miljøet rundt klubben) fremstår som den største utfordringen, spesielt innen narkotikakriminalitet og ved systematisk bruk av grov vold, trusler og utpressing.

De etniske kriminelle gjengene, som B-gjengen, Young Guns, Furuset Bad Boys og gjengmiljøet på Holmlia, har en sentral plass i kriminalitetsbildet i Norge, både som aktører i den profittbaserte kriminaliteten, men også som en trussel ved langvarige voldelige konflikter. Spenningsnivået har økt som følge av en rekke voldelige hendelser, og Kripos anser trusselnivået som høyt, med stor sannsynlighet for skyteepisoder i det offentlige rom. Profittbasert kriminalitet som ran, trusler, narkotika, torpedovirksomhet, utpressing, bedragerier og annen økonomisk kriminalitet, er en viktig del av gjengenes virke. Gjengene opererer hovedsakelig i Oslo og tilliggende distrikter, men har også et større nedslagsfelt, spesielt knyttet til innførsel og omsetning av narkotika. Gjengmedlemmer er i større grad enn tidligere involvert i tradisjonell forretningsvirksomhet, blant annet transportselskaper, bilpleiefirmaer, restauranter og dagligvareforretninger.

Også i Politianalysen NOU 2013: 9 punkt 3.1 side 19 fremgår det at kriminaliteten blir mer organisert og mobil, og at det har vært en tydelig fremvekst av mer komplekse og sammenvevde kriminelle nettverk.

I Kripos' *Trendrapport 2015 Organisert og annen kriminalitet i Norge* fremgår det at kriminelle nettverk fra Litauen, Balkan og Marokko har sentrale posisjoner i det norske narkotikamarkedet, og at de sannsynligvis spiller en kritisk rolle i koordineringen av store narkotikaleveranser til Norge. Norske kriminelle miljøer eller gjenger er primært mottakere og videredistributører av

narkotika. De lar utenlandske nettverk og mellommenn i Norge organisere narkotikaleveransene til Norge, blant annet for å redusere risikoen. Tendensen de siste årene har vært at de tradisjonelle gjengmiljøene i liten grad avgrenser sin kriminelle virksomhet til et bestemt miljø. De opererer også i langt løsere nettverk på siden og på tvers av gjengtilknytning eller kriminelle miljøer. Grensen mellom de ulike kriminelle gjengene har derfor blitt mer utydelig. 1 % MC-miljøet fortsetter å vokse i Norge. Samtidig fremstår det som mer fragmentert og mer skiftende enn tidligere. Denne utviklingen kan føre til at miljøet blir mer ustabilt.

I Kripos' *Trendrapport 2016 Organisert og annen kriminalitet i Norge* gis det uttrykk for at albanske, polske og litauiske aktører dominerer innførselen av narkotika til Norge. Personer knyttet til gjengmiljøet i Oslo eller 1 % MC-miljøet har god tilgang på våpen og kan gjøre stor skade ved eventuelle konflikter og voldelige oppgjør. Gjengenes narkotikavirksomhet har nedslagsfelt over hele landet. Enkelte gjenger søker kontinuerlig å utvide narkotikamarkedet sitt, og vold, trusler og hjemmeran følger ofte med i den sammenheng. Flere kriminelle med tilknytning til gjengmiljøet, forsøker å bygge opp lovlige virksomheter ved siden av eller i sammenheng med den ulovlige aktiviteten de holder på med.

4.4 Den teknologiske utviklingen

Et av de mest markante trekk ved kriminalitetsutviklingen de senere årene er betydningen av den teknologiske utviklingen, jf. Metodekontrollutvalgets rapport punkt 8.6.2 side 78. Økt tilgang til og bruk av Internett har generert både nye former for kriminalitet og nye versjoner av eller arenaer for tradisjonelle straffbare handlinger.

Begrepet datakriminalitet brukes ofte om straffbare handlinger som gjennomføres ved bruk av data- og kommunikasjonsteknologi, og om straffbare handlinger som er rettet mot datamaskiner eller datasystemer. Internett og datasystemer er blitt et viktig verktøy ved gjennomføringen av enkelte tradisjonelle former for kriminalitet, for eksempel vinningsforbrytelser og ulovlig etterretningsvirksomhet, men også ved befatning med overgrepsbilder av barn og forberedelse til seksuelle overgrep mot barn («grooming»).

I Dokument 7:1 (2011–2012) *Årsmelding for 2011* til Stortinget fra EOS-utvalget kapittel III punkt 3 side 11 nevnes teknologiens betydning for terrorlovbrudd:

> «[...] Bildet kompliseres ytterligere av at trusselaktørene gjerne har forgreininger i flere land og at den teknologiske utviklingen muliggjør forberedelser til terrorhandlinger på tvers av landegrenser, særlig ved bruk av Internett og annen moderne kommunikasjonsteknologi.»

I Kripos' rapport *Den organiserte kriminaliteten i Norge – trender og utfordringer 2013–2014* heter det på side 4:

> «Kriminelle bruker i økende grad informasjonsteknologi for å begå kriminalitet, som for eksempel bedrageri, distribusjon av narkotika og doping samt i annonsering og rekruttering av potensielle ofre for menneskehandel og til forenkling av ulovlig migrasjon.[…]
>
> Angrepene rettet mot IKT-systemer har økt betraktelig. Dette innbefatter blant annet datainnbrudd, digital spionasje, hacking og nettbankbedragerier. […].»

Det uttales følgende om «det digitale rom» i *Trusler og sårbarheter 2013 Samordnet vurdering fra E-tjenesten, NSM og PST*, på side 9:

> «Stadig mer sensitiv informasjon lagres i det digitale rom. I dagens situasjon er de alvorligste registrerte hendelsene mot norske interesser at aktører får innsyn i sensitiv informasjon vedrørende politiske, militære og høyteknologiske forhold. Samtidig utgjør skadeverk og annen kriminalitet i det digitale rom en betydelig utfordring for samfunnet.
>
> Aktørene som kan stå bak trusler i det digitale rom, spenner fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper til organiserte hackergrupper og enkeltpersoner.»

I *Åpen trusselvurdering 2016* side 6 vurderer PST det slik at utenlandske etterretningstjenester vil fortsette sitt omfattende arbeid i og mot Norge i 2016, herunder ved bruk av digital spionasje:

> «Spionasje i det digitale rom er blitt en integrert del av fremmede sikkerhets- og etterretningstjenesters arbeid og utføres i stort omfang mot Norge og norske interesser. Som etterretningsmetode er digital spionasje kostnadseffektiv og har høyt etterretningsutbytte. Nettverksoperasjoner kan kompromittere og skade grunnleggende nasjonale interesser. Vi

er bekymret for at virksomheter som forvalter store verdier, ikke tar trusselen fra nettverksoperasjoner tilstrekkelig på alvor, og at mangelfull sikkerhetskultur og kompetanse bidrar til at sårbarhetene vedvarer.

Etterretningsvirksomhet i det digitale rom innebærer også kartlegging av og digitale operasjoner mot kommunikasjons- og informasjonsinfrastrukturer. Datautstyr og programvare kan infiseres og manipuleres for avlyttings- og sabotasjeformål. Etterretningstjenester kan også utnytte leverandører, servicepersonell og utro tjenere som en inngang for å installere slike skadevarer. Gjennom digitale angrep kan fremmede staters etterretningstjenester uten forvarsel dermed ramme kritisk infrastruktur, med et betydelig skadepotensial for Norge som stat og samfunn.»

I tillegg til å representere nye utfordringer for politiet, kan den teknologiske utviklingen også legge til rette for å gi politiet nye verktøy til etterforskning, avverging og forebygging, for eksempel dataavlesing. Når lovbrudd gjennomføres ved hjelp av datateknologi, etterlates dessuten ofte elektroniske spor. Åpne og lukkede nettsteder og nettverk åpner også nye muligheter for spaning. Kriminelle utøvere tar del i samfunnets teknologiske utvikling, og økt bruk av mobiltelefoni, sosiale medier og annen IKT-basert kommunikasjon, er utbredt ved de fleste typer alvorlige lovbrudd hvor kriminelle aktører samarbeider. Skal politiet avdekke og oppklare alvorlige forbrytelser, vil skjult tilstedeværelse på disse arenaene kunne være avgjørende for å innhente informasjon og bevis.

4.5 Terrorisme

I EOS-utvalgets *Årsmelding for 2011* fremheves terrorisme og soloterrorisme som trusler, og det fremgår at dette stiller andre krav til sikkerhetstjenestene enn tidligere, jf. kapittel III punkt 3 side 11:

«Trusselbildet er i dag preget av internasjonal terrorisme og soloterrorisme, selv om også de mer tradisjonelle trusler fremdeles gjør seg gjeldende, for eksempel fremmed etterretningsvirksomhet og voldelige ekstreme grupperinger. At trusler kan komme fra enkeltpersoner og ikke-statlige organisasjoner, stiller andre krav til tjenestene enn tidligere og reiser en rekke personvernrelaterte problemstillinger […].»

22. juli-kommisjonen ga i NOU 2012: 14 på side 15 uttrykk for at PST, med en bedre arbeidsmetodikk, kunne ha kommet på sporet av gjerningsmannen før 22. juli. Om kommisjonens syn på hvilken adgang PST bør ha for å ta i bruk inngripende metoder for å bekjempe terror, heter det i utredningen punkt 16.6 side 390:

«Kommisjonen mener det er viktig at PST får tilgang til effektive metoder også innenfor IKT-basert informasjonsinnhenting, knyttet til de konkrete sakene hvor det foreligger et reelt behov for å undersøke om noen er i ferd med å planlegge et terrorangrep. Det vil være situasjoner der det er legitimt å ta i bruk inngripende tiltak for å beskytte det som terrorister ønsker å ramme – demokratiet som styreform og verdier som individets frihet og grunnleggende menneskerettigheter.»

Kommisjonen viser til at Metodekontrollutvalgets utredning, og henvendelser fra PST og Kripos om klarere regler, ligger i Justis- og beredskapsdepartementet i påvente av behandling, og i punkt 16.6 side 391 note 107 nevner kommisjonen blant annet dataavlesing som aktuelt tema.

I den samordnede trusselvurderingen fra E-tjenesten, NSM og PST for 2013 side 14–15 konkluderes det med at utviklingen de senere årene viser at vi står overfor et mer skjerpet, fragmentert og uoversiktlig trusselbilde. Personer og miljøer inspirert av ekstrem islamistisk ideologi, anses å utgjøre den mest alvorlige terrortrusselen i og mot Norge. Annen ideologisk forankring, herunder islamfiendtlighet samt høyre- og venstreekstremisme, kan også ligge til grunn for terrorhandlinger. På side 7 heter det:

«I Norge er det et multietnisk ekstremt islamistisk miljø som utgjør kjernen i terrortrusselen. Miljøet består hovedsakelig av unge menn oppvokst i Norge. Miljøet har flere handlingsorienterte ledere, og de formidler en ekstremistisk retorikk der blant annet Norge er sentral i fiendebildet. Det forventes at dette miljøet fortsatt vil være aktivt med på å radikalisere, rekruttere, spre voldelig propaganda samt samle inn penger.»

Sikkerhetstjenestene gir uttrykk for at en økning i politisk høyreekstremistisk aktivitet i Europa foreløpig ikke har påvirket trusselbildet i Norge. Det vurderes som mest sannsynlig at eventuelle terrortrusler fra høyreekstreme eller islamfiendtlige aktører, rettet mot Norge eller norske interesser i

utlandet, vil komme fra enkeltindivider eller små grupper.

Ovennevnte vurdering gjentas og utbygges noe i oppsummeringen i *Åpen trusselvurdering 2013* fra PST:

> «Ekstrem islamisme utgjør fortsatt den mest alvorlige terrortrusselen i Norge, og vi forventer at den vil gjøre det også i 2013. Personer i de ekstreme islamistiske miljøene vil fremdeles være opptatt av å formidle ekstremistisk retorikk, der blant annet Norge står sentralt i fiendebildet. Dette gjør propagandaen appellerende for påvirkelige ungdommer her i landet, og bidrar til at radikalisering fremdeles vil være et trekk ved trusselbildet.
>
> I løpet av 2013 kan det bli en økning av antall personer i de norske miljøene med erfaring fra treningsleire og kamphandlinger. Personer med denne type erfaring forventes å ha fått en lavere terskel for bruk av vold.
>
> De organiserte høyre- og venstreekstreme miljøene fremstår som mindre truende mot samfunnet enn de ekstreme islamistiske miljøene. De kan imidlertid utføre vold mot enkelte politiske motstandere eller religiøse og etniske minoriteter. Enkeltpersoner og små grupper som opererer uavhengig av de organiserte miljøene, representerer en stor utfordring i 2013.
>
> Anders Behring Breivik vil fortsatt være en inspirator for enkeltpersoner, både i Norge og internasjonalt. Selv om de fleste sympatisører i Norge synes å ta avstand fra terroraksjonen på Utøya, er det flere som støtter angrepet mot regjeringskvartalet og regjeringen.»

I *Åpen trusselvurdering 2014* slår PST fast at terrortrusselen mot Norge anses som skjerpet. Den største trusselen kommer fortsatt fra et multietnisk ekstremt islamistisk miljø på Østlandet. Et lite antall personer har stor betydning for aktiviteten i, og trusselen fra, dette miljøet. Flere ekstreme islamister fra Norge har, gjennom deltakelse i kamp og trening med militante grupper i utlandet, blant annet i Syria, fått økt kapasitet til å gjennomføre terrorhandlinger. Enkelte av dem som returnerer fra slike opphold, vurderes i 2014 å representere en potensiell trussel mot norske interesser.

I forbindelse med terrortrusselen sommeren 2014, der fire medlemmer av terrororganisasjonen Den islamske staten i Irak og Levanten (ISIL) ble antatt å være på vei til Norge for å gjennomføre en terroraksjon, ble beredskapen hevet og tiltak iverksatt for å trygge Norge. I EOS-utvalgets *Årsmelding for 2014* punkt 1.4.3 side 8 er følgende uttalt om terrorvarselet:

> «I slutten av juli 2014 offentliggjorde PST at tjenesten hadde mottatt informasjon fra utenlandske samarbeidende tjenester om at det var en gruppe personer på vei fra Syria til Europa med den hensikt å gjennomføre en terrorhandling i Norge. Norske myndigheter vurderte det som nødvendig å iverksette en rekke forebyggende sikkerhetstiltak på bakgrunn av terrorvarselet.
>
> Utvalget har fått grundige og informative orienteringer om hvordan PST, E-tjenesten og NSM har arbeidet med terrortrusselen, herunder særlig om samarbeidet og informasjonsutvekslingen mellom PST og E-tjenesten. Utvalget har i denne sammenheng også blitt orientert om mistanke om lekkasjer av sikkerhetsgradert informasjon i sakens anledning. Videre har utvalget inspisert arkiver og registre i PST og E-tjenesten, for å kontrollere om tjenestenes informasjonsinnhenting og metodebruk har vært i samsvar med de gjeldende rettslige vilkårene. […]
>
> Undersøkelsene i PST har ikke gitt grunn til videre oppfølging fra utvalgets side. […]»

PSTs trusselvurdering for 2014 ble supplert med et tillegg 5. november 2014, der de mest sannsynlige terrorscenarier basert på den senere tids utvikling skisseres. Her tas det utgangspunkt i at det den senere tid har vært gjennomført en rekke arrestasjoner i vestlige land for å avverge terrorangrep. Ved de fleste av disse arrestasjonene har det blitt påvist indirekte eller direkte knytninger til terrororganisasjonen ISIL og konflikten i Syria og Irak. PST og E-tjenesten har tidligere varslet om en negativ utvikling i trusselbildet, og PST slår i den supplerende trusselvurderingen fast at situasjonen har tilspisset seg de siste månedene. Det pekes blant annet på at ISIL i september 2014 publiserte en tale hvor terrororganisasjonen oppfordrer sine tilhengere til å gjennomføre angrep i alle land som er en del av den USA-ledede alliansen mot ISIL. I talen oppfordrer ISIL spesifikt til angrep mot militært personell samt medlemmer av politi-, sikkerhets- og etterretningstjenester. PST mener oppfordringene i talen må sees i sammenheng med endringene innen modus operandi for ekstrem islamistisk terror i Europa de siste årene. Ideologisk inspirasjon fra ISIL og andre terrororganisasjoner er en sentral driver for terrorhandlinger, også for personer som har en løs organisatorisk tilknytning. Ekstrem islamistisk terror i Europa har de siste årene vært preget av lite kom-

plekse angrep, utført med våpen og virkemidler som er enkle å anskaffe og bruke. Angrepene har i økende grad blitt rettet mot lett tilgjengelige, men symbolske mål. Slike angrep kan være vanskelige å forhåndsvarsle. PST mener imidlertid at risikoen vil kunne reduseres ved å iverksette effektive sårbarhetsreduserende tiltak.

I den oppdaterte trusselvurderingen 5. november 2014 fremgår det at Etterretningstjenesten og PST, gjennom Felles kontraterrorsenter (FKTS), utarbeidet en gradert trusselvurdering som er formidlet til relevante departementer og etater. Det konkluderes der med at det innenfor de kommende 12 månedene er sannsynlig at det kan trues med, og bli forsøkt utført, terrorangrep i Norge. Med utgangspunkt i gjeldende trender innenfor ekstreme islamisters mål og metoder, samt det fiendebildet som tegnes av ISIL, antas det at militært personell, politi og enkelte politiske beslutningstakere kan være særlig utsatte. Departementet bemerker at politidrap i Frankrike og en planlagt, men avverget terroraksjon i Belgia i januar 2015 tyder på at dette medfører riktighet.

I *Åpen trusselvurdering 2015* slår PST fast at den negative utviklingen av trusselsituasjonen i Norge forventes å fortsette i 2015. Det finnes aktive ekstreme islamistiske miljøer i Norge som tiltrekker seg nye tilhengere og rekrutterer fremmedkrigere. PST legger til grunn at norske fremmedkrigere som inngår i terrorgrupper i utlandet, kan utvikle voldsintensjon og -kapasitet, og at hjemvendte personer vil kunne ha en lavere terskel for voldsbruk i Norge. Norske fremmedkrigere som forblir i utlandet, er forbilder for sympatisører i Norge og kan være pådrivere for radikalisering og rekruttering. ISILs og al-Qaidas oppfordringer om hevnaksjoner, samt terrorhendelser i vestlige land, vil kunne påvirke enkeltpersoner til å gjennomføre voldsaksjoner i Norge. Det slås fast at Norge er en sentral del av fiendebildet til aktive ekstreme islamistiske miljøer i Norge, og at norsk militær deltakelse mot ISIL og al-Qaida vil kunne bidra til å forsterke fiendebildet. Dette fiendebildet favner dessuten mange ulike aktører. Ulike meningsmotstandere, både muslimer og ikke-muslimer, kan derfor bli gjenstand for truende eller voldelige handlinger fra ekstreme islamister. Dette kan inkludere forskere, journalister, politikere, religiøse talspersoner, og andre samfunnsdebattanter som konfronterer eller motarbeider ekstremistene.

Også E-tjenesten mener at terrortrusselen mot Norge øker, jf. *Fokus 2015* side 72 flg.:

> «Den spesifikke terrortrusselen mot Norge vurderes å øke i 2015. Det skyldes at personer med tilknytning til Norge og andre nordiske land i større grad enn tidligere har kontakt med internasjonale militante islamistgrupper. I tillegg er det en konsekvens av Norges bidrag til koalisjonen mot ISIL og sistnevntes oppfordringer om angrep mot land som inngår i koalisjonen. […]»

E-tjenesten påpeker at trusselen fremmedkrigerne utgjør, har minst tre dimensjoner. Den ene er trusselen fra små grupper eller individer som returnerer til Norge for å gjennomføre angrep på eget initiativ, etter å ha blitt ideologisk inspirert og radikalisert som følge av sitt opphold blant militante islamister. Den andre er trusselen fra organiserte celler som returnerer med oppdrag om å iverksette angrep. For det tredje kan fremmedkrigere fra Norge oppfordre og instruere personer i sitt kontaktnettverk i Norge til å gjennomføre angrep. Det er dermed også en mulighet for at personer som ikke selv reiser til konfliktområder, men som er en del av radikale miljøer, vil forsøke å gjennomføre angrep i Norge på eget initiativ etter inspirasjon fra grupper i utlandet.

Den 28. oktober 2015 uttalte PST at sannsynligheten for terrorangrep fra ISIL-sympatisører er noe redusert. Dette skyldes primært endringer knyttet til de norske ekstremistmiljøene. 18 personer fra miljøene er mest sannsynlig drept i Syria, mens 9 er varetektsfengslet og siktet for terrorrelatert kriminalitet. Dette innebærer at miljøene totalt sett fremstår som noe svekket.

I *Åpen trusselvurdering 2016* fremgår det at ekstrem islamisme fortsatt vurderes å utgjøre den største terrortrusselen, og det er mulig at det i løpet av 2016 vil bli forsøkt gjennomført terrorangrep i Norge. Det er usikkert hva som er den fremtidige strategien til ISIL og al-Qaida. I den grad de ønsker å gjennomføre sentralstyrte terroraksjoner i vestlige land, vil terrortrusselen kunne øke i Norge. PST påpeker likevel at Norge ikke er blant de mest profilerte landene som inngår i ISILs og al-Qaidas fiendebilde.

Trusselen fra de høyreekstreme miljøene i Norge er vurdert som økende. Antall sympatisører som ikke er en del av et organisert miljø, er også vurdert å være i vekst. Mobilisering rundt temaer knyttet til det høye antallet flyktninger og asylsøkere er årsaken til denne utviklingen.

I september 2015 ga PST uttrykk for at den økte tilstrømningen av flyktninger og asylsøkere til Norge kan få negative følger for trusselbildet knyttet til det høyreekstreme miljøet i Norge. Dette fordi motstand mot innvandring er en av de mest sentrale sakene, og en viktig mobiliserings-

faktor, for dette miljøet. Det ligger også et potensial for at venstreekstreme miljøer i Norge kan samles rundt saker relatert til flyktningkrisen. En eskalering av konflikten med det høyreekstreme miljøet kan føre til motreaksjoner og voldelige sammenstøt mellom høyre- og venstreekstremister. Asylsøkere knyttet til ekstrem islamisme framstår ikke som en sentral bekymring for PST på kort sikt. På lengre sikt er det mulig at enkelte asylsøkere vil kunne utgjøre en terrortrussel i Norge. PST begrunner dette med at asylsøkere er en sårbar gruppe for radikalisering, men her vil det også være store variasjoner, blant annet basert på landbakgrunn og sosioøkonomiske forhold. Det er heller ikke en nødvendig sammenheng mellom det å ha vært en voldsaktivist i et krigsherjet hjemland og det å bli en voldsutøver i et nytt land.

Departementet vil påpeke at man gjennom de ti siste årene har sett en utvikling i måten politisk motivert vold utføres på gjennom ulike terroraksjoner. USA 11. september 2001, Madrid 2004 og London 2005 er eksempler på store, spektakulære terroraksjoner. De siste årene har derimot vist en tendens til at mer spredte aksjoner blir forsøkt gjennomført og utført. Flere av disse terrorhandlingene er utført av enkeltpersoner som handler etter inspirasjon fra andre, men de står for selve gjennomføringen på egenhånd. Eksempler er terroraksjoner i Stockholm og København i 2010, der bare aktivistene selv ble rammet. Angrep mot mål i Europa er altså blitt mindre komplekse, jf. også E-tjenestens vurdering *Fokus 2015* side 72 flg. Det er en tendens til at det brukes enkle våpentyper, som håndvåpen og kniv, og at angrep rettes mot symboltunge mål. Terrorangrepene mot det jødiske museum i Brussel mai 2014 og mot redaksjonslokalene til satiremagasinet Charlie Hebdo i Paris 7. januar 2015, samt den påfølgende gisseltakingen i en jødisk butikk, er eksempler på dette. På et fransk nettforum ble det, etter angrepet mot Charlie Hebdo, gitt uttrykk for at Danmark og Norge var neste terrormål. Trusselen kan etter alt å dømme forstås i lys av karikaturstriden i 2006, hvor det spesielt var Danmark og Norge som var i søkelyset. I midten av februar 2015 ble to personer, i tillegg til terroristen, drept og flere såret i et dobbelt terrorangrep mot henholdsvis en synagoge og et debattmøte om ytringsfrihet i København, der Muhammed-tegner Lars Vilks var en av deltagerne.

Departementet legger til grunn at terrortrusselen mot Norge økte våren 2015, i tråd med sikkerhetstjenestenes vurderinger. Det bemerkes imidlertid at terrortrusselen synes å være noe mindre våren 2016, som følge av at en rekke personer fra de norske ekstremistmiljøene enten er drept, varetektsfengslet eller dømt for terrorrelaterte lovbrudd. Utviklingen fremover vil likevel være ustabil og usikker. Trusler og oppfordringer, blant annet fra ISIL, kan fortsatt påvirke enkeltpersoner eller små grupper til å gjennomføre terrorangrep. I den grad ISIL og al-Qaida ønsker å gjennomføre sentralstyrte terroraksjoner i vestlige land, vil terrortrusselen også kunne øke i Norge. Samtidig vil flyktningkrisen kunne medføre økt oppslutning om høyre- og venstreekstreme miljøer.

4.6 Menneskehandel, menneskesmugling og prostitusjon

I Kripos' rapport *Den organiserte kriminaliteten i Norge – trender og utfordringer 2013–2014* anføres det at de økonomiske nedgangstidene i Sør-Europa vil påvirke kriminalitetsbildet i Norge, og at det er en risiko for at antallet mennesker som oppholder seg ulovlig i Norge vil øke. Det vil igjen føre til alvorlig kriminalitet som menneskehandel, menneskesmugling, bruk av falske identiteter, svart arbeid, narkotika- og vinningskriminalitet. På side 4 uttales det:

> «Antallet irregulære migranter som oppholder seg i Norge uten avklart identitet, er bekymringsfullt. Irregulære migranter kan knyttes til ulike kriminalitetsområder, både som ofre og gjerningspersoner.[…]»

Menneskehandel og menneskesmugling omtales på side 22–28 i Kripos' rapport. Her påpekes det at grenseoppgangen mellom menneskesmugling og menneskehandel ofte er uklar ved at mange innsmuglede står i et gjeldsforhold til smuglerne og må gjøre opp for seg etter ankomst til Norge, for eksempel gjennom tvangsarbeid eller narkotikasalg.

I likhet med menneskesmugling er menneskehandel en relativt skjult kriminalitet i den forstand at selv om tjenestene/arbeidet offeret utfører er synlig, vil ikke nødvendigvis utnyttelsen, selve kontrollen eller kontrollmekanismene være det. Ofre for menneskehandel kan ha mange grunner til ikke å anmelde forholdet, for eksempel frykt for represalier mot dem selv eller deres familie hjemme, og det er opp til politiet å avdekke denne formen for kriminalitet. Tradisjonelt forbindes menneskehandel med utnyttelse av kvinner til prostitusjon. De siste årene har imidlertid opp-

merksomheten i økende grad blitt rettet mot utnyttelse til tvangsarbeid, tigging, vinningskriminalitet, samt utnyttelse av kvinner innen au pair-instituttet.

På prostitusjonsområdet finnes aktører fra Nigeria, Russland, Balkan og Øst-Europa. Mange av de kriminelle aktørene er fysisk plassert i hjemlandet og kontrollerer sine ofre «hjemmefra». Også norske menn er dømt for menneskehandel. Flere politidistrikter melder om at nettverk som er involvert i menneskehandel knyttet til prostitusjon er multikriminelle, ved at de også er involvert i narkotika-, volds- og vinningskriminalitet.

I *Trendrapport 2016 Organisert og annen kriminalitet i Norge* påpeker Kripos at migrasjonspresset på Europa er rekordhøyt. Flyktninger fra det krigsherjede Syria topper statistikken over ulovlige grensepasseringer til Europa, etterfulgt av personer fra Eritrea og Afghanistan. De fleste migrantene som kommer til Europa, benytter seg av menneskesmuglere på hele eller deler av reisen. Organisert menneskesmugling kan ha Norge som mål. Smuglerne er gode til å tilpasse seg, og de risikerer migrantenes sikkerhet for å øke profitten og minimere risikoen for å bli tatt. I en del tilfeller tvinges migrantene inn i kriminalitet eller det svarte arbeidsmarkedet når de ankommer Europa, for å kunne betale tilbake gjelden til smuglerne, men det er likevel lite sannsynlig at organisert menneskehandel er formålet med menneskesmuglingen.

I prostitusjonsmiljøene i de store byene er det i stor grad ulike etniske grupperinger som utmerker seg. På innemarkedene i flere av de store byene er rumenske og etnisk albanske nettverk aktive, mens utemarkedene det siste året fortsatt har vært dominert av nigerianske og rumenske aktører. I flere av de store byene er kriminelle nettverk som organiserer prostitusjon også aktive innen andre former for kriminalitet, blant annet narkotikaomsetning og helerivirksomhet. Ved å få sine ofre til å utføre kriminalitet, reduserer kriminelle bakmenn sin egen eksponering og risiko for å bli avslørt.

4.7 Spredning av masseødeleggelsesvåpen

Masseødeleggelsesvåpen er fellesbetegnelsen på våpen som har kjernefysiske, biologiske eller kjemiske stridsmidler som last, kombinert med et effektivt leveringsmiddel, og kjennetegnes ved stort skadeomfang, massedød og store materielle skader. Masseødeleggelsesvåpen utgjør derfor en av de største potensielle truslene mot internasjonal stabilitet og sikkerhet. Norge har ikke masseødeleggelsesvåpen, og vi har heller ikke noen umiddelbar trussel fra slike våpen mot oss. Vi har imidlertid meget avansert teknologi som kan inngå som viktige deler i utviklingen av masseødeleggelsesvåpen. I den samordnede vurderingen fra E-tjenesten, NSM og PST for 2013 side 10 nevnes spredning av masseødeleggelsesvåpen som en trussel:

> «Spredning av materiale, teknologi og utstyr til bruk i produksjon av [masseødeleggelsesvåpen] blir stadig mer krevende å avdekke og kontrollere for nasjonale og internasjonale eksportkontrolletater. For å omgå eksportkontrollregelverket benyttes ulike metoder, og det eksisterer en rekke fordekte anskaffelsesnettverk.
>
> Det finnes et betydelig antall virksomheter i Norge som har kunnskap og teknologi som kan brukes i utviklingen av [masseødeleggelsesvåpen]. De fremste målene i Norge omfatter små og store virksomheter innenfor sivile høyteknologmiljøer, forsvarsindustrien, samt et bredt spekter av forsknings- og utviklingsmiljøer. Svakheter i klareringsrutiner for studenter og forskere fra land av bekymring gjør det vanskeligere å kontrollere kunnskapsoverføring relatert til fagområder som har flerbruksverdi.»

Dette behandles også i oppsummeringen i PSTs *Åpen trusselvurdering 2013*:

> «De fleste forsøk på å skaffe teknologi fra norske virksomheter, som er relevant for utvikling av masseødeleggelsesvåpen, kan knyttes til iranske aktører. Mål i Norge for denne aktiviteten finnes blant både små og store virksomheter innenfor sivile høyteknologimiljøer, forsvarsindustrien, samt et bredt spekter av forsknings- og utviklingsmiljøer.»

I PSTs trusselvurdering fra 2014 bekreftes det at iranske aktører fortsatt står bak de fleste forsøk i Norge på å skaffe varer og teknologi som kan anvendes til fremstilling av masseødeleggelsesvåpen. Dette ses i sammenheng med de internasjonale sanksjonene, som har medført omfattende restriksjoner på handel med Iran.

I *Åpen trusselvurdering 2015* fremgår det at Iran forventes å fortsette som hovedaktør bak ulovlige og fordekte anskaffelsesforsøk til støtte

for sin produksjon av masseødeleggelsesvåpen. Forhandlingene mellom det internasjonale samfunnet og Iran har ikke ført til nedgang i antall skjulte anskaffelsesforsøk mot norske virksomheter. I tillegg forventes ulovlig kunnskapsoverføring å fortsette.

Det fremgår av *Åpen trusselvurdering 2016* side 9 at atomavtalen inngått i 2015 mellom Iran og de fem sikkerhetsrådsmaktene USA, Russland, Kina, Storbritannia og Frankrike, samt Tyskland, har til hensikt å sikre at Irans kjernefysiske aktiviteter er av sivil karakter. Imidlertid er eksport av varer, teknologi, tjenester og kunnskap som er relevant for masseødeleggelsesvåpen og leveringsmidler for slike, fortsatt regulert av eksportkontrollregelverket. Flere land i Asia og Midtøsten forsøker å gjennomføre fordekte anskaffelser i Europa. Hensikten er å anskaffe varer til egne nasjonale programmer for masseødeleggelsesvåpen eller avanserte våpenprogrammer. Private aktører og utdanningsinstitusjoner bidrar også til fordekte anskaffelser. Ofte er disse en del av et større internasjonalt anskaffelsesnettverk som samarbeider for å omgå norsk og europeisk eksportkontrollregelverk. PST påpeker at ulovlige leveranser fra Norge til bekymringsland, kan få store negative konsekvenser, og både norske bedrifter og norske myndigheters omdømme kan bli skadelidende.

4.8 Overgrepsbilder av barn

I Kripos' *Trendrapport 2015 Organisert og annen kriminalitet i Norge* gis det uttrykk for at det er påvist en sammenheng mellom fildeling av overgrepsbilder og fysiske seksuelle overgrep mot barn. Internett og teknologi har forenklet distribusjon, produksjon og deling av ulovlige overgrepsbilder, og det er rapportert om mange hendelser. Overgripere driver utstrakt fildeling seg imellom i såkalte P2P-nettverk, som fungerer som organiserte distribusjonssentre. I 2012 hentet Kripos ut tall på hvor mange nordmenn som delte straffbare overgrepsbilder i ett fildelingsnettverk (OP Share). Her fant man langt flere brukere som delte ulovlige bilder enn forventet. I etterkant har Kripos i 2013–14 opprettet 99 saker om ulovlig bildedeling, fordelt på alle politidistriktene. En sammenligning av antallet brukere av dette fildelingsnettverket før og etter aksjonen viser en markant nedgang – fra 2 331 brukere på 120 dager, til 1 291 brukere i en tilsvarende periode ett år senere. Det meste er gratis materiale som deles i ikke-kommersielle kanaler, hvor grovheten og nytt materiale er inngangsporten til å få tilsendt bilder eller delta i ulike fora. Nedgangen tyder på at slike aksjoner har en forebyggende effekt på kort sikt. Det er vanskelig å si hvor lenge en slik aksjon mot ett av mange nettverk vil virke allmennpreventivt, men Kripos finner det svært sannsynlig at deling av seksuelle overgrepsbilder av barn er et fenomen som vil øke i omfang.

Norsk politi har også vært involvert i en omfattende kanadisk sak, der en kanadier sto bak produksjon og salg av seksuelle overgrepsbilder og -videoer av barn. I Norge er det opprettet 36 saker i kjølvannet av denne etterforskningen. Begge de nevnte sakene har ført til en markant økning av saker i 2013–2014 der nordmenn er i besittelse av seksuelle overgrepsbilder via datasystemer. Det er grunn til å forvente at overgripere utvider sine grenser og deltar i grovere misbruk ved at de finner både likesinnede og ny informasjon samlet på anonyme arenaer på nett.

I Kripos' *Trendrapport 2016 Organisert og annen kriminalitet i Norge* uttales det at Internett har blitt et svært viktig verktøy for seksualforbrytere. De søker kontakt med potensielle ofre på Internett, etablerer anonyme nettverk med andre med samme preferanser og bruker Internett til å organisere overgrep, både i hjemlandet og i utlandet. Bestilling og strømming av seksuelle overgrep på Internett utgjør en stadig økende trussel. Denne kriminaliteten utføres gjerne av kriminelle nettverk som kontrollerer tilgang til barn som enten er hjemløse eller som selges av sine foreldre. Personer i andre land kan så se direkteoverførte overgrep på nett mot betaling. Overgrepene kan være vanskelige å spore, da de normalt ikke lagres og foregår via kryptering som gjør sporing vanskelig. Strømming av seksuelle overgrep på Internett skjer også til Norge. Kripos mener det er meget sannsynlig at strømming av seksuelle overgrep over Internett skjer i et langt større omfang enn hva som er kjent i dag, og det er forventet å øke i fremtiden.

5 Konstitusjonelle og menneskerettslige skranker for politiets metodebruk

5.1 Grunnloven § 102

5.1.1 Bakgrunn

De fleste reglene om bruk av skjulte tvangsmidler krever at det er skjellig grunn til å tro at det begås eller er begått et lovbrudd av en viss alvorlighetsgrad. Ved lov 17. juni 2005 nr. 87 ble imidlertid politiet gitt adgang til å anvende skjulte tvangsmidler for å innhente informasjon med sikte på å *avverge* og *forebygge* alvorlig kriminalitet. Det ble her åpnet for at både politiet og PST kan bruke ransaking og andre tvangsmidler for å avverge alvorlige lovbrudd, jf. straffeprosessloven § 222 d. Bestemmelsen stiller ikke krav til mistanke om at en straffbar handling er utført. Det er nok at vilkåret for å iverksette etterforskning er oppfylt, dvs. at det er rimelig grunn til å undersøke om det foreligger straffbart forhold, se nærmere nedenfor punkt 13.4.1. I tillegg må det være «rimelig grunn til å tro at noen kommer til å begå» en alvorlig straffbar handling. Videre ble PST gitt anledning til å bruke hemmelig ransaking også for forebyggende formål, jf. politiloven § 17 d. Her er vilkåret at det er «grunn til å undersøke om noen forbereder» terrorhandlinger, visse lovbrudd mot rikets sikkerhet eller attentat mot myndighetspersoner. Ransaking for forebyggende formål kan likevel ikke skje i «private hjem», jf. politiloven § 17 d andre ledd i.f. Ved den samme lovrevisjonen i 2005 ble det dessuten for første gang åpnet for romavlytting. Denne metoden kan brukes både når det er mistanke om at noen har begått en alvorlig straffbar handling, jf. straffeprosessloven § 216 m, samt for å avverge eller forebygge visse alvorlige lovbrudd, jf. henholdsvis straffeprosessloven § 222 d og politiloven § 17 d.

Som et ledd i evalueringen av de innførte politimetodene vurderte Metodekontrollutvalget grunnlovsmessigheten av adgangen til hemmelig ransaking og romavlytting i forebyggende og avvergende øyemed, jf. politiloven § 17 d og straffeprosessloven § 222 d. Utvalget har også vurdert ulike former for dataavlesing opp mot Grunnloven § 102. Utvalgsmedlem professor dr. juris Erling Johannes Husabø ble bedt om å utrede grunnlovsspørsmålet nærmere. Utvalget besluttet i tillegg å anvende ekstern ekspertise ved vurderingen, og det ble innhentet en betenkning av professor dr. juris Alf Petter Høgberg og (daværende) universitetsstipendiat Marius Stub.

Begge de innhentede betenkningene konkluderte med at enkelte av dagens lovtillatte metoder er i strid med Grunnloven § 102, slik den da lød. Både Husabø og Høgberg/Stub mente at «Hus-Inkvisisjoner» i Grunnloven § 102 ikke bare omfattet ransaking, men også romavlytting og visse former for dataavlesing. Videre la både Husabø og Høgberg/Stub til grunn at unntaket for kriminelle tilfeller bare kom til anvendelse der det allerede er begått en straffbar handling, slik at ransaking mv. i private hjem i avvergende øyemed ikke kan iverksettes dersom det for eksempel ikke er mistanke om at det har skjedd noe mer enn straffri forberedelse. Begge betenkningene konkluderte på den bakgrunn også med at adgangen til romavlytting i privat bolig i forebyggende øyemed etter politiloven § 17 d er grunnlovsstridig. Dessuten anså man hjemmelen for hemmelig ransaking og romavlytting i avvergende øyemed etter straffeprosessloven § 222 d å stå i et tvilsomt forhold til Grunnloven § 102, for så vidt gjaldt inngrep i private hjem. Også innbrudd for å legge til rette for dataavlesing ble vurdert å kunne være problematisk i relasjon til Grunnloven § 102.

Metodekontrollutvalgets flertall sluttet seg til hovedtrekkene i de to innhentede betenkningene, og fant at det var gode grunner for å mene at det forelå grunnlovsstrid. På denne bakgrunn foreslo flertallet endringer i politiloven § 17 d og straffeprosessloven § 222 d for å sikre at Grunnlovens krav tilfredsstilles.

Utvalgets mindretall mente derimot at Grunnloven ikke var til hinder for ransaking og romavlytting i privat bolig i forebyggende øyemed, og foreslo derfor en utvidelse av politiloven § 17 d for så vidt gjaldt ransaking. Mindretallet var, i motsetning til flertallet, ikke enig med Husabø og

Høgberg/Stub i at unntaket for kriminelle tilfeller krever at det allerede er begått en kriminell handling. Mindretallet synes dessuten å legge til grunn at PSTs forebyggende virksomhet ikke er å anse som husransakelse ettersom hovedformålet er informasjonsinnhenting og ikke strafforfølgning, se metodekontrollutvalgets rapport punkt 13.4 på side 156–157.

5.1.2 Oversikt

Grunnloven § 102 etablerer et generelt grunnlovsvern for privatlivets fred og personlig integritet. Bestemmelsen ble endret i forbindelse med grunnlovsreformen i mai 2014 (res. 14. mai 2014 nr. 628), trådte i kraft 18. mai 2014 og lyder slik:

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

Før grunnlovsendringen ble Grunnloven § 102 som forbød «Hus-Inkvisisjoner» med unntak av i «kriminelle Tilfælde» ansett som et begrenset utslag av retten til vern om privatliv og ga ikke noe generelt vern for privatlivets fred. Et slikt generelt vern ble i norsk rett først og fremst ivaretatt av EMK artikkel 8 og SP artikkel 17 gjennom menneskerettsloven, personopplysningsloven og ulovfestede personvernprinsipper.

Første ledd første punktum gir et generelt vern for privatlivets fred. Det fremgår uttrykkelig at dette vernet omfatter respekt for privatliv, familieliv, hjem og kommunikasjon. Ordlyden i første ledd første punktum er tilnærmet identisk med EMK artikkel 8 som fastslår at «enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse». Det generelle vernet for privatlivets fred i § 102 første ledd første punktum er utformet som en individuell rettighet. Om begrunnelsen for dette heter det i Menneskerettighetsutvalgets rapport (Dokument 16 (2011–2012)) punkt 30.6.6.2 side 177:

> «En annen begrunnelse for særskilt å fremheve privatliv, familieliv, hjem og kommunikasjon er at retten til respekt for disse verdiene bør utformes som en individuell rettighet i Grunnloven. Inngrep i privatliv, familieliv, hjem og kommunikasjon vil normalt oppleves som så krenkende at det er viktig at slike inngrep vurderes nøye i lovgivningsprosessen, og at de kan prøves for domstolene dersom lovgiver har gått for langt i å tillate slike inngrep. I en viss forstand kan man si at dette utgjør kjernen i den private sfære, der den enkelte har krav på et særlig vern mot krenkelser.»

I første ledd annet punktum fastslås det at «husransakelse» ikke må finne sted «unntatt i kriminelle tilfeller». Med dette videreføres forbudet mot husinkvisisjoner i den tidligere § 102, men med en annen og mer moderne språkdrakt. Menneskerettighetsutvalget foreslo å ta bestemmelsen ut, og anse det dekket av de mer generelle deler av ny § 102. Setningen ble likevel foreslått videreført i en av fire alternative formuleringer i Grunnlovsforslag Dokument 12:30 (2011–2012) side 179-180, uten nærmere begrunnelse, og innstilt på uten videre diskusjon. I grunnlovsforslaget ble for øvrig uttrykket husinkvisisjon i den tidligere bestemmelsen erstattet med «husundersøkelse». Dette uttrykket ble igjen endret til «husransakelse» i den vedtatte bestemmelsen.

I annet ledd fastslås det at statens myndigheter skal sikre den enkeltes personlige integritet. Integritetsvernet er utformet som en positiv forpliktelse for statens myndigheter. Ifølge Kontroll- og konstitusjonskomiteen er annet ledd utformet «mer som en politisk retningslinje, som imidlertid også innebærer en ytterste skranke for lovgiver», se Innst. 186 S (2013–2014) side 27. Komiteen viser til at samme presisering som her er foreslått, er gjennomført i samtlige menneskerettighetskonvensjoner og i EUs Charter of Fundamental Rights. Det kan i den sammenheng bemerkes at EMK artikkel 8 gir staten en positiv forpliktelse til å iverksette tiltak for å forhindre at andre griper inn i den enkeltes privatliv, selv om dette ikke fremgår like klart av ordlyden som i Grunnloven § 102 annet ledd, se også Menneskerettighetsutvalgets rapport punkt 30.4 side 170. Det er likevel usikkert hvor langt denne forpliktelsen rekker.

Menneskerettighetsutvalget legger tilsvarende til grunn at § 102 annet ledd innebærer at «myndighetene har en generell plikt til å sørge for lovgivning som sikrer den enkeltes kroppslige og mentale integritet, gjennom for eksempel lovgivning mot vold, mishandling og drap», se Menneskerettighetsutvalgets rapport (Dokument 16 (2011–2012)) punkt 30.6.6.2 side 177. Det fremgår her at vernet om den personlige integritet er ment å skulle beskytte den kroppslige så vel som den psykiske integritet. Dette innebærer at Grunnloven § 102 går lengre i å gi vern for den enkeltes

personlige integritet enn det personvernlovgivningen tradisjonelt har gjort. Det er vanlig å avgrense personvernet til de regler som har som formål å beskytte den psykiske integritet. Et hovedelement i personvernet er at personer i utgangspunktet skal kunne bestemme hva andre skal få vite om hans eller hennes egne personlige forhold. Regler som skal verne individet mot fysisk ubehag eller skade faller således utenfor det tradisjonelle personvernbegrepet. Den nye bestemmelsen supplerer i så måte Grunnloven § 93 fjerde ledd, som pålegger statens myndigheter å beskytte retten til liv, jf. nedenfor.

5.1.3 Adgangen til å foreta begrensninger i vernet

5.1.3.1 Begrensninger i vernet etter § 102 første ledd første punktum

De ulike politimetoder som ransaking, romavlytting, kommunikasjonskontroll, dataavlesing, visitasjon og spaning, vil på forskjellige måter kunne gripe inn i de vernede interesser etter Grunnloven § 102. Det reiser spørsmål om i hvilken grad det er adgang til å gjøre inngrep i dette vernet.

Grunnloven § 102 gir etter sin ordlyd uttrykk for et omfattende vern. Vernet etter første ledd første punktum er likevel ikke absolutt. Det er forutsatt i forarbeidene til grunnlovsforslaget at bestemmelsen ikke kan forstås slik at den enkelte har en udelt rett til å ha sitt privatliv i fred, se Menneskerettighetsutvalgets rapport (Dokument 16 (2011–2012)) side 178:

> «Forslag til første ledd vil da være utformet som en rettighet for den enkelte gjennom uttrykket «enhver». Den enkelte tildeles likevel ikke en udelt rett til å ha sitt privatliv i fred, men har rett til «respekt» for sitt privatliv.»

Grunnloven § 102 gir imidlertid ingen retningslinjer for når det er tillatt å gjøre inngrep i den vernedes sfære for eksempel gjennom bruk av ulike politimetoder. Bestemmelsen hviler på en forutsetning om at det vedtas en generell regel om begrensninger i rettighetene etter Grunnloven og at denne angir hvilke vilkår som må være oppfylt for at det skal kunne gjøres inngrep i den vernedes sfære etter § 102, se Menneskerettighetsutvalgets rapport side 178:

> «Formuleringen utelukker derfor ikke at enkelte personer kan utsettes for overvåking og kontroll, men da må vilkårene for dette være til stede, jf. utvalgets forslag til begrensningshjemmel for rettighetene i Grunnloven, se kapittel 13.»

En slik forutsetning fremgår også av flertallets merknader i Kontroll- og konstitusjonskomiteens innstilling (representantene fra Ap, Høyre og FrP), se Innst. 186 S (2013–2014) punkt 2.1.9:

> «Det alternativ flertallet stiller seg bak, gjør retten til privatliv mv. i første ledd til en rettighet for den enkelte. Når retten er til «respekt for» privatlivet, er det likevel for å synliggjøre at lovlig etterretning ikke er utelukket, som også diskutert av Menneskerettighetsutvalget.»

Høyesterett har i nyere avgjørelser slått fast at vernet etter § 102 første ledd første punktum vil bero på en vurdering av om inngrepet i de vernede interesser ivaretar et legitimt formål, er forholdsmessig og har tilstrekkelig hjemmel, se Rt. 2014 side 1105 (avsnitt 28) og Rt. 2015 side 93. I sistnevnte avgjørelse (avsnitt 60) uttales følgende om tolkningen av Grunnloven § 102:

> «Til forskjell fra SP artikkel 17 og EMK artikkel 8, inneholder Grunnloven § 102 ingen anvisning på om det overhodet kan gjøres lovlige begrensninger i privat- og familielivet. Men grunnlovsvernet kan ikke være – og er heller ikke – absolutt. I tråd med de folkerettslige bestemmelsene som var mønster for denne delen av § 102, vil det være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom tiltaket har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, jf. Rt-2014-1105 avsnitt 28.»

Det er således på det rene at vernet etter første ledd første punktum ikke er absolutt.

5.1.3.2 Begrensninger i vernet etter § 102 første ledd annet punktum

Første ledd annet punktum gir derimot trolig et absolutt vern mot inngrep som er å anse som «husransakelse», med unntak av når dette gjøres «i kriminelle tilfeller». Første og annet punktum inneholder således bestemmelser av forskjellig karakter: Første punktum gir anvisning på en avveining, mens annet punktum inneholder et forbud. Ved vurderingen av om bruk av de ulike skjulte politimetodene i forebyggende eller avvergende øyemed er forenlig med Grunnloven § 102, blir det dermed både spørsmål om de går

klar av forbudet i annet punktum, og om de kan forsvares etter avveiningen i første punktum.

Det er ikke tvil om at politimetoder som kommunikasjonskontroll, visitasjon og spaning ikke er å anse som «husransakelse», og slike metoder går dermed klar av forbudet mot husransakelse i annet punktum. Det er heller ikke tvilsomt at ransaking i private hjem er å anse som «husransakelse». Når det gjelder romavlytting og innbrudd ved dataavlesing eller romavlytting, er det noe mer usikkert om tvangsmidlene omfattes av begrepet «husransakelse». Både Metodekontrollutvalgets flertall og de to betenkningene som er vedlagt Metodekontrollutvalgets utredning la til grunn at forbudet mot «Hus-Inkvisisjoner», slik ordlyden da lød, omfattet romavlytting og innbrudd.

Flere forhold trekker i retning av å anse slike metoder for å falle utenfor. For det første er en slik tolkning forenlig med ordlyden i annet punktum, som nå altså er endret fra «husinkvisisjon» til det snevrere uttrykket «husransakelse». For det annet er det mindre behov for en vid tolking av «husransakelse» etter grunnlovsreformen i 2014, idet et mer generelt formulert grunnlovsvern nå følger av § 102 første ledd første punktum.

På den annen side tilsier Stortingets generelle intensjon – at det med språkrevisjonen ikke var meningen å forskyve meningsinnholdet i grunnlovsbestemmelsene – at en ved tolkningen av den enkelte bestemmelse bør være varsom med å legge vekt på at ordlyden i bestemmelsen er snevrere enn den var før reformen. Denne innvendingen har noe begrenset betydning ettersom også den tidligere rettstilstanden og rekkevidden av begrepet husinkvisisjon var uklar. Like fullt kan det hevdes at formålet med det opprinnelige forbudet mot husinkvisisjon var å verne om den private sfære, som både ransaking, romavlytting og innbrudd gjør inngrep i.

Departementet finner det imidlertid ikke nødvendig å ta endelig stilling til hvilke metoder som kan anses som «husransakelse» etter første ledd annet punktum, ettersom rekkevidden av begrepet «husransakelse» uansett ikke har vært avgjørende for de forslag som fremmes i proposisjonen her. Forslagene anses å være forenlig med Grunnloven § 102, også om en tar utgangspunkt i at de nevnte metodene, romavlytting og innbrudd ved dataavlesing eller romavlytting, omfattes av begrepet «husransakelse» i første ledd annet punktum.

Forbudet mot husransakelse er som nevnt ikke uten unntak. Selv om en politimetode omfattes av begrepet husransakelse, vil den ikke rammes av forbudet dersom den benyttes «i kriminelle tilfeller». Uttrykket «i kriminelle tilfeller» omfatter utvilsomt de tilfeller hvor de aktuelle politimetodene benyttes som ledd i undersøkelser knyttet til straffbare handlinger som allerede har funnet sted. Politiets undersøkelser er imidlertid ikke begrenset utelukkende til å oppklare allerede begåtte lovbrudd. Politiet har også som oppgave å avverge og forebygge fremtidig kriminalitet. For å styrke politiets avvergende og forebyggende funksjon, ble Politiets og PSTs adgang til å ta i bruk hemmelige tvangsmidler utvidet ved lov 17. juni 2005 nr. 87. Det ble her åpnet for at både politiet og PST kan bruke ransaking og andre tvangsmidler for å avverge alvorlige lovbrudd, jf. straffeprosessloven § 222 d. Videre ble PST gitt anledning til å bruke hemmelig ransaking også for forebyggende formål, jf. politiloven § 17 d. Bestemmelsene er nærmere omtalt nedenfor i kapittel 13. Politiets og PSTs adgang til å bruke hemmelige etterforskningsmetoder i avvergings- og forebyggingssituasjonene, aktualiserer spørsmålet om rekkevidden av unntaket fra forbudet mot husransakelse i Grunnloven § 102 første ledd annet punktum.

Både Metodekontrollutvalgets flertall og de to betenkningene som er vedlagt utredningen, konkluderte med at det av begrepet «i kriminelle tilfeller» kunne utledes et krav om at det allerede må være foretatt en straffbar handling, og det avgrenses således mot tvangsmiddelbruk i avvergende og forebyggende øyemed. Denne fortolkningen har imidlertid nokså usikker forankring i de tungtveiende rettskildene.

For det første kan det stilles spørsmål om det er mest nærliggende å tolke ordlyden så restriktivt som flertallet har gjort. Departementet mener at ordlyden åpner for flere fortolkninger og at den ikke er til hinder for at det foretas undersøkelser med sikte på å forebygge eller avverge kriminalitet. Preposisjonsbruken (i kriminelle tilfeller) kan også forstås som en tematisk henvisning til kriminalitetsbekjempelse, uten at det innebærer et særskilt krav om at grensen for det straffbare må være overtrådt.

Heller ikke bakgrunnen for det opprinnelige forbudet i § 102 mot husinkvisisjoner, gir støtte for det syn som flertallet målbærer. Referatet fra Riksforsamlingen gir en viss støtte for at bakgrunnen for at dette uttrykket ble valgt, var et ønske om å begrense undersøkelser som kunne føre til krenkende mistanke og strafforfølgning for mindre alvorlige lovbrudd, og at Eidsvollsfedrene ved valg av formulering ikke hadde noen intensjon om å begrense myndighetenes adgang til å foreta undersøkelser av private hjem for å forhindre alvorlig kriminalitet. I referatet står det at forslaget fra justis-

råd Diriks til endelig lovtekst ble «bifaldt især af Kjøbmændenene, der saaledes saae sig befriede fra Inkvisitioner om Toldsvig, hvilken Diriks ikkje ansaa for nogen offentlig Forbrydelse», jf. Storthings-efterretninger 1814-1833 1ste bind, Jacob Dybwads forlag, Christiania 1874 s. 76. Dette må igjen forstås på bakgrunn av at brudd på tollovgivningen på den tiden ble håndtert i sivilprosessuelle former. Kjernen i tidligere § 102 synes således å være å sette en terskel med hensyn til sakens alvor og å hindre vilkårlige krenkelser som kunne føre til mistanke og strafforfølgning for mindre alvorlige forhold, jf. Metodekontrollutvalgets mindretall i utredningen punkt 13.4 side 156. Den juridiske teori har også holdt fast på at husundersøkelser av mer forvaltningsmessig karakter faller utenfor, jf. Andenæs, Statsforfatningen i Norge (10. utg. ved Fliflet, 2006) s. 408–409.

Heller ikke lovforarbeidene utarbeidet i forbindelse med grunnlovsreformen 2014 gir støtte til den fortolkning som Metodekontrollutvalgets flertall bygger på. Spørsmålet om hvordan unntaket for kriminelle tilfeller skal forstås, er ikke kommentert i Kontroll- og konstitusjonskomiteens innstilling. Saksordføreren knyttet imidlertid enkelte kommentarer til dette i Stortinget, jf. referat fra Stortingsdebatten 14. mai 2014 sak 1 (Jette F. Christensen (A) [17:36:12]). Disse kan tolkes i retning av at begrepet «i kriminelle tilfeller» ikke må avgrenses mot politiets arbeid for å forebygge og avverge kriminalitet. Uttalelsen er likevel noe tvetydig og vil neppe tillegges særlig rettskildemessig verdi.

Departementet mener at en bør være tilbakeholden med å innfortolke begrensninger i Grunnloven som grunnlovskonsipistene neppe hadde gjort seg opp noen formening om ved valg av formulering, og som heller ikke følger klart av ordlyden.

Det kan videre anføres at både utvalgets flertall og de to betenkningene i for sterk grad har lagt vekt på hensynet til å verne om den enkeltes hjem og privatliv på bekostning av hensynet til å hindre at alvorlig kriminalitet blir begått. Departementet mener, slik også utvalgets mindretall er inne på, at denne avveiningen må foretas i lys av dagens syn på forholdet mellom enkeltmenneskets behov for vern og fellesskapets behov for beskyttelse. Metodekontrollutvalgets vurdering av hensynet til privatlivets fred opp mot hensynet til kriminalitetsbekjempelse og samfunnsvern, kan i ytterste konsekvens føre til at politiet mister noen av de virkemidler som er nødvendig for å avverge alvorlig kriminalitet, med den konsekvens at liv kan gå tapt.

Som nevnt ovenfor gir Grunnloven §§ 93 og § 102 annet ledd statens myndigheter en plikt til å beskytte retten til liv og til å verne om ulike sider ved den enkeltes fysiske og psykiske integritet. Formålet med å grunnlovfeste retten til liv er blant annet å gi denne rettigheten et høyere vern. Fra komiteens merknader i Innst. 182 S (2013–2014) hitsettes:

> «Komiteen viser til at retten til liv ofte blir fremhevet som den mest grunnleggende av menneskerettighetene. I FN finner vi retten til liv i konvensjonen om sivile og politiske rettigheter artikkel 6: «Every human being has the inherent right to life» og nesten likelydende i Den europeiske menneskerettighetskonvensjon (EMK) artikkel 2 (inkorporert i norsk lov gjennom menneskerettsloven): «Everyone's right to life shall be protected by law». […].
>
> Komiteen viser til Menneskerettighetsutvalgets rapport der retten til liv omtales som «en plikt for myndighetene til å respektere den enkeltes rett til liv, dvs. at myndighetene ikke kan ta liv (..), og til å beskytte den enkelte mot at andre tar deres liv».
>
> Komiteen viser til at Grunnloven i dag verken gir en eksplisitt rett til liv eller forbud mot dødsstraff. Tortur er forbudt, men kun som et ledd i straffeprosessen.
>
> Komiteen mener dette er grunnleggende rettigheter som bør få et høyere rettslig vern. Komiteen støtter forslag om at livet er en grunnleggende verdi som må vernes om og beskyttes.»

Samtidig er det, slik det fremgår at komiteens merknader til § 102 i Innst. 186 S (2013–2014) punkt 2, ikke grunnlag for å foreta en innbyrdes rangering av de rettighetene som nå er inntatt i Grunnloven: «[…] disse rettighetenes finnes på samme nivå som andre rettigheter de må avveies mot, slik som ytringsfriheten og religionsfriheten.»

Det er ikke tvilsomt at formålet med bestemmelsen i § 102 er å verne mot vilkårlige og uforholdsmessige inngrep i borgernes hjem. En reell vurdering av om et inngrep er vilkårlig og uforholdsmessig, bør ikke utelukkende baseres på om det allerede er begått en straffbar handling eller hvor nærstående den handling som søkes avverget er. Det er ikke nødvendigvis slik at behovet for tvangsmidler er sterkest i tilfeller der en kriminell handling allerede er begått. Det kan være større grunn til å gripe inn i en situasjon der en har sikre holdepunkter for at et svært alvorlig lovbrudd vil

kunne bli begått, uten at en har indikasjoner på at noe straffbart allerede har funnet sted. I det siste tilfellet har en ennå tid og mulighet til å avverge utfallet av lovbruddet og kanskje redde mange menneskeliv. Der det er begått et lovbrudd, er det kun hensynet til sakens oppklaring som kan legitimere husransakelse. En reell vurdering av et inngreps nødvendighet og forholdsmessighet vil derfor også måtte ta i betraktning alvorligheten av den handling som søkes avverget, hvilke konsekvenser det får dersom en ikke griper inn og hvor sikre holdepunkter en har for at en alvorlig straffbar handling vil bli begått.

Det kan også anføres at enkelte av argumentene som ble angitt til støtte for at begrepet «i kriminelle tilfelle» skal tolkes snevert, altså som forbeholdt tilfelle der det er begått et lovbrudd i motsetning til der disse vil kunne begås i fremtiden, ikke kan tillegges særlig vekt ved tolkningen av den nye grunnlovsbestemmelsen. I en av benkningene som er vedlagt Metodekontrollutvalgets utredning (se Husabø side 417), er det blant annet anført at dersom en aksepterer at myndighetenes uro for at noen kan komme til å gjøre noe straffbart, skal kunne utgjøre «kriminelle Tilfælde», vil det være svært vanskelig ut fra Grunnloven å trekke en grense for hvor langt dette unntaket går. Argumentet vil ikke lenger ha gyldighet når bestemmelsen i dag, slik den er fortolket av Høyesterett, i tillegg oppstiller en generell regel om beskyttelse av privatlivets fred, hvoretter inngrep må vareta et legitimt formål, være forholdsmessig og ha tilstrekkelig hjemmel. Også adgangen til husransakelse i «kriminelle tilfeller» vil være undergitt disse kravene som Høyesterett har innfortolket i første ledd første punktum. Kravene om at eventuelle inngrep i de vernede interesser må vareta legitime formål, ha tilstrekkelig hjemmel og være forholdsmessige er godt egnet til å fange opp de svært vanskelige vurderingene som lovgiver, og i siste instans domstolene, må foreta når det skal skje en avveining mellom individets behov for beskyttelse mot inntrengning i privatsfæren på den ene siden og de legitime samfunnsbehovene som begrunner inngrepet på den andre siden. Ved en forholdsmessighetsvurdering er det mulig å ta hensyn både til hvor omfattende inngrepet i privatsfæren er, hvor stor fare det er for at uskyldige tredjepersoner rammes, hvor alvorlige lovbrudd det er tale om, hvor sterke holdepunkter som foreligger for at lovbruddet vil kunne begås og hvilke rettssikkerhetsgarantier som er bygd inn. Departementet vil videre peke på at i mangel av klare holdepunkter i ordlyden og andre relevante rettskilder, bør lovgivers syn veie tungt med hensyn til hvordan disse hensyn best skal avstemmes i forbindelse med utforming av konkrete lovbestemmelser.

Etter departementets syn kan det av begrepet «kriminelle tilfeller» ikke utledes et krav om at et lovbrudd må være begått. Det understrekes likevel at adgangen til å foreta inngrep i hjemmet for å forhindre fremtidig kriminalitet ikke er ubegrenset. Det kan på bakgrunn av ordlyden og de hensyn som ligger til grunn for forbudet mot husransakelse, være grunn til å oppstille et generelt krav om at det må foreligge konkret informasjon som tilsier at det vil bli begått en kriminell handling i ikke alt for fjern fremtid. Prinsipielt sett bør det ikke være avgjørende for grunnlovsmessigheten om en i lovgivningen omtaler politiets tiltak som er rettet mot fremtidige straffbare handlinger som avverging eller forebygging. Likevel antas det at det bør utvises noe mer forsiktighet med å åpne for tvangsmiddelbruk i private hjem i forebyggende øyemed etter politiloven § 17 d enn tvangsmiddelbruk i avvergende øyemed etter straffeprosessloven § 222 d. Avstanden til den straffbare handlingen vil gjerne være større enn ved avverging, der det er grunnlag for å åpne etterforskning, og der det dessuten ofte foreligger et annet lovbrudd, for eksempel forberedelseslovbrudd til handlingen som søkes avverget. Det kan imidlertid bemerkes at grensen for når en forebyggingssak bør gå over i avvergingssporet ikke alltid er like enkel å trekke. PST kan motta troverdige, men ikke-verifiserte opplysninger, som gir grunn til å avvente den videre utvikling før eventuell etterforskning iverksettes. Det kan altså likevel foreligge en rekke holdepunkter for at alvorlige lovbrudd er i gjære fra enkelte miljøer. Her synes det mindre betenkelig å subsumere forholdet under «kriminelle tilfeller». Det vises til vurderingene i kapittel 13 nedenfor.

Departementet legger til grunn at vurderingstemaet og de krav som Høyesterett har oppstilt, om at inngrep i de vernede interessene må vareta et legitimt formål, være forholdsmessig og ha hjemmel i lov, også får anvendelse for tiltak som er å anse som husransakelse, *dersom disse benyttes «i kriminelle tilfeller»* og altså ikke rammes av den trolig absolutte forbudsregelen i annet punktum.

Vurderingen av om en bestemt metodebruk er forholdsmessig etter § 102 antas å være nokså sammenfallende med vurderingen etter EMK artikkel 8 nr. 2. Den innebærer at lovgiver, og i siste instans domstolene, må foreta en avveining mellom individets behov for beskyttelse mot inntrengning i privatsfæren på den ene siden og de

legitime samfunnsbehovene som begrunner inngrepet på den andre siden, nærmere bestemt kriminalitetsbekjempelse og samfunnsvern. I Høyesteretts dom inntatt i Rt. 2015 side 93 uttales følgende om denne vurderingen i avsnitt 60:

> «Forholdsmessighetsvurderingen må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre.»

For lovgiver innebærer dette at en ved vurderingen av hvilke metoder som lovgivningen skal gi hjemmel for og hvilke rammer som skal settes for politiets bruk av disse metodene, må foreta en avveining mellom de individuelle interessene og samfunnets behov for å beskyttes mot og oppklare alvorlige lovbrudd. I tillegg må en eventuell lovgivning være tilstrekkelig forutsigbar. Det er også av betydning hvilke rettssikkerhetsgarantier som foreligger, særlig i form av domstolskontroll. Det kan legges til at en i alle fall etter EMK har lagt stor vekt på hvorvidt lovgiver har konkretisert de samfunnsbehovene som begrunner avveiningen, samt foretatt den nærmere avveiningen.

5.2 EMK artikkel 8 som skranke for politiets metodebruk

5.2.1 Vernet etter EMK artikkel 8 nr. 1

Den europeiske menneskerettskonvensjon artikkel 8 nr. 1 gir, i likhet med Grunnloven § 102, et generelt vern av privatlivets fred. Det fremgår uttrykkelig av bestemmelsen at vernet omfatter den enkeltes privatliv, familieliv, hjem og korrespondanse. EMD har i liten grad skilt de ulike rettighetene fra hverandre. Langt på vei vil også retten til privatliv og retten til korrespondanse gli over i hverandre. Tilsvarende vil vernet om privatlivet og om det private hjem i mange tilfeller være vanskelig å holde helt atskilt.

Politiets etterforskningsmetoder vil på forskjellig måte kunne gripe inn i de sider av privatlivets sfære som er vernet etter EMK artikkel 8. Spaning, infiltrasjon, kommunikasjonskontroll og romavlytting vil kunne utgjøre inngrep i den enkeltes psykiske integritet. Det vil særlig være tilfelle når slike metoder benyttes skjult. Andre metoder som for eksempel ransaking og visitasjon, vil også gripe inn i den fysiske integritet.

Vernet etter artikkel 8 nr. 1 er sterkest når politimetoden retter seg mot det private hjem. Romavlytting og telefonavlytting faller normalt inn under EMK artikkel 8 nr. 1, se dommen *Klass m.fl. mot Tyskland* 6. september 1978 (sak 5029/71) og dommen *Khan mot Storbritannia* 12. mai 2000 (sak 35394/97). Det følger imidlertid av dommen *Niemietz mot Tyskland* (sak 13710/88) at vernet også gjelder utenfor det private hjem, se nærmere nedenfor under kapittel 12 om kameraovervåkning.

Metoder som griper inn i den *fysiske integritet* vil ofte være et inngrep etter EMK artikkel 8 nr. 1, se nedenfor punkt 10.4 om ransaking.

5.2.2 Vilkårene for å gripe inn i den vernede sfære

5.2.2.1 Innledning

Retten til respekt for privatlivets fred etter EMK artikkel 8 nr. 1 innebærer ingen udelt rett for den enkelte til å ha sitt privatliv i fred. Artikkel 8 nr. 2 angir hvilke betingelser som må være oppfylt for at offentlige myndigheter skal kunne gjør inngrep i de rettigheter som følger av artikkel 8 nr. 1. For det første må formålet med inngrepet falle inn under et av de formål som er angitt i bestemmelsen. Videre stilles det krav om at inngrepet har hjemmel i lov (lovkravet). Endelig må inngrepet anses nødvendig i et demokratisk samfunn.

5.2.2.2 Lovkravet

EMD har, i lys av prinsippet «the rule of law» knesatt i fortalen og hensynet til å beskytte borgerne mot vilkårlige inngrep fra statens side, stilt kvalitative krav til hjemmelsgrunnlaget. Lovkravet omfatter i hovedsak to ulike aspekter. Dels stilles det krav til regelens tilgjengelighet («accessibility») og dels et krav til presisjon («foreseeability»), se Lorenzen m.fl. Den Europeiske Menneskerettighedskonvention, Art. 1-9 (2011) side 764. Begge disse sidene av lovkravet fremgår blant annet av dommen *Sunday Times mot Storbritannia* 26. april 1979 (sak 6538/74) avsnitt 49:

> «Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a

> given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice.»

Sunday Times-saken gjaldt lovkravet i EMK artikkel 10, men lovkravet i EMK artikkel 8 nr. 1 er gitt samme betydning, se dommen *Silver m.fl. mot Storbritannia* 25. mars 1983 (sak 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 og 7136/75).

Kravet om tilgjengelighet skal sikre at borgeren kan finne ut om han er i en posisjon som kan gi grunnlag for inngrep mot ham. Av dette følger at den regel som hjemler inngrepet, må være offentliggjort. Det må således ses bort fra interne instrukser som er hemmeligholdt, for eksempel for å holde politiets fremgangsmåte skjult. I dommen *Malone mot Storbritannia* 2. august 1984 (sak 8691/79) kunne domstolen således ikke legge vekt på interne retningslinjer for bruken av romavlytting, ettersom disse ikke var tilgjengelig for klageren. Tilsvarende følger av dommen *Leander mot Sverige* 26. mars 1987 (sak 9248/81) avsnitt 51 som gjaldt overvåking.

Derimot vil det i noen grad være adgang til å innskrenke hjemmelens rammer i interne hemmelige rundskriv. Så lenge lovgivningen er tilstrekkelig klart formulert, slik at borgeren kan finne ut om han er i en posisjon som kan gi grunnlag for inngrep i privatlivet, vil vilkåret være oppfylt, se *Malone mot Storbritannia* 2. august 1984 (sak 8691/79) avsnitt 67:

> «In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.»

Et annet moment som tillegges vekt ved vurderingen av om lovkravet er oppfylt, er hvorvidt hjemmelsgrunnlaget fremstår som fragmentarisk. Dette har en side både til kravet om forutsigbarhet og kravet om tilgjengelighet. Dersom rettsregelen må utledes på bakgrunn av mange forskjellig rettskilder, vil dette svekke både forutberegneligheten og tilgjengeligheten. I dommen *Kruslin mot Frankrike* 24. april 1990 (sak 11801/85) avsnitt 34 måtte hjemmelen utledes av en rekke ulike kilder, og EMD kom blant annet av den grunn til at det forelå konvensjonsstrid. EMD la i den sammenheng også vekt på at telefonavlytting var et inngripende tiltak, og at hjemmelen som ble utledet i liten grad oppstilte prosessuelle garantier for den inngrepet var rettet mot. Likevel viser avgjørelsen at hjemmelsgrunnlaget inngrepet utledes fra, må være praktisk tilgjengelig.

Kravet til forutsigbarhet innebærer at hjemmelen må være noenlunde presist formulert for å sikre mot misbruk, se blant annet dommen *Huvig mot Frankrike* 24. april 1990 (sak 11105/84), som gjaldt telefonavlytting. I denne avgjørelsen ble det konstatert konvensjonsbrudd som følge av at hjemmelen var uklar. EMD la blant annet vekt på at det ikke var presisert i hjemmelsgrunnlaget hva slags lovovertredelser som kunne gi anledning til telefonavlytting i etterforskningsøyemed (avsnitt 34). I dommen *Malone mot Storbritannia*, som gjaldt kommunikasjonskontroll, la EMD vekt på at

> «..the essential elements of the power to intercept communications were laid down with reasonable precision in accessible legal rules that sufficiently indicate the scope and manner of the exercise of the discretion conferred on the relevant authorities [...]»

Det følger også av ovennevnte at lovkravet ikke er til hinder for at hjemmelen overlater en viss skjønnsutøvelse til forvaltningen. I så fall må loven som et minstemål angi hvilket formål inngrepet kan forfølge, se dommen *Olsson mot Sverige* 24. mars 1988 (sak 10465/83) avsnitt 61 (c):

> «A law which confers a discretion is not in itself inconsistent with the requirement of foreseeability, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.»

Utover kravet om formålsangivelse, vil det nærmere materielle innholdet i lovkravet bero på en mer sammensatt vurdering. Kravene til presisjon og tilgjengelighet er relative og vil blant annet øke med inngrepets styrke, se dommen *Klass mot Tyskland* 6. September 1978 (sak 5029/71) avsnitt 50:

> «The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by national law.»

Av den grunn skjerpes kravene til rettsgrunnlag ved skjult overvåking. I dommen *Kruslin mot Frankrike* 24. april 1990 (sak 11801/85) avsnitt 33 uttales:

> «Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.»

Videre vil også formålet ha betydning. I den grad det er tvingende nødvendig av hensyn til for eksempel rikets sikkerhet å holde deler av inngrepet eller fremgangsmåten ved inngrepet skjult, har EMD gitt den enkelte stat et større spillerom, se dommen *Leander mot Sverige* 26. mars 1987 (sak 9248/81) avsnitt 51.

Ved avgjørelsen av hvor presist hjemmelsgrunnlaget må være, vil EMD også legge vekt på hvilke prosessuelle garantier loven oppstiller. EMD legger blant annet vekt på om det foreligger adgang til domstolskontroll. I *Lambert mot Frankrike* 24. august 1998 (sak 23618/94) ble det konstatert konvensjonsstrid som følge av manglende adgang til domstolsprøving når avlyttingen vedrørte samtaler på telefonlinjen tilhørende andre personer. En slik mangel kunne i følge EMD «render the protective machinery void of any substance».

Lovkravet vil for øvrig kunne være oppfylt både gjennom formelle lover gitt av en lovgivende forsamling og rettsregler forankret i sedvane, rettspraksis og endog administrativ praksis, se blant annet dommen *Sunday Times mot Storbritannia* avsnitt 47. At også andre kompetansegrunnlag enn formell lov kan hjemle inngrep i konvensjonsrettigheter, må sees på bakgrunn av Storbritannias common law-system. I dommen *Leander mot Sverige* avsnitt 51 godtok EMD instrukser og lignende som relevante kilder. EMD godtar derimot ikke den alminnelige handlefrihet som hjemmel for inngrep i beskyttede rettigheter. I *Malone mot Storbritannia* uttalte EMD at selv om metoden ikke uttrykkelig var forbudt, måtte det kreves annet hjemmelsgrunnlag for at det engelske politiet kunne kreve innsyn i postverkets og televerkets kunderegistre.

Selv om lovskravet i EMK artikkel 8 nr. 2 ikke krever formell lov, har det i konvensjonspraksis vist seg at andre hjemler enn formell lov vanskelig vil oppfylle de øvrige deler av konvensjonens hjemmelskrav. Det gjenspeiles for så vidt i at de sentrale dommer som har utviklet vilkåret, gjelder saker der engelske rettsregler ikke er godtatt, se for eksempel *Sunday Times mot Storbritannia, Malone mot Storbritannia* og *Khan mot Storbritannia*. Dette har ført til at Storbrittania har fått et detaljert lovverk om politimetoder. Samme utvikling kan spores i andre land.

5.2.2.3 Formål som kan legitimere inngrep

For å kunne gjøre inngrep i vernede interesser etter artikkel 8 nr. 1, må for det første formålet med inngrepet falle inn under et av de formål som fremkommer i EMK artikkel 8 nr. 2. Relevante formål er blant annet hensynet til rikets sikkerhet («the interests of national security») og kriminalitetsbekjempelse («the prevention of disorder or crime»). Det kan derfor ikke være tvil om at politiets inngrep for å hindre kriminalitet oppfyller formålskravet. Også overvåkingspolitiets arbeid for å ivareta rikets sikkerhet, må anses relevant.

Hovedtendensen er likevel at domstolen i liten grad går inn og prøver den angitte formålsangivelse, se for eksempel *Leander mot Sverige* 26. mars 1987 (sak 9248/81) avsnitt 49. Domstolen har imidlertid i enkelte tilfeller overprøvd statens formålsangivelse.

5.2.2.4 Nødvendighetskravet

EMK artikkel 8 nr. 2 krever, i tillegg til lovkravet og kravet om at inngrepet må ivareta et bestemt formål, at inngrepet er nødvendig i et demokratisk samfunn. I dette vilkåret ligger et krav til forholdsmessighet. Borgernes forventning om å kunne

leve sine liv uten at staten blander seg inn i deres private sfære, må veies mot samfunnets behov for å kunne ta i bruk krenkende metoder for å sikre statens sikkerhet og bekjempe kriminalitet. Det kreves ikke at inngrepet skal anses uunnværlig. Det er på den annen side ikke tilstrekkelig at tiltaket er ønskelig eller nyttig. Balansepunktet ligger et sted imellom, se dommen *Olsson mot Sverige* (sak 10465/83) avsnitt 67. Hvor den nærmere grensen skal trekkes, vil bero på en konkret vurdering. Det er likevel mulig å trekke opp noen generelle utgangspunkter for vurderingen.

Skjønnsmarginen eller «the margin of appreciation» er et vesentlig trekk ved EMDs tolkning av konvensjonen. Det innebærer at EMD tillegger den enkelte stat en viss grad av skjønn ved utpensling av konvensjonens innhold. Statenes skjønnsmargin gjør at den enkelte stat i noen grad selv vil kunne vurdere hva som er en nødvendig metode. Likevel må det trekkes en grense. Graden av skjønnsfrihet varierer betydelig sett hen til det konkrete tilfellet.

I den grad en politimetode utgjør et ledd i beskyttelsen av rikets sikkerhet eller beskyttelse mot ytre farer, vil skjønnsmarginen være vid, se dommen *Leander mot Sverige* (sak 9248/81) avsnitt 59 og *Klass m.fl. mot Tyskland* (sak 5029/71) avsnitt 48. Men også innenfor kriminalitetsbekjempelse generelt har domstolen vist tilbakeholdenhet med å overprøve statenes vurdering av hva som er nødvendig i et demokratisk samfunn. Som det uttales i *Silver m.fl. mot Storbritannia* (sak 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 og 7136/75) avsnitt 97 vil statene:

> «[...] enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention [...]»

Selv for de mest inngripende metodene, som for eksempel telefonavlytting og romavlytting, har EMD i stor grad bare overprøvd om hjemmelen i tilstrekkelig grad oppstiller rettssikkerhetsgarantier, jf. *Klass m.fl. mot Tyskland* (sak 5029/71) avsnitt 50 referert i pkt. 5.2.2.2 ovenfor.

EMDs praksis viser at de hemmelige etterforskningsmetoder som straffeprosessloven hjemler, neppe vil være i strid med EMK artikkel 8 nr. 2. Romavlytting ble i prinsippet godtatt i *Malone mot Storbritannia* (sak 8691/79), og telefonavlytting har også ved flere anledninger blitt akseptert som politimetode.

Domstolen vil likevel prøve om hjemmelen er for vidt utformet, både om bestemmelsen som sådan er for vid og om en i forbindelse med en konkret bruk har gått utenfor det som er nødvendig i et demokratisk samfunn. Utgangspunkt for denne vurderingen må tas i inngrepet metoden medfører. Metoder som romavlytting og kommunikasjonskontroll vil lettere være uforholdsmessige enn alminnelig spaning. Sentralt i denne vurderingen står også hvilke rettssikkerhetsgarantier bestemmelsen oppstiller. Det gjelder kravet til saksbehandling og kravet til hvem som fatter beslutningen, se *Lüdi mot Sveits* (sak 12433/86). Et annet moment er om inngrepet utelukkende rammer personer som med god grunn kan mistenkes for forberedelse eller begått kriminalitet, se *Teixeira de Castro mot Portugal* (sak 25829/98). Sentralt vil det også være hvilket kriminalitetskrav bestemmelsen oppstiller og hvor alvorlig den konkrete planlagte handling eller begåtte kriminelle handling er.

6 Fellesspørsmål

6.1 Strafferammer som avgrensningskriterium

6.1.1 Gjeldende rett

Adgangen til å benytte skjulte tvangsmidler forutsetter som regel mistanke om et straffbart forhold av et visst alvor. I de fleste hjemlene for bruk av skjulte metoder er dette angitt slik at mistanken må være rettet mot overtredelse av et straffebud som må kunne medføre fengselsstraff i et visst antall år. Strafferammekravene gjenspeiler hvor inngripende de ulike metodene er ansett å være. Ved skjult ransaking, personnær teknisk sporing og kommunikasjonsavlytting er strafferammekravet ti års fengsel eller mer, jf. straffeprosessloven §§ 200 a, 202 c og 216 a. Ved teknisk sporing på objekt, fremtidig utleveringspålegg og kontroll av kommunikasjonsanlegg er strafferammekravet fem års fengsel eller mer, jf. §§ 202 b, 210 b og 216 b. Ved skjult kameraovervåking på offentlig sted, hemmelig beslag og utleveringspålegg er strafferammekravet seks måneders fengsel eller mer, jf. §§ 202 a og 208 a og § 210 a.

Samtidig er det i flere av bestemmelsene hvor metodebruken i utgangspunktet er knyttet til et strafferammekrav, nærmere oppregnet enkelte andre lovbrudd som kan gi grunnlag for å benytte skjulte tvangsmidler uavhengig av strafferammen. For eksempel kan mistanke om simple narkotikaforbrytelser gi grunnlag for kommunikasjonsavlytting, jf. straffeprosessloven § 216 a første ledd bokstav b, selv om den øvre strafferammen her er fengsel i to år, jf. straffeloven 1902 § 162 første ledd (straffeloven § 231).

For enkelte metoder – romavlytting og skjult båndlegging av formuesgoder – er metodebruken ikke knyttet til et strafferammekrav, men utelukkende til overtredelse av særlig oppregnede straffebud. Det samme gjelder hvor metodene brukes i avvergende eller forebyggende øyemed, jf. straffeprosessloven § 222 d og politiloven § 17 d.

Om begrunnelsen for at adgangen til bruk av skjulte tvangsmidler som regel er knyttet opp mot en strafferamme, vises det til Ot.prp. nr. 64 (1998–99) punkt 8.3.1.4 side 47.

6.1.2 Metodekontrollutvalgets forslag

Spørsmålet om straffebudenes strafferammer er et egnet avgrensningskriterium for adgangen til å ta i bruk skjulte tvangsmidler, behandles av utvalget i utredningen punkt 14.2 (side 157–159).

Utvalget presiserer at det ikke bør åpnes for bruk av skjulte metoder i større grad enn strengt nødvendig, og at hjemlene bør være så målrettede som mulig. Utvalget påpeker at en fordel ved en opplisting i de ulike tvangsmiddelbestemmelsene av hvilke straffebud som kan gi grunnlag for de aktuelle metodene, er at det vil kunne leses direkte ut av hver enkelt bestemmelse om det er anledning til skjult metodebruk. Videre vil lovgiver «tvinges» til å ta konkret stilling til om det aktuelle tvangsmiddelet skal kunne brukes ved etterforskning knyttet til overtredelse av det aktuelle straffebudet. Utvalget viser på den annen side til at dette kan resultere i mer omfangsrike og uoversiktlige bestemmelser, og et mindre fleksibelt lovverk.

Samtidig ser utvalget enkelte innvendinger mot å knytte bruken av skjulte metoder til straffebudenes strafferammer, og viser til at disse er vide og ikke nødvendigvis fullt ut gjenspeiler lovbruddenes alvor. Etter å ha gjennomgått hvilke lovbrudd som etter gjeldende rett gir anledning til bruk av skjulte metoder, foreslår utvalget likevel at straffebudenes øvre strafferamme fremdeles bør være avgjørende for metodetilgangen. Utvalget viser til at strafferammekravene er så vidt høye at adgangen til bruk av skjulte metoder er forbeholdt handlinger som er så alvorlige at dette kan rettferdiggjøres.

Utvalget fremhever likevel at en slik ordning bør suppleres med en liste over andre straffbare handlinger som etter en konkret vurdering også bør kunne gi grunnlag for å bruke det aktuelle tvangsmiddelet. I den forbindelse påpeker utvalget at det ut fra lovbruddenes karakter må kunne påvises et særlig behov for den aktuelle etterforskningsmetoden. Utvalget uttaler videre følgende (utredningen punkt 14.2 side 158–159):

> «[…] bruk av skjulte tvangsmidler i etterforskingen av mindre alvorlige handlinger kan rettferdiggjøres der det dreier seg om handlinger der offeret ikke kan forventes å bidra til oppklaring, kriminalitet som begås i lukkede miljøer som politiet av ulike grunner ikke kan forventes å få eller kunne innhente informasjon fra, og da særlig profesjonelle kriminelle miljøer, miljøer med sterk indre justis og miljøer som er så ensartede at de er vanskelig for politiet å infiltrere for eksempel fordi alle har den samme etniske bakgrunn.»

Utvalget legger dessuten til grunn at behovet for skjult metodebruk kan være særlig påtrengende i etterforskning av internasjonal eller grenseoverskridende kriminell virksomhet.

6.1.3 Høringsinstansenes syn

Høringsinstansene er delte i synet på om lovbruddets øvre strafferamme bør være avgjørende for om skjulte metoder kan tas i bruk. Det er også uenighet knyttet til det generelle spørsmålet om i hvilken grad lovbrudd som ikke oppfyller strafferammekravene bør gi grunnlag for slik metodebruk. Flere av høringsinstansene peker på at strafferammekravene generelt er for strenge, og at dette vanskeliggjør internasjonalt samarbeid.

Riksadvokaten har ikke avgjørende innvendinger mot utvalgets forslag om å beholde dagens ordning, men uttaler at:

> «[…] bestemmelsene kanskje blir lettere tilgjengelig dersom det for hvert enkelt tvangsmiddel konkret angis hvilke forbrytelseskategorier som kan gi grunnlag for å bruke det. I tillegg kommer at forbrytelsens alvor – uttrykt gjennom strafferammen – bare er et av flere momenter i vurderingen av om tvangsmidlet bør kunne benyttes. Også bl.a. *behovet* for etterforskingsmetoden for å kunne trenge inn i ellers lukkede kriminelle miljøer er av betydning, slik også utvalget peker på.»

Både *Riksadvokaten, Det nasjonale statsadvokatembetet (NAST)* og *Politidirektoratet* savner en vurdering av om dagens strafferammekrav ligger på et riktig nivå, særlig sett i lys av at strafferammekravene for skjult metodebruk i Danmark og Sverige er lavere enn i Norge. Disse høringsinstansene peker også på politiets utfordringer knyttet til grenseoverskridende kriminalitet. *NAST* uttaler i den forbindelse følgende:

> «Embetet arbeider i stor grad med grenseoverskridende kriminalitet. Dette er saker med utstrakt internasjonalt politisamarbeid, og vi ser at det er uheldig at muligheten for tvangsmiddelbruk er forskjellig i de enkelte land.»

Riksadvokaten viser på den annen side til at:

> «Dersom det åpnes for anvendelse av tvangsmidler for visse forbrytelseskategorier hvor strafferammen er lavere enn det alminnelige kravet reduseres betydningen av dette spørsmålet.»

Forsvarergruppen av 1977 er negativ til å beholde dagens ordning og er uenig i at en høy strafferamme alene bør medføre at en kategori forbrytelser kan gi grunnlag for bruk av skjulte tvangsmidler. Forsvarergruppen viser i den forbindelse til at strafferammer ikke er utformet ut fra hvilke prosessuelle virkninger som knyttes til dem, men ut fra den aktuelle forbrytelsens straffverdighet. Videre pekes det på at det innenfor samme lovbrudd vil kunne være et stort spenn i straffverdighet og et enda større spenn i hvilket behov det er for skjulte etterforskningsmetoder.

Forsvarergruppen advarer også mot følgene av å la mindre alvorlige straffbare forhold gi grunnlag for bruk av skjulte metoder. For å illustrere dette, trekker Forsvarergruppen frem metodebruk på bakgrunn av mistanke om overtredelse av straffeloven 1902 § 162 første ledd (simple narkotikaforbrytelser), og uttaler følgende:

> «[…] I så godt som i *samtlige* overtredelser av straffeloven § 162 første ledd, vil det ikke være noe offer som kan forventes å bidra til oppklaring. *Alle* saker etter § 162 første ledd synes etter dette å være kvalifisert for skjulte tvangsmidler (naturligvis med de tilleggsvilkår som ligger i subsidaritetskravet og indikasjonskravet der disse gjelder etc.). Allikevel synes utvalget å forutsette at skjulte etterforskningsskritt sjelden skal brukes i slike tilfeller (jfr kapittel 16). En skal selvsagt ikke glemme at straffeprosessloven § 170a får anvendelse, som nevnt, men det vil være vanskelig å henvise til at inngrepet er uforholdsmessig pga sakens relative lave grad av alvor, når denne kategorien lovbrudd som sådan er løftet opp av lovgiver og funnet alvorlig nok i seg selv til å begrunne skjulte etterforskningsskritt.»

På denne bakgrunn går Forsvarergruppen inn for en ordning hvor kvalifiserte straffebud velges ut

på bakgrunn av nødvendigheten av skjulte etterforskningsmetoder og alvorlighetsgraden av de aktuelle overtredelsene.

6.1.4 Departementets vurdering

Tilgangen til skjulte tvangsmidler bør fastlegges ut fra hensynet til å oppklare alvorlig kriminalitet vurdert mot betenkelighetene ved de enkelte metodene. Det sistnevnte hensynet medfører at inngripende metoder kun bør benyttes i utvalgte saker. Utvelgelsen kan foretas ved å reservere metodetilgangen til saker med en viss øvre strafferamme (strafferammekrav), eller en kan oppregne særskilt lovbrudd som anses alvorlige nok og egnet for bruk av skjulte metoder. Alternativt kan disse to tilnærminger kombineres. Dagens metodetilgang avgrenses i hovedsak av et strafferammekrav, men med enkelte eksempler på konkret oppregning av aktuelle straffebud, se punkt 6.1.1. Det første spørsmålet er om strafferammekravene gir en god nok avveining mellom behovet for skjulte metoder og de betenkeligheter som er knyttet til metodene, eller om det i større grad bør henvises til utvalgte bestemmelser.

Departementet påpeker at et strafferammekrav vil være et *grunnvilkår* for å kunne ta i bruk de skjulte metodene. I tillegg krever de fleste metodehjemlene at metodebruken etter sakens art og forholdene ellers ikke vil være et uforholdsmessig inngrep (forholdsmessighetskravet), at metodebruken må være av vesentlig betydning for å oppklare saken (indikasjonskravet) og at oppklaring ellers i vesentlig grad ville blitt vanskeliggjort (subsidiaritetskravet). Strafferammekravenes funksjon som grunnvilkår er dermed å avgrense metodetilgangen mot straffebud som *ikke* bør gi grunnlag for bruk av skjulte metoder. Strafferammekravet gir dermed ikke uttrykk for hvorvidt metodebruk knyttet til lovbrudd som oppfyller kravet er berettiget – det må avgjøres ut fra de øvrige kriteriene. I tillegg er tillatelse til metodebruk knyttet opp mot et «kan-skjønn», som innebærer at retten i det enkelte tilfelle vurderer om tillatelse bør gis – ut ifra hensyn som forholdsmessighet, hensiktsmessighet og behov.

Ved arbeidet med straffeloven ble det foretatt en fornyet vurdering av strafferammene, og departementet søkte å rette opp skjevheter i strafferammer mellom ulike kategorier av kriminalitet, jf. Ot.prp. nr. 8 (2007–2008) punkt 2.4 side 24. Strafferammene i den nye loven gjenspeiler derfor i stor grad alvoret i de ulike straffebudene. Når metodetilgangen knyttes til strafferammen, vil derfor de mest inngripende metodene være forbeholdt særlig alvorlige lovbrudd.

En løsning med strafferammekrav er også mest gunstig lovteknisk. En oppregning av alle aktuelle straffebud i hver metodehjemmel vil kunne gi omfangsrike og uoversiktlige bestemmelser, og dette fremstår uhensiktsmessig.

Departementet finner at et strafferammekrav, kombinert med de øvrige vilkårene, gir en god avveining mellom behovet for skjulte metoder og de betenkeligheter som er knyttet til metodene, forutsatt at strafferammekravet er tilstrekkelig høyt. Det anses å være tilfellet for de skjulte politimetodene i Norge. Det vises til oversikten ovenfor hva gjelder de mest inngripende metodene. Departementet ser heller ikke betenkeligheter ved at det for de mindre inngripende metodene gjelder lavere strafferammekrav.

I likhet med utvalget går departementet derfor inn for at straffebudenes øvre strafferamme fortsatt bør være et grunnvilkår for å benytte de skjulte metodene. Ved nykriminalisering eller endringer i eksisterende strafferammer er departementet likevel enig med Forsvarergruppen av 1977 i at det er grunn til å vurdere konkret om de aktuelle straffbare forholdene bør gi grunnlag for å benytte de enkelte metodene. Selv om metodebruk i utgangspunktet kan tillates fordi strafferammekravet er oppfylt, vil departementet ikke utelukke at det etter omstendighetene kan være grunn til å gjøre unntak i de enkelte metodehjemlene. Dette vil imidlertid sjelden komme på tale, siden strafferammekravet ikke i seg selv berettiger bruk av skjulte metoder i de enkelte sakene.

Det neste spørsmålet er om strafferammekravene bør senkes. Flere av høringsinstansene har som nevnt tatt til orde for dette eller påpekt at dette bør vurderes. Departementet finner imidlertid at dette ikke er ønskelig, sett hen til hvor inngripende metodene er. Departementet viser for så vidt til begrunnelsen som er gitt i Ot.prp. nr. 64 (1998–99) punkt 8.3.1.4 side 48. Det synes heller ikke *nødvendig* å senke strafferammekravene, siden det etter omstendighetene i visse tilfelle uansett bør åpnes for bruk av skjulte metoder ved mistanke om straffbare forhold med lavere strafferamme, se nedenfor. Hensynet til internasjonalt samarbeid kan være et moment i vurderingen av om en straffbar handling bør gi grunnlag for bruk av skjulte metoder. Det er imidlertid begrenset hvilken vekt andre lands rett kan tillegges, siden både strafferammene og anvendelsesområdet for metodene varierer en del mellom de ulike land.

Departementet slutter seg videre til utvalgets konklusjon om at strafferammekravet må supple-

res med en liste over andre straffbare handlinger som ikke oppfyller de aktuelle strafferammekravene, men som likevel etter en konkret vurdering også bør kunne gi grunnlag for å bruke det aktuelle tvangsmiddelet. Generelt sett innebærer dette en videreføring av gjeldende ordning. Hvorvidt det er grunn til å utvide virkeområdet for metodene til å gjelde flere straffebud, vurderes konkret i kapitlene om de enkelte metodene. Departementet er for øvrig i det vesentlige enig med utvalget i hvilke hensyn som må tas i betraktning dersom en vurderer slike utvidelser, det vil si at det som regel bør dreie seg om handlinger der offeret ikke antas å bidra til oppklaring, kriminaliteten begås i lukkede miljøer mv.

På bakgrunn av høringsuttalelsen fra Forsvarergruppen av 1977 vil departementet knytte noen kommentarer til bruken av skjulte metoder på overtredelser som i alminnelighet tilfredsstiller nevnte kriterier. Som foreningen viser til, kan simple narkotikaforbrytelser begrunne kommunikasjonskontroll, jf. straffeprosessloven § 216 a første ledd bokstav b og § 216 b første ledd bokstav b. Slike overtredelser begås ofte i lukkede miljøer og det vil ikke være noe offer som kan forventes å bidra med oppklaring. Fra lovgiverhold har det likevel ikke vært meningen at simple narkotikaforbrytelser uten videre skal begrunne bruk av skjulte tvangsmidler. I den forbindelse sluttet departementet i Ot.prp. nr. 64 (1998–99) punkt 8.3.1.4 side 49 seg til følgende uttalelse fra metodeutvalget i NOU 1997: 15 punkt 6.2.1 side 140:

> «I prakis vil det sjelden være aktuelt å anvende telefonkontroll i slike saker, men det kan foreligge spesielle omstendigheter som gjør dette ønskelig f eks mistanke om introduksjon av stoff i nye og spesielt utsatte miljøer, som f eks skoler og militærforlegninger.»

Metodekontrollutvalget uttaler dessuten følgende (utredningen punkt 16.4.2 side 185):

> «Det kan likevel tenkes situasjoner hvor kommunikasjonskontroll på bakgrunn av mistanke om overtredelse av straffeloven § 162 første ledd vil kunne aksepteres, for eksempel ved mistanke om salg til mindreårige.»

Departementet tar i punkt 7.4.2 stilling til om narkotikaovertredelser fortsatt bør kunne begrunne kommunikasjonskontroll. I denne sammenheng vil imidlertid departementet på generelt grunnlag fremheve at selv om lovgiver anser enkelte kategorier av lovbrudd som alvorlige nok til å begrunne bruk av skjulte tvangsmidler, må det i hver sak foretas en konkret vurdering av om forholdsmessighetskravet, indikasjonskravet og subsidiaritetskravet er oppfylt. Overtredelsens alvor vil være et sentralt moment i forholdsmessighetsvurderingen.

6.2 Vilkårene for å bruke straffeloven 1902 § 60 a (straffeloven § 79 bokstav c) ved skjulte tvangsmidler

6.2.1 Gjeldende rett

Ved lov 4. juli 2003 nr. 78 ble ny § 60 a tilføyd i straffeloven 1902. Dersom en straffbar handling er utøvet som ledd i aktivitetene til en organisert kriminell gruppe, bestemmer § 60 a første ledd at maksimumsstraffen i straffebudet forhøyes til det dobbelte, men ikke med mer enn fem års fengsel. Bakgrunnen for straffskjerpingen er at denne formen for kriminalitet anses svært samfunnsskadelig og bør slås hardt ned på, jf. Ot.prp. nr. 62 (2002–2003) punkt 5.5 side 50.

Straffskjerpingen har også betydning for politiets adgang til å bruke skjulte etterforskningsmetoder. I § 60 a tredje ledd er følgende bestemt:

> «Forhøyelse av maksimumsstraffen etter bestemmelsen her får anvendelse i forhold til lovbestemmelser som tillegger strafferammen rettslig virkning, hvis ikke annet er bestemt.»

En rekke av reglene om skjulte tvangsmidler er eksempler på slike lovbestemmelser. Straffeloven 1902 § 60 a har derfor i stor grad utvidet det saklige virkeområdet for de ekstraordinære etterforskningsmetodene. I Ot.prp. nr. 62 (2002–2003) punkt 5.5 side 50 ble en slik utvidelse vurdert å være både forsvarlig og hensiktsmessig.

Ved behandlingen av begjæringer om bruk av skjulte tvangsmidler, gjelder det beviskravet som er oppstilt i de ulike metodebestemmelsene – som hovedregel «skjellig grunn til mistanke» – også for vurderingen av om straffeloven 1902 § 60 a er overtrådt.

Bestemmelsen i straffeloven 1902 § 60 a er videreført i straffeloven § 79 bokstav c.

6.2.2 Metodekontrollutvalgets forslag

Utvalget påpeker at det på et tidlig stadium i etterforskningen kan være vanskelig å bevise at vilkårene i § 60 a er oppfylt. Utvalget finner likevel ikke grunn til å foreslå å lempe vilkårene for å ta § 60 a i bruk ved skjulte tvangsmidler. Det vises til at

politiet har adgang til å bruke skjulte tvangsmidler i etterforskningen av en rekke kriminelle handlinger som typisk begås som ledd i virksomheten til en organisert kriminell gruppe, selv uten å måtte ta i bruk § 60 a (se utredningen punkt 14.3 side 162). Dessuten viser utvalget til at § 60 a allerede i dag medfører en betydelig utvidelse av politiets metodetilgang, og at bestemmelsen ut fra personvern- og rettssikkerhetshensyn oppstiller rimelige begrensninger i denne tilgangen.

6.2.3 Høringsinstansenes syn

Det fåtall høringsinstanser som har uttalt seg på dette punktet går ikke inn for å senke mistankekravet, men peker på flere vanskeligheter knyttet til å ta i bruk skjulte metoder på grunnlag av mistanke om overtredelse av straffeloven 1902 § 60 a.

Riksadvokaten er av den oppfatning at det alminnelige mistankekravet bør opprettholdes, og uttaler følgende:

> «Tidlig i etterforskingen kan det være lite informasjon om hvorvidt de straffbare forhold begås som ledd i organisert kriminalitet. Riksadvokaten er likevel enig i at det alminnelige mistankekravet opprettholdes også når strafferammekravet oppfylles gjennom påberopelse av straffeloven § 60a. Heller enn å senke mistankekravet ved anvendelse av sistnevnte bestemmelse, bør noen flere alvorlige straffbare handlinger med strafferamme under 10 år gi adgang til skjult metodebruk, se nærmere under avsnitt 5.2, 5.3 og 11. Riksadvokaten er for eksempel enig i at skjult tvangsmiddelbruk må kunne iverksettes for å avverge drap uavhengig av om det planlagte drapet vil bli utført som ledd i virksomheten til en organisert kriminell gruppe.»

Kontrollutvalget for kommunikasjonskontroll gir uttrykk for at det i den innledende fasen av en etterforskning normalt ikke er tilstrekkelig informasjon om de faktiske forhold til at politiet og domstolen på forsvarlig grunnlag kan avgjøre om § 60 a kommer til anvendelse. Videre uttales følgende:

> «Utvalgets erfaring er at § 60 a påberopes i svært mange saker, hvor da vurderingene i stor grad bærer preg av antakelser om hvorvidt man har å gjøre med en virksomhet til en organisert gruppe.
>
> Utvalget ser at det kan være behov for metodebruk også i saker hvor den ordinære strafferammen er under 10 år (for eksempel alvorlig vinningskriminalitet), men mener § 60 a ikke er egnet som grunnlag for utvidet avlytting. I innledningsfasen av en sak er det som nevnt både for politiet og domstolene vanskelig å ta stilling til om vilkårene er oppfylt. Det bør derfor vurderes alternative måter å åpne for metodebruk i disse sakene. Dette kan for eksempel gjøres i form av en kasuistisk oppregning av lovbrudd hvor avlytting kan tillates, eller det kan gis adgang til en tidsbegrenset og kortvarig avlytting i slike saker.»

I kontrollutvalgets årsrapport for 2009 er dette utdypet noe:

> «For kommunikasjonskontroll kan et alternativ være at § 60 a ikke lenger er relevant, men at det i stedet innføres en adgang til tidsbegrenset kortvarig avlytting i saker med strafferamme under 10 år. Eksempelvis at det med domstolsgodkjennelse i forkant kan tillates avlytting i inntil to uker, og at det deretter konkret må påvises at denne avlyttingen har tilført etterforskingen vesentlig informasjon, for å kunne fortsette avlyttingen av den konkrete telefonen. En annen mulighet er at det foretas en konkret oppregning av konkrete straffebud der kommunikasjonskontroll kan skje, eller en kombinasjon av dette og tidsbegrensning.»

Norsk forening for kriminal reform (KROM) er av den oppfatning at forhøyelse av maksimumsstraffen på bakgrunn av mistanke om overtredelse av straffeloven 1902 § 60 a ikke bør komme i betraktning ved vurderingen av om strafferammekravene er oppfylt, og viser til at denne løsningen er valgt for gjentakelse og sammenstøt av forbrytelser.

6.2.4 Departementets vurdering

Innledningsvis finner departementet grunn til å slå fast at forhøyet maksimumsstraff etter straffeloven 1902 § 60 a (straffeloven § 79 bokstav c) fortsatt bør komme i betraktning ved vurderingen av om strafferammekravene i metodebestemmelsene er oppfylt. En eventuell stengsel for dette er ikke foreslått av utvalget og ville dessuten redusere politiets metodetilgang betydelig. Det synes heller ikke hensiktsmessig å oppstille et skjerpet mistankekrav for § 60 a-forhold. Den utvidede metodetilgangen som § 60 a innebærer, er som nevnt i punkt 6.2.1 vurdert forsvarlig og hensiktsmessig, og departementet er av den oppfatning at

et skjerpet mistankekrav vil kunne vanskeliggjøre etterforskningen av organisert kriminalitet.

På bakgrunn av høringen kan det imidlertid spørres om det er grunn til å utvide metodetilgangen i § 60 a-saker. I den forbindelse ser departementet at det i en tidlig etterforskningsfase kan by på utfordringer å avgjøre om det foreligger skjellig grunn til mistanke om overtredelse av § 60 a. Departementet finner likevel ikke grunn til å foreslå lempeligere krav for å anvende § 60 a ved bruk av skjulte tvangsmidler. Dette vil kunne medføre en uberettiget utvidelse av metodetilgangen. I stedet finner departementet – i tråd med uttalelsene fra Riksadvokaten og Kontrollutvalget for kommunikasjonskontroll – at en riktigere tilnærming er å vurdere om det er behov for at noen flere alvorlige straffbare handlinger med strafferamme under ti år bør gi adgang til bruk av skjulte metoder, se også punkt 6.1.4. Videre kan det vurderes om skjult tvangsmiddelbruk skal kunne iverksettes for å avverge drap uavhengig av om det planlagte drapet vil bli utført som ledd i virksomheten til en organisert kriminell gruppe, jf. punkt 8.4 og 13.4.3 nedenfor.

Departementet varslet i Meld. St. 7 (2010–2011) punkt 7 en gjennomgåelse av § 60 a for å vurdere om den er tilstrekkelig effektiv i bekjempelsen av organisert kriminalitet. I Prop. 131 L (2012–2013) ble anvendelsesområdet for bestemmelsen om organisert kriminalitet foreslått utvidet, og endringen ble vedtatt ved lov 21. juni 2013 nr. 85, som trådte i kraft straks. Definisjonen av organisert kriminell gruppe favner etter lovendringen også løsere grupperinger og nettverk, uten en klar, fast ledelse. Dette kan avhjelpe eventuelle vanskeligheter med å bevise at vilkårene i § 60 a er oppfylt.

Departementet stiller seg videre tvilende til om de praktiske problemene med å bevise at § 60 a er overtrådt, bør løses ved å tillate mer kortvarig metodebruk for handlinger som ikke tilfredsstiller strafferammekravene, slik Kontrollutvalget for kommunikasjonskontroll antyder. Det kan tenkes at det nettopp er § 60 a-forholdet som berettiger metodebruken. Departementet vil, i alle fall på det nåværende tidspunktet, ikke gå inn for en slik løsning.

6.3 Rettens kompetanse

6.3.1 Gjeldende rett

Skjulte tvangsmidler kan som hovedregel først tas i bruk etter tillatelse fra retten (forhåndskontroll). Har påtalemyndigheten gitt tillatelse til bruk av skjulte tvangsmidler i medhold av reglene om hastekompetanse, skal påtalemyndighetens beslutning så snart som mulig og senest innen 24 timer forelegges retten for godkjennelse (etterkontroll), se punkt 6.4.

Skjulte metoder som etter sin art pågår over et visst tidsrom – personnær teknisk sporing, kommunikasjonskontroll og romavlytting – tillates benyttet for en viss tid om gangen, jf. straffeprosessloven § 202 fjerde ledd og § 216 f, jf. § 216 m sjette ledd. Straffeprosessloven har ikke regler om at begjæringer om forlengelse av slike tvangsmidler må behandles av samme dommer som tillot metodebruken i den foregående perioden.

Videre gir straffeprosessloven i dag ingen begrensninger i dommerfullmektigers kompetanse til å behandle begjæringer om bruk av skjulte tvangsmidler. Dette gjelder selv om mistanken er knyttet til overtredelse av en bestemmelse med så høy strafferamme at hovedforhandlingen ikke kan settes med dommerfullmektig, jf. straffeprosessloven § 276.

6.3.2 Metodekontrollutvalgets forslag

Utvalget foreslår ikke å endre på at det som hovedregel er retten som beslutter om det skal gis tillatelse til bruk av skjulte tvangsmidler. Utvalget viser til at en slik ordning i størst grad sikrer kravet til uavhengighet, objektivitet og saklighet og dermed ivaretar rettssikkerheten best mulig, se utredningen punkt 15.2 side 165.

Utvalget har vurdert om det kan være grunnlag for å lovfeste at samme dommer som tillot den foregående tvangsbruken, skal behandle begjæringer om forlengelse av det skjulte tvangsmiddelet. Utvalget uttaler her følgende (utredningen punkt 15.2 side 165):

> «Det vil innebære at dommeren har noe større kunnskap om sakens bakgrunn og forløp. Utvalget har imidlertid kommet til at dette i for stor grad vil støte an mot det tilfeldighetsprinsipp som gjelder generelt ved rettens sammensetning. Det kan heller ikke utelukkes at nettopp en ordning hvor en annen dommer kan komme til å behandle spørsmålet om forlengelser vil innebære at sakens vurderes med andre øyne og i et annet lys. Utvalget vil derfor ikke foreslå noen endringer på dette punkt.»

Utvalget har også vurdert om dommerfullmektiger fortsatt bør ha kompetanse til å fatte beslutninger om bruk av skjulte tvangsmidler. Men heller ikke på dette punktet foreslår utvalget

endringer. Som begrunnelse anføres følgende (utredningen punkt 15.2 side 166):

> «Utvalget ser at det kan stilles spørsmål ved hvorvidt dommerfullmektiger, som normalt vil ha mindre erfaring enn embetsdommere, bør ha kompetanse til å gi tillatelse til bruk av skjulte tvangsmidler. Utvalget peker imidlertid på at dommerfullmektigenes erfaring og kompetanse, på samme måte som for embetsdommere, varierer. Utvalget kan derfor ikke i alminnelighet legge til grunn at dommerfullmektiger er mindre egnet til å vurdere denne type begjæringer enn embetsdommere. I tillegg kommer at dommerfullmektiger også i andre saker stilles overfor kompliserte vurderinger, både rettslige og faktiske. Utvalget vil på denne bakgrunn ikke foreslå endringer i dommerfullmektigenes kompetanse til å gi tillatelse til bruk av skjulte tvangsmidler, men vil likevel understreke at det vil være opp til domstolleder nøye å vurdere om det er forsvarlig å overlate saken til en dommerfullmektig.»

6.3.3 Høringsinstansenes syn

Ingen høringsinstanser har innvendinger mot utvalgets forslag om å videreføre hovedregelen om at det er retten som beslutter hvorvidt det skal gis tillatelse til bruk av skjulte tvangsmidler. Høringsinstansene er imidlertid delte i synet på hvorvidt samme dommer bør behandle alle begjæringer om skjulte tvangsmidler overfor mistenkte i samme sak.

Riksadvokaten slutter seg til utvalgets vurdering av at det ikke bør innføres en hovedregel om at samme dommer både skal behandle førstegangs- og forlengelsesbegjæringer i en sak. Tilsvarende standpunkt inntar *Domstoladministrasjonen,* under henvisning til tilfeldighetsprinsippet og at dette vil være en rettssikkerhetsgaranti for siktede.

Oslo politidistrikt er av den oppfatning at en ordning hvor begjæringer knyttet til samme sak behandles av samme dommer, har mye godt ved seg, og det anføres at spørsmålet bør diskuteres mer inngående. Politidistriktet viser til følgende:

> «Sett i lys av at utvalget foreslår en regel hvor en og samme advokat som hovedregel skal følge tvangsmiddelbruken – jf kap 15.5 – fremstår utvalgets standpunkt i forhold til dommerstanden som ubegrunnet. Den argumentrekken som utvalget viser til vedr advokater i kap 15.5 gjør seg gjeldende med minst samme styrke og omfang i forhold til en dommer. Det er hos dommeren beslutningskompetansen ligger. Det er dommeren som skal vurdere vilkårene for bruk av metoden, og det er utvilsomt i forhold til dommeren, som ansvarlig beslutningstaker, at utvalgets anførte argumenter knyttet til kontinuitet og saksoversikt bør ha størst relevans.»

Politidirektoratet tiltrer i det vesentlige Oslo politidistrikts synspunkter.

Når det gjelder spørsmålet om dommerfullmektigenes kompetanse, er *Riksadvokaten* enig med utvalget i at dommerfullmektiger bør kunne treffe beslutninger om bruk av skjulte tvangsmidler.

Domstoladministrasjonen slutter seg også til utvalgets vurdering av at dommerfullmektigenes kompetanse ikke bør endres. Det fremheves imidlertid at domstolleder – som i alle andre saker som tildeles dommerfullmektiger – må foreta en nøye vurdering av dommerfullmektigens egnethet.

KROM er uenig i at dommerfullmektiger skal kunne behandle begjæringer om skjulte tvangsmidler. Foreningen uttaler følgende:

> «Dommerfullmektiger har ett ansettelsesforhold og er således ikke uavhengige. Tillatelse til skjulte etterforskningsskritt er et alvorlig inngrep i personvernet til uskyldige tredjemenn, og på lik linje med at dommerfullmektiger ikke kan dømme i 6 års saker, bør de også være avskåret fra å ta avgjørelsene om hvorvidt vilkårene for skjulte etterforskningsskritt er oppfylt. Ved at denne typer saker er forbeholdt embetsdommere vil det også være ett signal om alvorlighetsgraden av inngrepet. Og at den som fatter avgjørelsen er uavhengig – ikke bare av partene, men også i sin stilling.»

6.3.4 Departementets vurdering

I saker om skjulte tvangsmidler blir domstolenes tradisjonelle rolle som rettssikkerhetsgarantist satt på prøve. Det er visse betenkeligheter ved å involvere domstolene gjennom en slik forhåndskontroll. Kontradiksjonsprinsippet vil nødvendigvis ikke kunne få normal gjennomslagskraft, og faktagrunnlaget for domstolene vil kunne være varierende. Involveringen av domstolene på dette stadiet av saken vil også kunne aktualisere spørsmålet om habilitet for dommere ved den senere behandlingen av straffesaken.

Departementet kan imidlertid vanskelig se gode alternativer til en ordning med domstolskontroll. Departementet er derfor enig med utvalget i

at en ordning hvor det kreves samtykke fra domstolen for å ta i bruk skjulte tvangsmidler, alt i alt gir best rettssikkerhet. Som utvalget påpeker er det denne prosessen som best sikrer kravet til uavhengighet, objektivitet og saklighet. Departementet vil på denne bakgrunn ikke gå inn for endringer her. Det er imidlertid nærliggende å vurdere tiltak som kan bidra til å styrke domstolskontrollen. Enkelte slike tiltak blir vurdert i punkt 6.6.2, 6.6.3, 6.6.9 og 6.7.

Av betydning i denne sammenheng er også spørsmålet om samme dommer skal følge alle begjæringer mot mistenkte i samme sak eller om en skal ta utgangspunkt i et tilfeldighetsprinsipp ved fordelingen av saker om skjulte tvangsmidler i domstolene. Her slår hensynet til dommeres uavhengighet og upartiskhet inn, hvilket isolert tilsier at sakene i en domstol fordeles mest mulig tilfeldig. Siden begjæringer om å ta i bruk skjulte metoder behandles uten mistenktes kjennskap, kan det sies at behovet for å vurdere disse med friske øyne veier enda tyngre. Dette forsterkes ved at tvangsmiddelbruk ofte pågår over tid med gjentatte fornyede prøvinger og utgjør således en kontinuerlig lukket prosess hos alle involverte aktører.

I tillegg er en tilfeldig fordeling det klart mest praktiske for domstolene, og dette muliggjør en smidig saksfordeling som tar hensyn til de enkelte dommeres kapasitet. På denne bakgrunn er departementet enig med utvalget i at gjeldende ordning videreføres.

Departementet ser for øvrig ikke grunn til å foreslå endringer som begrenser dommerfullmektigenes kompetanse i saker om skjulte tvangsmidler. Departementet støtter utvalget i at det i alminnelighet vanskelig kan legges til grunn at dommerfullmektiger er mindre egnet til å behandle denne typen saker enn embetsdommere. At dommerfullmektigene er ansatte og ikke embetsmenn kan heller ikke ses å ha særlig betydning. Det bør være opp til domstolleder å vurdere om det er forsvarlig å overlate saken til en dommerfullmektig. For øvrig vises det til utvalgets vurderinger (se utredningen punkt 15.2 side 165–166).

6.4 Påtalemyndighetens hastekompetanse

6.4.1 Gjeldende rett

Påtalemyndigheten er ved de fleste typer av skjulte tvangsmidler gitt en såkalt hastekompetanse, som midlertidig trer i stedet for rettens godkjenning. Nærmere bestemt kan påtalemyndigheten tillate skjult ransaking, personnær teknisk sporing, kommunikasjonskontroll og romavlytting dersom det ved opphold er «stor fare» for at etterforskningen vil lide, jf. straffeprosessloven §§ 200 a sjette ledd, 202 c tredje ledd, 216 d første ledd og 216 m sjette ledd. Ved utsatt underretning om beslag og utleveringspålegg er påtalemyndigheten gitt hastekompetanse dersom det ved opphold er «fare» for at etterforskningen vil lide, jf. straffeprosessloven §§ 208 a femte ledd og 210 a annet ledd. Ved samtlige av disse tvangsmidlene skal påtalemyndighetens beslutning så snart som mulig og senest innen 24 timer etter at bruken av tvangsmiddelet ble påbegynt, forelegges retten for godkjenning. Unntak gjelder i helger og på helligdager, se straffeprosessloven § 216 d første ledd tredje punktum.

Ved skjult kameraovervåking på offentlig sted og utleveringspålegg fremover i tid er påtalemyndigheten ikke gitt hastekompetanse.

I Ot.prp. nr. 64 (1998–99) punkt 8.6 side 63 uttalte departementet at hastekompetanse kun bør gis for etterforskningsmetoder hvor det er strengt nødvendig. Dette ble begrunnet slik:

> «Utvidede fullmakter forutsetter at påtalemyndigheten utøver et skjønn basert på rettssikkerhet og personvern. Videre er det viktig at allmennheten har tillit til at fullmaktene ikke misbrukes. I saker hvor påtalemyndigheten bruker sin hastekompetanse, vil ikke retten – når den får saken til etterfølgende kontroll – kunne forhindre inngrepet. Det har allerede skjedd.»

Hastekompetansen gjelder også ved bruk av skjulte tvangsmidler i avvergende øyemed, jf. straffeprosessloven § 222 d fjerde ledd.

Sjefen og assisterende sjef for PST er dessuten, med unntak for romavlytting, gitt hastekompetanse til å tillate bruk av skjulte tvangsmidler i forebyggende øyemed i saker om attentat mot representanter for Norges øverste statsmyndigheter eller tilsvarende organer i andre stater, jf. politiloven § 17 d tredje ledd, jf. første ledd bokstav c. I Ot.prp. nr. 60 (2004–2005) punkt 9.4.3.2 side 134 foreslo departementet at sjefen og assisterende sjef for PST skulle ha hastekompetanse i alle sakstyper som er nevnt i politiloven § 17 d første ledd. Begrensningen i hastekompetansen ble tatt inn under komitebehandlingen i Stortinget, med følgende begrunnelse (Innst. O. nr. 113 (2004–2005) side 35):

«Flertallet mener metodebruk i det forebyggende sporet uten rettslig kjennelse bør begrenses til et minimum. Flertallet viser til brev fra justisministeren 30. mai 2005 hvor han redegjør for at hastekompetansen til PST er viktigst i attentatsaker.»

6.4.2 Metodekontrollutvalgets forslag

Utvalget mener det er nødvendig å opprettholde påtalemyndighetens hastekompetanse, og viser til at det gjennomgående er alvorlige straffbare forhold som er bakgrunn for metodebruken. Det uttales følgende (utredningen punkt 15.3 side 167):

«Utenom kontortid, i helger og høytider vil det ikke være mulig å få rettens forhåndssamtykke til bruk av inngrepet. Også der mistenkte bytter telefoner eller sim-kort ofte, vil det kunne være behov for hastekompetanse. Et krav om innhenting av rettens tillatelse på forhånd, kan dermed medføre at kontrollen blir iverksatt for sent eller blir sterkt svekket. Utvalgets valg om ikke å gå inn for at tillatelser til kommunikasjonskontroll skal kunne knyttes til mistenkte som person heller enn til bestemte kommunikasjonsanlegg, jf. punkt 16.5, styrker behovet for å opprettholde politiets hastekompetanse.»

Utvalget har heller ikke holdepunkter for at hastekompetansen brukes ugrunnet, og det uttales i den sammenheng:

«Tallmateriale utvalget har fått tilgang til viser at hastekompetansen brukes ved drøyt en tredjedel av beslutningene om kommunikasjonskontroll. Utvalget har vurdert om det foreligger omstendigheter som tilsier at hastekompetansen brukes oftere enn det er grunnlag for, eventuelt om dette foranlediger lovendringer.

Utvalget har imidlertid ikke fått tilbakemeldinger om at påtalemyndighetens bruk av hastekompetanse til å iverksette skjulte tvangsmidler generelt oppfattes som problematisk. Den sterkeste indikasjonen på at hastekompetansen ikke brukes ugrunnet, er tallene som viser at svært få hurtigkoblinger ikke godkjennes ved domstolens etterkontroll, i snitt dreier det seg om ca. en prosent i året.»

Utvalget viser dessuten til at en styrking av domstolskontrollen vil omfatte domstolenes etterkontroll i saker hvor påtalemyndigheten har tillatt metodebruken i medhold av hastekompetansen. Utvalget legger til:

«I den grad det gjennom disse endringene synliggjøres mangler ved regelverket eller praktiseringen av ordningen, kan det selvsagt være aktuelt å vurdere ordningen på nytt.»

Utvalget omtaler for øvrig også PSTs hastekompetanse i saker om skjult tvangsmiddelbruk i forebyggende øyemed og spørsmålet om kompetansen bør utvides til flere sakstyper. Dette behandles i proposisjonen punkt 13.5.4.

6.4.3 Høringsinstansenes syn

Ingen av høringsinstansene tar til orde for å avvikle ordningen med hastekompetanse for påtalemyndigheten.

Både *Riksadvokaten* og *NAST* støtter uttrykkelig utvalgets vurdering av at det er nødvendig å beholde ordningen. *Riksadvokaten* peker på at skjult metodebruk ofte må settes i verk meget raskt for at ikke viktig informasjon skal gå tapt i påvente av rettens avgjørelse.

Forsvarergruppen av 1977 ser behovet for regler om hastekompetanse, men fremholder samtidig at denne myndigheten bare bør benyttes når det er strengt nødvendig. Samtidig bemerker foreningen at bruk av hastekompetanse i drøyt en tredjedel av kommunikasjonskontrollsakene synes mye. Forsvarergruppen mener derfor at departementet bør evaluere bruken av hastekompetanse særskilt og eventuelt vurdere om påtalemyndigheten gjennom utforming av nye retningslinjer bør bevisstgjøres ytterligere på vilkårene for å benytte hastekompetanse.

PST peker på at behovet for hastekompetanse også gjør seg gjeldende ved tvangsmiddelbruk i forebyggende øyemed. Det fremheves at de samme gode grunner for å gi hastekompetanse ved forebygging av trusler mot myndighetspersoner gjør seg gjeldende ved forebygging av terrorhandlinger.

6.4.4 Departementets vurdering

Departementet ser et klart behov for å opprettholde ordningen med hastekompetanse hos påtalemyndigheten. Det vises til utvalgets vurderinger som i det vesentlige har fått støtte under høringen. Spørsmålet blir om det er behov for endringer i reglene om påtalemyndighetens hastekompetanse.

Departementet er enig med utvalget i at det ikke foreligger holdepunkter for at hastekompetansen brukes ugrunnet. Det er på det rene at det i mange saker haster med å iverksette de skjulte

tvangsmidlene, for at ikke viktig informasjon skal gå tapt i påvente av rettens avgjørelse. At svært få tillatelser gitt av påtalemyndigheten underkjennes av retten i ettertid, taler dessuten for at ordningen ikke misbrukes. Departementet mener videre at en styrking av rollen til den offentlig oppnevnte advokaten vil kunne bidra til en enda mer betryggende rettslig etterprøving, se forslagene i punkt 6.6. På denne bakgrunn er departementet enig med utvalget i at det ikke er grunn til å foreslå endringer i reglene om påtalemyndighetens hastekompetanse. Departementet ser heller ikke foreløpig et behov for at ordningen med hastekompetanse bør evalueres særskilt.

Når det gjelder hastekompetanse ved skjulte tvangsmidler i forebyggende øyemed (politiloven § 17 d), ser departementet gode grunner for at Politiets sikkerhetstjeneste (PST) også gis hastekompetanse i terrorsaker. 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 om terror (straffeloven 1902 § 147 a) er meget alvorlige, og i dag kan det synes å gi lite sammenheng å la PST ha hastekompetanse i forebygging av attentatsaker, men ikke i terrorsaker. Faren for misbruk må dessuten sies å være minimal, ettersom PSTs hastebeslutning vil overprøves av retten i etterkant og dessuten vil inngå i EOS-utvalgets kontrollarbeid. Departementet går etter dette inn for at Sjefen og assisterende sjef for Politiets sikkerhetstjeneste (PST), tilsvarende som i attentatsaker, gis hastekompetanse til å tillate bruk av skjulte tvangsmidler i forebyggende øyemed i terrorsaker etter straffeloven 1902 § 147 a (straffeloven §§ 131–134), se punkt 13.5.4 og forslaget til endringer i politiloven § 17 d tredje ledd med merknader.

6.5 Status som siktet

Etter straffeprosessloven § 82 første ledd får mistenkte status som siktet når det er besluttet eller foretatt «pågripelse, ransaking, beslag eller liknende forholdsregler rettet mot ham». Ordningen er imidlertid annerledes for de skjulte tvangsmidlene. Straffeprosessloven § 82 tredje ledd første og annet punktum bestemmer følgende:

> «En mistenkt får ikke stilling som siktet ved at det besluttes å bruke et tvangsmiddel mot ham eller henne som det ikke skal gis underretning om. Er det besluttet utsatt underretning om et tvangsmiddel, inntrer stillingen som siktet først når underretning gis.»

I Ot.prp. nr. 64 (1998–99) punkt 13.7 side 112 begrunnet departementet hvorfor bruk av skjulte tvangsmidler ikke bør gi mistenkte status som siktet:

> «Formålet med forslagene om utsatt underretning er å unngå at den mistenkte får vite om tvangsmidlet mens det pågår. Han kan derfor ikke varsles til rettsmøter og kan heller ikke på annen måte gjøre krav på rettigheter som siktet. Departementet foreslår derfor, som utvalget, at man i loven bestemmer at unnlatt eller utsatt underretning om bruk av tvangsmidler ikke gir status som siktet. Den mistenkte bør først anses som siktet når underretning gis.»

Etter *utvalgets* syn tilsier den faktiske situasjonen at mistenkte gis status som siktet, men slik at det ikke gis slike rettigheter som ville undergrave at tvangsbruken er skjult. Utvalget går likevel ikke inn for en slik løsning, og dette begrunnes slik (utredningen punkt 15.4 side 167):

> «Dette ville imidlertid ikke innebåret noen endring i de rettigheter vedkommende kan og ikke kan gjøre gjeldende, og i så måte kun vært en lovteknisk endring. Et slikt forslag ville eventuelt fordret en grundig gjennomgang av andre mulige konsekvenser og lovendringsbehov som utvalget ikke har hatt kapasitet til å foreta. Utvalget finner derfor ikke grunn til å foreslå endringer på dette punkt, men anbefaler at spørsmålet vurderes nærmere i forbindelse med en eventuell revisjon av systematikken i straffeprosessloven.»

Av *høringsinstansene* er det kun *KROM* som uttaler seg om spørsmålet. Foreningen er av den oppfatning at det vil være riktig å gi mistenkte status som siktet og heller unnta rettigheter som ellers ville fulgt med en siktelse, og det vises til at dette vil harmonisere rettsreglene og understreke alvoret av inngrepet for den det rettes mot.

Departementet kan i det vesentlige slutte seg til utvalgets begrunnelse og finner ikke grunn til å foreslå endringer på dette punktet nå. Spørsmålet vil eventuelt bli vurdert nærmere ved en systematisk gjennomgåelse av straffeprosessloven.

6.6 Oppnevnelse av offentlig advokat etter straffeprosessloven § 100 a

6.6.1 Innledning

Ved domstolenes behandling av begjæringer om å ta i bruk skjulte tvangsmidler skal som regel det offentlige oppnevne en advokat til å vareta mistenktes interesser, jf. straffeprosessloven § 100 a.

Utvalget er av den oppfatning at de offentlige oppnevnte advokatene er av avgjørende betydning for at kontrollen med politiets begjæringer om bruk av skjulte tvangsmidler og domstolenes behandling av disse skal bli reell, se utredningen punkt 15.5 side 168. Utvalget fremhever at det har fått tilbakemeldinger om at ordningen ikke synes å fungere optimalt. Især pekes det på at arbeidsforholdene ved enkelte domstoler ikke er tilfredsstillende for de advokatene som er oppnevnt etter § 100 a.

Utvalget gir uttrykk for at det har vært vanskelig innenfor sitt mandat å foreslå endringer som vil kunne bedre denne situasjonen. Utvalget foreslår imidlertid i utredningen punkt 11.7.4 side 134, jf. punkt 15.5 side 168 at det gis et eget opplæringstilbud for de aktuelle advokatene. Dette behandles nærmere i punkt 6.6.9 nedenfor.

I tillegg foreslår utvalget på flere punkter å styrke rollen til den offentlig oppnevnte advokaten gjennom endringer i straffeprosessloven § 100 a. Disse forslagene behandles nærmere i punkt 6.6.2 til 6.6.7 nedenfor.

Enkelte høringsinstanser uttaler seg generelt om utvalgets forslag. *PST* uttaler:

> «Utvalget foreslår i det vesentlige en videreføring av de prinsipper som gjelder for oppnevning og bruk av offentlig advokat i saker om skjulte tvangsmidler. Utvalget foreslår likevel noen viktige presiseringer som i det alt vesentlige innebærer en styrking av kontradiksjonen. PST deler utvalgets syn i disse spørsmål.»

I motsatt retning uttaler *Oslo politidistrikt*:

> «Advokat oppnevnt i henhold til § 100a har utvilsomt en viktig rolle for å beskytte mistenktes interesser i sak om bruk av skjulte tvangsmidler. Mistenktes interesser er imidlertid bare ett av flere forhold som skal vektlegges når begjæringer om tvangsmiddelbruk skal vurderes. Å anse at advokaten er den avgjørende faktor for en riktig og veloverveid avgjørelse, gir advokaten en rolle, funksjon og et ansvar som etter vår vurdering mangler begrunnelse og grunnlag. Vi kan heller ikke se at utvalget har begrunnet nærmere hvilke konkrete forhold som begrunner en slik utvidelse av advokatens rolle, utover å vise til noen tilbakemeldinger fra enkelte advokater.»

Romerike politidistrikt er enig med utvalget i flere av dets forslag, men fremhever likevel generelt at så lenge man har akseptert en skjult etterforskningsmetode, har man også akseptert at det ikke vil bli full kontradiksjon slik som i åpne saker.

Selv om den offentlig oppnevnte advokaten etter straffeprosessloven § 100 a har en spesiell rolle sammenholdt med en vanlig forsvarer, mener departementet at ordningen med offentlig oppnevnt advokat er viktig for å søke å oppnå en størst mulig balanse mellom partene i saker om skjulte tvangsmidler. Ingen høringsinstanser har innvendinger mot ordningen som sådan. Siden den offentlige advokaten er avskåret fra å ha kontakt med mistenkte, er det imidlertid viktig at advokaten på andre måter settes i størst mulig stand til å vareta mistenktes interesser. I de følgende punktene behandles de ulike forslagene utvalget har fremsatt for å styrke ordningen.

6.6.2 Oppnevnelse av samme advokat ved forlengelser mv.

6.6.2.1 Gjeldende rett

Den offentlig oppnevnte advokaten skal vareta mistenktes interesser i forbindelse med «rettens behandling av begjæringen» om å ta i bruk et skjult tvangsmiddel, jf. straffeprosessloven § 100 a annet ledd. Etter ordlyden ligger det i dette at oppdraget er knyttet til hver enkelt begjæring og eventuelle rettsmidler, og ikke til sakskomplekset som sådant. Ved begjæringer om forlengelser står retten dermed fritt til å oppnevne en annen advokat enn den som har vært oppnevnt ved tidligere begjæringer i samme sak. Det samme gjelder ved begjæringer om andre tvangsmidler i samme sak. I Ot.prp. nr. 64 (1998–99) punkt 8.10.7 side 84 uttaler imidlertid departementet følgende:

> «Ved behandlingen av spørsmålet om å forlenge tillatelsen til å foreta kommunikasjonskontroll, bør retten så vidt mulig oppnevnte den samme forsvareren som sist. På den måten får forsvareren bedre oversikt over de samlede virkninger av kontrollen. Dessuten reduseres antallet personer som kjenner til kontrollen. Etter departementets syn er det ikke nødvendig å lovfeste en slik ordning.»

Formuleringen av straffeprosessloven § 100 a annet ledd innebærer videre at den offentlig oppnevnte advokatens oppdrag ikke er knyttet til selve gjennomføringen av tvangsmidlet. Heller ikke inngår det i oppdraget å bistå ved underretning til mistenkte eller å ta kontakt med kontrollorganer. I Ot.prp. nr. 64 (1998–99) side 145 tar imidlertid departementet forbehold om at enkelte oppgaver som ikke direkte er knyttet til begjæringen kan utføres av advokaten:

> «Selv om det ikke er uttrykkelig nevnt, må forsvareren også kunne begjære overfor retten at bruken av tvangsmidlet skal opphøre fordi vilkårene for kontrollen ikke lenger er oppfylt. På samme måte må forsvareren kunne begjære at det nå gis underretning til den mistenkte om et hemmelig tvangsmiddel.»

Straffeprosessloven § 100 a er ikke til hinder for at den offentlig oppnevnte advokaten varetar interessene til flere mistenkte i samme sak. Foreligger det i spesielle tilfeller interessekonflikt mellom de mistenkte på dette stadiet av saken, vil imidlertid de advokatetiske reglene være til hinder for at samme advokat varetar interessene til flere mistenkte.

6.6.2.2 Metodekontrollutvalgets forslag

Utvalget foreslår at advokaten så langt som mulig skal oppnevnes ved alle begjæringer om forlenget bruk av et tvangsmiddel og ved alle begjæringer om bruk av andre skjulte tvangsmidler som retter seg mot samme mistenkte i en sak. Videre foreslås det at oppdraget skal vare til tvangsmiddelbruken er avsluttet og underretning er gitt, se utredningen punkt 15.5 side 168 og lovutkastet § 100 a annet ledd annet og tredje punktum. Utvalget begrunner forslagene slik:

> «Etter utvalgets syn er det uheldig dersom ikke samme advokat oppnevnes. I praksis vil det bidra til oppstykking av arbeidet, manglende kontinuitet og manglende mulighet til å se effekten av de samlede tvangsmidler dersom det oppnevnes ny advokat ved begjæring om bruk av andre tvangsmidler eller eventuelle forlengelser av inngrepet. Dette gjelder kanskje særlig ettersom utvalget ovenfor har funnet at det ikke vil tilrå en ordning hvor samme dommer *skal* behandle eventuelle begjæringer om forlengelse av tvangsmiddelbruken. Dernest vil antallet personer som kjenner til kontrollen øke ved skifte av offentlig oppnevnt advokat. Utvalget anser det som viktig at den advokat som oppnevnes så langt som mulig fungerer for alle begjæringer som retter seg mot samme mistenkte og for den perioden tvangsmidlene er i bruk. Oppnevningen bør dermed gjelde frem til tvangsmiddelet er avsluttet og underretning er gitt til siktede og hans eventuelle forsvarer. Dette innebærer at påtalemyndigheten må sørge for å underrette advokaten om at ordinær underretning er gitt, og at advokaten selv har ansvar for å medvirke til at underretning faktisk blir gitt. Oppnevningen skal også gjelde for eventuelt etterarbeid i form av å kontakte kontrollorganene dersom saken gir grunnlag for dette, for eksempel fordi underretning ikke gis i tråd med reglene om dette.»

6.6.2.3 Høringsinstansenes syn

Ingen høringsinstanser er negative til at den offentlig oppnevnte advokaten varetar interessene til samme mistenkte ved alle begjæringer om bruk av skjulte tvangsmidler i saken, men flere understreker at en slik regel ikke må være absolutt. Flere instanser er dessuten kritiske til en eventuell utvidelse av rollen til den offentlig oppnevnte advokaten.

Riksadvokaten har ikke innvendinger mot at samme advokat så langt som mulig gjør tjeneste ved rettens behandling av alle begjæringer om bruk av skjulte metoder mot samme mistenkte i en sak, og at oppdraget varer frem til tvangsmiddelbruken er avsluttet og underretning gitt. Det uttales følgende:

> «En slik ordning vil gi advokaten bedre oversikt og større muligheter til å peke på svakheter i påtalemyndighetens begjæringer. Det er også en fordel at antallet personer som kjenner til metodebruken holdes så lavt som mulig.»

Heller ikke *NAST* har innvendinger mot at samme advokat som hovedregel skal følge behandlingen av begjæringer om skjulte tvangsmidler mot samme mistenkte gjennom hele saken, forutsatt at en slik regel ikke gjøres absolutt. Embetet begrunner dette slik:

> «Skjult etterforsking med metodebruk kan strekke seg over år, med begjæringer flere ganger i måneden, og det er ikke realistisk at en og samme advokat vil kunne følge opp hele veien. I tillegg vil det kunne by på uante praktiske problemer i gjennomføringen.»

Oslo politidistrikt gir uttrykk for at en hovedregel om at samme advokat skal følge behandlingen av begjæringer om skjulte tvangsmidler mot samme mistenkte i samme sak har mye godt ved seg, forutsatt at det samme gjelder på dommersiden, se punkt 6.6.3 ovenfor. Politidistriktet peker på at en slik ordning ikke trenger å innebære annet enn at man sørger for et system som i så stor grad som mulig sikrer at samme advokat kontaktes og benyttes ved forlengelser og andre begjæringer om skjulte tvangsmidler.

Oslo politidistrikt er atskillig mer skeptisk til forslaget om at advokatens rolle skal utvides til å overvåke selve gjennomføringen av inngrepet, og påpeker følgende:

> «Hva som ligger i dette sies det lite konkret om, utover at man tillegger advokaten ansvar og rettigheter tilknyttet underretning av mistenkte, samt synes å utvide advokatens rett til innsyn i opplysninger mens tvangsmiddelbruken pågår.»

Politidistriktet understreker at en rolle for advokaten ved gjennomføringen av inngrepet vil bryte totalt med rolle- og ansvarsfordelingen i straffeprosessen, ettersom etterforskningen hører under politi og påtalemyndighet.

Kripos vil sterkt fraråde at den offentlig oppnevnte advokatens oppdrag skal vare helt frem til mistenkte underrettes om tvangsmiddelbruken, og mener at advokatens oppdrag bør opphøre når den skjulte etterforskningen opphører. Kripos uttaler følgende:

> «En ordning hvor to forsvarere med ulik grad av innsynsrett skal ivareta mistenktes interesser parallelt synes lite hensiktsmessig. Det er uklart hvilken rolle utvalget mener at § 100a-forsvareren skal ha etter at den skjulte etterforskningen er over, med unntak av å kontrollere at underretning blir gitt. Og notoriteten omkring underretningen vil fremgå av den åpne straffesakens dokumenter, typisk som en protokollasjon i avhør eller i en begjæring til retten hvor opplysninger fra skjult etterforskning brukes som bevis.»

Kripos forstår videre utvalget dithen at det skal oppnevnes én offentlig advokat for hver mistenkt i saken. Kripos stiller seg kritisk til en slik løsning, og viser til at dette vil gjøre det vanskelig å gjennomføre muntlige forhandlinger. Også følgende fremheves:

> «Desto flere § 100a-forsvarere som har vært involvert i en og samme sak, desto vanskeligere vil det være å finne forsvarere som kan oppnevnes i den åpne fasen av etterforskningen. Dersom opplysninger fra den skjulte fasen senere er unntatt etter § 242a, kan ikke samme forsvarer benyttes. På større steder som Oslo vil det nok kunne løses, men i mindre rettskretser i landet vil det bli nærmest umulig å finne en habil forsvarer.»

Kripos foreslår på denne bakgrunn at det som hovedregel oppnevnes én offentlig advokat i hver sak, uavhengig av antallet mistenkte, men at det må kunne gjøres unntak etter en konkret vurdering.

Politidirektoratet tiltrer i det vesentlige vurderingene fra Oslo politidistrikt og Kripos, og uttrykker særlig støtte til forslaget fra Kripos om at advokatens oppdrag bør avsluttes når den skjulte etterforskningen opphører. Direktoratet har i den sammenheng vanskeligheter med å se avgjørende argumenter for at oppnevnelsen skal vare lengre enn bruken av tvangsmidlene.

Oslo statsadvokatembeter har ingen innvendinger mot utvalgets forslag, men peker på at det har en kostnadsside som ikke er nærmere vurdert av utvalget. Embetet mener at merkostnadene bør beregnes dersom departementet vurderer å følge opp forslaget, og at det antakelig kan reises spørsmål om nytteverdien av forslaget svarer til kostnadene.

Domstoladministrasjonen støtter forslaget, med tar forbehold dersom det viser seg at en slik ordning fører til vesentlige forsinkelser i rettens behandling.

Oslo tingrett peker på at et ubetinget krav om bruk av samme advokat ved forlengelser vil føre til forsinkelser. Tingretten fremhever at dette særlig vil bli tilfellet om det må avholdes muntlige forhandlinger ved begjæringer om forlengelse, se punkt 6.7. I likhet med Kripos, reiser Oslo tingrett spørsmål om det må oppnevnes en advokat for hver mistenkt. Tingretten foreslår at det oppnevnes én advokat der det ikke er sannsynliggjort interessekonflikt mellom de mistenkte.

Forsvarergruppen av 1977 slutter seg til utvalgets vurderinger og forslag, og føyer til at en ordning som foreslått vil virke ressursbesparende.

6.6.2.4 Departementets vurdering

Departementet ser en klar fordel i at samme advokat gjør tjeneste ved rettens behandling av alle

begjæringer om skjulte tvangsmidler mot samme mistenkte i en sak. Departementet er således enig i utvalgets vurderinger og forslag på dette punktet, og viser også til at høringsinstansene i stor grad slutter seg til en slik ordning. Departementet peker særlig på at dette vil gi advokaten en totaloversikt over tvangsmiddelbruken i saken. Advokaten vil bli bedre i stand til å vurdere om et skjult etterforskningsskritt er uforholdsmessig sett opp mot den øvrige metodebruken i saken. Dessuten vil det begrense antallet personer som har kjennskap til bruken av tvangsmidlene. I tillegg vil en slik ordning, særlig på mindre steder, gjøre det enklere å få tak i forsvarer som kan tjenestegjøre i den åpne saken, jf. punkt 6.6.6. Departementet er av den oppfatning at en ordning med oppnevnelse av samme advokat best varetar mistenktes rettssikkerhet. I Ot.prp. nr. 64 (1998–99) punkt 8.10.7 side 84 ble en slik ordning skissert, men ikke foreslått lovfestet.

En regel om at samme advokat skal gjøre tjeneste ved rettens behandling av alle begjæringer om skjulte tvangsmidler mot samme mistenkte i en sak vil ikke øke det offentliges advokatutgifter i disse sakene, men er snarere egnet til å redusere dem.

På den annen side er departementet enig med utvalget i at en slik regel ikke kan være absolutt. Ved hyppige begjæringer fra politiet i samme sak, kan det by på praktiske problemer å få samme advokat til å stille opp. Det er også viktig at en slik ordning ikke skaper forsinkelser som kan skade etterforskningen. Det vil i så fall kunne medføre et press på påtalemyndighetens hastekompetanse, noe som ikke er ønskelig. Det må vurderes fra sak til sak hvilke forsinkelser som kan godtas av hensyn til etterforskningen, men i alminnelighet bør det ikke store forsinkelsen til før et advokatskifte er akseptabelt. Departementet er i så måte enig med utvalget i at en egnet reservasjon ligger i at samme advokat «så langt det er mulig» oppnevnes for samtlige begjæringer om bruk av skjulte tvangsmidler mot mistenkte i samme sak, se lovforslaget § 100 a annet ledd nytt annet punktum.

Når det så gjelder spørsmålet om å utvide den offentlige advokatens oppgaver, er departementet enig med Oslo politidistrikt i at en rolle for den offentlige advokaten ved selve gjennomføringen av tvangsmidlet vil innebære en fremmed løsning og reise en rekke uklare spørsmål. Ved kommunikasjonskontroll og romavlytting vil dessuten metodebruken etterkontrolleres av Riksadvokaten og Kontrollutvalget for kommunikasjonskontroll. På området til Politiets sikkerhetstjeneste etterkontrolleres metodebruken av EOS-utvalget.

Departementet er videre enig med Kripos og Politidirektoratet i at advokatens oppdrag bør opphøre når den skjulte etterforskningen opphører, og foreslår ikke endringer i gjeldende rett på dette punktet. Departementet forutsetter i den forbindelse at politiet følger opp plikten til å underrette mistenkte. Eventuelle forsømmelser i så måte vil dessuten mest sannsynlig komme for dagen når saken går over i en åpen fase. Oppnevnes det etter hvert en ordinær forsvarer for mistenkte, synes denne nærmest til å ivareta mistenktes interesser på dette stadiet av saken. Departementet går etter dette ikke inn for å utvide den offentlig oppnevnte advokatens oppdrag i forbindelse med tvangsmiddelbruken. Som følge av at det er overlatt til en særskilt dommer å avgjøre spørsmålet om omgjøring av innsynsnekt etter § 242 a, er 100 a-advokatens rolle utvidet i disse sakene, jf. lov 21. juni 2013 nr. 86.

Departementet finner heller ikke grunn å endre på dagens ordning med at det som regel oppnevnes én advokat for alle mistenkte. Departementets forslag til endringer i § 100 a er imidlertid ikke til hinder for at det oppnevnes flere advokater der hvor det er interessekonflikt.

6.6.3 Frister for å begjære forlengelser og varsel til advokaten

Ved fengslinger skal eventuelle begjæringer om forlengelse fremsettes så tidlig at siktede og forsvareren kan få varsel senest dagen før rettsmøtet holdes, jf. straffeprosessloven § 185 fjerde ledd første punktum. Innen samme frist skal partene varsles om rettsmøtet, jf. annet punktum. Gjeldende rett oppstiller ingen tilsvarende regel ved begjæringer om forlengelse av skjulte tvangsmidler.

Under henvisning til straffeprosessloven § 185 fjerde ledd foreslår *utvalget* at begjæringer om forlengelse av skjulte tvangsmidler skal fremsettes så tidlig at advokaten kan få varsel senest dagen før rettsmøtet holdes (utredningen punkt 15.5 side 169 og lovutkastet § 100 a annet ledd sjette punktum).

Ingen *høringsinstanser* har uttalt seg om forslaget.

D e p a r t e m e n t e t er av den oppfatning at en regel som foreslått vil bidra til at den offentlige advokaten får satt seg tilstrekkelig inn i saken. I samsvar med utvalgets forslag foreslår derfor departementet å endre straffeprosessloven § 100 a, se lovforslaget § 100 a annet ledd fjerde punktum.

6.6.4 Den offentlig oppnevnte advokatens innsyn i sakens dokumenter

6.6.4.1 Gjeldende rett

Straffeprosessloven § 100 a annet ledd bestemmer at advokaten «skal gjøres kjent med begjæringen og grunnlaget for den». Grunnlaget for begjæringen er de rapporter og dokumenter som påtalemyndigheten legger frem for retten, jf. Rt. 2005 side 203.

Ved lovendring 17. juni 2005 nr. 85, som trådte i kraft 5. august samme år, ble det tilføyd at advokaten «etter anmodning» har «krav på innsyn i sakens dokumenter med de begrensninger som følger av §§ 242 og 242 a». Endringen kom inn under lovbehandlingen i Stortinget, jf. Innst.O. nr. 113 (2004–2005) punkt 6.2 side 20–21, hvor komiteen bemerket at den var opptatt av at den offentlige advokaten skulle kunne vareta mistenktes interesser ved domstolens behandling av begjæring om bruk av hemmelige tvangsmidler. Endringen førte til at offentlige advokater fikk samme tilgang til sakens dokumenter som forsvarere.

6.6.4.2 Metodekontrollutvalgets forslag

Utvalget foreslår i utredningen punkt 15.5 side 169, jf. lovutkastet § 100 a annet ledd fjerde punktum, at hele den foreliggende straffesaken, og ikke bare begjæringen og grunnlaget for den, automatisk skal oversendes den offentlig oppnevnte advokaten. Utvalget viser til at innsyn ikke bør være avhengig av en konkret begjæring fra advokaten eller retten, og at hele saken oversendes i fengslingssaker. Det uttales følgende:

> «Ved at dette gjøres automatisk, vil man også slippe utsettelser som følge av at retten eller advokaten begjærer innsyn i sakens dokumenter slik dagens system gir anledning til. Det vil også gjøre det lettere for – og gi ytterligere oppfordring til – advokaten å sette seg grundig inn i saken.»

6.6.4.3 Høringsinstansenes syn

De fire høringsinstansene som har uttalt seg om forslaget finner det problematisk.

Oslo politidistrikt, med støtte fra *Politidirektoratet*, er meget kritisk til forslaget, og påpeker at det er uklart hva utvalget mener med «hele den foreliggende straffesak» og hvordan det «automatiske innsynet» skal gjennomføres i en operativ skjult etterforskningsfase. Når det gjelder det siste uttaler politidistriktet:

> «Etterforskningen i en operativ skjult fase – for eksempel ved bruk av kommunikasjonskontroll (KK) – vil ofte være preget av store informasjonsmengder som løpende evalueres og brukes operativt av de tjenestepersoner som følger saken daglig. I den grad deler av informasjonen nedtegnes, skjer det ofte i form av notater eller i form av rapporter ment som grunnlag for begjæringer om skjulte tvangsmidler. Det foreligger således vanligvis ingen ordinær sak ved siden av den saken som fremmes for retten med begjæring om tvangsmiddelbruk. Oslo politidistrikt vil advare på det sterkeste mot en slik løsning, som vil ha massive konsekvenser for politiets mulighet til å bedrive kriminalitetsbekjempelse som samfunnet ønsker og forventer.»

NAST er ikke uenig i at den offentlig oppnevnte advokaten og retten skal ha innsyn i sakens dokumenter og ikke bare i begjæringen og grunnlaget for den, men – som Oslo politidistrikt – peker embetet på de samme problemer med å gjennomføre et automatisk innsyn i en operativ skjult etterforskingsfase, og at forholdsvis lite nedtegnes skriftlig. Embetet er derfor uenig i at innsyn skal gis uavhengig av begjæring fra advokaten eller retten.

Også *Riksadvokaten* er opptatt av disse problemstillingene, og uttaler følgende:

> «Mens tvangsmiddelbruken pågår vil det etter riksadvokatens syn ikke være praktikabelt å gjennomføre innsyn utover det som måtte foreligge av skriftlige rapporter. Noe annet vil være en tidsmessig og ressursmessig umulig oppgave. I likhet med politiet advarer riksadvokaten mot en løsning hvor advokaten på dette stadiet har krav på innsyn i all informasjon fra tvangsmiddelbruken. En slik ordning vil få betydelige konsekvenser for politiets mulighet til å drive effektiv kriminalitetsbekjempelse.
>
> […]
>
> Skulle utvalgets forslag bli videreført, er det etter riksadvokatens syn helt nødvendig at det vurderes nærmere hva innsynsretten i så fall skal omfatte og at dette utvetydig klargjøres i forarbeidene. Spørsmålet har naturligvis nær sammenheng med hva som skal anses som «sakens dokumenter» mens det foregår skjult etterforsking.»

6.6.4.4 Departementets vurdering

Enkelte høringsinstanser synes å forstå utvalget dit hen at det foreslås endringer i reglene om *hva* den offentlig oppnevnte advokaten kan gis innsyn i. Slik departementet forstår utvalget, foreslår det bare endringer i reglene om *hvordan* innsyn skal gis. Departementet har for så vidt sans for hensynene bak utvalgets forslag; nemlig å sette den offentlig oppnevnte advokaten bedre i stand til å vareta mistenktes interesser. Utvalgets forslag synes imidlertid lite praktikabelt, og departementet ser at en automatisk oversendelse av alt materiale i saken som er å anse som «sakens dokumenter», vil kunne by på store praktiske utfordringer for politiet. I den forbindelse vises det til at saker om kommunikasjonskontroll, romavlytting og personnær teknisk sporing ikke i samme grad som fengslingssaker består av nedtegnede avhør, protokoller og påtegninger. De høringsinstansene som har uttalt seg er kritiske. Departementet går på denne bakgrunn ikke videre med forslaget, men legger til grunn at påtalemyndigheten lojalt følger Stortingets intensjoner og gir den offentlig oppnevnte advokaten innsyn på begjæring der vilkårene for dette er oppfylt.

6.6.5 Tredjepersoners interesser

Etter straffeprosessloven § 100 a annet ledd er den offentlig oppnevnte advokatens oppdrag begrenset til å vareta «mistenktes interesser i forbindelse med rettens behandling av begjæringen». Tredjepersoners interesser skal likevel tas i betraktning ved at påtalemyndigheten og retten vurderer om metodebruken er forholdsmessig, jf. straffeprosessloven § 170 a. Også tredjepersoners interesser er relevante i denne vurderingen, jf. blant annet Ot.prp. nr. 60 (2004–2005) punkt 6.5.2 side 73. Dessuten må det ved kommunikasjonskontroll og romavlytting som kan berøre et større antall personer foreligge «særlige grunner» for å ta i bruk tvangsmidlet.

Utvalget foreslår at den offentlige oppnevnte advokaten også bør ha som oppgave å vareta tredjepersoners interesser i forbindelse med rettens behandling av begjæringen. Utvalget begrunner dette slik (utredningen punkt 15.5 side 169 og lovutkastet § 100a annet ledd første punktum):

> «Som det fremgår av kapittel 6 mener utvalget også at hensynet til tredjepersoners personvern bør stå sentralt ved avgjørelsen av om bruk av skjulte tvangsmidler skal tillates. Heller ikke disse kjenner til inngrepet, og det er etter dagens regelverk ingen formell ordning som ivaretar tredjepersoners interesser. Utvalget foreslår derfor at den offentlig oppnevnte advokaten etter § 100a også bør ha som oppgave å ivareta tredjepersoners interesser i forbindelse med rettens behandling av begjæringen. Utvalget kan ikke se at mistenkte og tredjepersoner i alminnelighet vil ha slike motstridende interesser at det vil innebære problemer i forhold til advokatens oppdrag.»

Høringsinstansene er delte i synet på om den offentlige advokaten bør vareta tredjepersoners interesser. Enkelte instanser foreslår at det gis adgang til å oppnevne en egen advokat for å vareta tredjepersoners interesser.

Riksadvokaten har i og for seg ikke innvendinger mot at den offentlig oppnevnte advokaten også skal vareta eventuelle tredjepersoners interesser i forbindelse med rettens behandling av begjæringer om bruk av skjulte tvangsmidler, men bemerker at både påtalemyndigheten og retten er forpliktet til å iaktta det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170 a. Riksadvokaten påpeker at hensynet til eventuelle uskyldige tredjepersoner her vil veie tungt. Dessuten vises det til at det ved kommunikasjonskontroll og romavlytting gjelder et tilleggskrav om særlige grunner der et større antall utenforstående kan bli berørt, jf. straffeprosessloven § 216 c annet ledd og § 216 m fjerde ledd annet punktum.

Oslo politidistrikt påpeker at personvernhensyn, og særlig forholdet til uskyldige som rammes av skjulte tvangsmidler, er tillagt stor vekt ved utformingen av hjemlene for skjult tvangsmiddelbruk. Politidistriktet uttaler i den forbindelse:

> «Alle parter i prosessen har i så måte et ansvar for å påse at vilkårene for bruk vurderes nøye før begjæringer fremmes og beslutninger treffes. Å tillegge advokaten et særlig ansvar for andre enn mistenktes interesser mener vi imidlertid igjen er å plassere ansvaret på andre enn der hvor det er ment å høre hjemme. Ansvaret for forholdsmessigheten av inngrepet ligger hos domstolen, og her må også ansvaret for å ivareta tredjepersoners interesser ligge. Vi kan ikke se at utvalget har anført noen slike særlige omstendigheter, kun en generell henvisning til betydningen av fokus på personvern. Etter vår oppfatning preges forslaget også her av manglende fokus på domstolene, og et for stort

fokus på advokaten som en rettssikkerhetsgaranti. For øvrig mangler utvalgets forslag en nærmere konkretisering av hva som eventuelt skal ligge i advokatens oppgave i forhold til tredjeperson. Kan hun for eksempel kunne anke på vegne av en tredjeperson osv?»

Politidirektoratet er enig med Oslo politidistrikt i at utvalgets forslag innebærer en ny og ukjent rolle for den offentlig oppnevnte advokaten. Det påpeker at det er uklart hvorvidt advokaten er tiltenkt noen formell rolle overfor berørte tredjepersoner. For øvrig uttaler direktoratet:

«Politidirektoratet er enig i at hensynet til eventuelt berørte tredjepersoner med fordel kan styrkes, men at et slikt ansvar naturlig vil måtte tillegges domstolen som kontrollør og godkjenner av tvangsmiddelbruken. Manglende opplysninger fra påtalemyndighetens side om eventuelle konsekvenser for berørte tredjepersoner vil kunne være et forhold som kan medføre at begjæringen ikke tas til følge.»

Forsvarergruppen av 1977 finner utvalgets forslag fornuftig, men foreslår at det også gis åpning for å oppnevne en egen offentlig advokat for berørte tredjepersoner. Forsvarergruppen uttaler i den forbindelse:

«En er enig i at mistenkte og tredjepersoner i alminnelighet ikke vil ha motstridende interesser, men det kan tenkes tilfeller der det skjulte tvangsmiddelet berører tredjepersoner i så stor grad at disse bør ha en egen partsrepresentant, eksempelvis ved overvåkning rettet mot privat sted – som foreslås tillatt av utvalget – over lengre tid, og som regelmessig oppsøkes av en fast krets av tredjepersoner. En vil videre kunne tenke seg at i enkelte få tilfelle må etterforskningshensynet vike, ikke grunnet hensynet til mistenktes rettssikkerhet og personvern, men nettopp av hensyn til utenforståendes personvern. Det vil i slike tilfelle kunne være fare for at hensynet til tredjepersoner vil få en subsidiær oppmerksomhet for den advokat som er oppnevnt som partsrepresentant for en mistenkt.»

Også *KROM* er opptatt av å vareta tredjepersoners interesser, men finner det problematisk at samme advokat skal vareta alle berørtes interesser. Foreningen foreslår derfor at det oppnevnes en egen bistandsadvokat med oppgave å vareta uskyldig tredjeparter som blir berørt av inngrepet.

Ettersom flere av de skjulte metodene i stor grad er inngripende også for tredjepersoner, ser d e p a r t e m e n t e t viktigheten av at også deres interesser varetas. Det kan argumenteres med at tredjepersons interesser blir tilstrekkelig varetatt gjennom forholdsmessighetsvurderingen og kravet til særlige grunner hvor en kommunikasjonskontroll eller romavlytting kan berøre et større antall personer, se ovenfor. I tillegg vil den offentlig oppnevnte advokaten i praksis fremsette innsigelser basert på tredjepersoners forhold, for å kunne vareta mistenktes interesser. Departementet har likevel tro på at en lovfesting av at den offentlige advokaten skal trekke inn tredjepersoners interesser kan ha en viss betydning for å gi domstolene et bredest mulig overblikk. En slik lovfesting vil ikke innebære noen formell rolle overfor eventuelle berørte tredjepersoner, og vil i praksis antakelig skille seg lite fra hvordan § 100 a-oppdraget allerede utføres i dag. Det foreslås etter dette lovfestet at den offentlige advokaten også skal vareta tredjepersoners interesser, se lovforslaget til straffeprosessloven § 100 a annet ledd første punktum med merknader.

For øvrig finner departementet at forslaget fra Forsvarergruppen av 1977 og KROM om å oppnevne en egen advokat for tredjepersoner fører for langt.

6.6.6 Begrenset adgang til senere forsvareroppdrag

Etter straffeprosessloven § 100 a fjerde ledd kan retten ved kjennelse beslutte at den offentlig oppnevnte advokaten ikke kan opptre som forsvarer senere i saken.

I Ot.prp. nr. 64 (1998–99) punkt 8.10.7 side 84 ble regelen begrunnet slik:

«En advokat som har blitt oppnevnt i en kommunikasjonskontrollsak, vil kunne komme i en vanskelig situasjon hvis han senere oppnevnes som forsvarer for den mistenkte i straffesaken fordi han ofte vil sitte inne med opplysninger som ikke kan bringes videre til klienten. Derfor bør det, som i Danmark, gjelde en regel om at retten kan bestemme at forsvareren ikke senere kan opptre som forsvarer for den mistenkte i samme sak. Men noe absolutt forbud bør ikke gjelde. Hvis den mistenkte gjennom dokumentinnsyn får de samme opplysninger som forsvareren, vil det ikke være særlig betenkelig at advokaten fortsetter som forsvarer.»

Utvalget foreslår at det uttrykkelig skal fremgå av lovteksten at en begrensning i den offentlig oppnevnte advokatens adgang til å påta seg forsvareroppdrag i samme sak ikke strekker seg lenger enn til tidspunktet hvor mistenkte gjennom dokumentinnsyn får de samme opplysninger som forsvareren, altså også de opplysninger forsvareren har fått som tidligere offentlig oppnevnt advokat etter straffeprosessloven § 100 a, se utredningen punkt 15.5 side 169 og lovutkastet § 100 a fjerde ledd.

De *høringsinstansene* som har uttalt seg er samstemte om at den offentlig oppnevnte advokaten ikke nødvendigvis bør ta oppdrag som forsvarer senere i saken.

Oslo politidistrikt har ingen innvendinger til utvalgets forslag, og forstår det slik at en advokat etter beslutning fra retten ikke senere skal kunne være forsvarer i en kommunikasjonskontrollsak som inneholder opplysninger som unntas fra dokumentinnsyn etter straffeprosessloven § 242 a mv.

Gudbrandsdal politidistrikt er av den oppfatning at skillet mellom oppnevnte advokater etter straffeprosessloven § 100 a og offentlig oppnevnte forsvarere bør være skarpere enn i dag, og uttaler:

> «Vi mener at det er uheldig at samme advokat kan opptre som advokat etter 100 a i en sak og være offentlig oppnevnt forsvarer i en senere sak mot det samme miljøet, da problemstillingene rundt informanter/kilder kan være identiske.»

Kripos gir uttrykk for at den offentlig oppnevnte advokaten ikke bør være forsvarer i den åpne saken hvor det i rettsmøte om metodebruken har fremkommet taushetsbelagte opplysninger ut over det som fremgår av de skriftlige dokumentene, og viser til at dette vil stille advokaten i en vanskelig situasjon. Videre hevder Kripos at den offentlig oppnevnte advokaten ikke kan opptre som forsvarer, dersom dokumenter som danner direkte grunnlag for iverksettelse av den skjulte etterforskningen (inngangsinformasjon) ikke skal anses som «sakens dokumenter».

Politidirektoratet tiltrer i det vesentlige uttalelsene som er gjengitt ovenfor.

Som høringsinstansene har påpekt og som ble lagt til grunn i Ot.prp. nr. 64 (1998–99) punkt 8.10.7 side 84, ser departementet at det kan det være gode grunner til at oppdraget som offentlig oppnevnt advokat i enkelttilfeller bør stenge for senere oppnevning som forsvarer i samme sak. Departementet er imidlertid fortsatt av den oppfatning at advokatens kjennskap til informasjon som mistenkte ikke får innsyn i, ikke uten videre bør stenge for senere forsvareroppdrag, slik høringsinstansene synes å ta til orde for. Beslutningen her bør fortsatt være gjenstand for rettens skjønn, men det bør særlig være aktuelt å vurdere stengning for senere forsvareroppdrag i de situasjonene Oslo politidistrikt og Kripos nevner.

Departementet er videre enig med utvalget i at det ikke er grunn til å stenge for tjenestegjøring som forsvarer når mistenkte får samme opplysninger som forsvareren har kjennskap til gjennom sin tidligere rolle som offentlig oppnevnt advokat etter straffeprosessloven § 100 a, se lovforslaget § 100 a fjerde ledd annet punktum.

6.6.7 Oppnevnelse av advokat i flere sakstyper

6.6.7.1 Gjeldende rett

Offentlig advokat etter straffeprosessloven § 100 a oppnevnes i saker om skjult ransaking (§ 200 a), personnær teknisk sporing (§ 202 c), utsatt underretning om båndlegging av formuesgoder (§ 202 e), utsatt underretning om beslag (§ 208 a), utsatt underretning om utleveringspålegg (§ 210 a og § 210 c), kommunikasjonskontroll (§§ 216 a og 216 b) og romavlytting (§ 216 m), samt ved enkelte avgjørelser om innsyn og bevisavskjæring (§ 242 a, § 264 sjette ledd, § 267 første ledd tredje punktum og § 292 a).

Oppnevning skal også skje når tvangsmidlene benyttes i Politiets sikkerhetstjenestes forebyggende virksomhet etter politiloven § 17 d, jf. politiloven § 17 e, og hvor inngrepet foretas for å avverge alvorlig kriminalitet etter straffeprosessloven § 222 d, jf. Ot.prp. nr. 60 (2004–2005) side 144.

Plikten til å oppnevne offentlig advokat gjelder derimot ikke i saker om skjult kameraovervåking på offentlig sted etter straffeprosessloven § 202 a og heller ikke i saker om teknisk sporing på objekt, jf. straffeprosessloven § 202 b.

6.6.7.2 Metodekontrollutvalgets forslag

Utvalget foreslår at plikten til å oppnevne offentlig advokat etter straffeprosessloven § 100 a utvides til å omfatte *alle* saker om bruk av skjulte tvangsmidler, dvs. også skjult kameraovervåking på offentlig sted og teknisk sporing på objekt, se utredningen punkt 15.5 side 169 og lovutkastet § 100 a første ledd første punktum.

Forslaget om å innføre plikt til å oppnevne offentlig advokat ved kameraovervåking begrun-

nes med at utvalget i tillegg foreslår at det klargjøres i loven at skjult kameraovervåking på offentlig sted også kan rettes mot privat sted, og at kameraovervåking etter omstendighetene kan finne sted på privat sted, unntatt i privat bolig, se punkt 12.6.

6.6.7.3 Høringsinstansenes syn

De få høringsinstansene som har uttalt seg om forslaget om oppnevning av advokat ved skjult kameraovervåking, synes enige i at dette forslaget fører noe for langt. Også forslaget om å oppnevne offentlig advokat ved teknisk sporing på objekt møter motstand hos disse høringsinstansene.

Riksadvokaten er i tvil om behovet for offentlig advokat ved behandling av begjæring om skjult kameraovervåking på offentlig sted, og uttaler:

> «Det er mulig slik oppnevning bør begrenses til begjæringer om fjernsynsovervåking på *privat sted,* jf. utvalgets utkast til ny § 202a annet ledd flg. Skjult fjernsynsovervåking på eller fra offentlig sted etter bestemmelsens første ledd kan ikke anses særlig inngripende, noe straferammekravet på fengsel i mer enn 6 måneder gjenspeiler.»

Oslo politidistrikt mener at oppnevning av advokat etter § 100 a bør begrenses til overvåking av privat sted, og får støtte av *Politidirektoratet.*

Videre er høringsinstansene kritiske til forslaget om at den offentlige advokaten skal oppnevnes ved teknisk sporing etter straffeprosessloven § 202 b. *NAST* finner dagens ordning betryggende, og går imot forslaget. Embetet påpeker at teknisk sporing i medhold av straffeprosessloven § 202 b hovedsakelig benyttes samtidig med spaning, og uttaler i den forbindelse:

> «Forslaget om i stedet å legge beslutningskompetansen til retten med oppnevning av forsvarer etter strpl. § 100a, er derfor en endring som innebærer at det blir vanskelig å iverksette metodene samtidig. Spaning skal jo fortsatt være en operativ politimetode. Dermed bortfaller i stor grad formålet med å kunne bruke teknisk sporing.
>
> Det kan og bemerkes at spørsmålet om beslutningskompetanse for å iverksette teknisk sporing med hjemmel i strpl. 202b ble drøftet i Ot.prp.nr 64 (1998-99), og Departementet kom den gang til at det var både forsvarlig og praktisk at kompetansen lå hos påtalemyndigheten i politiet. Dette ut fra forståelsen av at hjelpemiddelet først og fremst ville være et nyttig middel i forbindelse med spaning for å få kontroll på det aktuelle objekt. En slik beslutning må som hovedregel treffes raskt, og det vil kun unntaksvis være tid til forelegge saken for retten på forhånd. Teknisk sporing med hjemmel i § 202b må og sies å være et mindre inngripende tvangsmiddel, særlig når det plasseres på gjenstander som for eksempel inneholder narkotika som er det vanligste. Embetet kan ikke se at det er fremkommet vektige argumenter som tilsier at dette bør endres og at beslutningskompetansen bør legges til retten.»

Av de samme grunner går *Oslo politidistrikt*, med støtte fra *Politidirektoratet*, og *Riksadvokaten* imot forslaget. *Riksadvokaten* uttaler følgende:

> «Oppnevning av offentlig advokat ved skjult etterforsking som ikke involverer domstolene, ville være noe helt nytt, og kan ikke støttes herfra. […] Det er for eksempel ikke sagt noe om hvem som i tilfelle skal oppnevne advokaten, om advokaten skal kunne bringe påtalemyndighetens beslutning inn for retten for etterprøving eller om den skal kunne påklages til overordnet påtalemyndighet etc.»

Både *Riksadvokaten, NAST* og *Oslo politidistrikt* påpeker at det i utvalgets utkast til endringer i § 202 b ikke fremkommer at kompetansen skal legges til retten.

6.6.7.4 Departementets vurdering

Som det fremgår av proposisjonen punkt 12.5.3 og 12.6.3 om kameraovervåking, slutter departementet seg til utvalgets forslag om å presisere at skjult kameraovervåking på offentlig sted kan rettes mot privat sted, samt å åpne for slik overvåking også på privat sted, unntatt i private hjem. Dette reiser spørsmål om det også – slik utvalget foreslår – bør innføres regler om oppnevning av advokat for mistenkte i denne sakstypen. Etter departementets syn har et slikt forslag gode grunner for seg.

Departementet er samtidig enig med Riksadvokaten i at det ville føre for langt å innføre en regel om at det skal oppnevnes advokat i alle saker om skjult kameraovervåking. Dette skyldes at slik overvåking må anses som mindre inngripende enn øvrige tvangsmidler hvor § 100 a-advokat oppnevnes, noe som også illustreres av det lave kriminalitetskravet i straffeprosessloven

§ 202 a første ledd. Skjult kameraovervåking på offentlig sted kan dessuten iverksettes når det foreligger «skjellig grunn til mistanke om en eller flere straffbare handlinger», altså uten noe krav om at mistanken må rette seg mot en eller flere bestemte personer. Dette gjør at det ikke alltid vil være noen mistenkt hvis interesser den offentlig oppnevnte advokaten skal ivareta. Departementet går på denne bakgrunn inn for at forslaget om oppnevning av advokat begrenses til å gjelde skjult kameraovervåking på privat sted, jf. lovforslaget § 202 a annet ledd.

Når det gjelder forslaget om at det skal oppnevnes offentlig advokat i saker om teknisk sporing på objekt, presiserer departementet innledningsvis at det ikke forstår utvalget dit hen at det foreslår å flytte myndigheten til å tillate teknisk sporing på objekt til retten, og departementet kan heller ikke se at en slik endring er nødvendig ettersom slik metodebruk utgjør et forholdsvis beskjedent inngrep. Dessuten forutsettes påtalemyndigheten å være objektiv, og det anses generelt forsvarlig å legge kompetansen til å fatte beslutninger om skjulte metoder av mindre inngripende karakter til påtalemyndigheten. Det må også legges vekt på at tillatelse må gis av høyere påtalemyndighet eller politimesteren, jf. straffeprosessloven § 202 b annet ledd.

Departementet ser heller ikke grunnlag for å foreslå at det skal oppnevnes offentlig advokat i denne sakstypen, og kan i vesentlig grad slutte seg til innvendingene som har fremkommet under høringen. Departementet er i den forbindelse enig med Riksadvokaten i at det vil bryte med systematikken i straffeprosessloven å oppnevne offentlig advokat i saker som besluttes av påtalemyndigheten. Dessuten taler argumentene ovenfor om å ikke flytte myndigheten til retten, også for at det ikke synes nødvendig med offentlig oppnevnt advokat i denne sakstypen. Det aktuelle tvangsmiddelet må sies å være av mindre inngripende karakter. Departementet vil på denne bakgrunn ikke gå inn for å utvide ordningen med offentlig oppnevnt advokat til å gjelde teknisk sporing på objekt.

6.6.8 Hvem som bør oppnevnes

Gjeldende rett er ikke til hinder for at advokater som til vanlig arbeider med straffesaker, påtar seg oppdrag etter straffeprosessloven § 100 a. Enkelte *høringsinstanser* tar imidlertid til orde for at advokater som oppnevnes i saker om skjulte tvangsmidler ikke bør ha straffesaker til vanlig. *Oslo Politidistrikt* uttaler følgende:

> «[…] Oslo politidistrikt har tidligere foreslått bruk av advokater som ikke driver med strafferett, og dermed ikke har slike klienter. Vi mener at dette er en god og hensiktsmessig ordning. Selv om advokater vil [...] tilstrebe en korrekt tilnærming [til] slike oppgaver, er det ikke umiddelbart alltid enkelt å ha tilstrekkelig oversikt over en stor klientmengde.»

Gudbrandsdal politidistrikt argumenterer tilsvarende i sin uttalelse:

> «I et så lite strafferettslig miljø som vi har i Norge med til dels nære knytninger mellom en del strafferettsadvokater, mener vi at dette er nødvendig for å hindre at meget ømfintlig informasjon tilflyter det kriminelle miljøet.»

Disse uttalelsene får støtte av *Politidirektoratet.*

Av samme grunner mener *NAST* at det for dette formålet bør etableres en gruppe advokater som ikke arbeider med strafferett til vanlig.

Spørsmålet har ikke vært på høring, og departementet har derfor ikke nå et grunnlag som er tilstrekkelig til å ta endelig stilling til spørsmålet. Uansett ser departementet betenkeligheter knyttet til generelt å stenge for at advokater med verdifull erfaring fra straffesaker kan ta oppdrag etter § 100 a. Mer nærliggende synes det å være at domstolene er særlig nøye med hvem som gis oppdrag som offentlig advokat. Domstolene står fritt til å danne grupper med advokater som anses spesielt egnet for slike formål. Departementet vil følge utviklingen på dette punktet, og eventuelt ta spørsmålet opp til ny vurdering.

6.6.9 Særskilt opplæring av advokater som oppnevnes etter § 100 a

Utvalget foreslår at det gis et særskilt opplæringstilbud til advokater som oppnevnes etter straffeprosessloven § 100 a. Utvalget uttaler følgende (se utredningen punkt 11.7.4 side 134 og punkt 15.5 side 168):

> «I lys av den viktige rolle utvalget mener advokater oppnevnt etter straffeprosessloven § 100 a har og de særlige utfordringer den manglende kontakten med mistenkte oppdraget innebærer, mener utvalget det bør gis et eget opplæringstilbud til de aktuelle advokatene. På utvalgets høringsmøte pekte representanter fra domstolene på at det fremmes få innsigelser fra advokatene. Utvalget har også selv hatt til-

gang til rettens avgjørelser og advokatens merknader til påtalemyndighetens begjæringer i saker om kommunikasjonskontroll og PST-saker ved Oslo tingrett. En gjennomgang av de siste års saker bekrefter tingrettsdommernes inntrykk. Det er ikke sjeldent at advokatens påtegninger lyder: «Jeg har ikke grunnlag for å hevde at begjæringen ikke kan tas til følge». Advokatens oppgave er å fremsette motargumenter slik at saken er best mulig opplyst før dommeren fatter sin avgjørelse. Utvalget mener det er grunn til å sette advokatene bedre i stand til å gjøre dette gjennom et eget opplæringstilbud. Opplæringen kan tenkes organisert som et tilbud gjennom de enkelte domstoler, eller gjennom for eksempel Juristenes Utdanningssenter (JUS). Opplæringen bør være en del av oppdraget som offentlig advokat. Opplæringen bør derfor etter utvalgets syn være obligatorisk og betalt.»

Høringsinstansene uttaler seg ikke om dette forslaget utover det *Romerike politidistrikt* generelt uttaler om ordningen med oppnevnelse av offentlig advokat, se punkt 6.6.1.

D e p a r t e m e n t e t er av den oppfatning at kjennskap til de enkelte sakene, erfaring og praktisk tilrettelegging fra domstolenes og påtalemyndighetens side trolig er det som gjør advokaten best rustet i sin tjeneste. Tilstreber en å oppnevne samme advokat under hele saken, vil advokatenes funksjon som kontrollinstans styrkes, se punkt 6.6.2. Om domstolene i tillegg fordeler oppdragene på en begrenset mengde advokater, vil dette bidra til å styrke den enkeltes kompetanse. Når det så gjelder spørsmålet om praktisk tilrettelegging, er det særlig viktig at domstolene sørger for en arbeidsplass, tilgjengelige kilder for advokaten og tid og mulighet til å gjøre seg kjent med sakens dokumenter. Dessuten kan påtalemyndigheten bidra ved å fremme forlengelsesbegjæringer så tidlig som mulig, se punkt 6.6.3, og effektivt behandle innsynsbegjæringer fra den offentlig oppnevnte advokaten.

Departementet vil samtidig ønske velkommen ethvert initiativ, fra Juristenes utdanningssenter, Den Norske Advokatforening, domstolene eller andre, til særskilt opplæring av advokater som tjenestegjør ved domstolenes behandling av skjulte tvangsmidler. Departementet ser imidlertid ikke nødvendigvis at slik opplæring bør bekostes av det offentlige, og heller ikke at advokatene bør betales av det offentlige for å delta på kurs. Dette er heller ikke ordningen for andre advokatgrupper, som ordinære forsvarere og bistandsadvokater.

På denne bakgrunn går ikke departementet videre med ytterligere tiltak på dette punktet.

6.7 Muntlige forhandlinger

6.7.1 Gjeldende rett

Gjeldende rett oppstiller ikke noe krav om at det avholdes muntlige forhandlinger ved rettens behandling av begjæringer om tillatelse til å ta i bruk skjulte tvangsmidler. Retten kan imidlertid – som ved andre beslutninger som i utgangspunktet avgjøres på bakgrunn av skriftlig behandling – velge å innkalle til rettsmøte på eget initiativ eller på begjæring fra for eksempel den offentlig oppnevnte advokaten.

6.7.2 Metodekontrollutvalgets forslag

Utvalget har gjennomført en undersøkelse blant dommere, advokater, politijurister og statsadvokater, med spørsmål om muntlige forhandlinger ved begjæringer om kommunikasjonskontroll vil kunne forsterke rettssikkerheten til dem som er gjenstand for kontrollen. Utvalget uttaler følgende om resultatene av undersøkelsen (se utredningen punkt 15.6 side 170):

«Et stort flertall av advokatene (ca. 71 prosent) mener at muntlige forhandlinger ved begjæring om kommunikasjonskontroll vil kunne styrke rettssikkerheten for dem som blir kontrollert. Flere av advokatene har gitt uttrykk for at muntlige forhandlinger vil gi bedre mulighet for kontradiksjon og at det sannsynligvis vil føre til at påtalemyndighetens begjæringer og rettens avgjørelser må begrunnes bedre.

Omtrent halvparten av dommerne (ca. 49 prosent) mener at muntlige forhandlinger kan styrke rettssikkerheten. Det er flere av dommerne som har pekt på at muligheten for oppklarende spørsmål og kontradiksjon vil kunne gi et bedre beslutningsgrunnlag. Det er også pekt på at en slik ordning vil kunne virke skjerpende på aktørene. Enkelte dommere har imidlertid motforestillinger mot en slik ordning, særlig at det vil være ressurskrevende og i liten grad tilføre noe nytt.

Blant politijuristene svarte omtrent halvparten (ca. 52 prosent) at muntlige forhandlinger ikke vil bidra til å styrke rettssikkerheten, mens noen færre (ca. 39 prosent) av statsadvokatene svarte det samme. Nærmere halvparten av statsadvokatene (ca. 47 prosent) er imid-

lertid usikre. Mange av politijuristene har utdypet svaret nærmere. Flere peker på at muntlige forhandlinger kan bidra til å opplyse saken bedre og «synliggjøre forhold som dokumentene ikke viser». Motforestillingene går på at en slik ordning vil være upraktisk og ressurskrevende for eksempel i saker der mistenkte skifter telefonnummer ofte. Noen mener også at en slik ordning ikke vil frembringe noe substansielt og kun vil være en form for «skinnrettssikkerhet».

Så vidt utvalget har forstått praktiseres en hovedregel om muntlige forhandlinger blant annet ved tingrettene i Bergen og Trondheim. Utvalget har derfor fått skilt ut svarene fra advokater og politijurister fra Hordaland og Sør–Trøndelag, statsadvokater fra Hordaland og Trøndelag statsadvokatembeter og dommere som sokner til Gulating og Frostating lagmannsrett, og holdt disse opp mot de øvrige respondentene i undersøkelsen.

En sammenlikning av disse respondentene med de øvrige respondentene tyder på at praksisen med muntlige forhandlinger i liten grad påvirker utfall og prosess. Det er for eksempel liten forskjell i anslagene på hvor ofte kommunikasjonskontroll har vært av vesentlig betydning for å oppklare saken. Videre er vurderingene av hvor grundige begjæringene er og i hvilken grad dommerne foretar en reell og grundig vurdering, nokså like i de to gruppene. Derimot er det en betydelig forskjell mellom de to gruppene på spørsmålet om muntlige forhandlinger kan medføre sterkere rettssikkerhet. Svarene fremgår av tabell 15.4 nedenfor.

Tallene tyder på at respondentene fra steder hvor det praktiseres en ordning med muntlige forhandlinger er langt mer positive til en slik ordning enn den øvrige respondentgruppen.»

På denne bakgrunn foreslår utvalget at det som hovedregel skal gjennomføres muntlige forhandlinger ved begjæringer om tillatelse til bruk av skjulte tvangsmidler, se utredningen punkt 15.6 side 171–172. Dette foreslås inntatt i straffeprosessloven § 216 e, og vil gjennom henvisninger gjelde for skjult ransaking (§ 200 a), skjult kameraovervåking (§ 202 a), personnær teknisk sporing (§ 202 c), utsatt underretning om beslag (§ 208 a), utsatt underretning om utleveringspålegg fremover i tid (§ 210 c), kommunikasjonskontroll (§§ 216 a og 216 b) og romavlytting (§ 216 m).

Gjennom henvisningen i straffeprosessloven § 222 d femte ledd vil en lovendring som foreslått også gjelde skjulte tvangsmidler som benyttes i avvergende øyemed. Utvalget sier ikke noe direkte om forslaget er ment å omfatte skjulte tvangsmidler som benyttes i forebyggende øyemed, jf. politiloven § 17 d.

Utvalget foreslår at muntlige forhandlinger bør kunne unnlates dersom «retten finner det klart at slik behandling ikke er nødvendig for sakens opplysning», se lovutkastet til endringer i straffeprosessloven § 216 e.

6.7.3 Høringsinstansenes syn

Et flertall av de høringsinstansene som har uttalt seg på dette punktet er negative til en hovedregel om at det skal avholdes muntlige forhandlinger ved begjæringer om tillatelse til å ta i bruk skjulte tvangsmidler. Dette gjelder *Riksadvokaten, NAST, Oslo statsadvokatembeter, Politidirektoratet, Kripos, PST, Oslo politidistrikt, Søndre Buskerud politidistrikt* og *Politiets fellesforbund*. Flere av instansene argumenterer med at en hovedregel om muntlige forhandlinger fremstår som unødvendig, og at dagens ordning gir god nok rettssikkerhet.

Både Riksadvokaten, NAST, Politiets sikkerhetstjeneste og *Kripos* viser til at gjeldende rett allerede gir adgang til å avholde muntlige forhandlinger. *Riksadvokaten* uttaler i den forbindelse:

> «Det bør fortsatt være opp til retten å avgjøre om det skriftlige materialet som foreligger i en sak gir et tilstrekkelig beslutningsgrunnlag eller om muntlige forhandlinger er nødvendig.»

Riksadvokaten og *Kripos* understreker dessuten at domstolene står fritt til å innhente skriftlig tilleggsinformasjon og at den offentlig oppnevnte advokaten ved behov kan fremsette begjæring om innsyn i flere av sakens dokumenter. *Kripos* viser i tillegg til at domstolene kan ta telefonisk kontakt med påtalemyndigheten dersom noe i begjæringen fremstår som uklart.

Riksadvokaten og *Kripos* legger videre til grunn at begjæringen i praksis utgjør tilstrekkelig grunnlag for rettens vurdering. *Riksadvokaten* uttaler:

> «Alle kommunikasjonskontroll- og romavlyttingsaker i landet innberettes fortløpende til riksadvokaten. Erfaringen er at retten i saker som avgjøres på grunnlag av skriftlig materiale svært sjelden etterspør ytterligere informasjon fra politiet. Tilsvarende gjelder for advokatene. En naturlig slutning er at begjæringen og

> grunnlagsmaterialet for øvrig, sammen med advokatens anførsler, gjennomgående gir et tilstrekkelig og sikkert grunnlag for rettens avgjørelse.»

I samme retning gir *PST* uttrykk for at det i dag finnes gode rutiner for samhandlingen med retten og at det skrives utfyllende anmodninger og begjæringer.

Dessuten viser *Kripos* til den kontrollfunksjonen som er tillagt kommunikasjonskontrollutvalget.

For øvrig peker både *Riksadvokaten, NAST, Politidirektoratet* og *Oslo politidistrikt* på at utvalgets egen undersøkelse gir lite belegg for at muntlige forhandlinger på dette stadium i strafforfølgningen påvirker prosessen og utfallet av saken.

Riksadvokaten, Søndre Buskerud politidistrikt og *Politiets Fellesforbund* er videre av den oppfatning at en ordning som foreslått vil kunne medføre forsinkelser i rettens behandling, og fremhever viktigheten av at begjæringer om skjulte tvangsmidler behandles raskt, slik at verdifull informasjon ikke går tapt. *Riksadvokaten* og *Søndre Buskerud politidistrikt* fremhever at risikoen for at muntlige forhandlinger vil forsinke saken vil øke dersom en viderefører forslaget om at samme advokat så langt som mulig skal bistå ved samtlige begjærer mot mistenkte i samme sak og for hele perioden tvangsmidlene er i bruk, jf. punkt 6.6.2.

Oslo politidistrikt er av den oppfatning at en ordning som foreslått vil vidløftiggjøre sakene. Politidistriktet uttaler i den forbindelse:

> «[…] Aktor vil normalt ikke ha noe å tilføye ut over begjæringen, og vitneførsel vil etter vår mening være lite ønskelig. Det mest nærliggende ville i så fall være å innkalle den eller de som hadde skrevet aktuelle rapporter som vitne(r). Ofte vil imidlertid dette være personer som bare har hatt som oppgave å samle de aktuelle opplysninger i en rapport. Kildene til opplysningene – de som har overhørt samtaler, iakttatt bevegelser eller på annen måte fått informasjonen vil være flere, og normalt andre enn rapportskriver. Det kan i så fall bli en rekke personer som må innkalles dersom den enkelte skal forklare seg om hva han har iakttatt eller erfart. Det kan medføre en omstendelig bevisførsel, nærmest en «hovedforhandling», hvilket ikke kan antas å ha vært lovgivers mening. Det vises i den anledning til Ot.prp.nr. 64 (1998–99) hvor det på s. 83 vedrørende kommunikasjonskontroll er uttalt «....For at kommunikasjonskontroll skal være et mest mulig effektivt etterforskningsmiddel, bør rettens avgjørelse treffes så raskt som mulig og forsvarlig».»

Riksadvokaten, Kripos og *Søndre Buskerud politidistrikt* påpeker også at de foreslåtte endringene kan lede til at påtalemyndigheten i flere saker benytter seg av hastekompetansen, og gir uttrykk for at det ikke vil være en ønsket utvikling. *Kripos* uttaler i den forbindelse:

> «En praktisk konsekvens kan være at det tar lengre tid før retten kan vurdere gyldigheten av en hurtigordre. Dette er i så fall uheldig, siden lovgiver har forutsatt at slike begjæringer skal fremlegges for retten så snart som mulig.»

Politidirektoratet, NAST og *Politiets Fellesforbund* er videre samstemte om at forslaget ikke kan forsvares opp mot de kostnader det vil medføre. *Politidirektoratet* uttaler følgende:

> «Politidirektoratet er enig i at en hovedregel om muntlige forhandlinger kan fremstå som et aktuelt tiltak for å styrke kontradiksjonen om påtalemyndighetens begjæring om bruk av tvangsmidler. Direktoratet er likevel svært usikker på i hvilken utstrekning en slik regel i praksis vil tilføre mistenkte/siktede et signifikant rettsikkerhetsmessig bidrag, samtidig som de økonomiske og administrative konsekvensene fremstår som relativt betydelige. At rettsikkerhet koster er et anerkjent faktum. Politidirektoratet mener likevel at det her, som ellers, går en grense for når den samfunnsmessige nytten av ytterligere tiltak blir marginal sett opp mot kostnaden.»

I samme retning uttaler *NAST*:

> «Selv om ethvert tiltak for å bedre rettssikkerheten i utgangspunktet må vurderes som positivt, må også tiltakets praktiske konsekvenser tas i betraktning. Innføring av en hovedregel om å ha muntlige forhandlinger ved beslutning om hemmelig tvangsmiddelbruk, vil få store ressursmessige konsekvenser. I en operativ etterforskingsfase fremmes det vanligvis et stort antall begjæringer, og muntlige forhandlinger vil medføre en belastning på de som har ansvaret for saken, herunder politi og påtalemyndighet. Særlig vil det binde opp uforholdsmessig mye tid for politiet i en hektisk hverdag. Dertil er det risiko for vidløftiggjøring av

behandlingen av begjæringene, noe som forsterkes av uklarheten omkring rekkevidden av innsynsretten i den foreliggende straffesak.

Som en oppsummering savner NAST et dokumentert behov for å snu dagens hovedregel for behandling av slike begjæringer. Siden ulempene kan bli betydelige fremstår det som uklart om målet om bedret rettsikkerhet nås, idet svekket effektivitet i politiets arbeid også har omkostninger for rettssikkerheten.»

Også *Riksadvokaten, Kripos, Oslo politidistrikt* og *Søndre Buskerud politidistrikt* fremhever at en hovedregel om å avholde muntlige forhandlinger vil ha betydelig ressursmessige konsekvenser. *Riksadvokaten* viser i den forbindelse til at det i operative og hektiske faser under den skjulte etterforskningen i løpet av kort tid kan fremsettes et stort antall begjæringer. Både *Politidirektoratet* og *Oslo statsadvokatembeter* peker på at kostnadene knyttet til forslaget ikke er nærmere vurdert av utvalget.

En annen innsigelse, som fremmes av *Riksadvokaten* og *Oslo statsadvokatembeter*, er at muntlige forhandlinger kan svekke muligheten til notoritet og etterkontroll. *Oslo statsadvokatembeter* uttaler i den forbindelse:

«Det bør i denne sammenheng nevnes at retten, i mange sammenhenger, har en begrenset mulighet til å etterprøve det faktiske bevismaterialet som ligger til grunn for begjæringer om f. eks. kommunikasjonskontroll. Ved en skriftlig behandling vil en i det minste sikre notoritet omkring begjæringen og det faktiske grunnlaget for denne. Utvalget har påpekt at domstolene ikke sjelden anvender standardformuleringer i sine begrunnelser som kan vanskeliggjøre overprøvning, jfr. kap. 15.8 (side 172). Ved muntlige forhandlinger kan grunnlaget for overprøving bli ytterligere svekket, og etter vår oppfatning må det vurderes å innføre begrunnelseskrav som går utover dagens ordning. Etter vår vurdering bør man heller fastsette skriftlig behandling som hovedregel, dog slik at retten kan beslutte å avholde muntlig forhandling når dette ansees nødvendig.»

Oslo politidistrikt ser også en annen utfordring ved å avholde muntlige forhandlinger i saker om skjulte tvangsmidler, og uttaler:

«For øvrig vil tjenestepersoner lett kunne tenkes å komme i vanskelige situasjoner dersom det stilles spørsmål om forhold man bevisst har valgt å ikke utdype i en rapport (typisk informant- /kildesensitiv informasjon). Rapporter utarbeidet i anledning begjæring om tvangsmiddelbruk, vil ofte være et resultat av grundige og vanskelige vurderinger hva gjelder bruk av informasjon, og muntlige forhandlinger og vitneavhør vil gjøre det vanskeligere å ha kontroll over denne informasjonsbruken.»

Domstoladministrasjonen støtter forslaget og uttaler følgende:

«Domstoladministrasjonen er prinsipielt enig i at en hovedregel om muntlige forhandlinger vil bedre rettens grunnlag for å treffe beslutninger i disse sakene, herunder å foreta en reell og selvstendig vurdering av begjæringene. Blant annet anses det viktig at forsvareren på denne måten gis bedre reell mulighet til kontradiksjon. Derfor tiltres forslaget med den mulighet for unntak som også er foreslått.»

Oslo tingrett har ikke innvendinger mot forslaget, men fremhever at det må tas høyde for at det ved en rekke begjæringer vil være upraktisk og unødvendig med muntlige forhandlinger:

«Dette kan være tilfelle hvor mistenkte bytter telefon og det er nødvendig med ny tillatelse fra retten. Videre bør det kunne gjøres unntak fra muntlige forhandlinger ved forlengelse av tvangsmiddelbruken. Vi er derfor enig i forslaget om at det kan gjøres unntak fra hovedregelen om muntlige forhandlinger hvor retten finner det *klart* at slik behandling ikke er nødvendig for sakens opplysning.»

Domstoladministrasjonen og *Oslo tingrett* peker begge på at forslagene for domstolenes vedkommende vil medføre økt ressursbruk. *Oslo tingrett* viser dessuten til at Oslo tinghus i dag ikke er rustet for å gjennomføre muntlige forhandlinger i saker som kommer fra Politiets sikkerhetstjeneste.

For øvrig får utvalgets forslag støtte fra *Forsvarergruppen av 1977,* som tror en hovedregel om muntlige forhandlinger vil bidra vesentlig til å bedre domstolskontrollen på feltet, og fra *KROM,* som viser til at det vil virke skjerpende og legge til rette for kontradiksjon.

6.7.4 Departementets vurdering

Departementet ser at en hovedregel om muntlige forhandlinger vil kunne gjøre det enklere for dom-

meren og den offentlig oppnevnte advokaten å få avklart eventuelle uklare sider ved begjæringene, og at advokaten vil kunne få en lavere terskel for å fremme innsigelser mot begjæringen. Som flere av høringsinstansene har påpekt, finner imidlertid departementet at slike hensyn ikke fullt ut kan veie opp for innvendingene mot en slik ordning. En viktig innvending mot forslaget er etter departementets syn at muntlige forhandlinger kan forsinke gjennomføringen av et tvangsmiddel, slik at metodenes effektivitet svekkes. Dette vil videre kunne ha som følge at påtalemyndighetens hastekompetanse brukes i større utstrekning enn ønskelig. Som påpekt av Riksadvokaten og Oslo statsadvokatembeter kan dessuten en hovedregel om muntlige forhandlinger svekke notoriteten omkring en begjæring og muligheten for etterkontroll.

Det er videre grunn til å fremheve at dagens ordning i stor grad legger til rette for at saker om skjulte tvangsmidler blir tilstrekkelig belyst. Etter gjeldende rett kan dommeren innkalle til muntlige forhandlinger ved behov. Dessuten forutsettes den offentlig oppnevnte advokaten å begjære muntlige forhandlinger dersom det synes nødvendig av hensyn til sakens opplysning. Både retten og den offentlig oppnevnte advokaten kan i tillegg som regel få innsyn i sakens øvrige dokumenter. Departementet peker også på at den offentlig oppnevnte advokatens reelle mulighet for kontroll vil styrkes dersom samme advokat oppnevnes ved begjæringer om forlengelser mv., se punkt 6.6.2.

For øvrig finner departementet at utvalgets undersøkelse i begrenset grad tilsier at en ordning med muntlige forhandlinger påvirker utfall og prosess i sakene. Departementet går på denne bakgrunn ikke inn for å videreføre utvalgets forslag.

6.8 Tillatelsens varighet og forlengelse av tillatelsen

Det følger av det generelle kravet om forholdsmessighet i straffeprosessloven § 170 a at det ikke må gis tillatelse til tvangsmidler som varer over et visst tidsrom – det vil si teknisk sporing, kommunikasjonskontroll og romavlytting – for en lengre periode enn strengt nødvendig. Dette er også uttrykkelig presisert i straffeprosessloven § 202 c fjerde ledd og § 216 f første ledd.

Tillatelse gis for inntil fire uker om gangen, med mulighet for forlengelse. Gjelder mistanken overtredelse av straffeloven kapittel 17 (vern av Norges selvstendighet og andre grunnleggende nasjonale interesser), kan imidlertid tillatelse til kommunikasjonskontroll og romavlytting gis for inntil åtte uker av gangen dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter fire uker vil være uten betydning.

Dersom vilkårene ikke lenger antas å være til stede eller dersom inngrepet ikke lenger anses hensiktsmessig, skal kontrollen stanses før utløpet av fristen som er satt i rettens kjennelse, jf. straffeprosessloven § 202 c fjerde ledd tredje punktum og § 216 f annet ledd. Det samme følger av det generelle kravet om forholdsmessighet i straffeprosessloven § 170 a.

Utvalget foreslår ikke endringer i dagens regler om varighet og forlengelse av skjulte tvangsmidler, men understreker viktigheten av at det fortløpende vurderes om det er grunnlag for fortsatt bruk av tvangsmiddelet, se utredningen punkt 15.7 side 172. Utvalget oppfordrer for øvrig til at det fra sentralt hold gis tilsvarende retningslinjer om kommunikasjonskontroll som for romavlytting.

Bare *NAST* har uttalt seg om utvalgets vurderinger på dette punktet. Embetet er enig i utvalgets konklusjon om at det ikke er hensiktsmessig å endre gjeldende rett på dette punktet.

D e p a r t e m e n t e t slutter seg til utvalgets vurderinger, og finner ikke grunn til å foreslå endringer på dette punktet.

6.9 Krav til rettens begrunnelse

Retten avgjør begjæringer om bruk av skjulte tvangsmidler ved kjennelse. Straffeprosessloven § 52 fastslår at «kjennelser skal ha grunner». I Rt. 2010 side 1269 uttaler Høyesteretts ankeutvalg generelt om dette kravet:

> «Normalt er det etter denne bestemmelse tilstrekkelig at det fremgår av kjennelsesgrunnene at de spørsmål som saken reiser, er vurdert. Forholdene kan imidlertid ligge slik an at det kan være nødvendig med en mer omfattende begrunnelse, jf. Rt-1998-1081, Rt-1999-475 og Rt-2000-371.»

I Ot.prp. nr. 64 (1998–99) side 145 uttalte departementet følgende om begrunnelseskravet i relasjon til den offentlig oppnevnte advokatens mulighet til å begjære kjennelsen overprøvd:

> «Forsvareren kan påkjære rettens kjennelse, jf *tredje punktum*. For at denne retten ikke skal bli illusorisk, må begrunnelsen i kjennelsen

være slik at det er mulig å etterprøve om vilkårene for tvangsmidlet 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.»

I samme proposisjon punkt 8.10.7 side 84 kom departementet til at det foreløpig ikke var grunn til å skjerpe kravene til begrunnelse i telefonkontrollsaker. Det ble uttalt følgende:

«[…] Etter departementets syn vil en ordning med forsvarer for den mistenkte bidra til at flere sider av saken kommer frem. Det vil igjen kunne prege rettens begrunnelse. Man bør derfor se an den nye ordningen før det eventuelt vurderes å endre kravene til begrunnelse.»

Utvalget er av den oppfatning at rettens begrunnelser i kjennelser som tillater bruk av skjulte tvangsmidler gjennomgående er for knappe, og at departementets forutsetninger i Ot.prp. nr. 64 (1998–99) ikke synes fulgt opp, se utredningen punkt 15.8 side 172–173. Utvalget finner det imidlertid ikke hensiktsmessig å foreslå lovfesting av et skjerpet begrunnelseskrav. Utvalget viser i den forbindelse til at kravet til begrunnelse vil kunne variere fra sak til sak, og at hvilke krav som gjelder bør fastlegges i rettspraksis.

Det fåtall *høringsinstanser* som har uttalt seg her, er uenige i om det bør innføres et skjerpet begrunnelseskrav i saker om skjulte tvangsmidler.

Forsvarergruppen av 1977 slutter seg til utvalgets vurderinger og forslag.

I motsatt retning beklager *Datatilsynet* at utvalget ikke foreslår å lovfeste et skjerpet krav til rettens begrunnelse for å tillate bruk av skjulte tvangsmidler. Tilsynet viser til viktigheten av at domstolene foretar en selvstendig, reell og forsvarlig proporsjonalitetsvurdering i det enkelte tilfellet, og er av den oppfatning at et skjerpet krav til begrunnelse vil kunne sikre at domstolene rent faktisk foretar en selvstendig vurdering og sørge for at vurderingene er dokumenterte.

Oslo statsadvokatembeter er av den oppfatning at det må vurderes å innføre begrunnelseskrav som går utover dagens ordning.

Siden skjulte tvangsmidler utgjør et særlig inngrep i personvernet til dem som er gjenstand for metodebruken, vil departementet fremheve viktigheten av at kjennelser som tillater bruk av skjulte tvangsmidler gir konkrete og grundige begrunnelser for hvorfor vilkårene for metodebruken anses å være oppfylt i den enkelte sak. I likhet med utvalget, vil departementet likevel ikke foreslå endringer på dette punktet. I den forbindelse må det tas i betraktning at den offentlig oppnevnte advokaten har et særlig ansvar for å anke kjennelser som ikke holder mål. Departementet mener at advokatens rolle vil styrkes dersom forslaget om å oppnevne samme advokat for alle begjæringer om skjulte tvangsmidler i samme sak vedtas, siden advokaten vil gis en totaloversikt over tvangsbruken i saken, se punkt 6.6.2.4. Samtidig kan en frist for påtalemyndigheten til å begjære forlengelser med varsel til advokaten gjøre advokaten bedre i stand til å ha et kritisk blikk på rettens kjennelse, se punkt 6.6.3. Dette vil igjen kunne gi grundigere begrunnelser som kan knyttes til den enkelte sak. Departementet går på denne bakgrunn ikke inn for å skjerpe kravene til begrunnelse i kjennelser som tillater bruk av skjulte tvangsmidler.

6.10 Underretningsplikt

6.10.1 Gjeldende rett – oversikt

Det er avgjørende for de skjulte metodenes effektivitet at mistenkte ikke skal ha kunnskap om dem mens de pågår. Tillatelse til metodebruken gis derfor uten at mistenkte og andre som måtte rammes av metodebruken, gis adgang til å uttale seg, og kjennelsen blir ikke meddelt dem. For de fleste skjulte tvangsmidler skal imidlertid mistenkte underrettes når tvangsmiddelbruken er opphørt, se straffeprosessloven § 202 c femte ledd om personnær teknisk sporing og § 208 første ledd om beslag. Det samme følger forutsetningsvis av §§ 200 a, 210 a og 210 c hva gjelder henholdsvis skjult ransaking, utleveringspålegg og utleveringspålegg fremover i tid. Ved båndlegging av formuesgoder har mistenkte normalt krav på varsel før retten avgjør om påtalemyndighetens beslutning skal opprettholdes, jf. § 202 e. For kommunikasjonskontroll og romavlytting er ordningen en annen – her skjer underretning kun på begjæring, se nærmere nedenfor.

Når det gjelder skjult ransaking, personnær teknisk sporing, beslag, utleveringspålegg og utleveringspålegg fremover i tid, er det gitt adgang til å utsette underretningen dersom det er «strengt nødvendig». I så fall kan *retten* beslutte at underretning utsettes i inntil åtte uker om gangen. I Ot.prp. nr. 64 (1998–99) punkt 13.6 side 111 vurderte departementet denne fristen som såpass lang at den trolig ikke ville skape for store praktiske problemer ved forlengelser, samtidig som

den ikke er uforsvarlig lang. For alle de nevnte tvangsmidlene gjelder det at underretning senest skal gis når tiltale tas ut.

Ved ransaking, beslag og utleveringspålegg kan påtalemyndigheten treffe foreløpig beslutning om utsatt underretning etter reglene om hastekompetanse. Det samme gjelder for personnær teknisk sporing. Er sporingen planlagt å ha en viss varighet, er det imidlertid ikke praktisk å beslutte utsatt underretning i en hasteavgjørelse, siden dennes varighet er begrenset til 24 timer, se punkt 6.4.

Saker om rikets sikkerhet (straffeloven kapittel 17, straffeloven 1902 kapittel 8 og 9) er ansett å stå i en særstilling siden etterforskningen ofte pågår over lang tid, jf. Ot.prp. nr. 64 (1998–99) punkt 13.6 side 111–112. I denne typen saker er derfor kompetansen til å beslutte utsatt underretning ved personnær teknisk sporing, beslag, utleveringspålegg og utleveringspålegg fremover i tid lagt til *påtalemyndigheten*. Den bestemmer hvor lenge underretningen skal utsettes, og er også gitt kompetanse til å beslutte at underretning helt skal unnlates. I nevnte proposisjon er ordningen vurdert å være forsvarlig siden påtalemyndighetens beslutning er gjenstand for kontroll av det stortingsoppnevnte EOS-utvalget. Utsatt underretning ved skjult ransaking er likevel ansett å være såpass inngripende at det må besluttes av retten, jf. § 200 a tredje ledd og Ot.prp. nr. 64 (1998–99) punkt 13.6 side 112. Ved skjult ransaking i saker om rikets sikkerhet kan retten beslutte at underretning kan utsettes for inntil seks måneder om gangen eller unnlates helt, jf. § 200 a annet ledd.

Ved kommunikasjonskontroll og romavlytting er ordningen annerledes – her blir mistenkte underrettet om tvangsbruken når det tas ut tiltale eller på begjæring, jf. straffeprosessloven §§ 264 og 216 j. Underretning etter § 216 j kan tidligst gis ett år etter at kontrollen er avsluttet, jf. annet ledd. I saker om rikets sikkerhet gis det ikke underretning.

Frem til det tas ut tiltale eller mistenkte underrettes etter § 216 j, er § 216 i om taushetsplikt, sammenholdt med § 242 om innsyn, avgjørende for mistenktes kjennskap til kontrollen. Såfremt opplysningene fra den skjulte tvangsbruken ikke er «brukt» i etterforskningen, er dokumentene unntatt fra innsyn, jf. Rt. 2004 side 2023. Dersom materiale fra den skjulte metodebruken ikke brukes som ledd i etterforskning, og det heller ikke tas ut tiltale eller underrettes i medhold av § 216 j, vil mistenkte ikke få underretning om tvangsbruken, jf. også påtaleinstruksen § 17-2 tredje ledd.

I Ot.prp. nr. 64 (1998–99) punkt 8.8.4 side 72–73 begrunner departementet hvorfor reglene her avviker fra det som gjelder for de øvrige skjulte tvangsmidlene:

> «Spørsmålet er om det bør innføres en automatisk plikt til å gi underretning om kommunikasjonskontroller selv om det ikke er tatt ut tiltale. Det vil ikke av § 242 følge noen automatisk plikt til å gi underretning, slik tilfellet er med § 264. Spørsmålet har vært vurdert tidligere, forut for vedtakelsen av § 216j i 1992. I Ot.prp.nr.40 (1991–92) uttaler departementet om spørsmålet (s 36):
>
> «Etter departementets forslag skal underretning bare gis på begjæring. Det er etter departementets syn grunn til å frykte at en regel om automatisk underretning vil kunne ha uheldige konsekvenser ved at personer som driver med narkotikakriminalitet, får et varsel om at de er i politiets søkelys. [..] Departementet ser det som like sannsynlig at et slikt «varsel» ikke fører til annet enn at den kriminelle, dersom han eller hun har konkrete planer om å begå nye narkotikaforbrytelser, tar ytterligere forholdsregler for ikke å bli avslørt, som at vedkommende avstår fra denne typen kriminalitet.»
>
> Disse synspunktene har fortsatt gyldighet. Men hvis underretning ikke skal skje automatisk, vil det bero på store tilfeldigheter om den mistenkte kommer på å begjære underretning eller ikke. Det gjør at effekten med ordningen blir redusert. Derfor er det et spørsmål om det burde innføres en mellomløsning, hvor den mistenkte får krav på underretning senest når forfølgningen mot han innstilles (eller det tas ut tiltale, jf ovenfor).
>
> Det kan godt være at påtalemyndigheten fortsatt mener at det er grunn til å mistenke vedkommende, men finner at bevisene ikke vil holde i retten. Selv om forfølgningen innstilles, kan det være at den mistenkte blir holdt under oppsikt. Det kan da være uheldig om han blir klar over kommunikasjonskontrollen. Rettssikkerheten er her etter departementets syn tilstrekkelig ivaretatt ved at retten til å begjære opplysninger om det har vært foretatt kommunikasjonskontroll vil være i behold, jf § 216 j. En viss innsynsrett kan også følge av påtaleinstruksen § 4-1. Departementet foreslår etter dette ingen bestemmelse om automatisk rett til underretning ut over den plikten som ligger i § 264.»

Ved tvangsmiddelbruk i forebyggende øyemed etter politiloven § 17 d har den som tvangsmiddelet retter seg mot ikke krav på underretning, jf. politiloven § 17 e annet ledd.

Ved tvangsmiddelbruk i avvergende øyemed etter straffeprosessloven § 222 d er lovreguleringen av tvangsmiddelbruk under etterforskningen avgjørende for om det skal underrettes eller ikke, jf. henvisningene i § 222 d femte ledd første punktum. Det vises til fremstillingen ovenfor.

Enkelte uttalelser fra EMD er egnet til å stille spørsmål ved om EMK artikkel 8 tillater at mistenkte ikke underrettes. Forholdet til EMK vurderes i punkt 6.10.6.1 og 6.10.6.2.

Etter utleveringsloven § 24, jf. straffeprosessloven kapittel 15, 15 a, 16, 16 a og 16 b, kan det på begjæring fra fremmede stater blant annet iverksettes ransaking, teknisk sporing, beslag, utleveringspålegg, kommunikasjonskontroll og romavlytting på samme måte som i en norsk straffesak, såfremt vilkårene i § 24 er oppfylt. Det er nærliggende å forstå dette slik at norske regler om underretning gjelder når norske myndigheter bistår utenlandske myndigheter ved bruk av skjulte tvangsmidler.

6.10.2 En generell underretningsplikt – også ved kommunikasjonskontroll og romavlytting?

6.10.2.1 Gjeldende rett

Etter gjeldende rett skal det som hovedregel underrettes om skjult ransaking, personnær teknisk sporing, båndlegging av formuesgoder, beslag, utleveringspålegg og utleveringspålegg fremover i tid etter at tvangsmidlene er gjennomført. Kommunikasjonskontroll og romavlytting underrettes det derimot bare om på begjæring, se nærmere ovenfor.

6.10.2.2 Metodekontrollutvalgets forslag

I utredningen punkt 15.9 side 173–175 går utvalget i det vesentlige inn for å videreføre reglene om underretning ved ransaking, personnær teknisk sporing, båndlegging av formuesgoder, beslag, utleveringspålegg og utleveringspålegg fremover i tid. I tillegg er utvalget av den oppfatning at mistenkte også ved kommunikasjonskontroll og romavlytting som hovedregel bør ha rett til etterfølgende underretning, og foreslår at de samme reglene skal gjelde her. Utvalget begrunner sitt standpunkt slik (utredningen punkt 15.9 side 174):

> «Utvalget har vanskelig å se hvorfor reglene om underretning skal være annerledes for kommunikasjonskontroll og romavlytting enn for de øvrige skjulte tvangsmidler. De hensynene som er påpekt ovenfor gjør seg etter utvalgets oppfatning i like sterk grad gjeldende ved slik tvangsmiddelbruk. De særlige reglene for kommunikasjonskontroll synes å henge igjen fra en tid da kommunikasjonskontroll var det eneste skjulte tvangsmiddelet politiet hadde adgang til å bruke.»

Utvalget går inn for at reglene om utsatt underretning fortsatt skal reguleres i tilknytning til de aktuelle tvangsmidlene, men foreslår at reglene gjøres mer ensartet.

6.10.2.3 Høringsinstansenes syn

Høringsinstansene er delte i synet på spørsmålet om en skal videreføre gjeldende regler om underretning på begjæring ved kommunikasjonskontroll og romavlytting eller om det også for slik tvangsmiddelbruk skal innføres en ordning med etterfølgende underretning. Et flertall av de høringsinstansene som har uttalt seg på dette punktet er imidlertid negative til å innføre underretningsplikt ved kommunikasjonskontroll og romavlytting. Disse høringsinstansene har seg imellom noe ulikt syn på hvordan en best kan regulere spørsmålene om underretning.

For øvrig er det ikke fremmet innvendinger mot at underretningsplikt ved skjult ransaking, båndlegging av formuesgoder, personnær teknisk sporing, beslag, utleveringspålegg og utleveringspålegg fremover i tid videreføres.

Riksadvokaten og *Oslo politidistrikt* uttrykker forståelse for at utvalget ønsker å samkjøre reglene om utsatt underretning, men mener at en absolutt underretningsplikt for kommunikasjonskontroll og romavlytting vil virke negativt på politiets mulighet til effektiv kriminalitetsbekjempelse.

Også *Politidirektoratet* og *NAST* stiller seg negative til en absolutt underretningsplikt ved slike tvangsmidler. Disse høringsinstansene mener at departementets vurderinger i Ot.prp. nr. 64 (1998–99) punkt 8.8.4 side 72–73, se ovenfor, fortsatt har gyldighet, og at det er grunn til å særbehandle kommunikasjonskontroll og romavlytting. *Politidirektoratet* gir uttrykk for at dagens regler bør videreføres. Dessuten er direktoratet av den oppfatning at «individer som har beveget seg inn i en kvalifisert samfunnsskadelig sfære, må tåle en viss «avkortning» i sine *personvernmes-*

sige rettigheter sammenliknet med befolkningen for øvrig».

Lignende argumenter fremsettes av *Riksadvokaten*, som uttaler:

> «Det kan fortsatt være holdepunkter for at den etterforskingen har vært rettet mot er, eller har vært, involvert i straffbar virksomhet selv om saken av taktiske, resurssmessige eller andre grunner ikke følges videre opp nå. Det er et åpenbart behov for at mistenkte i slike tilfeller ikke får kunnskap om etterforskingen, i det minste i en viss tid. Underretning kan føre til forspillelse av avgjørende bevis, eller at den straffbare virksomheten innrettes ut fra kunnskapen om tvangsmiddelbruken. Underretning kan også skade etterforskingen i andre saker fordi informasjon om politiets arbeid mot bestemte personer og miljøer eller metodebruk blir kjent.»

Riksadvokaten og *Oslo politidistrikt* er begge av den oppfatning at det bør gjøres unntak fra underretningsplikten der kommunikasjonskontrollen eller romavlyttingen ikke leder over i en åpen sak. *Riksadvokaten* foreslår i den forbindelse følgende mulige formulering av nytt nest siste og siste ledd i straffeprosessloven 216 j:

> «Når fristen for utsatt underretning er ute eller tiltale er tatt ut skal siktede underrettes om kjennelsen.
>
> Underretning skal også gis etter at saken er henlagt med mindre underretning vil være til vesentlig skade for fremtidig oppklaring av saken, etterforsking av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskingsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. Utsatt underretning etter henleggelse besluttes av retten.»

Også *Romerike politidistrikt* ser med bekymring på en eventuell ubetinget underretningsplikt ved kommunikasjonskontroll, og mener at dette vil medføre at metoden ikke blir anvendelig på samme måte som i dag. Politidistriktet uttaler følgende om utviklingen i kriminalitetsbildet:

> «I de seneste årene har den organiserte kriminaliteten i Norge stadig vært i utvikling. Kriminalitet er langt mer internasjonal enn den var i 1992. I tillegg preges kriminalitet i dag i alle ledd av at de involverte partene har høy kunnskap om politiets etterforskningsmetoder og at det brukes store ressurser på å undra seg politiets søkelys. Her har det vært en særlig utvikling de siste årene. Generelt kan man si at bakmenn gjennom organisering, tekniske løsninger og kommunikasjon, fjerner seg lenger vekk fra arenaen der den straffbare handlingen finner sted. En tvungen underrettelsesplikt vil gi de kriminelle nettverkene informasjon hver gang politiet har hatt søkelys på dem uten å lykkes.»

Romerike politidistrikt understreker også at kommunikasjonskontroll – til forskjell fra skjult ransaking – ofte benyttes tidlig i etterforskningen. På et slikt stadium er det ikke uvanlig at etterforskningen avsluttes uten at det tas videre skritt rettet mot mistenkte. Politidistriktet mener på denne bakgrunn at en absolutt underretningsplikt ved kommunikasjonskontroll – mer enn for de øvrige tvangsmidlene – vil gjøre det vesentlig vanskeligere å gjenoppta etterforskningen.

Videre gir både *Politidirektoratet* og *Romerike politidistrikt* uttrykk for at en absolutt underrettingsplikt kan gjøre det vanskelig for politiet å beskytte sine informanter. *Politidirektoratet* fremhever i den forbindelse viktigheten av informantopplysninger:

> «Bruk av kommunikasjonskontroll utgjør et sentralt instrument for å få verifisert kildeopplysningene og skaffe til veie bevis som kan danne grunnlag for videre etterforskningskritt, eller tiltale. Bruk av informantinformasjon kombinert med kommunikasjonskontroll utgjør sammen viktige redskaper for politiet skal få "hull på byllen" i de svært lukkede miljøer det her erfaringsmessig er tale om.»

Romerike politidistrikt uttaler:

> «Et annet viktig argument for å ikke gjennomføre underretning til personer som er utsatt for kommunikasjonskontroll er politiets inngangsinformasjon i sakene. De fleste sakene det her er snakk om har sin opprinnelse i informasjon fra aktører i de kriminelle miljøene, informanter. Informasjonen fra disse blir etterforsket og kontrollert slik at den ikke umiddelbart kan knyttes til personen som har kommet med informasjonen til politiet.
>
> En påfølgende tiltale og hovedforhandling fjerner ytterligere fokus fra dette. Det er ikke vanskelig å tenke seg at en underretning fra politiet om at en sentral aktør i et kriminelt nettverk har vært utsatt for kommunikasjonskontroll, uten at det ender opp i noen hovedfor-

handling, gjør at miljøet er villig til å gå mye lenger for å finne opprinnelsen til informasjonen enn om man har straffesakens lys over seg. Underretningsplikten vil derfor ytterligere vanskeliggjøre politiet og påtalemyndighetens forhold til informanter og bruk av informasjon fra de kriminelle miljøene.»

For øvrig påpeker *Oslo politidistrikt* at dersom utvalgets forslag følges opp, må det gå klart frem av ordlyden når plikten til å underrette inntrer og når fristene for å be om utsatt underretning utløper. Politidistriktet reiser også spørsmålet om straffeprosessloven § 216 i må endres dersom § 216 j endres slik utvalget foreslår.

Politidirektoratet gir i det vesentlige sin tilslutning til de synspunkter fra Oslo politidistrikt og Romerike politidistrikt som er gjengitt ovenfor.

Datatilsynet støtter forslaget om at det også ved kommunikasjonskontroll og romavlytting skal gis underretning til dem som har vært gjenstand for tvangsmiddelbruken. Tilsynet kan ikke se at det foreligger tungtveiende hensyn som taler for å gjøre unntak fra underretningsplikten, og uttaler at dette vil kunne være i strid med EMK.

Utvalgets forslag får også støtte fra *Forsvarergruppen av 1977* og *Oslo statsadvokatembeter*.

6.10.2.4 Departementets vurdering

Departementet vil innledningsvis slutte seg til utvalgets vurdering om å videreføre reglene om underretningsplikt ved skjult ransaking, personnær teknisk sporing, båndlegging av formuesgoder, beslag, utleveringspålegg og utleveringspålegg fremover i tid.

Når det så gjelder spørsmålet om underretningsplikt ved kommunikasjonskontroll og romavlytting, vil departementet fremheve at det hemmelige preget til tvangsmidlene innebærer et betydelig inngrep i personvernet til den som er gjenstand for metodebruken. Et stykke på vei kan underretning i ettertid til mistenkte og eventuelt andre om bruken av de skjulte tvangsmidlene være egnet til å dempe virkningene av metodebruken. Når mistenkte får kjennskap til en kommunikasjonskontroll eller en romavlytting, vil han kunne klage til kommunikasjonskontrollutvalget, jf. kommunikasjonskontrollforskriften § 15. Ved skjult beslag vil spørsmålet om å opprettholde beslaget kunne bringes inn for retten, jf. straffeprosessloven § 208. En underretning i ettertid kan dessuten være egnet til å bevisstgjøre politiet og påtalemyndigheten, og på denne måten bidra til å forhindre uberettiget metodebruk. Samtidig ser departementet at det kan være uheldig å rette kriminelles oppmerksomhet mot politiets bruk av skjulte metoder. Særlig ved alvorlig kriminalitet kan det argumenteres med at gjerningspersonene ikke har noen berettiget forventning om å få kjennskap til at de har vært overvåket. I ytterste konsekvens kan underretning forhindre oppklaring av kriminalitet, ved at kriminelle miljøer blir mer vare for politiets bruk av skjulte metoder, og eventuelt går under jorden.

Denne typen hensyn var utslagsgivende for at departementet i Ot.prp. nr. 64 (1998–99) punkt 8.8.4 side 72–73 foreslo en ordning for kommunikasjonskontroll som avviker fra de øvrige tvangsmidlene, hvor det før eller siden må underrettes om metodebruken. En «automatisk» underretningsplikt ved kommunikasjonskontroll ble ansett å kunne ha en uheldig innvirkning på kriminalitetsbekjempelsen. I nevnte proposisjon gikk departementet derfor inn for å opprettholde regelen om at underretning kun gis på begjæring, se punkt 6.10.1. Den samme løsningen ble valgt for romavlytting ved lovendringene i 2005. En rekke høringsinstanser er opptatt av at det samme bør gjelde fortsatt. Disse høringsinstansene fremhever at det i lang tid etter at den skjulte tvangsbruken er avsluttet – ikke minst etter en eventuell henleggelse – kan være behov for å sikre hemmelighold omkring metodebruken.

Departementet har kommet til at det også ved kommunikasjonskontroll og romavlytting bør gjelde en *hovedregel* om underretningsplikt. Det vises i den forbindelse til at disse metodene er inngripende, og personvernhensyn gjør seg i minst like stor grad gjeldende her som ved de metodene en har plikt til å underrette om. Også i andre land det er naturlig å sammenlikne oss med; Sverige, Danmark, Finland, Island, Tyskland og Østerrike, skal mistenkte som regel underrettes ved slik metodebruk. En slik løsning samsvarer nok dessuten best med våre menneskerettslige forpliktelser, se punkt 6.10.6.1.

Er det besluttet utsatt underretning, vil mistenkte underrettes når tiltale tas ut, jf. straffeprosessloven § 264. Tas det ikke ut tiltale, bør underretning etter departementets syn normalt gis senest ved henleggelse av saken, se punkt 6.10.5.5. Departementet er imidlertid av den oppfatning at innvendingene fra høringen hensyntas dersom det etter henleggelse – på nærmere bestemte vilkår – gis adgang til å unnlate underretning. Riksadvokaten og Oslo politidistrikt stiller seg positive til å innføre en generell underretningsplikt, såfremt det gis egnede unntaksmuligheter. I den forbindelse har Riksadvokaten frem-

satt et forslag til unntaksregel som departementet mener dekker politiets behov for å unnlate underretning, se punkt 6.10.6.1.

Det skal i tillegg nevnes at andre land som oppstiller en underretningsplikt, også gir en viss adgang til å gjøre unntak fra denne.

Departementet foreslår på denne bakgrunn at underretningsplikten skal gjelde generelt – det vil si også for kommunikasjonskontroll og romavlytting – men med et visst rom for unntak, se nedenfor i punkt 6.10.6.1. Det tilføyes at departementet fortsatt går inn for at reglene om underretning reguleres i tilknytning til de enkelte metodene, siden særtrekk ved de ulike tvangsmidlene kan nødvendiggjøre spesialregulering.

Departementet er for øvrig enig med Oslo politidistrikt i at det bør gå klart frem når plikten til å underrette inntrer. Som for de fleste øvrige tvangsmidler bør underretning som utgangspunkt gis når kontrollen er avsluttet. Departementet foreslår at dette uttrykkelig kommer til uttrykk i loven, se lovforslaget til straffeprosessloven § 216 j første ledd.

Det må videre tas stilling til hvem som skal underrettes, siden både kommunikasjonskontroll og romavlytting som regel vil ramme flere enn mistenkte. I utvalgets utkast til endringer i straffeprosessloven § 216 j forutsettes det at bare mistenkte underrettes, uten at utvalget kommenterer dette nærmere. Spørsmålet er heller ikke berørt under høringen. Personvernhensyn kan imidlertid tilsi at også andre enn mistenkte etter omstendighetene bør underrettes. En kunne tenke seg at personkretsen som har krav på underretning ved kommunikasjonskontroll og romavlytting avgrenses på samme måte som ved beslag og utleveringspålegg – det vil si at underretning skal gis til den som «rammes» av metodebruken, jf. straffeprosessloven § 208 a. En plikt til å underrette enhver som rammes av kommunikasjonskontrollen eller romavlyttingen kan på den annen side synes vanskelig å gjennomføre, siden identiteten til tredjepersoner ofte vil være ukjent. Dessuten vil personkretsen her kunne være langt større enn ved beslag og utleveringspålegg. I tillegg vil mistenkte og aktuelle tredjepersoner ofte være del av det samme miljøet, og i et slikt perspektiv kan det synes forsvarlig å nøye seg med underretning til mistenkte. Departementet er av den oppfatning at en ordning med å underrette enhver som rammes av metodebruken, vil kunne binde opp politiets ressurser i betydelig grad, samtidig som det ikke kan ses at den gir en klar personvernmessig gevinst.

Uttalelsene fra EMD som er gjengitt nedenfor i punkt 6.10.6.1, forutsetter at underretning gis til «the persons concerned». Det er ikke uten videre klart hva som ligger i dette kriteriet.

Etter *svensk rett* skal mistenkte og innehaveren av teleadressen underrettes ved kommunikasjonskontroll, jf. rättegångsbalken 27. kap. 31 §. Ved romavlytting skal mistenkte og innehaveren av det stedet som avlyttes, underrettes, jf. lag om hemlig rumsavlyssning 15 §. I *Danmark* gis underretning ved telefonavlytting til innehaveren av telefonen og ved romavlytting til den som har rådighet over det aktuelle stedet, jf. retsplejeloven § 788.

Ved kommunikasjonskontroll finner departementet det rimelig at den som har rådighet over kommunikasjonsanlegget – i praksis telefonen eller datamaskinen – underrettes, i tillegg til mistenkte. En slik regel har selvstendig betydning dersom den som har rådigheten er en annen en mistenkte. Yter eier eller tilbyder av nettet eller den aktuelle tjenesten bistand ved kontrollen, vil vedkommende være underrettet, jf. straffeprosessloven § 216 a fjerde ledd. Departementet ser ikke grunn til at eier eller tilbyder skal underrettes utover det som følger av disse reglene.

Ved romavlytting tilsier personvernhensyn at den som har rådigheten over det aktuelle stedet underrettes. En slik regel har selvstendig betydning dersom den som har rådigheten er en annen enn mistenkte.

Departementet foreslår etter dette at mistenkte og den som har rådigheten over det kommunikasjonsanlegget eller det stedet som overvåkes, skal underrettes, se lovforslaget til straffeprosessloven § 216 j første ledd og § 216 m sjette ledd med merknader.

Departementet er for øvrig enig med Oslo politidistrikt i at straffeprosessloven § 216 i bør endres dersom det innføres en underretningsplikt ved kommunikasjonskontroll og romavlytting. Departementet foreslår at det tas inn i § 216 i første ledd tredje punktum at taushetsplikten ikke er til hinder for at det gis underretning etter § 216 j, se lovforslaget. Departementet finner i den forbindelse grunn til å presisere at underretning etter § 216 j ikke nødvendigvis gir innsyn i sakens dokumenter. Hvorvidt innsyn kan gis må fortsatt avgjøres av § 242 sammenholdt med § 216 i, jf. punkt 6.10.1.

6.10.3 Underretningsplikt ved skjult kameraovervåking?

Etter gjeldende rett er det ingen underretningsplikt ved bruk av skjult kameraovervåking på offentlig sted etter straffeprosessloven § 202 a. Når departementet nå går inn for i større grad å

ensrette reglene om underretning, oppstår spørsmål om underretningsplikten også skal gjelde ved bruk av skjult kameraovervåking. Spørsmålet er ikke behandlet av Metodekontrollutvalget eller av noen av høringsinstansene.

Etter departementets syn er det ikke hensiktsmessig å innføre underretningsplikt ved overvåking *på eller fra offentlig sted*. Dette skyldes særlig at metoden kan iverksettes uten at det foreligger mistanke mot en eller flere bestemte personer, slik at det ikke alltid vil være noen mistenkt å underrette. Det kan neppe heller være aktuelt å underrette alle som rammes av overvåkingen – som potensielt vil kunne være en meget stor gruppe. En slik underretningsplikt ville være meget ressurskrevende for politiet og ikke gi noen klar personvernmessig gevinst.

Som det fremgår av punkt 12.6.3, foreslår departementet å åpne for bruk av skjult kameraovervåking også *på privat sted*, unntatt i private hjem. Etter departementets syn bør reglene om underretning ved skjult kameraovervåking på privat sted utformes i tråd med det som gjelder ved kommunikasjonskontroll og romavlytting, jf. punkt 6.10.2 ovenfor. Metodens inngripende karakter tilsier her at det er større grunn til å innføre regler om underretning enn ved overvåking på eller fra offentlig sted. Ettersom bruk av metoden forutsetter at det foreligger konkret mistanke mot en eller flere bestemte personer, oppstår heller ikke samme utfordring med å identifisere den som skal underrettes. Departementet foreslår derfor at mistenkte som hovedregel skal gis underretning når politiet har iverksatt skjult kameraovervåking på privat sted. Videre bør underretning – på samme måte som ved romavlytting – også gis til den som har rådigheten over det aktuelle stedet. Regelen har selvstendig betydning når den som har rådigheten over stedet er en annen enn mistenkte.

6.10.4 Særlig om underretningsplikt ved beslag og utleveringspålegg

Uten at det er berørt av utvalget, ønsker *Oslo politidistrikt* en konkretisering av når det foreligger et beslag og hvilke personer som rammes og som har partsrettigheter. Politidistriktet peker på at personkretsen «enhver som rammes» er uklar, og at usikkerhet omkring hva som regnes som et «beslag» kan lede til tilfeldige forskjeller i praksis. Det uttales i den forbindelse følgende:

> «Det er svært gode grunner som taler for at besitterens frivillige overlevering ikke er å anse som beslag, hvilket medfører at kontrollmekanismene uteblir, selv om politiet får hånd om det samme materialet. Dette var situasjonen for kort tid siden da Netcom overleverte samtaledata frivillig hvilket følgelig ikke medførte bruk av et tvangsmiddel fra politiets side, mens det motsatte var tilfellet ved overlevering av samtaledata fra Telenor.»

Det første spørsmålet knytter seg til om besitterens frivillige overlevering er å anse som et beslag i relasjon til reglene om underretningsplikt. Departementet mener at det må være tilfellet. Om mistenkte skal underrettes eller ikke, bør ikke være avhengig av om besitteren samtykker i utlevering eller ikke. For mistenkte er inngrepet like stort i begge situasjoner. § 208 annet ledd synes dessuten å forutsette at frivillig overlevering av en ting er å anse som et beslag. Departementet har imidlertid ut fra det som har vært på høring, ikke grunnlag for å foreslå en klargjøring av dette i loven nå.

Når det gjelder spørsmålet om hvem som skal underrettes ved beslag og utleveringspålegg, har departementet forståelse for at grensedragningen av hvilke personer som skal underrettes om et beslag eller et utleveringspålegg i praksis kan by på vanskeligheter. Uttrykket «rammes» er imidlertid i lovteknisk forstand fleksibelt, siden det vil kunne variere hvem som har tilstrekkelig interesse i å underrettes om et beslag eller utleveringspålegg. Dessuten er kretsen av personer som kan anke over kjennelser og beslutninger avgrenset på tilsvarende måte, jf. straffeprosessloven § 377. Departementet finner det rimelig at en nærmere grensedragning her foretas av domstolene.

6.10.5 Utsatt underretning

6.10.5.1 «strengt nødvendig»-vilkåret

Som det fremgår i punkt 6.10.1 er det etter gjeldende rett bare adgang til å beslutte utsatt underretning der det er «strengt nødvendig».

Utvalget er av den oppfatning at dette kriteriet gir liten veiledning ved den konkrete vurderingen, se utredningen punkt 15.9 side 175. Utvalget foreslår derfor at det i alle de aktuelle bestemmelsene presiseres at underretning kan utsettes hvor «underretning vil være til vesentlig skade for etterforskingen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig».

Ingen av *høringsinstansene* kommenterer utvalgets forslag på dette punktet.

D e p a r t e m e n t e t er enig med utvalget i at vilkåret om at det må være «strengt nødvendig» å utsette underretning, med fordel kan klargjøres. Samtidig bør det tydelig fremgå at det er en viss terskel for å utsette underretning. Departementet slutter seg derfor til utvalgets forslag om at underretning kan utsettes dersom «underretning vil være til vesentlig skade for etterforskingen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig», se lovforslaget til straffeprosessloven § 200 a tredje ledd, § 202 c sjette ledd, § 202 e annet ledd, § 208 a første ledd, § 210 a første ledd og § 210 c første ledd og merknadene til disse endringsforslagene.

6.10.5.2 Frist for å begjære utsatt underretning

Der hvor det som utgangspunkt skal underrettes om metodebruken, kan det etter gjeldende rett synes noe uklart når eventuell begjæring om utsatt underretning må fremsettes.

Som redegjort for i punkt 6.10.2.2 foreslår *utvalget* at det som hovedregel også skal underrettes om kommunikasjonskontroll og romavlytting i ettertid. Utvalget problematiserer imidlertid ikke når fristen for å begjære utsatt underretning ved kommunikasjonskontroll og romavlytting bør utløpe.

Av høringsinstansene er det bare *Oslo politidistrikt* som berører spørsmålet. Politidistriktet mener det bør lovreguleres når begjæring om utsatt underretning bør fremsettes.

D e p a r t e m e n t e t er enig med Oslo politidistrikt i at dette bør angis i loven. Som regel antas det å være klart for politiet at underretning bør utsettes før kommunikasjonskontrollen eller romavlyttingen er avsluttet. I så fall bør begjæring om utsatt underretning fremsettes umiddelbart. Det synes likevel ikke hensiktsmessig med en lovregel om at utsatt underretning må begjæres før tvangsbruken er avsluttet. Departementet foreslår i stedet at begjæringen må fremsettes innen to uker etter at tvangsbruken har opphørt. Dette samsvarer med den danske retsplejeloven § 788. Departementet foreslår videre at retten uten ugrunnet opphold skal ta stilling til begjæringen, se lovforslaget til straffeprosessloven § 216 j annet ledd.

Det er nærliggende å spørre om tilsvarende bør klargjøres for skjult ransaking, personnær teknisk sporing, beslag og utleveringspålegg. Verken utvalget eller høringsinstansene har imidlertid problematisert dette, og departementet ser inntil videre ikke grunnlag for å foreslå lignende presiseringer her.

6.10.5.3 Kompetansespørsmål knyttet til utsatt underretning – domstolskontroll?

Etter gjeldende rett besluttes utsatt underretning i etterforskningssporet og i avvergende øyemed av domstolene, med mindre påtalemyndigheten avgjør spørsmålet etter reglene om hastekompetanse eller det gjelder saker om rikets sikkerhet, se nærmere punkt 6.10.1.

Utvalget foreslår at kompetansen til å beslutte utsatt underretning i alle tilfelle skal ligge hos retten, likevel slik at det ikke gjøres endringer i bestemmelser som gir påtalemyndigheten hastekompetanse, se utredningen punkt 15.9 side 175.

De høringsinstansene som har uttalt seg om dette, er uenige om hvilken rolle domstolene skal ha. Flere av høringsinstansene peker på at dagens ordning er unødig ressurskrevende.

Domstoladministrasjonen tiltrer forslaget om at kompetansen til å beslutte utsatt underretning i saker om skjult tvangsmiddelbruk gjennomgående legges til domstolene.

Kripos er av den oppfatning at dagens regler om utsatt underretning er unødvendig ressurskrevende, og er opptatt av hvilken betydning dette har for domstolskontrollen. Det uttales:

> «Kripos har tidligere fremhevet overfor utvalget at det er behov for harmonisering av regelverket. Dagens regler om utsatt underretning medfører at det i en og samme sak løper flere parallelle frister, noe som er uoversiktlig og medfører unødig bruk av ressurser for både politiet, forsvarerne og domstolen ifm forlengelse av disse fristene. I tillegg medfører de ulike fristreglene at vi oppretter separate saker for hvert enkelt tvangsmiddel, og at vi i våre rapporter og begjæringer aldri kan henvise til et tvangsmiddel som er bedre «vernet» mot innsyn enn det tvangsmidlet den aktuelle begjæring eller rapport angår. Eksempelvis vil vi i en begjæring om utleveringspålegg med utsatt underretning aldri kunne opplyse om at det også benyttes romavlytting. Dette betyr i realiteten at domstolen ikke har mulighet til å vurdere den samlede effekten av politiets metodebruk i den konkrete saken, noe som er uheldig.»

Kripos har følgende forslag til hvordan regelverket om utsatt underretning best kan utformes:

> «Så lenge det pågår skjult metodebruk i saken, mener vi at det bør gjelde en generell, lovfestet taushetsplikt helt frem til det tidspunkt taushetsplikten opphører som følge av et av alternativene i strpl § 216i. Dette vil likevel ikke medføre at taushetsplikten opphører for andre tvangsmidler enn de som taushetsplikten eksplisitt oppheves for. Så lenge vilkårene for bruk av skjulte tvangsmidler er oppfylt kan det vanskelig tenkes tilfeller hvor utsatt underretning om et eller flere av tvangsmidlene vil være uforholdsmessig. Vi mener at løsningen med «utsatt underretning» i inntil 8 uker om gangen har lite for seg.
>
> Kripos foreslår derfor at § 216i gis anvendelse for alle skjulte tvangsmidler i samme sak. Lovteknisk kan dette gjøres ved en henvisning fra de aktuelle metodehjemler til § 216i.»

Oslo politidistrikt er særlig opptatt av de prosessuelle reglene som gjelder ved utsatt underretning om beslag og utleveringspålegg. Politidistriktet er av den oppfatning at prosessreglene for utsatt underretning om beslag og utleveringspålegg bør være annerledes enn for utsatt underretning om ransaking. Det vises til at utsatt underretning om beslag og utleveringspålegg utgjør langt mer beskjedne inngrep enn utsatt underretning om ransaking:

> «Hemmelig ransaking reiser i større grad tyngre betenkelige rettssikkerhets- og personvernmessige innvendinger, enn beslag og utleveringspålegg med utsatt underretning. Ransaking er klart det mest inngripende, og særlig hemmelig ransaking der politiet gjennomsøker private rom og eiendeler uten at dette straks bekjentgjøres for husstandsmedlemmene. Dette kan følgelig også ramme husstandsmedlemmer som ikke er mistenkt i saken.
>
> Beslag innebærer at politiet bemektiger seg et objekt, eller tar kopi av opplysninger (eks bankkontoopplysninger eller samtaledata). Beslag er et midlertidig inngrep som varer frem til at saken er rettskraftig avgjort. Beslag med utsatt underretning vil være mindre inngripende enn hemmelig ransaking, blant annet fordi mistenkte ikke selv besitter tingen, i tillegg til at besitteren naturlig nok vil være underrettet.»

Politidistriktet fremhever særlig at en stor personkrets skal underrettes om et beslag, og at det i enkelte saker fattes en stor mengde beslutninger om utsatt underretning. Oslo politidistrikt gir også uttrykk for at selve prosessen med å begjære utsatt underretning er krevende:

> «Saken må redigeres ferdig og kopieres slik at den kan oversendes til retten. Politimesteren må orienteres, som må vurdere saken og være den som fremmer begjæringen. Saken må oversendes tingretten som oppnevner en § 100a-advokat. § 100a-advokaten må lese påtegningen, og evt. be om innsyn i sakskomplekset. Deretter skriver advokaten et notat om sitt syn på begjæringen. Retten tar deretter stilling til begjæringen. Avgjørelsen meddeles § 100a-advokaten, som tar stilling til en eventuell anke. Dette er et ganske omfattende apparat for at politiet kan innhente forholdsvis alminnelige og lite sensitive opplysninger, for eksempel opplysninger om en bompassering.
>
> Som nevnt må disse prosedyrene iverksettes for *hver eneste gang* det tas et beslag. Eksempelvis hver gang politiet avdekker et nytt telefonnummer i saken (hvilket kan skje daglig i en aktiv fase av etterforskningen) mv. Idet påtalemyndighetens har hastekompetanse i bare 24 timer, forutsetter loven at en begjæring om utsatt underretning må fremmes straks materialet er mottatt. Politiet kan følgelig ikke vente, og samle opp flere beslag i samme begjæring.»

Oslo politidistrikt kan heller ikke se at det er nødvendig med *prøving* av vilkårene for utsatt underretning ved beslag og utleveringspålegg, og foreslår lovfestet at det skal underrettes om et beslag senest ved tiltale eller henleggelse. Politidistriktet finner det klart at en slik løsning ikke er i strid med EMK, og viser til at forslaget ikke medfører at de med rettslig interesse taper sin rettsstilling, men bare gis en utsettelse i når de kan få vurdert den. Politidistriktet tillegger ikke hensynet til gjerningspersonen særlig vekt, ettersom utsatt underretning om beslag i all hovedsak vil være aktuelt ved tredjemannsbeslag hvor gjerningspersonen selv har satt seg i en stilling der andre enn han selv besitter opplysningene. Det påpekes også at det bør være tilstrekkelig med påtalemyndighetens kontroll for de etterforskningsmetoder det her er tale om.

Subsidiært foreslår politidistriktet en lovendring som går ut på at det – i motsetning til det prinsipale forslaget – fattes en egen avgjørelse om utsatt underretning, men at kompetansen her legges til påtalemyndigheten og ikke retten.

Videre problematiserer *Oslo politidistrikt* at kompetansen til å begjære utsatt underretning er lagt til politimesteren:

> «I en aktiv fase i en stor etterforskning vil det med gjeldende regler, daglig gå et forholdsvis omfattende dokumentsett til retten via politimesteren, med begjæring om utsatt underretning. Skal politimesteren vurdere realiteten i begjæringene, må vedkommende også kunne faktum i sakene, hvilket etter omstendighetene kan være krevende. I slike tilfeller vil politimesteren bli bundet opp til å arbeide med enkeltsaker. Politiadvokatene har bred kompetanse, og kan blant annet beslutte pågripelser og begjære varetektsfengsling, som er atskillig mer integritetskrenkende enn utsatt underretning. Utsatt (og ikke unnlatt) underretning av beslag er inngrep av vesentlig mindre inngripende karakter enn kommunikasjons- og romavlytting mv. som politimesteren for øvrig skal begjære.»

Politidistriktet uttaler følgende om konsekvensene av dagens regler:

> «At etterforskningen blir prosessuelt krevende, selv om en bare utfører etterforskningsskritt av mindre inngripende karakter, vil føre til at politiet blir ledet over mot saker som ikke krever et slikt ressursuttak. Dette vil være uheldig for bekjempelsen av bl.a. organisert kriminalitet og finansiell etterforskning, som særlig har som formål å inndra straffbart utbytte.
>
> Erfaringsmessig begjæres utsatt underretning ved beslag forholdsvis sjelden. Politiet skulle antagelig ha bedt om utsatt underretning i mye større grad en hva som er tilfelle […]. På Lovdata er det pr i dag to saker om dette. Sakene illustrerer at disse reglene ikke utnyttes slik lovgiver har ment.»

D e p a r t e m e n t e t er enig med utvalget i at myndigheten til å beslutte utsatt underretning bør ligge hos retten – også i saker om rikets sikkerhet. Departementet finner at en domstolsbehandling er best egnet til å avveie behovet for hemmelighold mot hensynet til mistenktes personvern. I den forbindelse vil departementet, i likhet med Kripos, fremheve viktigheten av at retten – så langt som mulig – gis kjennskap til den totale metodebruken i en sak. Dette er spesielt viktig dersom begjæringene i en sak behandles av ulike dommere. Departementet mener at straffeprosessloven § 242 gir såpass rom for å hindre innsyn at det som regel ikke bør være grunn til i en begjæring å unnlate å opplyse om andre tvangsmidler i saken. Det tilføyes for øvrig at oppnevnelse av samme offentlige advokat i hele sakskomplekset vil kunne bidra til å gjøre retten bedre i stand til å vurdere den samlede metodebruken, jf. punkt 6.6.2.

Særlig på bakgrunn av høringsuttalelsen fra Oslo politidistrikt finner departementet grunn til å foreslå enkelte unntak fra utgangspunktet om at utsatt underretning må besluttes av retten. Departementet ser i den forbindelse at det kan være behov for at prosessen knyttet til utsatt underretning i saker om beslag og utleveringspålegg forenkles noe. Foretas det flere beslag i en sak, medfører den begrensede varigheten av beslutninger fattet i medhold av påtalemyndighetens hastekompetanse at det ikke er kurant for politiet å bringe spørsmålet om utsatt underretning inn for retten samtidig for flere beslag. Det kan derfor være nødvendig i en og samme sak å fremsette en rekke begjæringer om utsatt underretning, med den ressursbruk dette medfører. Videre bør det tas i betraktning at hemmelig beslag og hemmelig utleveringspålegg normalt er langt mindre inngripende enn skjult ransaking, personnær teknisk sporing, kommunikasjonskontroll og romavlytting. Etter departementets syn bør det derfor for beslag og utleveringspålegg gjøres et unntak fra utgangspunktet om at utsettelsesspørsmålet må prøves av retten. Departementet finner likevel at en ordning med at underretning ved beslag og utleveringspålegg utsettes uten påtalemyndighetens medvirkning – slik Oslo politidistrikt primært synes å ønske – går for langt.

Derimot er departementet av den oppfatning at det er forsvarlig og hensiktsmessig at påtalemyndigheten ved beslag, utleveringspålegg og utleveringspålegg fremover i tid gis myndighet til å beslutte utsatt underretning for en viss tid. Departementet finner det passende at påtalemyndigheten her kan utsette underretning i inntil åtte uker, se lovforslaget til straffeprosessloven §§ 208 a første ledd og 210 c første ledd. Ønskes ytterligere utsettelser, må beslutning om dette fattes av retten. Om ønskelig kan politiet begjære fortsatt utsatt underretning for flere beslag under ett, selv om fristen for å underrette for de enkelte beslagene i utgangspunktet løper ut til ulik tid. En slik ordning synes et godt stykke på vei å imøtekomme Kripos' innvendinger til dagens ordning, siden det blir enklere å unngå parallelle frister i en sak.

Gis påtalemyndigheten en begrenset myndighet til å beslutte utsatt underretning ved beslag og

utleveringspålegg, vil overordnet påtalemyndighet – i praksis statsadvokaten – alltid ha kompetanse. Når politiet ber om rettens samtykke, avgjør som regel politimesteren spørsmålet, jf. henvisningen til § 216 d i § 208 a femte ledd første punktum, jf. § 210 a annet ledd. Ut fra det som har vært på høring har departementet ikke grunnlag for å foreslå endringer i regelen om at politimesteren i utgangspunktet avgjør om det skal bes om rettens samtykke til å utsette underretning. Som nevnt ovenfor er Oslo politidistrikt kritisk til denne ordningen. Ved en større gjennomgåelse av straffeprosessloven er det imidlertid naturlig å vurdere behovet for endringer på dette punktet.

I likhet med utvalget ser ikke departementet grunn til å foreslå endringer i påtalemyndighetens begrensede adgang til å utsette underretning etter reglene om hastekompetanse.

6.10.5.4 Tidsrommet for utsatt underretning

Etter gjeldende rett kan underretning utsettes i inntil åtte uker om gangen. I saker om rikets sikkerhet er det ikke gitt regler om utsettelsens lengde. For skjult ransaking i slike saker er imidlertid tidsrommet begrenset til seks måneder om gangen, se punkt 6.10.1.

Utvalget går inn for å videreføre reglene om at underretning kan utsettes i inntil åtte uker om gangen, se utredningen punkt 15.9 side 175. Utvalget erkjenner imidlertid at saker om rikets sikkerhet står i en særstilling, samtidig som det mener at utsatt underretning også her må besluttes for en viss tid om gangen. Det foreslår derfor at utsatt underretning i slike saker gjennomgående kan besluttes for inntil seks måneder om gangen, i samsvar med det som i dag gjelder for skjult ransaking i slike saker. Det foreslås å endre reglene i politiloven om skjulte metoder i forebyggende øyemed tilsvarende, likevel slik at retten her kan beslutte utsatt underretning i inntil ett år om gangen dersom særlige omstendigheter tilsier at fornyet prøving etter seks måneder vil være uten betydning. Utvalget begrunner dette slik (utredningen punkt 15.9 side 175):

> «Utvalget ser imidlertid at en ny prøving hver sjette måned når det gjelder tvangsmidler som har vært anvendt som ledd i PSTs forebyggende virksomhet kan være uhensiktsmessig. Det vises her blant annet til saken Klass mot Tyskland hvor det ble uttalt at «[t]he activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures». Utvalget foreslår derfor at hovedregelen bør være at underretning kan utsettes i inntil seks måneder om gangen også i denne typen saker, men at retten kan beslutte utsatt underretning i inntil ett år om gangen dersom særlige omstendigheter tilsier at fornyet prøving etter seks måneder vil være uten betydning.»

Av høringsinstansene er det kun *Kripos* og *Oslo politidistrikt* som direkte uttaler seg om tidsrommet for utsatt underretning. Som påpekt i punkt 6.10.5.3 er disse høringsinstansene negative til dagens ordning, fordi den anses å være for ressurskrevende.

D e p a r t e m e n t e t har vurdert om en bør opprettholde dagens ordning hvor spørsmålet om utsatt underretning må prøves med jevne mellomrom, eller om en ordning hvor utsettelse gis helt frem til tiltale eller henleggelse, kombinert med en adgang til å oppnå underretning på begjæring, kan være mer hensiktsmessig. Som redegjort for i punkt 6.10.2.4, er underretning til mistenkte viktig for å avdempe de skjulte metodenes karakter av inngrep i personvernet. Det kan derfor reises spørsmål om det er forsvarlig å utsette underretning helt frem til tiltale eller henleggelse, selv om mistenkte etter omstendighetene kan gis underretning på begjæring. Spørsmålet om prøvingshyppigheten av underretningsspørsmålet når det gjelder skjult ransaking, personnær teknisk sporing, beslag og utleveringspålegg har heller ikke vært gjenstand for høring. Dersom det innføres regler om underretningsplikt og utsatt underretning også ved kommunikasjonskontroll og romavlytting, bør ikke reglene her være annerledes enn det som gjelder for de andre skjulte metodene. Departementet vil på denne bakgrunn gå inn for å videreføre dagens ordning med enkelte tilpasninger, og foreslår at dette også skal gjelde for kommunikasjonskontroll og romavlytting. Siden ordningen utvides til også å gjelde slike metoder, vil departementet se an erfaringene med ordningen og spesielt vurdere om prøvingshyppigheten av underretningsspørsmålet innebærer en uforholdsmessig byrdefull prosess.

Når det så gjelder utvalgets konkrete forslag, er departementet enig i at det i saker som ikke gjelder rikets sikkerhet, er rimelig å videreføre dagens ordning med at underretning kan utsettes med inntil åtte uker om gangen, og at dette også bør gjelde for kommunikasjonskontroll og romavlytting. Det kan imidlertid forekomme at det på tidspunktet for begjæringen om utsatt

underretning er på det rene at etterforskningen ennå vil pågå i lang tid, og at ny prøving av underretningsspørsmålet etter åtte uker ikke vil bringe noe nytt. Dette kan for eksempel være tilfellet ved etterforskning av alvorlige forbrytelser med flere involverte og hvor politiet er avhengig av bistand fra andre lands myndigheter. Departementet foreslår derfor at retten i de ulike bestemmelsene om utsatt underretning gis myndighet til å utsette underretning i inntil fire måneder, dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter åtte uker vil være uten betydning, se lovforslaget til straffeprosessloven §§ 200 a tredje ledd, 202 c sjette ledd, 208 a første ledd, 210 a første ledd, 210 c første ledd og 216 j første ledd. En slik løsning er valgt ved fornyet prøving av fengslingsspørsmålet, jf. straffeprosessloven § 185 første ledd fjerde punktum. Departementet finner denne løsningen også forsvarlig for underretningsspørsmålet, siden adgangen til å beslutte lengre utsettelse er forholdsvis snever, behovet må prøves av retten og den offentlig oppnevnte advokaten vil kunne fremsette innsigelser mot en lengre frist. En slik regel vil – i alle fall et stykke på vei – imøtekomme Kripos' og Oslo politidistrikts innvendinger mot dagens ordning, se også punkt 6.10.5.3.

Gjennom henvisningen i § 222 d femte ledd foreslås disse reglene også å gjelde for bruk av skjulte tvangsmidler i avvergende øyemed.

I likhet med utvalget foreslår departementet at det i saker om rikets sikkerhet gis anledning til å utsette underretning i inntil seks måneder om gangen, slik regelen i dag er for skjult ransaking i slike saker, se punkt 6.10.1. Det samme foreslås å gjelde hvor skjulte tvangsmidler i disse sakene benyttes i avvergende øyemed.

Ved bruk av skjulte tvangsmidler i forebyggende øyemed etter politiloven § 17 d, har departementet kommet til at dagens ordning bør videreføres, se punkt 6.10.6.2.

6.10.5.5 Når underretning senest bør skje

Etter gjeldende rett skal det underrettes om skjult ransaking, personnær teknisk sporing, beslag, utleveringspålegg og utleveringspålegg fremover i tid senest når tiltale tas ut, se punkt 6.10.1.

Utvalget foreslår at underretning senest skal gis når tiltale tas ut «eller saken henlegges», men med mulighet for å utsette underretning når saken henlegges, se utredningen punkt 15.9 side 175 og side 353. Det siste er ikke gjenspeilet i utvalgets lovutkast.

Høringsinstansene er særlig opptatt av at en regel om underretning ved henleggelse ikke bør være absolutt, se punkt 6.10.2.3.

D e p a r t e m e n t e t er enig med utvalget i at det bør lovfestes at underretning senest skal gis når tiltale tas ut «eller saken henlegges». Samtidig bør det gis en viss åpning for helt å unnlate underretning etter henleggelse, se punkt 6.10.6.1.

Hensynet til å sikre senere oppklaring av den aktuelle saken eller etterforskning i andre saker, tilsier etter departementets syn at «henleggelse» i denne sammenhengen bør forstås som tidspunktet for utløpet av fristen på tre måneder overordnet påtalemyndighet har til å omgjøre en henleggelsesbeslutning, jf. straffeprosessloven § 75 annet ledd. Dette foreslås presisert i straffeprosessloven § 200 a fjerde ledd, § 202 c syvende ledd, § 208 a annet ledd, § 210 c annet ledd og § 216 j tredje ledd, se lovforslaget til disse bestemmelsene.

6.10.6 Adgang til å unnlate underretning? Forholdet til EMK

6.10.6.1 Adgang til å unnlate underretning etter henleggelse?

Med unntak for etterforskning og forebyggende metodebruk i saker om rikets sikkerhet, gir ikke gjeldende rett adgang til å helt unnlate underretning.

Utvalget mener at underretning ikke bør kunne unnlates for alltid, og viser til at dette antakelig ville stride mot våre menneskerettslige forpliktelser, se utredningen punkt 15.9 side 175.

Som referert i punkt 6.10.2 er en rekke høringsinstanser opptatt av at underretningsplikten ikke gjøres absolutt. *Riksadvokaten* foreslår endringer i straffeprosessloven § 216 j, slik at det etter henleggelse bør kunne gjøres unntak fra underretningsplikten dersom «underretning vil være til vesentlig skade for fremtidig oppklaring av saken, etterforsking av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig». Riksadvokaten foreslår tilsvarende endringer i de øvrige hjemlene for skjulte metoder, slik at underretningsplikt heller ikke her er absolutt.

D e p a r t e m e n t e t er også av den oppfatning at det bør gis visse åpninger for å unnlate underretning etter henleggelse. Departementet ser at politiet for å sikre en effektiv kriminalitetsbekjempelse, kan ha behov for å hemmeligholde

kommunikasjonskontroll og romavlytting. Det samme gjelder de metodene der en i dag har en plikt til å underrette mistenkte på et eller annet tidspunkt.

Det kan synes noe uklart om Riksadvokatens forslag innebærer at spørsmålet om underretning etter henleggelse skal prøves med jevne mellomrom eller om det kan besluttes at underretning helt kan unnlates. Etter henleggelse vil en rettslig prøving av underretningsspørsmålet med jevne mellomrom etter departementets oppfatning synes uforholdsmessig ressurskrevende, tatt i betraktning at mistenkte så langt ikke er underrettet og at det ved henleggelsen er vurdert at vedkommende fortsatt ikke bør underrettes. Departementet mener derfor at retten etter henleggelse bør kunne gi påtalemyndigheten en adgang til helt å unnlate underretning.

I den forbindelse slutter departementet seg til Riksadvokatens forslag til at dette i så fall er betinget av at «underretning vil være til vesentlig skade for fremtidig oppklaring av saken, etterforsking av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig». Det siste alternativet i vilkåret må anses å gi rom for å unnlate underretning for å beskytte informanter, slik Politidirektoratet og Romerike politidistrikt fremhever som viktig, se punkt 6.10.2.3.

En slik adgang til å unnlate underretning etter henleggelse bør etter departementets syn suppleres med en adgang til å gi underretning på begjæring, både i løpet av en periode hvor det er besluttet at underretning kan utsettes og etter at det eventuelt er besluttet at underretning kan unnlates. Det vises til at dagens regler om utsatt underretning ved ransaking, personnær teknisk sporing, beslag og utleveringspålegg ikke er til hinder for at mistenkte henvender seg til påtalemyndigheten med begjæring om underretning. Tilsvarende bør mistenkte ved kommunikasjonskontroll og romavlytting fortsatt kunne henvende seg til Kontrollutvalget for kommunikasjonskontroll med begjæring om underretning. Kommer påtalemyndigheten eller kommunikasjonskontrollutvalget til at underretning ikke vil være til vesentlig skade for fremtidig oppklaring av saken, etterforsking av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, og heller ikke hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig å hemmeligholde metodebruken, må underretning gis, selv om dette ble vurdert anner-ledes på tidspunktet for rettens kjennelse. Kommer påtalemyndigheten eller kommunikasjonskontrollutvalget til at det ikke er grunnlag for å gi underretning, vil en slik avgjørelse kunne begjæres overprøvd av retten.

Enkelte uttalelser fra EMD er egnet til å så tvil om en adgang til å unnlate underretning er i overensstemmelse med EMK artikkel 8 om retten til respekt for privatlivet. I praksis fra EMD er det slått fast at skjulte tvangsmidler er i strid med art. 8 nr. 1. Slike tvangsmidler kan imidlertid være tillatt etter unntaksbestemmelsen i artikkel 8 nr. 2.

Med utgangspunkt i vilkåret «necessary in a democratic society», har EMD utviklet et proporsjonalitetsprinsipp, hvoretter det må være forholdsmessighet mellom de mål som søkes oppnådd – for eksempel å forhindre alvorlig kriminalitet – og de midler som tas i bruk for å nå dette målet. I denne vurderingen har domstolen gjennomgående lagt til grunn at det må foreligge tilfredsstillende og effektive garantier mot misbruk av metodene, jf. Ot.prp. nr. 60 (2004–2005) punkt 3.3 side 23. I dommen *Klass mot Tyskland* 6. september 1978 (saksnummer 5029/71) er dette utdypet slik i avsnitt 50:

> «This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.»

I flere dommer har EMD lagt til grunn at statene har en relativt vid skjønnsmargin på dette området. EMD har i den forbindelse slått fast at det i seg selv ikke er uforholdsmessig i artikkel 8 sin forstand å unnlate underretning når den skjulte tvangsbruken har opphørt, jf. blant annet dommen *Klass mot Tyskland*. EMD uttaler følgende i avsnitt 58 i dommen:

> «In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.
>
> The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Con-

> stitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the «interference» resulting from the contested legislation is in principle justified under Article 8 para. 2 (art. 8-2) (see paragraph 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the «interference».»

Resten av avsnittet må forstås slik at en underretningsplikt etter de nasjonale reglene er et argument for at den aktuelle ordningen gir tilstrekkelige rettssikkerhetsgarantier. Domstolen uttaler i den forbindelse følgende om den aktuelle tyske ordningen:

> «Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction (see paragraphs 11 and 19 above).»

En lignende uttalelse er gitt i dommen *Leander mot Sverige* 26. mars 1987 (saksnummer 9248/81) avsnitt 66.

I avgjørelsen *Weber og Saravia mot Tyskland* 29. juni 2006 (saksnummer 54934/00), avsnitt 135, kan domstolen imidlertid forstås å legge sterkere føringer på hvordan de nasjonale ordningene med underretning må innrettes:

> «As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned […]»

Det samme uttales i dommen *Association for European integration and human rights and Ekimdzhiev mot Bulgaria* 30. januar 2008 (saksnummer 62540/00), avsnitt 90. Domstolen prøvde her lovligheten av de bulgarske reglene om telefonavlytting. Bulgarsk rett ga ingen anledning for mistenkte til å få kjennskap til hvorvidt han var avlyttet, siden slike opplysninger var underlagt taushetsplikt. I avsnitt 91 uttaler domstolen om denne ordningen:

> «The result of this is that unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights. Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance.»

I artikkelen «Beskyttelsen mod overvågning i den fysiske og elektroniske verden. Forhandlingerne ved Det 38. nordiske Juristmøde i København 21. – 23. august 2008» gir Inger Marie Sunde på side 474 uttrykk for at det på et eller annet tidspunkt må gis underretning, og at norske regler som gir adgang til helt å unnlate underretning står i et tvilsomt forhold til EMDs minimumskrav.

Uttalelsene fra EMD kan etter departementets syn imidlertid ikke trekkes så langt som til at mistenkte i alle tilfeller må underrettes. Departementet er enig med Politiets sikkerhetstjeneste (PST), se nedenfor i punkt 6.10.6.2, i at de nevnte avgjørelsene direkte gir uttrykk for at berørte personer *bør* underrettes. Videre taler avsnitt 91 i dommen *Association for European integration and human rights and Ekimdzhiev mot Bulgaria* etter departementets syn for at det sentrale er at det eksisterer en *mulighet* for mistenkte til å oppnå kjennskap om tvangsmiddelbruken.

Til dette kommer at statene har en relativt vid skjønnsmargin på området, og at et absolutt forbud mot å unnlate underretning vil underkjenne ordningen i en rekke land. Interessant i denne sammenheng er reglene i Sverige om underretningsplikt ved telefonavlytting og romavlytting som trådte i kraft 1. januar 2008. Her kan underretning helt unnlates dersom det på grunn av taushetsplikt ikke er gitt underretning innen et år etter at etterforskningen ble avsluttet, jf. rättegångsbalken 27 kap. 33 § og Lag om hemlig rumsavlyssning 15 §. Reglene ble innført uten at uttalelsen i avgjørelsen *Weber og Saravia mot Tyskland* ble problematisert.

Departementet legger til grunn at spørsmålet om underretning til siktede fortsatt bare inngår som et moment i forholdsmessighetsvurderingen, hvor det sentrale er om det foreligger tilfredsstillende og effektive garantier mot misbruk av metodene.

Når det konkret gjelder den ordningen som foreslås i proposisjonen her, må det særlig tas i

betraktning at adgangen til å unnlate underretning etter henleggelse foreslås å være forholdsvis snever, og at mistenkte vil kunne oppnå kjennskap til metodebruken gjennom begjæring. Dessuten er domstolsprøving av underretningsspørsmålet og oppnevning av offentlig advokat sentrale rettssikkerhetsgarantier i norsk rett som bør tillegges betydelig vekt i vurderingen. Ved kommunikasjonskontroll og romavlytting, som jevnt over må anses å være mer inngripende enn de øvrige metodene, foretas dessuten en etterkontroll av Riksadvokaten og kommunikasjonskontrollutvalget.

Departementet finner etter dette at en ordning som er foreslått ovenfor ikke er i strid med EMK artikkel 8.

Spørsmålet om underretning har også en side til EMK artikkel 13, som bestemmer at den krenkede skal ha en effektiv prøvingsrett for nasjonale myndigheter. En alminnelig prøving lar seg vanskelig gjennomføre uten at mistenkte har kjennskap til inngrepet. Dersom et tvangsmiddel etter artikkel 8 nr. 2 først anses «necessary in a democratic society» på tross av manglende underretning, vil en imidlertid ikke kunne utlede en underretningsplikt fra artikkel 13, jf. *Klass mot Tyskland* avsnitt 68. Dermed anses heller ikke artikkel 13 å være til hinder for en ordning som beskrevet ovenfor.

Departementet går på denne bakgrunn inn for at underretning, på de vilkår som foreslått, kan unnlates både ved ransaking, personnær teknisk sporing, beslag, utleveringspålegg, kommunikasjonskontroll og romavlytting. Samtidig foreslås det at mistenkte fortsatt bør ha mulighet til å underrettes på begjæring, se lovforslaget til straffeprosessloven § 216 j sjette ledd, jf. § 200 a fjerde ledd, § 202 c syvende ledd, § 208 a annet ledd og § 210 c annet ledd. Disse endringene, sammenholdt med forslaget i punkt 6.10.2 om en generell underretningsplikt, krever dessuten enkelte endringer i kommunikasjonskontrollforskriften.

6.10.6.2 Adgang for Politiets sikkerhetstjeneste til å unnlate underretning?

Ved bruk av skjulte tvangsmidler i forebyggende øyemed etter politiloven er det etter gjeldende rett ikke krav til underretning, se punkt 6.10.1.

Utvalget går inn for å innføre en underretningsplikt også her, og viser til at dagens ordning neppe er i overensstemmelse med våre menneskerettslige forpliktelser, se utredningen punkt 15.9 side 175.

De to høringsinstansene som har uttalt seg har innvendinger mot forslaget. *PST* bemerker følgende:

> «Utvalgets forslag vil få store konsekvenser for PST. Forslaget rokker ved en helt avgjørende premiss for en sikkerhetstjeneste – muligheten til å bevare taushet om hvem virksomheten rettes mot. Det er PSTs vurdering at underretning alltid vil kunne være til vesentlig skade for PST, og det er derfor avgjørende at tvangsmiddelbruk i regi av PST også i fremtiden skal kunne forbli skjult.
>
> Det synes videre noe usikkert hvilke generelle rettsetninger som kan utledes fra de konkrete og situasjonsbetingende avgjørelser som utvalget har redegjort for fra den europeiske menneskerettighetsdomstol. En ren språklig forståelse av de sitater som er hentet fra EMD-avgjørelsene, synes ikke å gå lenger enn til å si at den som er utsatt for tvangsmiddelbruk i ettertid *burde* bli gjort kjent med tvangsmiddelbruken.
>
> På denne bakgrunn vil PST fremheve viktigheten av en ordning med unnlatt underretning må kunne videreføres såfremt dette, slik som i dag, balanseres av virkemidler som sikrer rettsikkerheten for den som er utsatt for tvangsmiddelbruken. Ikke bare er den som utsettes for tvangsmiddelbruk i dag representert gjennom en egen advokat i forhold til om vilkårene for tvangsmiddelbruken er tilstede. I tillegg etterkontrollerer EOS-utvalget at vilkårene for tvangsmiddelbruken rent faktisk etterfølges og at opplysninger fra tvangsmiddelbruken brukes etter forutsetningene.»

Videre fremhever PST at det er viktig at spørsmålene om underretning utredes videre med hensyn til deres særskilte behov.

Oslo statsadvokatembeter uttaler følgende:

> «Hva gjelder PST's saksområde er man enig med utvalget at det her gjør seg særlige hensyn gjeldende. Disse er imidlertid knyttet til utenlandske institusjoner i Norge. Her oppstår det spesielle problemstillinger hva gjelder bruk av tvangsmidler. En vil her likevel peke på at det kunne gis en særskilt lovhjemmel som gjelder bruk av kommunikasjonskontroll i forhold til disse. Dette er en løsning som er valgt i enkelte land. Hva gjelder norske statsborgere og personer med fast bopel i Norge, bør disse falle inn under de generelle regler som foreslås av utvalget.»

Departementet vil fremheve at PST skal etterforske og forebygge straffbare handlinger som truer sikkerheten i samfunnet eller grunnleggende samfunnsinstitusjoner, jf. politiloven § 17 b. Ofte begås slike handlinger av lukkede og profesjonelle miljøer. For personer med planer om å begå så alvorlige straffbare handlinger, antas straffens allmennpreventive effekt å spille en begrenset rolle. Dette gjør forebyggingsarbeidet særdeles viktig. Kjernen i sikkerhetstjenestens virksomhet er å oppdage mulige trusler mot samfunnssikkerheten tidligst mulig, og helst lenge før hendelsesforløpet har kommet så langt at grensen for det straffbare er nådd. I Ot.prp. nr. 60 (2004–2005) punkt 9.4.3.2 side 134 og i merknaden på side 153 la departementet til grunn at særtrekkene ved denne forebyggende virksomheten som regel gjør det nødvendig å bevare metodebruken hemmelig for den som er utsatt for inngrepet.

Departementet er fremdeles av den oppfatning at det er grunn til å særbehandle PSTs forebyggende arbeid, slik at det fortsatt bør være adgang til å unnlate underretning her. Departementet kan ikke se at dette er i strid med EMK artikkel 8. Bruken av skjulte metoder i forebyggende øyemed kontrolleres av domstolene og den offentlig oppnevnte advokaten i forkant, og i etterkant av Justis- og beredskapsdepartementet som overordnet myndighet for PST og av EOS-utvalget. Det må også tas i betraktning at tillatelse gis på strenge vilkår og at adgangen til skjult tvangsmiddelbruk i forebyggende øyemed gjelder for et meget begrenset saksområde; terrorhandlinger, ulovlig etterretningsvirksomhet og de mest alvorlige formene for vold eller trusler mot representanter for våre øverste statsmyndigheter eller representanter for tilsvarende organer i andre land. Slike oppgaver tør være i kjernen for den nasjonale handlefrihet, se punkt 6.10.6.1 som refererer avsnitt 58 i dommen *Klass mot Tyskland*. Ut fra foreliggende rettspraksis fra EMD mener departementet at det – særlig på dette området – er grunn til å være varsom med å innfortolke absolutte skranker i EMK artikkel 8.

Departementet går etter dette inn for å videreføre regelen i politiloven § 17 e om at den tvangsmidlet retter seg mot, ikke har krav på underretning etter at tvangsmiddelbruken har opphørt.

Når det gjelder PSTs bruk av skjulte metoder under etterforskning, herunder i avvergende øyemed etter straffeprosessloven § 222 d, synes det noe uklart om høringsuttalelsene fra PST og Oslo statsadvokatembeter kan tas til inntekt for en særbehandling av sikkerhetstjenesten. Uansett kan departementet vanskelig se grunner til at sikkerhetstjenestens etterforskning bør behandles annerledes enn etterforskningen til politiet ellers, all den tid det også for sistnevnte åpnes for å unnlate underretning. Skjulte tvangsmidler som benyttes under etterforskning vil også på PSTs område – om ikke saken henlegges – som regel komme til mistenktes kjennskap når det tas ut tiltale. Departementet foreslår på denne bakgrunn at de foreslåtte alminnelige regler om underretningsplikt også bør gjelde her.

6.10.7 Utsatt eller unnlatt underretning ved sikringspålegg

6.10.7.1 Gjeldende rett

Straffeprosessloven § 215 a gir påtalemyndigheten hjemmel til midlertidig sikring av elektronisk lagrede data som ledd i etterforskningen av straffesaker. Bestemmelsen ble tilføyd ved lov 8. april 2005 nr. 16 og gjennomfører Europarådets konvensjon 23. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (CETS nr. 185) artikkel 16 og 17.

Reglene om sikringspålegg tar sikte på å sikre bevis til bruk i en etterfølgende straffesak. Påtalemyndigheten får ikke rådigheten over dataene, noe som gjør sikringspålegg mindre inngripende enn beslag.

§ 215 a tredje ledd gjelder underretning:

> «Den som har rådigheten over de data som omfattes av sikringspålegget, skal underrettes om pålegget. En mistenkt skal underrettes straks dataene er sikret og han får status som siktet i saken. For øvrig skal underretning gis straks dataene er sikret.»

Den som har rådigheten over dataene skal altså underrettes om sikringspålegget, noe som normalt er en forutsetning for å kunne sikre dataene.

En mistenkt skal gis underretning om beslutningen straks dataene er sikret og han får status som siktet i saken, jf. straffeprosessloven § 82. Han vil dermed ha krav på underretning senest på det tidspunkt påtalemyndigheten har erklært ham for siktet, forfølgning mot ham er innledet ved retten eller det er besluttet eller foretatt pågripelse, ransaking, beslag eller lignende forholdsregler rettet mot ham, jf. straffeprosessloven § 82 første ledd. Sikringspålegg er ikke å anse som «lignende forholdsregler». Sikringspålegg alene gir dermed ikke siktede status som siktet.

Er det besluttet å bruke et tvangsmiddel som den mistenkte ikke varsles om, for eksempel hemmelig ransaking (§ 200 a), personnær teknisk sporing (§ 202 c), kommunikasjonskontroll (§§ 216 a og 216 b) eller skjult kameraovervåkning (§ 202 a), får man status som siktet først når underretning gis, jf. straffeprosessloven § 82 tredje ledd. Det samme gjelder dersom det er besluttet utsatt underretning om et tvangsmiddel, for eksempel beslag (§ 208 a), utleveringspålegg (§ 210 a) eller fremtidig utleveringspålegg (§ 210 c). I så fall skal den siktede samtidig gis underretning om sikringspålegget.

6.10.7.2 Forslaget i høringsnotatet

I høringsnotat 12. juli 2012 behandles forslag fra PST om å gi en egen bestemmelse om utsatt eller unnlatt underretning ved sikringspålegg. Spørsmålet om utsatt eller unnlatt underretning ved sikringspålegg er ikke særskilt omtalt av Metodekontrollutvalget.

PST anfører at straffeprosessloven § 215 a ikke er anvendelig der det er behov for skjult etterforskning. Sikringspålegg kan være aktuelt svært tidlig i etterforskningen, for å unngå å miste informasjon som senere kan vise seg å være viktig som bevis. PST mener det er lite hensiktsmessig at mistenkte allerede da får kjennskap til at han eller hun er under etterforskning og at vedkommende får status som siktet.

PST foreslår at det inntas en bestemmelse i straffeprosessloven § 215 a om utsatt eller unnlatt underretning ved sikringspålegg. Bestemmelsen vil tilsvare den som gjelder ved hemmelig ransaking, jf. straffeprosessloven § 200 a tredje ledd, og for beslag, jf. straffeprosessloven § 208 a annet ledd annet punktum.

6.10.7.3 Høringsinstansenes syn

Kripos har en annen forståelse enn PST når det gjelder kravene til når en mistenkt skal underrettes. Kripos uttaler:

> «Slik Kripos forstår bestemmelsen skal vedkommende først underrettes når han av en eller annen grunn har fått status som siktet. Kripos mener det er tvangsmidlene som brukes for å følge opp sikringspålegget, og som eventuelt gir mistenkte siktetstatus, som utløser plikten til å underrette. Dersom det er gitt utsatt underretning ved bruk av de aktuelle tvangsmidler vil også underretning om sikringspålegget utsettes. Det er ikke sikringspålegget i seg selv som gir ham status som siktet. Underretningsplikt vil imidlertid utløses dersom den mistenkte av en annen grunn (enn de tvangsmidler som brukes for å følge opp sikringspålegget) skulle få status som siktet i saken, jfr strpl. § 82. Dette er imidlertid sjelden praktisk når det pågår skjult etterforskning.
>
> […]
>
> Kripos er etter dette av den oppfatning at strpl. § 215a i stor grad vil være anvendelig i sin nåværende form også i en skjult etterforskningsfase.»

Riksadvokaten deler heller ikke PSTs lovforståelse om at straffeprosessloven § 215 a ikke er anvendelig ved skjult etterforskning. Riksadvokaten uttaler:

> «Etter vårt syn skal det ikke gis underretning før mistenkte får stilling som siktet. Det vises til bestemmelsens ordlyd og merknadene til denne.»

NAST uttaler at straffeprosessloven § 215 a i sin nåværende form er anvendelig i en skjult fase av en etterforskning, og er enige i Kripos' redegjørelse og lovforståelse. *Politidirektoratet* uttaler at de er i tvil om PSTs syn om at sikringspålegg ikke er anvendelig ved skjult etterforskning medfører riktighet, og slutter seg til uttalelsen fra Kripos vedrørende forståelsen av straffeprosessloven § 215 a. Også *Politijuristene* slutter seg til Kripos' lovforståelse, og etterlyser en avklaring fra departementet.

6.10.7.4 Departementets vurdering

PSTs forståelse om at § 215 a om sikringspålegg ikke er anvendelig i en skjult fase av etterforskningen, har fått en rekke entydige reaksjoner i høringsrunden. Høringsinstansene som har uttalt seg, med unntak av Hordaland politidistrikt, støtter ikke PSTs lovforståelse.

Departementet slutter seg til Kripos' forståelse av reglene om underretning. Departementet viser til uttalelsene i forarbeidene, jf. Ot.prp. nr. 40 (2004–2005) Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet) punkt 4.2.4.3 side 27:

> «Den som besitter de data som skal sikres – typisk en tjenestetilbyder – må naturligvis få *underretning* om pålegget om midlertidig sikring for at dette skal bli gjennomført. Et annet

spørsmål er om den som eventuelt er mistenkt for en handling som pålegget skal sikre bevis for, skal ha krav på underretning. Departementet er enig med utvalget i at en mistenkt bør ha krav på underretning fra det tidspunkt han får status som siktet i saken, men bare dersom sikringspålegget gjelder data som den siktede selv har lovlig tilgang til. En tjenestetilbyder blir for eksempel pålagt å sikre data som knytter seg til den mistenktes e-postkonto eller hans hjemmeside på internett. I slike tilfeller vil han ha krav på underretning senest på det tidspunkt når påtalemyndigheten har erklært ham for siktet, når forfølging mot ham er innledet ved retten eller når det er besluttet eller foretatt pågripelse, ransaking, beslag eller lignende forholdsregler rettet mot ham, jf. straffeprosessloven § 82 første ledd. Er det besluttet utsatt underretning om et tvangsmiddel, blir vedkommende først siktet når underretning gis, jf. straffeprosessloven § 82 tredje ledd. I slike tilfeller skal det samtidig gis underretning om sikringspålegget.»

Det samme uttales i merknadene i punkt 7.2 side 35:

«Det fremgår av utkastet til *tredje ledd* at en mistenkt skal gis underretning om beslutningen straks dataene er sikret og han får status som siktet i saken, jf. straffeprosessloven § 82. Han vil dermed ha krav på underretning senest på det tidspunkt når påtalemyndigheten har erklært ham for siktet, når forfølging mot ham er innledet ved retten eller når det er besluttet eller foretatt pågripelse, ransaking, beslag eller lignende forholdsregler rettet mot ham. Er det besluttet utsatt underretning om et tvangsmiddel, inntrer stillingen som siktet først når underretning gis, jf. straffeprosessloven § 82 tredje ledd. I så fall skal den siktede samtidig gis underretning om sikringspålegget.»

Departementet deler således ikke PSTs syn om at § 215 a ikke er anvendelig i en tidlig og skjult fase av etterforskningen. Mistenkte skal først underrettes om sikringspålegget når han får status som siktet i saken. Sikringspålegget i seg selv gir ikke mistenkte status som siktet. Dersom det er besluttet å bruke et tvangsmiddel det ikke skal gis underretning om, eller det er besluttet utsatt underretning, får mistenkte status som siktet først når underretning gis, jf. straffeprosessloven § 82 tredje ledd. Med en slik lovforståelse, er de gjeldende reglene om underretning ved sikringspålegg anvendelige i en tidlig og skjult fase av etterforskningen, og det er etter departementets syn ikke behov for endringer i straffeprosessloven § 215 a.

6.10.8 Særlig om underretning ved gjensidig bistand i straffesaker

Etter gjeldende rett kommer trolig de norske reglene om underretningsplikt til anvendelse når norske myndigheter bistår utenlandske myndigheter ved bruk av skjulte tvangsmidler, se punkt 6.10.1.

Utvalget berører ikke spørsmålet om underretningsplikt ved bistand til utenlandske myndigheter. Det gjør imidlertid enkelte høringsinstanser. Både *Romerike politidistrikt* og *NAST* er opptatt av at utvalgets forslag om en generell underretningsplikt kan vanskeliggjøre etterforskning i saker med internasjonalt opphav. *Romerike politidistrikt* uttaler i den forbindelse:

«Flere av sakene der metoden kommunikasjonskontroll brukes, startes med bakgrunn i, eller som støtte til etterforskning i utlandet. Disse sakene kan ut fra utviklingen i etterforskningen få helt andre tidsperspektiver enn etterforskningen av saken i Norge. I disse tilfellene måtte påtalemyndigheten ha logistikk på underrettelsesplikt og omfanget av dette knyttet til en rekke personer over tid. Slik utviklingen av sakene der kommunikasjonskontroll benyttes har blitt, involverer sakene ofte mange avlyttede personer over tid. Muligheten for at pågående etterforskninger blir skadelidende eller helt stopper opp er derfor overhengende.»

NAST savner en vurdering av hvilke konsekvenser en ubetinget underretningsplikt vil få for Norges evne til å delta i dette samarbeidet, og det vises til at embetet jevnlig mottar rettsanmodninger fra andre lands myndigheter om å innhente tillatelse til bruk av skjulte tvangsmidler. For øvrig uttaler embetet:

«Det vil også kunne være problematisk å dokumentere behovet for utsatt underretning dersom slik begjæring skal fremmes. Ytterligere er det risiko for at Norge kan bli forhindret fra å bistå dersom reglene i det land som begjærer tvangsmidlet tillater unnlatt underretning i større utstrekning enn etter norsk rett. Det

synes klart at dette vil kunne bli hemmende for det internasjonale politisamarbeidet som er nødvendig for effektiv bekjempelse av grenseoverskridende kriminalitet. NAST mener, i likhet med det som er anført vedrørende strafferammekravet for skjulte tvangsmidler (pkt. II.1.a), at det er behov for *sammenlignende undersøkelser* med andre lands rettssystemer, for å påse at norske vilkår er hensiktsmessige i lys av samarbeidsforpliktelsene. Eventuelle endringer i dagens underrettelsesregler bør avventes til en slik undersøkelse er utført.»

NAST er videre av den oppfatning at Norge ikke uten videre bør ha byrden med underretning, og uttaler:

«Et annet praktisk problem er når norsk politi bistår med skjulte tvangsmidler mot en person som er midlertidig i landet, typisk på gjennomreise. En absolutt varslingsplikt av den personen som er i utlandet vil være svært problematisk. En ser for seg en regel om at varsling om tvangsmiddelbruk i bistandssaker overlates til begjærende lands myndigheter. På den måten kan norsk politi gjennomføre bistanden og utkvittere saken. Varsling vil uansett måtte gjennomføres ved at norske myndigheter via rettsanmodning anmoder det land mistenkte befinner seg i, om bistand til å gjennomføre varsling. Hvis de nekter å gjennomføre dette er vi like langt. En kommer således antakelig ikke unna at varsling avhenger av begjærende lands medvirkning Da kan ansvaret like godt legges der med en gang. En norsk domstols vurdering av vilkårene for fortsatt utsatt varsling vil uansett ikke kunne bli særlig opplyst. Det samme gjelder når vår bistand kreves fordi kommunikasjon av tilfeldige årsaker rutes via Norge. Dette skjer ikke sjelden uten at mistenkte noen gang har befunnet seg på norsk territorium. For norske myndigheter vil det være svært krevende og urimelig byrdefullt å skulle følge opp en slik utenlandsk etterforsking i måneder og år. Det taler med styrke for at varsling overlates til begjærende myndigheter.»

Departementet ser at en underretningsplikt kan skape særlige utfordringer hvor skjulte tvangsmidler gjennomføres på anmodning fra utenlandske myndigheter. Norske myndigheter kan ha vanskelig for å begrunne utsatt underretning dersom etterforskningen for øvrig gjennomføres av utenlandske myndigheter, og vil kunne trenge bistand fra utlandet både for å få kjennskap til om mistenkte bør underrettes, og for å gjennomføre selve underretningen. Det er videre grunn til å spørre om det i slike saker er rimelig at byrden med å underrette påhviler norske myndigheter.

Departementet ser derfor at det kan være behov for særregler om underretning ved gjensidig bistand i straffesaker, og vil vurdere hvordan de særlige hensyn som gjør seg gjeldende her best kan ivaretas.

Departementet foreslår derfor at Kongen gis hjemmel til å gi særregler om underretning ved gjennomføring av tvangsmidler på begjæring fra utenlandske myndigheter, se forslaget til endringer i § 216 j syvende ledd, jf. § 200 a fjerde ledd, § 202 c syvende ledd, § 208 a annet ledd og § 210 c annet ledd. Det bemerkes i den forbindelse at utleveringsloven § 28 nr. 2 ikke synes å gi tilstrekkelig hjemmel i så henseende. Det samme gjelder straffeprosessloven § 216 k som bare gjelder for kommunikasjonskontroll og romavlytting.

7 Kommunikasjonskontroll

7.1 Gjeldende rett

7.1.1 Bakgrunn for dagens regelverk

Adgangen til å foreta kommunikasjonskontroll ble første gang innført ved lov 24. juni 1915 nr. 5 om kontroll med post- og telegrafforsendelse og med telefonsamtaler. Loven gjaldt opprinnelig kun post- og telegrafkontroll, men ble ved lov 15. desember 1950 nr. 5 utvidet til også å omfatte kontroll med telefonsamtaler. 1915-loven er en fullmaktslov, som gir Kongen eller den han gir fullmakt adgang til å utferdige bestemmelser om kontroll når dette antas påkrevet av hensyn til rikets sikkerhet, jf. § 1. Det sentrale anvendelsesområdet for loven er avdekking av etterretningsvirksomhet rettet mot Norge.

Ut over saker om rikets sikkerhet, ble bruk av kommunikasjonskontroll først tillatt ved midlertidig lov 17. desember 1976 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen. Loven ga politiet, etter rettens tillatelse, adgang til å avlytte samtaler til og fra bestemte telefoner, teleksanlegg og lignende anlegg for telekommunikasjon som den mistenkte hadde eller kunne antas å ville bruke, jf. § 1 første ledd. Tillatelsen kunne også gjelde innstilling eller avbrytelse av samtaler, stenging av telefoner for samtaler eller pålegg til styrer av telefonsentral om å gi opplysninger om hvilke telefoner som ble eller hadde vært satt i forbindelse med hverandre, jf. § 2.

Den midlertidige lovens anvendelsesområde var begrenset til å gjelde narkotikakriminalitet. Bakgrunnen for den særskilte reguleringen var at narkotikasakene representerte en ny kriminalitetsform som bød på særlige etterforskningsmessige utfordringer. I Ot.prp. nr. 10 (1976–77) punkt 5 side 5 ble behovet omtalt slik:

> «Man står her overfor en meget farlig kriminalitet. De grovere former har dessuten en slik karakter at konvensjonelle etterforskingsmetoder lett kommer til kort. Fra politihold hevdes det at man i stor utstrekning bare finner frem til misbrukerne, ikke til de større forbrytere som står bak den illegale virksomhet. Den mer omfattende illegale omsetning av narkotika er gjennomorganisert og drives i stor utstrekning av profesjonelle, ofte internasjonale forbrytere. Forbindelser kontaktes i stor utstrekning via telefon, som bl.a. også brukes til bestillinger. Svenske erfaringer, som det er redegjort for i nyere svenske lovforarbeider (prp. 1975/76:202 og prp. 1975:69) bekrefter betydningen av telefonkontroll som etterforskingsmiddel i narkotikasaker. Det er der bl.a. opplyst at i så godt som alle tilfelle hvor avlytting har funnet sted, har det ført til at en har kunnet gripe inn mot personer som har vært engasjert i illegal narkotikahandel. På denne måten har man fått kartlagt flere vidt forgrente distribusjonskjeder.»

Gyldighetstiden for den midlertidige loven om telefonkontroll i narkotikasaker ble forlenget i flere omganger. Reglene ble deretter ved lov 5. juni 1992 nr. 52 gjort permanente og tatt inn i et nytt kapittel 16 a i straffeprosessloven. I den forbindelse uttalte Stortingets justiskomité følgende (Innst.O. nr. 61 (1991–1992) punkt 3.1):

> «Komiteens flertall […] vil understreke at telefonavlytting er et ekstraordinært etterforskningsmiddel som bare må tillates brukt ved alvorlig og sterkt samfunnsskadelig kriminalitet der andre etterforskningsmetoder kommer til kort. Etter flertallets oppfatning er narkotikakriminalitet av et slikt omfang og gir så betydelige samfunnsskadelige virkninger at telefonavlytting må kunne benyttes på bestemte vilkår.»

Ved lov 3. desember 1999 nr. 82 ble reglene i straffeprosessloven kapittel 16 a endret. Betegnelsen «telefonkontroll» ble erstattet av «kommunikasjonskontroll», for å reflektere at kontrolladgangen er uavhengig av hvilket overføringsmedium som benyttes. Adgangen til å foreta kommunikasjonskontroll ble dessuten utvidet. Bakgrunnen for dette var blant annet endringer i kriminalitetsbildet, samt det særlige behovet for etterforsk-

ningsmetoder som melder seg ved såkalt offerløs kriminalitet, jf. Ot.prp. nr. 64 (1998–99) punkt 8.3.1.4 side 45 flg. Fra tidligere kun å gjelde narkotikalovbrudd, ble området for kommunikasjonsavlytting etter straffeprosessloven § 216 a utvidet til å gjelde generelt ved lovbrudd med en strafferamme på fengsel i ti år eller mer. Samtidig ble kommunikasjonsavlytting tillatt ved overtredelser av straffeloven 1902 kapittel 8 (forbrytelser mot statens selvstendighet og sikkerhet) og kapittel 9 (forbrytelser mot Norges statsforfatning og statsoverhode), samt ved brudd på eksportkontrolloven § 5. Området for kommunikasjonskontroll etter straffeprosessloven § 216 b (annen kontroll enn avlytting) ble utvidet til å gjelde generelt for lovbrudd med minst fem års strafferamme, samt ved visse andre lovbrudd – nærmere bestemt overtredelser av straffeloven 1902 kapittel 8 og 9, datainnbrudd, befatning med overgrepsbilder av barn og fredsforstyrrelse.

Reglene om kommunikasjonskontroll ble igjen endret ved lov 17. juni 2005 nr. 87, hvor en blochenvisningen til straffeloven 1902 kapittel 8 og 9 ble tatt ut og erstattet med henvisninger til konkrete straffebud. Metodenes anvendelsesområde forble imidlertid i all hovedsak det samme.

7.1.2 Kommunikasjonsavlytting – straffeprosessloven § 216 a

Kommunikasjonsavlytting medfører «å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke», jf. straffeprosessloven § 216 a tredje ledd. Avlytting kan skje av ethvert «anlegg for elektronisk kommunikasjon», uavhengig av hvilke tekniske hjelpemidler eller overføringsmedier som brukes i kommunikasjonen, jf. Ot.prp. nr. 64 (1998–99) punkt 8.4.1.5 side 58–59. Som kommunikasjonsanlegg regnes både telefoner og datamaskiner, men også andre medier som blant annet telefaksmaskiner, personsøkere og nettbrett. Det er dessuten uten betydning på hvilken måte informasjonen transporteres. Avlytting kan dermed skje av kommunikasjon over fastnett og mobilnett, så vel som informasjonsutveksling over satellitt. Derimot gir bestemmelsen ikke adgang til å avlytte kommunikasjon over svært små private nettverk, som for eksempel interne hustelefoner eller callinganlegg, jf. Ot.prp. nr. 64 (1998–99) punkt 23 side 157. Avlyttingen kan rette seg mot enhver informasjonsutveksling mellom ulike kommunikasjonsanlegg, uavhengig av hvilken form eller hvilket innhold informasjonen måtte ha. Dermed omfattes i tillegg til samtaler også overføring av for eksempel tekst (herunder e-post), bilde eller film.

Som kommunikasjonsavlytting regnes også identifisering av kommunikasjonsanlegg ved hjelp av teknisk utstyr, der dette skjer ved å avlytte samtaler eller annen kommunikasjon, jf. § 216 a tredje ledd siste punktum. Metoden – ofte kalt «temporær masseavlytting» – innebærer at politiet i en bestemt periode lytter til all kommunikasjon i området hvor mistenkte antas å befinne seg. Avlyttingen gjennomføres for å finne identiteten, for eksempel såkalte IMEI- eller IMSI-nummer, til kommunikasjonsanlegg mistenkte benytter. Dette kan brukes med sikte på en senere begjæring om ordinær avlytting av kommunikasjonsanlegget, men også som grunnlag for andre etterforskningsskritt – for eksempel en begjæring om innsyn i abonnementsopplysninger. Fordi temporær masseavlytting også vil ramme utenforstående tredjepersoner, er dette ansett som en særlig inngripende etterforskningsmetode, jf. Ot.prp. nr. 60 (2004–2005) punkt 8.5.3 side 110.

Kommunikasjonsavlytting etter straffeprosessloven § 216 a kan iverksettes dersom noen med skjellig grunn mistenkes for å ha begått en handling eller forsøk på handling som kan medføre fengsel i 10 år eller mer, jf. første ledd bokstav a. Forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelser kommer ikke i betraktning. Dersom vilkårene i straffeloven § 79 bokstav c (straffeloven 1902 § 60 a) om organisert kriminalitet er oppfylt, slik at maksimumsstraffen forhøyes til det dobbelte, vil kommunikasjonsavlytting kunne foretas i saker med ned til fem års strafferamme. Adgangen til kommunikasjonsavlytting gjelder etter bokstav b også ved etterforskning av handling som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136 a, 231, 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231 (straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90, 104 a første ledd annet punktum, eller av § 162 eller § 317, jf. § 162) eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5. I utgangspunktet kreves sannsynlighetsovervekt for at mistenkte har begått en handling som objektivt sett svarer til gjerningsbeskrivelsen i det aktuelle straffebudet, at det ikke foreligger noen straffrihetsgrunn og at mistenkte har utvist skyld. Det følger imidlertid av § 216 a annet ledd at kommunikasjonsavlytting kan besluttes selv om det er sannsynlig at mistenkte var utilregnelig på grunn av sinnssykdom eller bevisstløshet, eller under

den kriminelle lavalder, jf. straffeloven § 20 første ledd (straffeloven 1902 §§ 44 og 46). Dette gjelder også når tilstanden har medført at mistenkte ikke har utvist skyld.

I tillegg til strafferammekravet i § 216 a oppstiller straffeprosessloven § 216 c visse materielle tilleggsvilkår for bruk av kommunikasjonsavlytting. I henhold til første ledd kan tillatelse bare gis dersom det må antas at avlyttingen vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad ville bli vanskeliggjort. Det første vilkåret oppstiller det såkalte indikasjonskravet, som innebærer at metodebruken må antas å frembringe opplysninger av stor betydning for etterforskningen i saken. Det andre er det såkalte subsidiaritetskravet, som innebærer at kommunikasjonsavlytting ikke skal benyttes der samme resultat må antas å kunne oppnås ved mindre inngripende metoder. Er kommunikasjonsanlegget den mistenkte antas å ville bruke tilgjengelig for et større antall personer, kreves i tillegg «særlige grunner», jf. annet ledd. Det samme gjelder ved avlytting av kommunikasjonsanlegg som tilhører advokat, lege, prest eller andre som erfaringsmessig fører samtaler av svært fortrolig art eller redaktør eller journalist, såfremt vedkommende ikke selv er mistenkt i saken.

Ved siden av de omtalte vilkårene, gjelder det generelle kravet etter straffeprosessloven § 170 a om at tvangsmidler bare kan brukes når det er tilstrekkelig grunn til det, og inngrepet etter sakens art og forholdene ellers ikke vil være uforholdsmessig.

7.1.3 Annen kontroll av kommunikasjonsanlegg – straffeprosessloven § 216 b

Straffeprosessloven § 216 b åpner for at retten kan gi politiet tillatelse til å foreta annen kontroll av kommunikasjonsanlegg enn kommunikasjonsavlytting. Til forskjell fra avlytting etter § 216 a, gir bestemmelsen ingen hjemmel for kontroll av *innholdet* i kommunikasjonen. Kontroll etter § 216 b kan for det første gå ut på å innstille eller avbryte kommunikasjon til eller fra bestemte anlegg som mistenkte besitter eller kan antas å ville bruke, jf. annet ledd bokstav a. Det samme gjelder å stenge anlegget for kommunikasjon (bokstav b), eller å identifisere kommunikasjonsanlegg ved hjelp av teknisk utstyr (bokstav c). Sistnevnte alternativ ble tilføyet ved lov 17. juni 2005 nr. 87, og gir politiet adgang til å bruke peileutstyr eller andre tekniske innretninger for å identifisere telefoner og andre kommunikasjonsanlegg. Etter annet ledd bokstav d kan kommunikasjonskontroll dessuten gå ut på å pålegge eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjonen, å gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som mistenkte besitter eller kan antas å ville bruke – såkalte trafikkdata. Adgangen omfatter historiske og fremtidige trafikkdata, så vel som andre data knyttet til kommunikasjonen – for eksempel opplysninger om samtalens varighet, mobiltelefoners geografiske plassering idet samtalen finner sted eller hvem som var logget på en datamaskin på det tidspunkt den ble benyttet til kommunikasjon.

Kommunikasjonskontroll etter straffeprosessloven § 216 b kan iverksettes når noen med skjellig grunn mistenkes for å ha begått en handling eller forsøk på handling som kan medføre fengsel i fem år eller mer, jf. første ledd bokstav a. Dersom vilkårene i straffeloven § 79 bokstav c (straffeloven 1902 § 60 a) er oppfylt, vil slik kontroll av kommunikasjonsanlegg kunne foretas i saker med tre års strafferamme. Tillatelse kan også gis dersom handlingen rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 198, 231, 266, 306, 311, 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231 (straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90, 145 annet ledd, 162, 162 c, 201 a, 204 a, 317, jf. §§ 162 eller 390 a). Forhøyelse av straffen ved gjentakelse eller sammenstøt av lovbrudd tas ikke i betraktning.

Som for kommunikasjonsavlytting etter straffeprosessloven § 216 a er det krav om at kommunikasjonskontrollen vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort, jf. straffeprosessloven § 216 c første ledd. Likeledes gjelder kravet om særlige grunner ved kontroll av anlegg som er tilgjengelig for et større antall personer, eller som tilhører advokat, lege, prest mv. Kravet til særlige grunner gjelder likevel ikke ved identifisering av kommunikasjonsanlegg ved hjelp av teknisk utstyr som nevnt i § 216 b annet ledd bokstav c, jf. § 216 c siste ledd.

Også for kommunikasjonskontroll etter straffeprosessloven § 216 b gjelder dessuten det alminnelige kravet om forholdsmessighet etter § 170 a.

7.1.4 Prosessuelle garantier ved bruk av kommunikasjonskontroll

I tillegg til de omtalte materielle vilkår finnes det en rekke prosessuelle garantier som skal ivareta hensynet til personvern og rettssikkerhet ved bruk av kommunikasjonskontroll etter straffepro-

sessloven §§ 216 a og 216 b. For begge former for kontroll gjelder en hovedregel om at inngrepet skal besluttes av retten. Påtalemyndigheten er imidlertid gitt hastekompetanse i tilfeller hvor det ved opphold er stor fare for at etterforskningen vil lide, jf. § 216 d første ledd. Påtalemyndighetens beslutning skal i så fall snarest mulig, og senest innen 24 timer etter at kontrollen ble påbegynt, forelegges retten for godkjennelse.

Det følger av straffeprosessloven § 216 f at tillatelse til kommunikasjonskontroll gis for et bestemt tidsrom, som ikke må være lenger enn strengt nødvendig og maksimalt fire uker om gangen. Gjelder mistanken overtredelse av straffeloven kapittel 17 (straffeloven 1902 kapittel 8 eller 9), kan tillatelsen likevel gis for inntil åtte uker om gangen dersom fornyet prøving etter fire uker ville være uten betydning. Uansett hvilken tidsbegrensning retten har fastsatt, skal inngrepet avbrytes dersom vilkårene ikke lenger antas å være oppfylt eller kontrollen ikke lenger anses hensiktsmessig, jf. § 216 f siste ledd. Det gjelder ingen begrensning for hvor mange ganger politiet kan begjære forlengelse av kommunikasjonskontrollen, og således heller ingen absolutt grense for hvor lenge kontrollen totalt kan pågå. Lengden vil imidlertid være et sentralt moment i forholdsmessighetsvurderingen etter straffeprosessloven § 170 a.

Bruk av kommunikasjonskontroll innebærer vanligvis at også en del ikke-etterforskningsrelevant informasjon samles inn. For å ivareta personvernhensyn inneholder straffeprosessloven § 216 g regler om sletting av overskuddsmateriale. Bestemmelsen ble endret ved lov 21. juni 2013 nr. 86, og foreskriver nå at materiale som ikke er fremlagt som bevis skal slettes ved rettskraftig dom dersom det åpenbart er uten betydning for saken, og ellers sperres. Dersom saken henlegges, skal materiale fra kommunikasjonskontroll som hovedregel slettes. Påtalemyndigheten kan likevel beslutte at materialet i stedet skal sperres, dersom det er grunn til å regne med at siktede vil kreve erstatning i anledning av forfølgning eller at materialet kan få vesentlig betydning for senere etterforskning eller forebygging. Opplysninger omfattet av vitneforbud eller -fritak etter straffeprosessloven §§ 117 til 120 og 122, skal i alle tilfelle slettes så snart som mulig. De omtalte lovendringene har foreløpig ikke trådt i kraft.

Ved siden av alminnelig domstolskontroll overvåkes politiets bruk av kommunikasjonskontroll av Kontrollutvalget for kommunikasjonskontroll, jf. straffeprosessloven § 216 h. Utvalget kontrollerer at politiets bruk av kommunikasjonskontroll skjer innenfor rammen av lov og instrukser, at bruken av kommunikasjonskontroll begrenses mest mulig, og at kommunikasjonskontroll ikke skjer av hensyn til etterforskning i andre saker enn dem som er nevnt i straffeprosessloven § 216 a eller § 216 b. Videre kontrolleres at opplysningene fra kommunikasjonskontrollen brukes på lovlig måte, og at reglene om oppbevaring og sletting blir fulgt. Utvalget skal også påse at bestemmelser om taushetsplikt blir fulgt, jf. forskrift 31. mars 1995 nr. 281 om kommunikasjonskontroll § 14.

Kontrollutvalget for kommunikasjonskontroll avgir årlige rapporter, hvor politiets bruk av kommunikasjonskontroll foregående år vurderes. I rapporten for 2014 konkluderte utvalget med at politiets bruk av metoden gjennomgående er forsvarlig og godt begrunnet. Konklusjonen er den samme som tidligere år.

7.2 Folkerettslige forpliktelser

7.2.1 Kommunikasjonsavlytting

Inngrep overfor enkeltpersoner i form av kontroll av deres kommunikasjon, berører verdier som er beskyttet av EMK artikkel 8 og SP artikkel 17. Departementet legger til grunn at innholdet i SP artikkel 17 i sin helhet er dekket også av EMK artikkel 8, og vil i det følgende begrense omtalen til den sistnevnte bestemmelsen.

Artikkel 8 beskytter retten til respekt for privatliv og familieliv, hjem og korrespondanse. Det er på det rene at beskyttelsen også omfatter fortroligheten i samtaler som føres over telefon. Dette fremgår av EMDs avgjørelse i saken *Klass m.fl. mot Tyskland* 6. september 1978 (sak 5029/71), hvor domstolen i avsnitt 41 uttaler:

> «Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision.»

Ettersom telefonsamtaler er beskyttet av artikkel 8 nr. 1, representerer myndighetsorganers avlytting av disse et inngrep i innbyggernes rett til respekt for privatliv og korrespondanse, jf. også plenumssaken *Malone mot Storbritannia* 2. august 1984 (sak 8691/79) avsnitt 64. Det samme gjelder for andre former for elektronisk kommunikasjon, herunder blant annet «facsimile and e-mail communications», jf. *Liberty m.fl. mot Storbritan-*

nia 1. juli 2008 (sak 58243/00). Dette betyr at politiets avlytting av kommunikasjonsanlegg etter straffeprosessloven § 216 a i utgangspunktet utgjør et inngrep i EMK artikkel 8.

I sin praksis har imidlertid EMD gått ett skritt lenger og funnet at selve forekomsten av lovgivning som tillater kommunikasjonsavlytting utgjør et inngrep i artikkel 8. I den nevnte *Klass*-saken er dette formulert på følgende måte (avsnitt 41):

> «Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence.»

Prinsippet er fulgt opp i andre saker, herunder plenumsavgjørelsen i *Malone*-saken nevnt ovenfor (avsnitt 64).

Ettersom kommunikasjonsavlytting utgjør et inngrep i retten til respekt for privatliv og korrespondanse etter EMK artikkel 8 nr. 1, kan den bare skje innenfor de rammer som er oppstilt i artikkel 8 nr. 2. Bestemmelsen krever for det første at inngrepet må ha hjemmel i lov. Lovkravet omfatter i hovedsak to ulike aspekter. Dels stilles det krav til hjemmelens tilgjengelighet og dels et krav til presisjon. Førstnevnte krav skal sikre at loven er tilgjengelig for borgerne og gir en tilstrekkelig grad av forutsigbarhet. Det fremgår av saken *Kennedy mot Storbritannia* 18. mai 2010 (sak 26839/05) at vilkåret om forutsigbarhet blant annet innebærer at det må fremgå klart hvilke kriminelle handlinger som kan danne grunnlag for bruk av kommunikasjonsavlytting. Domstolen uttaler i avsnitt 159:

> «As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question.»

I tillegg til kravet om lovhjemmel må det aktuelle inngrepet være nødvendig i et demokratisk samfunn av hensyn til visse nærmere angitte formål. Som legitime formål regnes blant annet myndighetenes forebygging av uorden eller kriminalitet. Inngrepet som iverksettes må dessuten være forholdsmessig sett hen til formålet. Det er på det rene at kommunikasjonsavlytting etter omstendighetene kan anses som et nødvendig og forholdsmessig virkemiddel i politiets arbeid, jf. blant annet *Malone*-saken avsnitt 81.

Med hensyn til hva slags kriminalitet som kan begrunne bruk av kommunikasjonsavlytting, foreligger ikke spesifikke retningslinjer fra EMD. Det vil følgelig være kravet om forholdsmessighet som i første rekke setter grenser. Det er grunn til å tro at statene har en ikke ubetydelig skjønnsmargin på dette punktet, men rettspraksis indikerer at det likevel går en grense for hvor mange og hva slags lovbrudd som kan begrunne kommunikasjonsavlytting. I saken *Iordachi m.fl. mot Moldova* 10. februar 2009 (sak 25198/02) uttalte EMD seg om en moldovisk lov som ga adgang til å iverksette avlytting ved over halvparten av straffebudene i straffeloven. Det var derfor gitt tillatelse til et meget høyt antall avlyttinger. Domstolen uttalte (avsnitt 51):

> «[T]he Court considers it necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising it.»

Det følger av dette at kommunikasjonsavlytting bør reserveres for saker som gjelder alvorlig kriminalitet («serious criminal activity»).

På grunn av den særlige misbruksfaren ved bruk av kommunikasjonsavlytting, har domstolen i sin praksis også stilt krav om prosessuelle garantier mot misbruk, jf. *Malone*-saken avsnitt 81. Slike garantier kan blant annet være domstolskontroll eller annen uavhengig kontroll med myndighetenes bruk av tiltak som medfører avlytting.

7.2.2 Kontroll av trafikkdata

Også annen kontroll av elektronisk kommunikasjon enn avlytting vil i utgangspunktet medføre et inngrep i EMK artikkel 8. EMDs praksis gir imidlertid grunnlag for å anta at kontroll som ikke innebærer at innholdet i kommunikasjonen fanges opp, behandles på en noe annen måte enn

avlytting. I den tidligere nevnte *Malone*-saken uttalte domstolen seg om de engelske reglene om såkalt «metering» (avsnitt 84):

> «As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified.»

Domstolen aksepterte imidlertid ikke statens anførsel om at innhenting av trafikkdata overhodet ikke kunne utgjøre et inngrep etter artikkel 8:

> «The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).»

Uttalelsene medfører at også kommunikasjonskontroll etter straffeprosessloven § 216 b normalt vil utgjøre et inngrep i retten til respekt for privatliv og korrespondanse etter EMK artikkel 8. Den kan følgelig bare skje innenfor rammene som oppstilles i artikkel 8 nr. 2. Ettersom kontroll etter bestemmelsen er mindre inngripende enn avlytting etter § 216 a, vil likevel vurderingen av tiltakets nødvendighet og forholdsmessighet kunne være noe annerledes.

7.3 Andre lands rett

7.3.1 Dansk rett

Etter den danske retsplejeloven § 780 kan politiet foreta såkalt «indgreb i meddelelseshemmeligheden». Inngrep kan skje i form av avlytting av telefonsamtaler eller annen tilsvarende telekommunikasjon («telefonaflytning») eller avlytting av andre samtaler eller uttalelser ved hjelp av et apparat («anden aflytning»). Videre kan politiet uten innehaverens tillatelse innhente opplysninger om hvilke telefoner eller andre tilsvarende kommunikasjonsapparater som settes i forbindelse med en bestemt telefon eller annet kommunikasjonsapparat («teleoplysning»), samt innhente opplysninger om hvilke telefoner eller andre tilsvarende kommunikasjonsapparater som settes i forbindelse med andre telefoner eller kommunikasjonsapparater innenfor et nærmere angitt område («udvidet teleoplysning»).

De nærmere vilkår for inngrep i meddelelseshemmeligheten fremgår av retsplejeloven § 781. Ifølge bestemmelsen forutsetter bruk av metoden for det første at det er bestemte grunner til å anta at det på den aktuelle måte gis meddelelser til eller fra en mistenkt. Vilkåret gjelder ikke for utvidet teleopplysning, jf. § 781, stk. 5, annet punktum. Videre kreves at inngrepet må antas å være av avgjørende betydning for etterforskningen (indikasjonskravet), og det oppstilles krav til den straffbare handling som etterforskes. Som hovedregel kan inngrep i meddelelseshemmeligheten iverksettes dersom etterforskningen gjelder et lovbrudd som etter loven kan straffes med fengsel i seks år eller mer. I tillegg kan metoden benyttes ved forbrytelser mot statens sikkerhet og selvstendighet (straffeloven kapittel 12), mot statsforfatningen og de øverste statsmyndighetene (kapittel 13), befrielse fra fengsel og bistand til rømte (§ 124, stk. 2), unndragelse fra militærtjeneste (§ 125), driftsforstyrrelser (§ 127, stk. 1), bordellvirksomhet (§ 228), overgrepsbilder av barn (§ 235), utpressing (§ 266), trusler (§ 281) og menneskesmugling (udlændigeloven § 59, stk. 7, nr. 1 til 5).

Telefonavlytting og teleopplysning kan etter § 781, stk. 2 også benyttes i saker som gjelder datakriminalitet som omhandlet i straffeloven § 263, stk. 2. Straffebudet rammer den som uberettiget skaffer seg adgang til en annens opplysninger eller programmer som er bestemt til å brukes i et informasjonssystem. Teleopplysning kan dessuten benyttes dersom det foreligger begrunnet mistanke om at en person har krenket en annens fred ved å forfølge eller sjenere ham eller henne ved personlig, muntlig eller skriftlig henvendelse, eller om annet straffbart forhold som kan sidestilles med slik fredskrenkelse, jf. retsplejeloven § 781, stk. 3 jf. lov om tilhold, opholdsforbud og bortvisning § 2, stk. 1. Det samme gjelder ved mistanke om overtredelse av straffeloven § 279 a (databedrageri) eller § 293, stk. 1 (uberettiget bruk av ting som tilhører en annen), når den er begått ved bruk av telekommunikasjonstjeneste, samt lov om værdipapirhandel m.v. § 35,

stk. 1 (innsidehandel), § 36 (videreformidling av innsideopplysninger) eller § 39, stk. 1 (kursmanipulasjon).

For annen avlytting enn telefonavlytting, samt for utvidet teleopplysning, gjelder et tilleggsvilkår om at forbrytelsen har medført eller kan medføre fare for menneskers liv eller velferd, jf. retsplejeloven § 781, stk. 5. For alle former for inngrep i meddelelseshemmeligheten gjelder dessuten etter § 782, stk. 1 et generelt forholdsmessighetskrav.

Telefonavlytting eller annen avlytting kan ikke foretas av den mistenktes kommunikasjon med personer som etter retsplejeloven § 170 er avskåret fra å gi forklaring som vitne – herunder prester, leger, forsvarere mv. Unntaket gjelder ikke for teleopplysning, ettersom metoden ikke avslører selve innholdet i kommunikasjonen.

Kompetansen til å tillate inngrep i meddelelseshemmeligheten tilligger retten, som fatter sin avgjørelse ved kjennelse, jf. retsplejeloven § 783, stk. 1. Tillatelsen gis for et bestemt tidsrom som skal være så kort som mulig, og ikke overstige fire uker. Politiet er imidlertid gitt hastekompetanse dersom inngrepets hensikt ville forspilles ved å vente på rettens kjennelse, jf. § 783, stk. 4. Politiets beslutning skal forelegges retten så snart som mulig, og senest innen 24 timer etter at inngrepet ble iverksatt. Dersom retten finner at inngrepet ikke burde vært foretatt, skal det rapporteres til Justisministeriet.

Rettens kjennelse skal i henhold til § 783, stk. 1 angi de telefonnumre, lokasjoner, adressater eller forsendelser som inngrepet angår. Dersom etterforskningen gjelder visse særlig alvorlige lovbrudd, kan angivelsen i stedet knyttes til en person (den mistenkte), jf. stk. 2. I så fall skal politiet etter utløpet av tillatelsen underrette retten om de telefonnumre som inngrepet har vært rettet mot, og som ikke er angitt i kjennelsen.

Etter § 784 skal det ved bruk av inngrep i meddelelseshemmeligheten oppnevnes særskilt advokat for mistenkte.

7.3.2 Svensk rett

I svensk rett skilles det mellom «hemlig avlyssning» og «hemlig övervakning» av elektronisk kommunikasjon. Hemmelig avlytting innebærer etter rättegångsbalken 27 kap. 18 § at meddelelse som i et elektronisk kommunikasjonsnett overføres eller har blitt overført til eller fra et telefonnummer eller annen adresse, i hemmelighet avlyttes eller tas opp ved bruk av teknisk hjelpemiddel for gjengivelse av innholdet i meddelelsen. Slik avlytting er tillatt i etterforskningen av lovbrudd som har en minstestraff på minst to års fengsel, samt ved enkelte former for særlig samfunnsfarlig kriminalitet, jf. 18 § 2 mom. Det samme gjelder ved forsøk, forberedelse eller forbund, dersom slike handlinger er straffbare. Avlytting kan også benyttes ved lovbrudd med en lavere minstestraff, såfremt straffeutmålingen i det aktuelle tilfellet kan antas å overstige fengsel i to år. Denne såkalte «straffvärdeventilen» er ment å fange opp alvorlige tilfeller hvor sannsynlig straffenivå i betydelig grad overstiger minstestraffen, og det derfor er særlig viktig med en effektiv etterforskning, jf. prop. 2002/03:74 punkt 6.1 side 33.

Ifølge 27 kap. 19 § innebærer hemmelig overvåkning av elektronisk kommunikasjon at det i hemmelighet hentes inn opplysninger om meddelelser som overføres eller har blitt overført til eller fra et telefonnummer eller annen adresse i et elektronisk kommunikasjonsnett, om hvilke elektroniske kommunikasjonsinnretninger som har vært innenfor et visst geografisk område, eller om hvilket geografisk område en viss elektronisk kommunikasjonsinnretning er eller har vært i. Hemmelig overvåkning kan også bestå i at elektronisk kommunikasjon fra slike meddelelser hindres i å nå frem, jf. 19 § 2 mom. Hemmelig overvåkning av elektronisk kommunikasjon kan benyttes i etterforskningen av lovbrudd med en minstestraff på seks måneders fengsel, samt ved visse særskilte angitte straffebud. De aktuelle straffebudene gjelder datainnbrudd, overgrepsbilder av barn av en viss alvorlighet, narkotikalovbrudd og narkotikasmugling, samt enkelte former for særlig samfunnsfarlig kriminalitet. Også forsøk, forberedelse eller forbund er omfattet, dersom slike handlinger i seg selv er straffbare.

Det følger av 27 kap. 18 § 3 mom. at en tillatelse til hemmelig avlytting etter 18 § også gir anledning til å iverksette hemmelig overvåking som nevnt i 19 §.

Hemmelig kommunikasjonsavlytting eller -overvåking kan som hovedregel bare benyttes dersom noen er skjellig mistenkt for lovbruddet og inngrepet er av «synnerlig vikt» for etterforskningen, jf. 27 kap. 20 §. I tillegg foreskriver 27 kap. 1 § et alminnelig forholdsmessighetskrav, hvoretter tvangsmidler bare kan benyttes dersom «skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse».

Tillatelsen til hemmelig avlytting eller overvåking kan bare omfatte telefonnummer eller annen adresse eller kommunikasjonsinnretning som mistenkte innehar eller har innehatt i tiden

for tillatelsen, eller som på annen måte kan antas å ha vært anvendt eller ville bli anvendt av den mistenkte. Alternativt kan tillatelsen omfatte telefonnummer eller annen adresse eller kommunikasjonsinnretning som det er særlig grunn til å anta at den mistenkte har kontaktet eller kommer til å kontakte i løpet av tidsrommet tillatelsen er gitt for. Ut over dette kan hemmelig overvåking – men ikke avlytting – brukes med det formål å avgjøre hvem som med skjellig grunn kan mistenkes for lovbruddet, dersom det er av særlig betydning for etterforskningen, jf. 27 kap. 20 § 2 mom. Slik tvangsmiddelbruk forutsetter imidlertid at de strengere vilkårene for avlytting etter 18 § 2 mom. er til stede, jf. 19 § 4 mom. Overvåking som innebærer at det innhentes opplysninger om meddelelser, kan bare gjelde historiske opplysninger. Avlytting eller overvåking kan ellers ikke omfatte meddelelser som bare overføres eller har blitt overført i elektronisk kommunikasjonsnett som på grunn av sitt begrensede omfang og omstendighetene for øvrig må anses å være av mindre betydning fra et allment kommunikasjonssynspunkt, jf. 20 § 3 mom.

Beslutning om å tillate kommunikasjonsavlytting eller -overvåking fattes av retten, jf. 27 kap. 21 §. I rettens beslutning skal det fremgå hvilket tidsrom tillatelsen gjelder. Dette tidsrommet kan ikke være lenger enn nødvendig og høyst én måned. Påtalemyndigheten er gitt hastekompetanse i tilfeller der innhenting av rettens tillatelse ville medføre en forsinkelse som er av vesentlig betydning for etterforskningen, jf. 27 kap. 21 a §. Påtalemyndighetens beslutning skal i så fall forelegges retten for prøving.

Beslutning om å tillate kommunikasjonsavlytting eller -overvåking skal etter 21 § 2 mom. angi hvilket telefonnummer eller annen adresse, hvilken elektronisk kommunikasjonsinnretning eller hvilket geografisk område tillatelsen gjelder. Det skal videre angis særskilt om metoden kan iverksettes utenfor allment tilgjengelige elektroniske kommunikasjonsnett, jf. 3 mom.

7.3.3 Finsk rett

Bruk av hemmelige tvangsmidler er regulert i 10 kap. i tvångsmedellagen 2011/806, som trådte i kraft 1. januar 2014. Såkalt «teleavlyssing» er i 10 kap. 3 § definert som at en meddelelse som tas imot av eller sendes fra en viss teleadresse eller teleterminalutrustning gjennom et allment kommunikasjonsnett eller nett som er koblet til et slikt, avlyttes, tas opp eller på annen måte behandles for å undersøke innholdet i meddelelsen og identifiseringsopplysninger knyttet til den. Teleavlytting kan bare rettes mot meddelelser fra eller tiltenkt en person som er mistenkt for et lovbrudd.

Kravet til den straffbare handling ved bruk av teleavlytting fremgår av 10 kap. 3 § 2 mom. flg. Det er her ikke angitt noe generelt strafferammekrav, men opplistet en rekke lovbrudd som kan danne grunnlag for avlytting. Opplistingen nevner blant annet folkemord og folkemordrelaterte forbrytelser, forbrytelser mot rikets sikkerhet, forræderi, seksuell utnyttelse av barn, drap, menneskehandel, samt visse vinningslovbrudd og narkotikalovbrudd.

Beslutning om teleavlytting treffes av domstolen på begjæring fra en pågripelsesbemyndiget tjenestemann, jf. 10 kap. 5 § 1 mom. Tillatelse kan gis for høyst en måned av gangen, jf. 2 mom.

«Teleövervakning» reguleres i tvångsmedelslagen 10 kap. 6 §. Metoden innebærer at identifiseringsopplysninger om en meddelelse som har blitt sendt fra eller til en teleadresse eller teleterminalinnretning som er koblet til et allment kommunikasjonsnett eller nett som er koblet til et slikt, hentes inn, eller at opplysninger om en teleadresse eller teleterminalinnretning hentes inn eller blir forhindret brukt. Tillatelsen kan gjelde en teleadresse eller teleterminalinnretning som en mistenkt besitter eller på annen måte kan antas å bruke. Metoden kan benyttes i etterforskningen av lovbrudd med en strafferamme på minst fire års fengsel, samt ved lovbrudd som er begått ved bruk av en teleadresse eller teleterminalinnretning dersom strafferammen er minst to år. I tillegg kan teleovervåking benyttes i etterforskningen av visse særskilt angitte lovbrudd, herunder hallikvirksomhet, narkotikalovbrudd, forberedelse til terrorvirksomhet, grov tollkriminalitet og grov skjuling av ulovlig utbytte, jf. 6 § 2 mom.

Beslutning om teleovervåking treffes av retten på begjæring fra en pågripelsesbemyndiget tjenestemann, jf. 9 §. Pågripelsesbemyndigede tjenestemenn er imidlertid gitt hastekompetanse i tilfeller der spørsmålet ikke kan utsettes. Tillatelse til teleovervåking gis for høyst en måned av gangen.

7.3.4 Islandsk rett

Reglene om telefonavlytting og lignende inngrep finnes i straffeprocessloven kapitel 11. Inngrep kan etter § 80 bestå i å pålegge et teleselskap å gi opplysninger om telefonsamtaler eller annen kommunikasjon i en bestemt telefon, datamaskin eller

annet kommunikasjonsapparat. Videre kan politiet etter § 81 pålegge teleselskapet å tillate avlytting eller opptak av telefonsamtaler eller annen tilsvarende telekommunikasjon med et bestemt kommunikasjonsapparat, eller kommunikasjonsapparat som tilhører en bestemt person eller som vedkommende har rådighet over. Likeledes kan politiet gis tillatelse til å avlytte telekommunikasjon og foreta opptak av denne med utstyr som er beregnet til dette formål.

For bruk av de her nevnte metoder er det en forutsetning at inngrepet skjer som ledd i etterforskningen av en sak. Videre må inngrepet antas å gi opplysninger som anses for å være av vesentlig betydning for etterforskningen, jf. § 83, stk. 2. For avlytting og opptak som nevnt i § 81, er det dessuten et vilkår at saken gjelder lovbrudd som kan straffes med fengsel i åtte år eller mer, eller at vektige samfunnsinteresser eller private interesser gjør inngrepet påkrevet. Beslutning om inngrep treffes av retten ved kjennelse for en periode på inntil fire uker av gangen, jf. § 84.

7.4 Kravet til den straffbare handling

7.4.1 Generelt

Som det fremgår av proposisjonen punkt 6.1.4 mener departementet at adgangen til å benytte skjulte etterforskningsmetoder fremdeles bør være knyttet til det enkelte straffebuds øvre strafferamme. Dette gjelder også for kommunikasjonskontroll etter straffeprosessloven § 216 a og § 216 b. Visse kriminalitetsformer representerer imidlertid en slik etterforskningsmessig utfordring at det er nødvendig å tillate ekstraordinære metoder selv om strafferammekravet ikke er oppfylt. For kommunikasjonskontroll er behovet reflektert ved at straffeprosessloven § 216 a og § 216 b opplister visse enkeltstraffebud som kan begrunne slik metodebruk, uavhengig av strafferamme (begge bestemmelser første ledd bokstav b).

Metodekontrollutvalget behandler i sin utredning punkt 16.4 side 184 flg. kravet til den straffbare handling ved bruk av kommunikasjonskontroll. Det vurderes her om det er grunn til å *innsnevre* gjeldende adgang til kommunikasjonskontroll i etterforskningen, eller om man bør *utvide* adgangen til å gjelde flere straffebud enn i dag. Departementet vurderer utvalgets konklusjoner i punkt 7.4.2 flg. Etter høringsrunden har departementet dessuten funnet grunn til å vurdere behovet for kommunikasjonskontroll ved enkelte andre typer lovbrudd enn dem utvalget behandler.

7.4.2 Narkotikaovertredelse

7.4.2.1 Gjeldende rett

Straffeloven § 231 gjelder simpel narkotikaovertredelse. Bestemmelsen rammer den som «ulovlig tilvirker, innfører, utfører, erverver, oppbevarer, sender eller overdrar stoff som etter regler med hjemmel i legemiddelloven § 22 er å anse som narkotika». Bruk og besittelse rammes ikke av straffeloven, men av de mildere bestemmelsene i legemiddelloven. Strafferammen for simpel narkotikaovertredelse er bøter eller fengsel inntil to år. Bestemmelsen er en videreføring av straffeloven 1902 § 162 første ledd, med samme strafferamme.

Med en øvre strafferamme på to års fengsel tilfredsstiller straffeloven § 231 (straffeloven 1902 § 162 første ledd) i utgangspunktet ikke strafferammekravet for bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a eller annen kontroll av kommunikasjonsanlegg etter § 216 b. I begge bestemmelser er imidlertid § 231 i sin helhet tatt med i oppregningen av straffebud som kan gi grunnlag for slik metodebruk.

7.4.2.2 Metodekontrollutvalgets forslag

Metodekontrollutvalget vurderer i sin utredning punkt 16.4.2 side 184–185 om adgangen til å benytte kommunikasjonskontroll ved simple narkotikaovertredelser bør oppheves. Det peker på at strafferammen klart skiller seg fra utgangspunktet om at kommunikasjonsavlytting og annen kommunikasjonskontroll bare kan brukes ved mistanke om lovbrudd som kan straffes med fengsel i henholdsvis ti og fem år. Utvalget fremhever videre at det ikke er en tilstrekkelig begrunnelse for å beholde adgangen, at narkotikakriminalitet har vært inkludert siden det først ble åpnet for telefonkontroll ved midlertidig lov 17. desember 1976 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen.

Utvalget legger til grunn at kommunikasjonskontroll normalt ikke brukes ved mistanke om simpel narkotikaovertredelse, og at slik metodebruk lett ville bli ansett uforholdsmessig i lys av straffeprosessloven § 170 a. Etter utvalgets oppfatning kan det likevel tenkes situasjoner hvor bruk av kommunikasjonskontroll kan aksepteres, eksempelvis ved mistanke om salg til mindreårige. Det vises herunder til en høringsuttalelse fra politimesteren i Narvik, som ble avgitt i forbindelse med Metodeutvalgets utredning i NOU 1997: 15. Politimesteren uttalte her (gjengitt i Ot.prp.nr. 64 (1998–99) punkt 8.3.1.3 side 43):

> «Metodeutvalget uttaler at det sjelden vil være aktuelt å anvende telefonkontroll i saker etter strl. § 162, første ledd. En er ikke enig i dette. Mange små og mellomstore politidistrikt vil ikke kunne vise til narkotikasaker av det omfang som de store byer har. Det betyr ikke at narkotika*problemene* er mindre.
>
> Som eksempel kan nevnes at et hasjparti på henimot ett kilo langt på vei vil dekke etterspørselen i en periode for store deler av brukermiljøet i Narvik by. Man er fremdeles innenfor strl. § 162 første ledd. Tradisjonell etterforskning som spaning og infiltrasjon er vanskeligere på små steder enn i store bymiljøer. Vår erfaring er at telefonkontroll ofte er et avgjørende tiltak for å kunne få kunnskap om og kartlegge leverandører og mottakere i slike saker for derved å bryte tilførselslinjene til tettsteder i politidistrikt av vår størrelse.»

Når utvalget har kommet til at det fremdeles bør være åpent for kommunikasjonskontroll i simple narkotikasaker, er dette særlig fordi narkotikakriminalitet har kjennetegn som kan rettferdiggjøre skjult tvangsmiddelbruk. Herunder er det tale om en kriminalitetsform hvor offeret ikke kan forventes å bidra til oppklaring, som forutsetter en viss organisasjon og profesjonalitet, og som ofte er grenseoverskridende. Utvalget legger videre til grunn at bruk av andre etterforskningsmetoder, som spaning og infiltrasjon, ofte vil være vanskelig i de aktuelle miljøene.

Avgjørende for utvalgets vurdering har også vært at all narkotikakriminalitet springer ut fra noe større. I initialfasen kan det være vanskelig å identifisere omfanget av lovbruddet og derfor problematisk å vurdere om mistanken knytter seg til overtredelse av straffeloven 1902 § 162 første eller annet ledd (straffeloven §§ 231 eller 232 første ledd). Utvalget har på denne bakgrunn kommet til at det ikke vil tilrå å fjerne adgangen til kommunikasjonskontroll i saker om simpel narkotikaovertredelse.

7.4.2.3 Høringsinstansenes syn

I høringsrunden er det bare *Forsvarergruppen av 1977* og *Norsk forening for kriminalreform (KROM)* som har uttalt seg om kommunikasjonskontroll i etterforskning av simple narkotikaovertredelser. Begge argumenterer for at adgangen til å bruke metoden bør oppheves.

KROM mener bruk av skjulte etterforskningsmetoder utgjør et så alvorlig inngrep at det må forbeholdes saker med en høyere strafferamme enn straffeloven 1902 § 162 første ledd (straffeloven § 231). Foreningen understreker at kommunikasjonskontroll er personvernkrenkende overfor den eller de mistenkte, men også rammer en rekke uskyldige tredjepersoner. Den mener også at synlig politi og ordinære etterforskningskritt vil være mindre integritetskrenkende, mer preventivt og tilstrekkelig i relasjon til den narkotikakriminaliteten det her er tale om.

KROM er videre uenig i utvalgets antakelse om at all narkotikakriminalitet springer ut av noe større og at dette kan begrunne bruk av kommunikasjonskontroll også i mindre alvorlige saker. Dersom virksomheten springer ut av noe større, må det etter *KROM*s syn foreligge skjellig grunn til mistanke om dette større, før skjulte etterforskningskritt iverksettes.

Også *Forsvarergruppen av 1977* kommenterer argumentet om at mindre alvorlig narkotikakriminalitet bunner i noe større og at det i initialfasen ofte er vanskelig å identifisere omfanget:

> «Forsvarergruppen mener at dette er en merkelig form for sirkelresonnering, som dessuten står i kontrast til den måte utvalget argumenterer i forhold til de øvrige drøftelsene i utredningen. I motsetning til utvalgets generelle, klare standpunkt om at kun alvorlige handlinger kan begrunne denne type tvangsmidler, dog med noen unntak når det er særlig begrunnet osv, hopper man her bukk over det hele, tar snarveien innom en ullen empirisk påstand, og ender opp med at «holder ikke mistanken til et mer alvorlig forhold, så skal det kunne igangsettes et tvangsmiddel på bakgrunn av mistanke om et mindre alvorlig forhold» — altså noe som ser ut som et forsøk på å komme seg rundt beviskravet ift de mer alvorlige narkotikaforbrytelser.»

Forsvarergruppen anfører videre at i det store flertall av narkotikasakene der det er behov for kommunikasjonskontroll, er det straffeloven 1902 § 162 annet og tredje ledd (straffeloven § 232) som er aktuelle. På denne bakgrunn mener gruppen at verken behovet eller den positive gevinsten taler for å gi hensynet til kriminalitetsbekjempelse større vekt enn hensynene til rettssikkerhet og personvern i dette spørsmålet.

Både *Forsvarergruppen av 1977* og *KROM* er dessuten skeptiske til synspunktene om narkotikaproblemer i små og mellomstore politidistrikt knyttet til uttalelsene fra politimesteren i Narvik. De peker blant annet på at integritetskrenkelsen ved bruk av kommunikasjonskontroll kan bli større på småsteder enn i større byer.

7.4.2.4 Departementets vurdering

Straffeloven § 231 om simpel narkotikaovertredelse (straffeloven 1902 § 162 første ledd) har en strafferamme på bøter eller fengsel inntil to år. Departementet ser at lovbruddets alvorlighetsgrad dermed kan fremstå lav sammenliknet med kravet til henholdsvis ti og fem års strafferamme i straffeprosessloven § 216 a første ledd bokstav a og § 216 b første ledd bokstav a. Departementet er likevel enig med utvalget i at det på nåværende tidspunkt ikke er grunnlag for å oppheve politiets adgang til å iverksette kommunikasjonskontroll ved mistanke om simpel narkotikaovertredelse.

Grensegangen mellom straffeloven §§ 231 og 232 første ledd (straffeloven 1902 § 162 første og annet ledd) om grov narkotikaovertredelse knytter seg i praksis hovedsakelig til kvantum narkotika. Selv med et forholdsvis lite kvantum stoff, vil det imidlertid kunne oppstå situasjoner som nødvendiggjør og berettiger kommunikasjonskontroll. Dette kan for eksempel gjelde saker om salg av narkotika til mindreårige på skoler eller til andre utsatte grupper. Til tross for at simpel narkotikaovertredelse har en forholdsvis lav øvre strafferamme, representerer lovbrudd som her nevnt et alvorlig samfunnsproblem som krever effektive etterforskningsmetoder.

Narkotikakriminaliteten har visse kjennetegn som gjør den særlig utfordrende å avdekke og iretteføre. Det er tale om såkalt offerløs kriminalitet, hvor de involverte i liten grad kan forventes å inngi anmeldelse eller på annen måte bidra til oppklaring. Deler av virksomheten foregår dessuten ofte i godt organiserte og lukkede miljøer, og utøves av særlig sikkerhetsbevisste aktører. Videre kan virksomheten ha betydelige internasjonale forgreininger. Disse forhold gjør at kunnskap om narkotikakriminalitet er vanskelig å skaffe til veie ved bruk av tradisjonelle etterforskningsmetoder som spaning og infiltrasjon.

Etter departementets vurdering er politiets faktiske bruk av kommunikasjonskontroll egnet til å illustrere behovet for skjult tvangsmiddelbruk i narkotikasaker. Det fremgår av de siste års rapporter fra Kontrollutvalget for kommunikasjonskontroll at om lag 70–80 % av avlyttingene som gjennomføres, knytter seg til narkotikakriminalitet. Det fremgår ikke hvor stor andel av sakene som gjelder simple narkotikaovertredelser etter straffeloven § 231 (straffeloven 1902 § 162 første ledd). Tallene viser likevel narkotikakriminalitet som det primære anvendelsesområdet for kommunikasjonskontroll, og understøtter et generelt behov for adgang til å bruke metoden i denne sakstypen.

Departementet antar også at en ordning hvor kommunikasjonskontroll tillates i saker som gjelder grov, men ikke simpel narkotikaovertredelse, vil kunne være utfordrende å praktisere. I en tidlig fase av etterforskningen vil det ofte være vanskelig å identifisere omfanget av lovbruddet, herunder om det omfattes av straffeloven §§ 231 eller 232 første ledd (straffeloven 1902 § 162 første eller annet ledd). Som det ble poengtert i forbindelse med vedtakelsen av 1976-loven, må politiet ofte «starte med å undersøke «detaljistleddet», for deretter å arbeide seg videre tilbake til de ledende forbrytere som står bak virksomheten», jf. Ot.prp. nr. 10 (1976–77) punkt 6 side 6. Etter departementets oppfatning har dette synspunktet fremdeles gyldighet.

Det er likevel grunn til å understreke at adgangen til bruk av kommunikasjonskontroll i simple narkotikasaker er underlagt vesentlige begrensninger. Etter straffeprosessloven § 170 a kan ethvert tvangsmiddel bare brukes når det er tilstrekkelig grunn til det, og inngrepet etter sakens art og forholdene ellers ikke vil være uforholdsmessig. Departementet antar at forholdsmessighetskravet vil ha særlig betydning i saker som gjelder simple narkotikaovertredelser. Det er dessuten grunn til å tro at ressurshensyn og behovet for prioritering i politiet i praksis bidrar til at kommunikasjonskontroll relativt sjelden benyttes i saker som gjelder straffeloven § 231. Departementet antar derfor at bruken av kommunikasjonskontroll først og fremst vil gjelde de mer alvorlige sakene, men at adgangen til slik tvangsmiddelbruk ved mistanke om simpel narkotikaovertredelse bør beholdes som en sikkerhetsventil i de sakene det likevel er nødvendig.

7.4.3 Grov menneskesmugling

7.4.3.1 Gjeldende rett

Strafferegler om menneskesmugling er inntatt i lov 15. mai 2008 nr. 35 om utlendingers adgang til riket og deres opphold her (utlendingsloven) § 108. *Simpel* menneskesmugling straffes etter bestemmelsens fjerde ledd bokstav b, som rammer det å hjelpe «en utlending til ulovlig å reise inn i riket eller til et annet land». *Grov* menneskesmugling karakteriseres av at smuglingen skjer med vinnings hensikt, samt enten foregår som ledd i organisert ulovlig virksomhet eller medfører livsfare for den smuglede, jf. § 108 femte ledd.

Paragraf 108 femte ledd bokstav a retter seg mot den som «i vinnings hensikt driver organisert ulovlig virksomhet med sikte på å hjelpe utlendinger til å reise inn i riket eller til en annen stat». Bestemmelsen rekker forholdsvis vidt, og er ment å ramme «både den som åpent sier til vedkommende utlendinger at de ikke fyller vilkårene for å få oppholdstillatelse i Norge, men at han kan hjelpe dem med innreisen og så får de selv prøve å få bli i landet, og den som organiserer reiser til Norge for utlendinger som fyller kravene for å få bli her, f.eks. flyktninger som oppfyller vilkårene for å få asyl», jf. Ot.prp.nr. 46 (1986–87) punkt IV side 252.

Paragraf 108 femte ledd bokstav b rammer situasjoner hvor noen «i vinnings hensikt hjelper en utlending til ulovlig å reise inn i riket eller til en annen stat dersom handlingen medfører at personen som berøres av handlingen blir utsatt for livsfare». Eksempler omfatter situasjoner hvor mennesker er fraktet i stengte containere som har gått tom for oksygen, hvor havområder er forsøkt krysset på små flåter eller mangelfullt utstyrte båter, eller hvor mennesker er fraktet om bord i lasterom på fly, jf. Vevstad (red.): Utlendingsloven kommentarutgave (Oslo, 2010) side 625.

Strafferammen for grov menneskesmugling er bot eller fengsel inntil seks år. Strafferammen tilfredsstiller følgelig kravet for bruk av kommunikasjonskontroll etter straffeprosessloven § 216 b, men ikke kommunikasjonsavlytting etter § 216 a.

7.4.3.2 Metodekontrollutvalgets forslag

Metodekontrollutvalget vurderer i utredningen punkt 16.4.3 side 187 flg. om det bør åpnes for bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a i saker om grov menneskesmugling. Bakgrunnen er blant annet at Riksadvokaten i flere brev til Justis- og beredskapsdepartementet har bedt om en slik vurdering. Utvalget anser menneskesmugling for å være en alvorlig kriminalitetsform, som har flere av de kjennetegn som kan rettferdiggjøre skjult tvangsmiddelbruk. Det peker særlig på at ofrene normalt vet at de involverer seg med ulovlig virksomhet, og at de ofte oppholder seg ulovlig i forskjellige land under transporten og i ankomstlandet. Ofrene vil derfor gjerne være tilbakeholdne med å samarbeide med politiet. Videre viser utvalget til at menneskesmugling nødvendigvis har internasjonale forgreininger, og derfor kan være vanskelig å kartlegge. Særlig vil det kunne være vanskelig å nå frem til bakmennene gjennom tradisjonell etterforskning.

Samtidig peker utvalget på at tiltak mot menneskesmugling også kan ramme en svært sårbar gruppe – de smuglede. Det presiserer derfor at eventuelle skjulte tvangsmidler bare bør kunne brukes mot dem som med skjellig grunn kan mistenkes for menneskesmuglingen. De smuglede selv skal ikke kunne være gjenstand for slik tvangsmiddelbruk.

Etter dette konkluderer utvalget med at det bør åpnes for bruk av kommunikasjonsavlytting i saker om grov menneskesmugling. Det går derfor inn for at utlendingsloven 1988 § 47 fjerde ledd, som nå er erstattet av utlendingsloven 2008 § 108 femte ledd, tilføyes listen over straffebud som kan begrunne slik avlytting i straffeprosessloven § 216 a første ledd bokstav b.

7.4.3.3 Høringsinstansenes syn

Politidirektoratet, *Riksadvokaten, Det nasjonale statsadvokatembetet (NAST), Oslo statsadvokatembeter, Oslo politidistrikt, Østfold politidistrikt, Norges politilederlag* og *Politiets Fellesforbund* støtter utvalgets forslag om at det åpnes for bruk av kommunikasjonsavlytting i saker om grov menneskesmugling. *Advokatforeningen* er imot forslaget.

Østfold politidistrikt fremhever at det her er tale om en kriminalitetsform hvor både gjerningsmann og offer ofte har interesse i at forholdet ikke blir avdekket, noe som vanskeliggjør etterforskningen. Det pekes videre på at menneskesmuglingen ofte foregår som ledd i organisert kriminalitet, med avsenderapparat i utlandet og mottakerapparat her i landet. Politidistriktet mener at kommunikasjonskontroll vil være et godt virkemiddel for å avdekke slik ulovlig virksomhet.

NAST understreker hensynet til internasjonalt politisamarbeid, og finner det uheldig at Norge er et av få land i Vest-Europa hvor politiet ikke har adgang til å bruke kommunikasjonskontroll i menneskesmuglingssaker.

Riksadvokaten viser i høringsuttalelsen til sitt brev til departementet 3. april 2002, med senere oppfølgingsbrev 5. juli 2004 og 25. april 2007. I brevene tilrår embetet at utlendingslovens bestemmelse om grov menneskesmugling tilføyes listen over straffebud som kan gi adgang til bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a. Fra brevet av 2002 hitsettes:

> «Behovet for kunne bruke kommunikasjonsavlytting i menneskesmuglingssaker ble tatt opp med riksadvokaten i brev fra Kriminalpolitisentralen av 11. desember 2001. Det er vist til erfaringene fra Danmark hvor det er åpnet adgang

til å bruke kommunikasjonsavlytting i denne sakstype. I tillegg til de oppgaver som er inntatt i brevet fra Kripos kan nevnes: I perioden 1998-2001 hadde Danmark ca. 45 000 registrerte asylsøkere, og mens tallet i Norge var ca. 43 000. Danmark avdekket i samme periode knapt 1 600 menneskesmuglingssaker, mens tallet i Norge var ca. 260. Det må være grunn til å anta at deler av denne formidable forskjell i effektivitet må ha sammenheng med de etterforskningsmetoder politiet har adgang til å benytte idet problemets reelle omfang ikke kan være så mye mindre i Norge.

Menneskesmuglingssaker har det til felles med narkotikakriminaliteten at både de som står for kriminaliteten og de som reelt sett er offer for den, ønsker å holde virksomheten skjult for de rettshåndhevende myndigheter. Når forhold avdekkes, er erfaringene at ingen av de involverte synes interessert i å gi opplysninger som kan bidra til oppklaring. I tillegg følger det at menneskesmuglingskriminaliteten med nær sagt iboende nødvendighet må være grenseoverskridende og følgelig er det uheldig med for store forskjeller mellom de nordiske land i spørsmålet om hvilke metoder som kan benyttes.»

Riksadvokaten bekrefter å være av samme syn i dag.

Politiets Fellesforbund kommenterer utvalgets uttalelser om at det ikke skal være adgang til å avlytte kommunikasjonsmidler som disponeres av ofrene for menneskehandelen:

«Utvalget poengterer at de smuglede er svært sårbare personer som ikke vil kunne være gjenstand for tvangsmiddelbruk. PF er på prinsipielt grunnlag enig i dette, men ønsker å understreke ofte vil bakmenn som smugler barn til Norge utstyre ofrene med telefoner og benytte disse til å gi ordre (jf. Kineserbarnsaken).

Det bør derfor være mulig å avlytte telefoner som reelt sett eies av bakmenn, men som disponeres av ofrene. Erfaring har vist at disse bakmennene ofte oppholder seg i land hvor det er juridisk/praktisk krevende å få iver[k]satt kommunikasjonskontroll.»

Advokatforeningen er den eneste høringsinstansen som uttrykkelig går imot utvalgets forslag. Foreningen begrunner sin skepsis med prinsipielle betenkeligheter knyttet til utvidelse av adgangen til skjult tvangsmiddelbruk:

«Advokatforeningen ser at politiet for sitt arbeid kan ønske seg størst mulig frihet til å anvende flest mulige tvangsmidler under sin etterforsking — for så vidt uavhengig av strafferammer. I særlig grad når det er tale om skjulte tvangsmidler, vil imidlertid disse hensyn umiddelbart komme i konflikt med så vel hensynet til personvernet for den eller de berørte enkeltpersoner som med de samme personers krav på og berettigede forventning om rettssikkerhet.

Advokatforeningen ser med bekymring på at slike viktige hensyn stadig blir skjøvet til side til fordel for påståtte behov for mer effektive etterforskingsmetoder. Om slike tendenser, som over tid jevnlig har fått utvikle seg så å si alltid i samme retning, ikke avgrenses til det strengt samfunnsmessig nødvendige, vil dette ikke bare påvirke enkeltindividets følelse av trygghet, egenverdi og respekt for eget privatliv. Det også bidra til å bryte ned maktapparatets — og derved selve statens — avstand til og respekt for det enkelte menneskes behov for privatliv, individualitet og naturlige ønske om i private sammenhenger å kunne gi uttrykk for sine meninger, opplevelser, lengsler, fantasier eller drømmer uten at det offentlige maktapparat i det skjulte overvåker, sensurerer og eventuelt forfølger ytringenes innhold eller mulige konsekvenser av disse.»

Foreningen mener derfor at mistanke om grov menneskesmugling ikke bør kunne gi grunnlag for bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a.

7.4.3.4 Departementets vurdering

Departementet finner innledningsvis grunn til å understreke at menneskesmugling er en svært alvorlig kriminalitetsform, som innebærer et angrep på offentlige så vel som private interesser. I tillegg til å representere et betydelig samfunnsmessig problem, er det tale om aktiviteter som utnytter en særlig sårbar gruppe – de smuglede. Dette er mennesker som ofte betaler betydelige summer for å komme seg ut av en desperat situasjon, og som risikerer å måtte betale gjeld til smuglerne i lang tid. Utlendingslovens straffebestemmelse om menneskesmugling er blant annet ment å skulle beskytte denne sårbare gruppen mot utnyttelse. For at beskyttelsen skal være reell, er det etter departementets syn nødvendig at politiet har tilgang på etterforskningsverktøy som kan avdekke smuglingen på en effektiv måte.

Som både utvalget og enkelte høringsinstanser peker på, har menneskesmugling visse særtrekk som gjør den til en særlig utfordrende kriminalitetsform å etterforske. Det er som regel tale om en godt organisert virksomhet, som nødvendigvis har internasjonale forgreininger. Dette gjør det vanskelig for politiet å nå frem til bakmennene ved hjelp av tradisjonelle etterforskningsmetoder. Ettersom ofrene for menneskehandelen vet om – og selv har interesse av – den ulovlige virksomheten, vil de som regel være tilbakeholdne med å samarbeide med politiet. Dette gjør det særlig utfordrende å skaffe bevis som er tilstrekkelige til å iretteføre de ansvarlige for smuglingen. Departementet er enig i at disse forhold taler for at politiet gis ytterligere virkemidler i etterforskningen av menneskesmuglingssaker.

Departementet har merket seg Advokatforeningens bekymring for at hensynet til borgernes personvern og rettssikkerhet settes til side ved utvidelse av politiets hjemler for skjult tvangsmiddelbruk. Dette er tungtveiende hensyn, som kontinuerlig må avveies mot etterforskningsmessige behov. Når det gjelder menneskesmugling, mener imidlertid departementet at særtrekkene ved kriminalitetsformen gjør at politiet på nærmere vilkår bør ha anledning til å benytte kommunikasjonsavlytting. Det vises særlig til de etterforskningsmessige utfordringer som er pekt på ovenfor. Hvorvidt metoden skal anvendes i en konkret sak, vil selvsagt bero på de konkrete omstendighetene, herunder om det er forholdsmessig etter straffeprosessloven § 170 a.

Med hensyn til merknadene fra Metodekontrollutvalget og Politiets Fellesforbund om hvorvidt kommunikasjonsavlytting kan rettes mot de smuglede, viser departementet til ordlyden i straffeprosessloven § 216 a tredje ledd. Det fremgår at avlyttingen kan rettes mot «bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke». Ordlyden i den nevnte bestemmelsen er avgjørende for hvilke kommunikasjonsmidler det i den enkelte sak er adgang til å avlytte. Departementet kan ikke se at dette spørsmålet vil stå i noen særstilling ved bruk av kommunikasjonsavlytting i menneskesmuglingssaker.

7.4.4 Menneskehandel

7.4.4.1 Gjeldende rett

Menneskehandel rammes av straffeloven § 257 (straffeloven 1902 § 224), som ble inntatt ved lov 4. juli 2003 nr. 78 på bakgrunn av Norges ratifisering av Palermoprotokollen for å forebygge, bekjempe og straffe handel med mennesker, særlig kvinner og barn. Paragraf 257 første ledd setter straff for den som ved vold, trusler, misbruk av sårbar situasjon eller annen utilbørlig atferd utnytter en person til prostitusjon eller andre seksuelle ytelser, arbeid eller tjenester, herunder tigging, krigstjeneste i fremmed land eller fjerning av vedkommendes organer, eller som forleder en person til å la seg bruke til slike formål.

Mens første ledd retter seg mot den som står for selve utnyttelsen eller forledelsen, rammer annet ledd de typiske bakmannshandlinger. Bestemmelsen setter straff for den som legger forholdene til rette for tvang, utnyttelse eller forledelse som nevnt i første ledd ved å anskaffe, transportere eller motta den fornærmede, som på annen måte medvirker til tvangen, utnyttelsen eller forledelsen, som gir betaling eller annen fordel for å få samtykke til utnyttelsen fra en person som har myndighet over den fornærmede, eller som mottar slik betaling eller annen fordel. Formålet er blant annet å ramme dem som sørger for den nødvendige infrastruktur for at utnyttelse eller forledelse som nevnt i første ledd kan skje, jf. Ot.prp.nr. 62 (2002–2003) punkt 6.5.1.3 side 64.

Dersom en handling som nevnt i § 257 første eller annet ledd er begått mot en person som er under 18 år, kan den i henhold til tredje ledd straffes uavhengig av om det er anvendt vold, trusler, misbruk av sårbar situasjon eller annen utilbørlig atferd. Villfarelse om alder utelukker ikke straffeskyld, med mindre ingen uaktsomhet foreligger i så måte. Strafferammen for simpel menneskehandel er i alle tilfelle fengsel inntil fem år.

Straffeloven 1902 § 224 om menneskehandel er videreført med enkelte språklige endringer i straffeloven §§ 257 og 258. Strafferammen for alminnelig menneskehandel er hevet til fengsel i seks år, mens grov menneskehandel fremdeles skal kunne straffes med fengsel inntil ti år. Endringen skyldes at fem års strafferamme på generelt grunnlag ikke er videreført i den nye straffeloven.

Med en strafferamme på fem (og seks) års fengsel, kan mistanke om simpel menneskehandel gi grunnlag for bruk av kommunikasjonskontroll etter straffeprosessloven § 216 b, men ikke avlytting etter § 216 a. Gjelder mistanken grov overtredelse, som har en strafferamme på ti års fengsel, kan også avlytting etter § 216 a benyttes. Det samme gjelder dersom lovbruddet kan knyttes til aktivitetene til en organisert kriminell gruppe, jf. straffeloven § 79 bokstav c (straffeloven 1902 § 60 a).

7.4.4.2 Metodekontrollutvalgets forslag

På bakgrunn av innspill fra Kripos vurderer utvalget i utredningen punkt 16.4.4 side 188 flg. om kommunikasjonsavlytting bør kunne benyttes i saker om simpel menneskehandel etter straffeloven § 224 første og annet ledd (straffeloven § 257). Utvalget legger her til grunn at enhver form for menneskehandel utgjør alvorlig kriminalitet, som kan få store konsekvenser for dem som rammes. Samtidig legger utvalget vekt på at det i straffeloven går et skille mellom simpel og grov menneskehandel.

Selv om menneskehandel ikke er et typisk offerløst lovbrudd, er det en kriminalitetsform hvor ofrene ikke kan forventes å samarbeide med politiet. Etter utvalgets oppfatning kan dette skyldes ulike forhold, blant annet at de fornærmede ikke ser seg selv som ofre eller at de blir truet av bakmennene. Videre nevnes manglende tillit til politiet og ofrenes ofte svært sårbare situasjon som mulige årsaker til manglende bidrag til oppklaring. Utvalget erkjenner at disse forhold kan tilsi et behov for særskilte etterforskningsmetoder også i simple menneskehandelssaker.

Til tross for dette vil utvalget ikke tilrå at det åpnes for kommunikasjonsavlytting i saker om simpel menneskehandel. Etter utvalgets syn er behovet ikke tilstrekkelig dokumentert. Utvalget fremhever at dersom det er holdepunkter for at handlingen er grov eller skjer som ledd i virksomheten til en organisert kriminell gruppe, vil det allerede i dag være adgang til kommunikasjonsavlytting som følge av at strafferammen øker til fengsel i ti år. Det viser videre til at personer involvert i menneskehandel ofte kan mistenkes også for andre typer lovbrudd som etter omstendighetene kan gi grunnlag for bruk av kommunikasjonsavlytting. Dette gjelder blant annet tvang etter straffeloven 1902 § 222, frihetsberøvelse etter § 223, slaveri etter § 225, trusler etter § 227, legemsbeskadigelse etter § 229 og seksuallovbrudd etter §§ 192 flg (straffeloven §§ 251, 254, 259, 263, 273 og kapittel 26).

Metodekontrollutvalget viser dessuten til at behovet for kommunikasjonsavlytting ikke ble vurdert av departementet ved vedtakelsen av straffeloven 1902 § 224 i 2003. Dette til tross for at Riksadvokaten og Oslo politidistrikt tok opp spørsmålet i høringsrunden. Spørsmålet ble heller ikke tatt opp av justiskomiteens flertall, men kun av et mindretall bestående av representanten for Sosialistisk Venstreparti. Representanten ga uttrykk for samme synspunkter som Riksadvokaten og Oslo politidistrikt, og foreslo at straffeloven 1902 § 224 skulle legges til i opplistingen av straffebud som kan gi grunnlag for kommunikasjonsavlytting etter straffeprosessloven § 216 a første ledd bokstav b. Mindretallets forslag ble ikke fulgt opp i den videre stortingsbehandlingen. Mot denne bakgrunn legger utvalget til grunn at spørsmålet om kommunikasjonsavlytting i simple menneskehandelssaker relativt nylig har vært vurdert av både departement og Storting, uten at det har fremkommet sterke argumenter for å innføre en slik adgang.

7.4.4.3 Høringsinstansenes syn

Advokatforeningen og *Forsvarergruppen av 1977* støtter utvalgets vurderinger, og ønsker ikke at adgangen til kommunikasjonsavlytting utvides til saker om simpel menneskehandel. *Politidirektoratet, Riksadvokaten, Asker og Bærum politidistrikt, Hordaland politidistrikt, Oslo politidistrikt* og *Politiets Fellesforbund* er uenig i utvalgets syn.

Forsvarergruppen av 1977 fremhever at kommunikasjonsavlytting er et av de potensielt mest invaderende virkemidler som politiet er gitt, og uttrykker bekymring for å la effektivitetshensyn få for stor vekt. Foreningen mener derfor at det ikke bør innføres adgang til kommunikasjonsavlytting i saker etter straffeloven 1902 § 224 første og annet ledd (straffeloven § 257). *Advokatforeningen* forankrer samme standpunkt i prinsipielle motforestillinger til en utvidelse av adgangen til skjult tvangsmiddelbruk. Synspunktene er gjengitt i punkt 7.4.3.3 ovenfor.

De øvrige høringsinstansene som uttaler seg, mener det foreligger et dokumentert behov for kommunikasjonsavlytting i simple menneskehandelssaker. *Riksadvokaten* uttaler:

> «Riksadvokaten er ikke enig i at behovet for kommunikasjonsavlytting er for dårlig dokumentert. Det er vel kjent at slik virksomhet foregår i lukkede miljøer og de involverte avdekker sjelden kriminaliteten frivillig. Tvert om gjøres betydelige anstrengelser for å holde virksomheten skjult. Det kan ha mange grunner. For bakmennene gjelder selvsagt at de ikke ønsker sine kriminelle forhold eksponert. Men også for fornærmede er det mange forhold som gjør anmeldelse lite aktuelt. Ofrene kan for eksempel være fysisk forhindret fra å komme i kontakt med politiet eller frykte represalier fra bakmenn mot dem selv eller familie i hjemlandet. Det kan også være at mange fornærmede på grunn av tidligere

> erfaringer generelt ikke har tillit til de rettshåndhevende myndigheter. En ytterligere omstendighet som kan svekke incitamentet til å anmelde er at de fornærmede reelt sett kan ha bedret sin økonomiske situasjon ved virksomheten og at avsløring vil ha dramatiske økonomiske konsekvenser for dem selv og deres familie. Mange av dem som er utsatt for menneskehandel har ikke noe sosialt nettverk her i landet slik at politiets mulighet til å fange opp informasjon gjennom slike kanaler er liten.»

Riksadvokaten peker også på at materiale fra kommunikasjonsavlytting vil kunne være viktig som bevis i menneskesmuglingssaker, ettersom fornærmedes forklaring i slike saker lett vil stå svakt uten støtte i andre bevis.

7.4.4.4 Departementets vurdering

Etter departementets vurdering utgjør menneskehandel en alvorlig kriminalitetsform, som representerer betydelige etterforskningsmessige utfordringer. Dette skyldes at virksomheten ofte er godt organisert og utføres på en måte som gjør det vanskelig å avdekke den og skaffe tilstrekkelige bevis for iretteføring. Omfangsrike nettverk og internasjonale forgreininger gjør det vanskelig for politiet å nå frem med tradisjonelle etterforskningsmetoder som spaning og infiltrasjon. De fornærmede kan dessuten sjelden forventes å samarbeide med politiet, fordi de blir truet av bakmennene eller fordi de ikke har den nødvendige tilliten til myndighetene. Etter hva departementet forstår, kan det også være et problem at de fornærmede ikke blir i Norge lenge nok til å kunne bidra under straffesaken mot bakmennene. Departementet mener dette er forhold som bekrefter et behov for særskilte etterforskningsmetoder i menneskehandelssaker.

Departementet vil dessuten fremheve den nære sammenhengen som foreligger mellom menneskehandel og menneskesmugling som omtalt i punkt 7.4.3 ovenfor. Skillet mellom de to kriminalitetsformene er i Ot.prp. nr. 62 (2002–2003) punkt 6.1 side 55 omtalt slik:

> «Skillet mellom menneskehandel og menneskesmugling trekkes ved hjelp av formålet med handlingene. Ved menneskehandel er formålet å utnytte en person med bestemte tvangsmidler. At handlingen har skjedd over landegrenser er ikke avgjørende for straffbarheten. Ved menneskesmugling er formålet å transportere mennesker ulovlig over landegrenser. Her er det uten betydning for straffbarheten hva personen skal gjøre i mottakerlandet.»

At formålet med handlingen er avgjørende, gjør det vanskelig på et tidlig tidspunkt i etterforskningen å avgjøre hvilket straffebud som vil komme til anvendelse. Det samme gjelder for spørsmålet om handlingen er grov. Dette kan etter departementets syn tilsi at kommunikasjonsavlytting generelt bør være tilgjengelig i menneskehandelssaker uavhengig av alvorlighetsgrad.

Departementet finner ikke å kunne legge samme vekt som utvalget på at kommunikasjonsavlytting allerede i dag kan benyttes ved mistanke om simpel menneskehandel når handlingene skjer som ledd i aktivitetene til en organisert kriminell gruppe. Hvorvidt den nødvendige tilknytningen til organisert kriminalitet er til stede kan være vanskelig å avgjøre på et tidlig tidspunkt i etterforskningen, og det vil dermed kunne herske usikkerhet med hensyn til om kommunikasjonsavlytting kan benyttes. Etter departementets oppfatning er menneskehandel en så alvorlig kriminalitetsform, med så vidtrekkende etterforskningsmessige utfordringer, at tilgangen til kommunikasjonsavlytting her bør stå på egne ben.

Departementet finner videre grunn til å legge vekt på at kommunikasjonsavlytting i betydelig utstrekning er tilgjengelig som etterforskningsverktøy i menneskehandelssaker i de øvrige nordiske land. Samtidig er menneskehandel en kriminalitetsform som ikke kjenner landegrenser. Departementet mener derfor at både muligheten for profesjonelle bakmenn til å kunne tilpasse sin virksomhet etter oppdagelsesrisikoen og hensynet til ensartethet mer generelt, tilsier at kommunikasjonsavlytting bør tillates i simple menneskehandelssaker også i Norge.

7.4.5 Hallikvirksomhet

7.4.5.1 Gjeldende rett

Straffeloven § 315 (straffeloven 1902 § 202 første ledd) retter seg mot såkalt hallikvirksomhet. Bestemmelsen rammer for det første den som «fremmer andres prostitusjon», jf. første ledd bokstav a. Et eksempel på å fremme prostitusjon er det å drive mellommannsvirksomhet eller å organisere sex-klubber der de prostituerte deltar frivillig, jf. Ot.prp. nr. 62 (2002–2003) punkt 13.1 side 97. Videre rammes etter første ledd bokstav b også den som «leier ut lokaler og forstår at lokalene skal brukes til prostitusjon eller utviser grov uaktsom-

het i så måte». Med prostitusjon menes at en person har seksuell omgang eller handling med en annen mot vederlag. Vederlagets form er likegyldig. Oftest vil det være snakk om penger, men det kan også være narkotika, alkohol, mer eller mindre kostbare gjenstander eller motytelser mv., jf. Ot.prp. nr. 28 (1999–2000) punkt 16.1 side 117.

Strafferammen for hallikvirksomhet er bøter eller fengsel inntil fem år.

Bestemmelsen om hallikvirksomhet i straffeloven 1902 § 202 er med enkelte mindre endringer videreført i straffeloven § 315. Strafferammen er hevet fra fem til seks års fengsel, som følge av at fem års strafferamme på generelt grunnlag ikke er videreført i den nye straffeloven. Endringen er ikke ment å ha betydning for straffenivået, jf. Ot.prp. nr. 22 (2008–2009) punkt 16.7 side 449.

Strafferammen på fem (og seks) års fengsel gjør at kommunikasjonskontroll etter straffeprosessloven § 216 b, men ikke avlytting etter § 216 a, kan benyttes i etterforskningen av saker om hallikvirksomhet. Kan lovbruddet knyttes til aktivitetene til en organisert kriminell gruppe, vil strafferammen etter straffeloven § 79 bokstav c (straffeloven 1902 § 60 a) forhøyes, slik at også avlytting etter straffeprosessloven § 216 a kan benyttes.

7.4.5.2 Metodekontrollutvalgets forslag

Spørsmålet om kommunikasjonsavlytting i saker om hallikvirksomhet er ikke eksplisitt inntatt i Metodekontrollutvalgets mandat. På bakgrunn av Stoltenberg II-regjeringens handlingsplan 2006–2009 «Stopp menneskehandelen», samt innspill fra politiet, har utvalget likevel valgt å vurdere spørsmålet. Dette gjøres i utredningen punkt 16.4.5 side 191.

Utvalget understreker her at hallikvirksomhet utgjør en alvorlig straffbar handling. Likevel har utvalget ikke villet tilrå å tillate kommunikasjonsavlytting i halliksaker, da det ikke anser alvorlighetsgraden som tilstrekkelig høy. Utvalget peker herunder på at straffeloven 1902 § 202 (straffeloven § 315) også rammer grovt uaktsomme overtredelser. Det legger dessuten betydelig vekt på at mer tradisjonelle etterforskningsmetoder, som for eksempel spaning, fortsatt må antas å ha stor nytteverdi i halliksaker.

7.4.5.3 Høringsinstansenes syn

Advokatforeningen og *Forsvarergruppen av 1977* støtter utvalgets vurderinger, og mener at det ikke bør åpnes for kommunikasjonsavlytting ved mistanke om hallikvirksomhet. Dette begrunnes med prinsipielle argumenter mot utvidelse av adgangen til skjult tvangsmiddelbruk. Det vises til høringsinstansenes synspunkter gjengitt i punkt 7.4.3.3 og 7.4.4.3 ovenfor.

Politidirektoratet, Riksadvokaten, Oslo politidistrikt og *Politiets Fellesforbund* er uenig i utvalgets vurderinger.

Riksadvokaten og *Oslo politidistrikt*, med tilslutning fra *Politidirektoratet*, fremhever særlig den nære sammenhengen mellom saker om menneskehandel og hallikvirksomhet. Høringsinstansene påpeker at et forhold som viser seg å være menneskehandel, ofte vil begynne som en halliksak. *Riksadvokaten* viser til sine tidligere uttalelser i forbindelse med innføringen av straffebudet om menneskehandel ved lov 4. juli 2003 nr. 78. Det ble i den forbindelse argumentert for at de prosessuelle reglene, herunder adgangen til tvangsmiddelbruk, burde være den samme i halliksaker som i saker om menneskehandel. Embetet hevder at senere erfaringer underbygger behovet for kommunikasjonsavlytting ved mistanke om hallikvirksomhet. Det fremholdes:

> «Det kan, særlig tidlig i etterforskningsfasen, være vanskelig [å] sannsynliggjøre overtredelse av § 224 om menneskehandel. Men det vil gjerne være enklere å fremlegge tilstrekkelige opplysninger til at det kan konstateres skjellig grunn til mistanke i det minste om overtredelse av hallikbestemmelsen. Reelt sett vil det antakelig være liten forskjell på forholdenes straffverdighet og betydningen av å kunne stanse dem.»

Oslo politidistrikt uttaler seg om den antatte nytten av å bruke kommunikasjonsavlytting i saker om hallikvirksomhet:

> «Det er åpenbart at det må foregå en god del kommunikasjon mellom halliken(e) og de prostituerte mens virksomheten pågår. Det er grunn til å tro at en stor del av kontakten skjer pr. telefon, og at innholdet i slike samtaler kan ha stor bevisverdi. Ved åpen etterforskning i slike saker er det naturlig å begynne med å avhøre de prostituerte, og det er rimelig å tro at halliken(e) i etterkant vil ta kontakt for å få vite hva disse eventuelt har forklart til politiet osv. Skulle politiet få adgang til å avlytte halliken(e)s telefon(er) vil dette åpenbart bidra i vesentlig grad til å opplyse saken.»

Politidistriktet mener på denne bakgrunn det er grunnlag for å tillate kommunikasjonsavlytting ved etterforskning av halliksaker.

7.4.5.4 Departementets vurdering

Departementet foreslår i punkt 7.4.4 ovenfor å utvide adgangen til kommunikasjonskontroll i saker som gjelder menneskehandel. Som enkelte høringsinstanser påpeker, er det betydelig nærhet mellom straffbare forhold som rammes av bestemmelsene om henholdsvis menneskehandel og hallikvirksomhet. I begge tilfeller kan det være tale om utnyttelse av andre mennesker, som ofte befinner seg i en vanskelig og sårbar posisjon. Det er likevel grunn til å understreke den betydelige forskjellen i alvorlighetsgrad mellom menneskehandel og hallikvirksomhet. Mens menneskehandel med nødvendighet innbefatter et tvangselement, kan hallikvirksomhet i prinsippet også gå ut på å fremme frivillig prostitusjon.

Departementet ser at hallikvirksomhet – i likhet med menneskehandel – har en del særtrekk som kan vanskeliggjøre bruk av tradisjonelle etterforskningsmetoder. Selv om prostitusjonen som sådan nødvendigvis medfører en viss eksponering, kan den bakenforliggende hallikvirksomheten være vanskelig å avdekke. Dette skyldes blant annet at virksomheten ofte foregår i lukkede miljøer. Ofrene for hallikvirksomheten – de prostituerte – vil dessuten sjelden ønske å bidra til oppklaring. Dette kan skyldes at de ikke ønsker å stanse prostitusjonsvirksomheten, eller at de frykter represalier fra bakmenn eller negative reaksjoner fra andre. Slike argumenter ble tillagt betydelig vekt da Danmark i 2003 åpnet for bruk av kommunikasjonsavlytting i etterforskningen av halliksaker.

Riksadvokaten fremhever i sin høringsuttalelse at det tidlig i etterforskningen er vanskelig å sannsynliggjøre menneskehandel, men at det gjerne foreligger tilstrekkelige indikasjoner på hallikvirksomhet. Høringsinstansen ser dette som et argument for å tillate samme metodebruk i begge sakstyper. Departementet understreker at det er grunn til å vise varsomhet med å tillate inngripende etterforskningsmetoder for å avdekke bakenforliggende kriminell virksomhet. Det klare utgangspunkt må være at det må foreligge skjellig grunn til mistanke om et lovbrudd som i seg selv kan begrunne skjult tvangsmiddelbruk, for at så inngripende virkemidler skal kunne tas i bruk.

På denne bakgrunn har departementet kommet til at det på det nåværende tidspunkt ikke bør gis hjemmel til bruk av kommunikasjonsavlytting i halliksaker. Avgjørende har særlig vært at en adgang til slik tvangsmiddelbruk i prinsippet også ville gjelde i saker hvor den prostituerte samtykker til hallikens virksomhet, og som dermed har en begrenset alvorlighetsgrad. Etter departementets syn kan straffebudets alvorlighetsgrad derfor vanskelig forsvare å åpne for bruk av et så inngripende virkemiddel som kommunikasjonsavlytting.

7.4.6 Frihetsberøvelse

7.4.6.1 Gjeldende rett

Straffeloven § 254 (straffeloven 1902 § 223 første ledd) retter seg mot den som «ved innesperring, bortføring eller på annen måte rettsstridig fratar noen friheten». Eksempler på frihetsberøvelse kan være å holde en person fast, sperre personen inne eller å fjerne gjenstander som er nødvendige for at vedkommende skal kunne flytte på seg. Bestemmelsen stiller ikke krav til frihetsberøvelsens varighet, men det er antatt at ikke enhver kortvarig frihetsberøvelse vil utgjøre en overtredelse av straffebudet, jf. diskusjonen i Bratholm/Matningsdal: Straffeloven kommentarutgave bind II (Oslo, 1995) side 522–523 (til straffeloven 1902).

Bestemmelsen om frihetsberøvelse er en videreføring av straffeloven 1902 § 223, med visse justeringer av språklig og lovteknisk karakter. Strafferammen for ordinær overtredelse er her redusert fra fem år til tre år, jf. straffeloven § 254. Etter ikraftsettingen av straffeloven er det i utgangspunktet ikke adgang til å benytte kommunikasjonskontroll i saker om frihetsberøvelse. Kun dersom lovbruddet kan knyttes til organisert kriminalitet, jf. § 79 bokstav c, vil det være adgang til bruk av kommunikasjonskontroll etter straffeprosessloven § 216 b, men ikke avlytting etter § 216 a. Grov frihetsberøvelse etter straffeloven § 255 har en strafferamme på inntil ti års fengsel, og vil følgelig kunne gi grunnlag for alle former for kommunikasjonskontroll etter straffeprosessloven §§ 216 a og 216 b.

7.4.6.2 Metodekontrollutvalgets forslag og høringsinstansenes syn

Adgangen til bruk av kommunikasjonsavlytting i saker om frihetsberøvelse behandles ikke i Metodekontrollutvalgets utredning. Spørsmålet er i høringsrunden tatt opp av *Riksadvokaten*, samt av *Oslo politidistrikt* med tilslutning fra *Politidirektoratet*.

Riksadvokaten anfører at situasjoner som involverer frihetsberøvelse kan være høyst alvorlige og dramatiske, for eksempel fordi det er grunn til å frykte for den bortførtes liv. Etter høringsinstansens syn bør politiet i slike situasjoner kunne bruke blant annet kommunikasjonsavlytting for å bringe på det rene hvor den bortførte og gjerningsmannen befinner seg. Dette for at vedkommende skal kunne befris så raskt som mulig og for å sikre bevis.

Høringsinstansene opplyser at man i dag benytter nødrett som hjemmel for kommunikasjonsavlytting i frihetsberøvelsessaker. Både *Riksadvokaten* og *Oslo politidistrikt* anser dette som problematisk. *Riksadvokaten* uttaler:

> «I dag dekkes behovet, i alle fall i hovedsak, ved at nødrett brukes som hjemmel for å ta i bruk visse metoder for å avverge alvorlige straffbare handlinger mot liv og helse. Dette er ikke tilfredsstillende. Grensene for nødrett er på dette området usikre og den manglende uttrykkelig lovhjemmel gir liten veiledning. Bruk av nødrett som hjemmel gir heller ikke rettslig kontroll med virksomheten.»

Riksadvokaten og *Oslo politidistrikt* foreslår på denne bakgrunn at straffeloven 1902 § 223 første ledd om frihetsberøvelse (straffeloven § 254) skal gi grunnlag for bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a. Det samme foreslås for hemmelig ransaking etter straffeprosessloven § 200 a, personnær teknisk sporing etter § 202 c, samt kameraovervåking på privat sted etter § 202 a, dersom det åpnes for dette.

7.4.6.3 Departementets vurdering

Frihetsberøvelse rammes av straffeloven § 254 (straffeloven 1902 § 223), som er inntatt i lovens kapittel om vern av den personlige frihet og fred. Plasseringen understreker kriminalitetsformens alvorlighetsgrad, og illustrerer slektskapet med visse andre alvorlige integritetskrenkelser, som for eksempel menneskehandel. En høy alvorlighetsgrad er imidlertid ikke i seg selv en tilstrekkelig begrunnelse for å tillate et så inngripende tvangsmiddel som kommunikasjonsavlytting. Spørsmålet er om det også kan påvises et konkret etterforskningsmessig behov for metoden i saker som gjelder frihetsberøvelse.

Sammenlignet med kriminalitetsformer som menneskesmugling og menneskehandel (omtalt i punkt 7.4.3 og 7.4.4 ovenfor), er saker om frihetsberøvelse ikke i samme grad kjennetegnet ved at man ikke kan forvente at offeret bidrar til oppklaring. Det er derfor neppe grunnlag for å konstatere samme problemer med avdekking og etterforskning som ved de nevnte lovbrudd. Frihetsberøvelsens ofte akutte karakter gjør imidlertid at politiet her støter på andre former for etterforskningsmessige utfordringer. Især i bortføringssaker kan etterforskningen være preget av en tidsnød som gjør det nødvendig å agere umiddelbart for å motvirke fare for den bortførtes liv og helse. Dette gjør det særlig påkrevet med målrettede og effektive etterforskningsmetoder.

Ifølge Riksadvokaten gjør behovet for rask aksjon at politiet i enkelte tilfeller benytter nødrett som grunnlag for bruk av kommunikasjonsavlytting når annen hjemmel ikke foreligger. Det er på det rene at nødrett kan tjene som grunnlag for tvangsmiddelbruk for å avverge eller stanse en fare, eksempelvis ved en pågående frihetsberøvelse. Om dette uttales i Ot.prp. nr. 64 (1998–99) punkt 3.2 side 17:

> «Det kan vanskelig tenkes at nødrett kan gi grunnlag for å bruke etterforskningsmetoder som er forbudt hvis formålet utelukkende er å oppklare en forbrytelse. Men hvis den ulovlige virksomhet ikke er avsluttet, eller hvis det er fare for gjentagelse av alvorlige handlinger, kan nødrett gjøre at politiet kan bruke metoder som ellers er forbudt. I en gisselsituasjon med overhengende fare for gislenes liv vil for eksempel romavlytting kunne foretas hvis det er nødvendig for å få gislene frigitt.»

Departementet understreker samtidig at straffelovens nødrettsbestemmelse er en unntaksregel, som ikke bør fungere som en regulær hjemmel for tvangsmiddelbruk. Når nødrettsbestemmelsen med mer eller mindre jevne intervaller benyttes som grunnlag for kommunikasjonsavlytting ved frihetsberøvelser, er dette etter departementets oppfatning egnet til å demonstrere at det foreligger et behov for ordinær metodetilgang i disse sakene. Ved å gi ordinær hjemmel for bruk av kommunikasjonsavlytting i saker om frihetsberøvelse, gjøres rettsgrunnlaget klarere samtidig som det sikres at tvangsmiddelbruken blir gjenstand for rettslig prøving.

På denne bakgrunn finner departementet det forsvarlig å åpne for kommunikasjonsavlytting etter straffeprosessloven § 216 a i etterforskningen av saker om frihetsberøvelse etter straffeloven § 254. Bruken vil selvsagt være underlagt de alminnelige vilkår og rettssikkerhetsgarantier, herunder for-

holdsmessighetskravet i straffeprosessloven § 170 a. Det foreslås også – med samme begrunnelse – å åpne for hemmelig ransaking etter straffeprosessloven § 200 a, personnær teknisk sporing etter § 202 c samt kameraovervåking på privat sted etter § 202 a i den her omtalte sakstypen, jf. nedenfor i de aktuelle kapitler.

7.4.7 Forberedelse til seksuelle overgrep mot barn (grooming)

7.4.7.1 Gjeldende rett

Straffeloven § 306 (straffeloven 1902 § 201 a) om såkalt grooming ble inntatt ved lov 13. april 2007 nr. 14. Bestemmelsen setter straff for den som har avtalt et møte med et barn under 16 år, og som med forsett om å begå en handling som nevnt i straffeloven §§ 299-304, § 305 bokstav b eller § 311 første ledd bokstav a har kommet frem til møtestedet eller et sted hvor møtestedet kan iakttas. Grooming-bestemmelsen retter seg mot en spesiell type forberedelseshandling, og supplerer det alminnelige forsøksansvaret etter de her nevnte bestemmelsene.

Skyldkravet ved grooming er i utgangspunktet forsett. I tillegg til at gjerningsmannen forsettlig må ha avtalt møtet og kommet frem til det avtalte møtestedet eller et sted hvor møtestedet kan iakttas, må vedkommende dessuten ha hatt forsett om å begå visse handlinger – nærmere bestemt voldtekt av barn under 14 år, seksuell omgang eller handling med barn under 16 år eller tvang eller forledelse av barn under 16 år til å utvise seksuelt krenkende eller annen uanstendig atferd. Med hensyn til barnets alder er skyldkravet uaktsomhet, jf. straffeloven § 307.

Bakgrunnen for at straffebudet om grooming kom inn i straffeloven i 2007 var særlig at nye kommunikasjonsmidler som internett og mobiltelefon hadde gjort barn mer utsatt for overgrep enn tidligere. Formålet med det nye straffebudet var blant annet å gi politiet mulighet til å stoppe planlagte overgrep før selve det fysiske overgrepet er påbegynt, jf. Innst.O. nr. 42 (2006–2007) punkt 2 side 3. Grooming-paragrafen i straffeloven 1902 § 201 a er – med samme begrunnelse – videreført i straffeloven § 306 jf. § 307. Det er imidlertid foretatt en viss utvidelse for å oppfylle kravene i Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk. Utvidelsen består i at forsett om produksjon av fremstilling av seksuelle overgrep mot barn eller som seksualiserer barn, nå kan kvalifisere til straff etter bestemmelsen.

Strafferammen for grooming er etter både straffeloven 1902 og straffeloven fengsel inntil ett år. Strafferammen er følgelig i utgangspunktet for lav til å kunne gi grunnlag for bruk av kommunikasjonskontroll etter straffeprosessloven §§ 216 a eller 216 b.

7.4.7.2 Metodekontrollutvalgets forslag

Da det ble åpnet for kommunikasjonskontroll etter straffeprosessloven § 216 b i groomingsaker, etterlyste Barneombudet i høringsrunden en vurdering av om det også burde åpnes for bruk av avlytting av kommunikasjonsanlegg etter § 216 a. Departementet gikk ikke inn for en slik endring, men viste til Metodekontrollutvalgets pågående arbeid. Blant annet på bakgrunn av Barneombudets innspill har utvalget vurdert om politiet nå bør få adgang til å bruke kommunikasjonsavlytting i grooming-saker (utredningen punkt 16.4.6 side 191 flg.).

Utvalget legger til grunn at seksuelle overgrep mot barn er alvorlige straffbare handlinger, og at hensikten med å kriminalisere grooming – nemlig å avverge slike overgrep – må anses aktverdig. Samtidig betrakter utvalget den gjerning som er kriminalisert i grooming-bestemmelsen som avledet fra selve det seksuelle overgrepet. Groominghandlingen – det å avtale et møte i den hensikt å begå seksuelle overgrep – er etter utvalgets syn ikke i seg selv alvorlig nok til å rettferdiggjøre bruk av et så inngripende tvangsmiddel som kommunikasjonsavlytting.

Utvalget kommenterer også forholdet mellom straffeloven 1902 § 201 a og andre straffebud som gjelder seksuelle overgrep mot barn. I utredningen punkt 16.4.6 side 194–195 uttales:

> «Utvalget peker på at kriminaliseringen av «grooming» må sees i sammenheng med de straffbare handlinger som gjerningspersonen ifølge straffeloven § 201 a må ha til hensikt å begå. Forbudet mot seksuell omgang med barn under 14 år har i mange sammenhenger en strafferamme på fengsel inntil 15 eller 21 år, og skjellig grunn til mistanke om forsøk på slik handling kan således ofte gi grunn til kommunikasjonskontroll både etter §§ 216a og 216b. Seksuell omgang med barn under 16 år kan straffes med fengsel inntil fem år, og kan dermed gi grunn til kontroll av kommunikasjonsanlegg etter § 216b. Seksuell handling med barn under 16 år eller forledelse av barn under 16 år til å utvise seksuelt krenkende eller annen uanstendig atferd kan straffes med fengsel inn-

til tre år, og kan således ikke danne grunnlag for tillatelse etter §§ 216a eller 216b. Det vil imidlertid fremstå som påfallende hvis politiet gis adgang til å bruke straffeprosessuelle tvangsmidler i større grad i etterforskingen av forberedelsen av slike handlinger etter § 201 a, enn i etterforskingen av selve handlingen.»

Følgelig vil utvalget ikke foreslå å gi politiet adgang til kommunikasjonsavlytting i saker om forberedelse til seksuelle overgrep mot barn etter straffeloven 1902 § 201 a (straffeloven § 306).

7.4.7.3 Høringsinstansenes syn

Av høringsinstansene som har uttalt seg, støtter *Riksadvokaten*, *Advokatforeningen* og *Forsvarergruppen av 1977* utvalgets konklusjon. *Riksadvokaten* bemerker at selv om kommunikasjonsavlytting trolig ville vært effektivt i grooming-saker, kan man vanskelig gå inn for at et forhold som kun kan straffes med bøter eller fengsel i inntil ett år skal gi adgang til et så integritetskrenkende tvangsmiddel.

Politidirektoratet, Kripos, Hordaland politidistrikt og *Politiets Fellesforbund* er uenig med utvalget. *Kripos* mener at handlingen som beskrives i straffeloven 1902 § 201 a (straffeloven § 306) må karakteriseres som et selvstendig overgrep, og er følgelig uenig i at grooming i seg selv ikke er tilstrekkelig alvorlig til å begrunne kommunikasjonsavlytting. *Politiets Fellesforbund* anfører på sin side at kommunikasjonskontroll og andre utradisjonelle metoder er nødvendig for å kunne beskytte barn mot overgrep på en effektiv og tilfredsstillende måte. Forbundet peker på at det på tidspunktet for høringen ikke forelå noen domfellelser for grooming, og mener dette skyldes at sakene er svært vanskelige å etterforske. Mangelen på fellende dommer demonstrerer etter høringsinstansens syn at det er behov for nye etterforskningsmetoder.

7.4.7.4 Departementets vurdering

Strafferammen for grooming etter straffeloven § 306 (straffeloven 1902 § 201 a) er bøter eller fengsel inntil ett år. Den foreskrevne straff er dermed atskillig lavere enn strafferammekravet på ti års fengsel som i utgangspunktet gjelder for bruk av kommunikasjonsavlytting. Strafferammen kan ses som et uttrykk for lovgivers oppfatning om at grooming er en kriminalitetsform med begrenset alvorlighetsgrad. På den annen side er det klart at alvorligheten øker ved at ofrene består av en særlig utsatt gruppe – nemlig barn under den seksuelle lavalder.

Grooming-bestemmelsen supplerer det alminnelige forsøksansvaret for seksuelle overgrep mot barn, og må ses i sammenheng med bestemmelser som rammer slike overgrep. Det straffverdige ved grooming knytter seg først og fremst til overgrepsfaren som skapes ved at den voksne har initiert et møte med forsett om å begå overgrep. Alvorligheten ved forberedelseshandlinger vil naturligvis være lavere enn fullbyrdelse av selve overgrepet. Som utvalget påpeker, er det ikke alle fullbyrdede overgrepshandlinger mot barn som kan begrunne kommunikasjonsavlytting. Eksempelvis kan en seksuell handling med barn under 16 år etter straffeloven § 304 (straffeloven 1902 § 200 annet ledd) kun straffes med fengsel inntil tre år. Mistanke om overtredelse kan verken danne grunnlag for kommunikasjonsavlytting etter straffeprosessloven § 216 a eller for annen kontroll av kommunikasjonsanlegg etter § 216 b. Ved å åpne for kommunikasjonsavlytting i grooming-saker, vil politiet gis en videre metodetilgang i etterforskningen av forberedelseshandlingen enn i etterforskningen av selve overgrepet. Departementet er enig med utvalget i at sammenhengen i regelverket derfor taler imot en adgang til kommunikasjonsavlytting ved grooming.

Spørsmålet er om lovbruddet er av en slik art at det likevel er behov for å tillate kommunikasjonsavlytting. Departementet har funnet dette tvilsomt. Grooming-bestemmelsen i straffeloven var særlig begrunnet i utbredelsen av nye elektroniske kommunikasjonskanaler og den økte risikoen for overgrep disse medfører. Det kan derfor anføres at avlytting av kommunikasjonskanalene, for eksempel et chatterom, vil være et virkemiddel som kan bidra til å målrette etterforskningen på en effektiv måte. På den annen side er det grunn til å tro at etterforskning av grooming-saker effektivt kan innrettes også ved bruk av allerede tilgjengelige metoder. Med en øvre strafferamme på ett års fengsel kan politiet iverksette pågripelse og fengsling etter straffeprosessloven § 172 og § 184, ransaking etter straffeprosessloven §§ 192 og 195, skjult fjernsynsovervåking på offentlig sted etter straffeprosessloven § 202 a og avlytting av samtale etter straffeprosessloven § 216 l (samtale som politiet selv deltar i eller med samtykke fra en av samtalepartene). I tillegg kan det gjøre bruk av provokasjon og infiltrasjon innenfor de rammer som er trukket opp gjennom rettspraksis og riksadvokatens retningslinjer, samt overvåke åpne chattesider på samme måte som annen virksomhet i det offentlige rom.

Departementet finner grunn til å kommentere Politiets Fellesforbunds uttalelse om at manglende domfellelser for grooming illustrerer at de her nevnte metoder er utilstrekkelige som etterforskningsverktøy. Det foreligger nå flere eksempler på domfellelser basert på bevis innhentet ved de etterforskningsmetodene som er tilgjengelige i dag, jf. blant annet Høyesteretts avgjørelse i Rt. 2013 side 699. Høringsinstansens beskrivelse av den faktiske situasjonen er følgelig ikke lenger treffende. Etter departementets syn er det ikke godtgjort et tilstrekkelig behov for tilgang på ytterligere verktøy i etterforskningen av grooming-saker. Dette inngår i en helhetsvurdering som gjør at det å åpne for en så inngripende metode som kommunikasjonsavlytting etter departementets syn ville være uforholdsmessig. Departementet har merket seg at også Riksadvokaten er av denne oppfatning.

7.4.8 Fremstilling av seksuelle overgrep mot barn

7.4.8.1 Gjeldende rett

Straffeloven inneholder, som den opphevede straffeloven 1902, en egen bestemmelse om fremstilling av seksuelle overgrep mot barn og fremstilling som seksualiserer barn, jf. straffeloven § 311. I tillegg er det inntatt en ny bestemmelse som setter straff for den som overværer en fremvisning av seksuelle overgrep mot barn eller fremvisning som seksualiserer barn, jf. straffeloven § 310. Bestemmelsen er ment å oppfylle forpliktelsene i Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk.

Straffeloven § 311 rammer ulike former for befatning med fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn. Bestemmelsen kom inn i straffeloven 1902 § 204 a ved endringslov 20. mai 2005 nr. 29, på bakgrunn av anmodningsvedtak fra Stortinget 16. juni 2003 (vedtak nr. 521). Formålet med det nye straffebudet var å synliggjøre forskjellene mellom overgrepsbilder av barn og pornografiske fremstillinger. Herunder skulle bestemmelsen fremheve at forbudet mot overgrepsbilder av barn først og fremst har til formål å beskytte barn mot seksuelle overgrep. Bestemmelsen i straffeloven 1902 § 204 a er innholdsmessig videreført i straffeloven § 311, men med enkelte utvidelser og i en endret lovteknisk utforming.

Straffeloven § 311 første ledd har fem gjerningsalternativer i bokstav a til e. Bokstav a rammer den som «produserer fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn». Bokstav b retter seg mot den som «utgir, tilbyr, selger, overlater til en annen, gjør tilgjengelig eller på annen måte søker å utbre fremstillinger som nevnt i bokstav a». Bokstav c gjelder den som «anskaffer, innfører eller besitter fremstillinger som nevnt i bokstav a, eller forsettlig skaffer seg tilgang til slikt materiale». Bokstav d omfatter den som «holder offentlig foredrag eller istandbringer offentlig forestilling eller utstilling av fremstillinger som nevnt i bokstav a», mens bokstav e gjelder den som «forleder noen under 18 år til å la seg avbilde som ledd i kommersiell fremstilling av rørlige eller urørlige bilder med seksuelt innhold». Som barn regnes personer som er eller fremstår som under 18 år, jf. § 311 annet ledd. Bestemmelsen gjelder ikke for fremstillinger som må anses forsvarlige ut fra et kunstnerisk, vitenskapelig, informativt eller lignende formål, eller for film eller videogram som Medietilsynet ved forhåndskontroll har godkjent til ervervsmessig fremvisning eller omsetning, jf. 311 siste ledd.

Strafferammen for befatning med overgrepsbilder av barn er etter så vel straffeloven 1902 som straffeloven inntil tre års fengsel. Dette tilfredsstiller i utgangspunktet ikke strafferammekravene for bruk av kommunikasjonsavlytting eller annen kommunikasjonskontroll etter straffeprosessloven §§ 216 a og 216 b. Straffeloven § 311 er imidlertid inntatt i opplistingen av enkeltstraffebud i straffeprosessloven § 216 b første ledd bokstav b. Dersom de øvrige vilkår er oppfylt, er det følgelig i dag adgang til å iverksette kontroll av kommunikasjonsanlegg etter § 216 b, men ikke avlytting etter § 216 a, i etterforskningen av saker som gjelder overgrepsbilder av barn.

7.4.8.2 Metodekontrollutvalgets forslag og høringsinstansenes syn

Metodekontrollutvalget omtaler ikke spørsmålet om behov for ytterligere etterforskningsmetoder i saker om overgrepsbilder av barn. Spørsmålet er imidlertid tatt opp av enkelte høringsinstanser under høringen. Dette gjelder blant annet *Kripos*, som særlig påpeker de etterforskningsmessige utfordringene det skaper at distribusjon av overgrepsbilder av barn som oftest skjer via internett:

> «Samordnede politiaksjoner mot barnepornografi og pedofile nettverk dreier seg om tilfeller hvor internett er benyttet til å distribuere bilder og filmer av seksuelle overgrep mot barn. Distribusjon er mer alvorlig enn bare besittelse

av de ulovlige filene, idet man opprettholder barnets lidelse ved å bidra til at overgrepene spres og tilgjengeliggjøres til evig tid. Det er også viktig å påpeke at denne typen etterforskning ofte avdekker de underliggende reelle overgrep, og kan bidra til å redde barn fra pågående misbruk.

Når politiet ikke gis anledning til kommunikasjonskontroll knyttet til strl. §204a, representerer internett, sammen med utviklingen av digitale media, en perfekt motor for produksjon og distribusjon av overgrepsbilder. Internetts anonymitet gjør at politiet har svært få muligheter til å avdekke reelle seksuelle overgrep, annet enn gjennom etterforsking av den enkelte besitter eller distributør som man får kjennskap til gjennom nasjonale eller internasjonale operasjoner.»

Høringsinstansen anfører på denne bakgrunn at kommunikasjonskontroll synes å være eneste mulighet for effektiv bekjempelse av internettrelaterte seksuelle overgrep.

Også *Politiets Fellesforbund* fremhever hensynet til effektiv etterforskning i saker som gjelder overgrepsbilder av barn:

«[…] Internett skal ikke være et friområde for pedofile nettverk som distribuerer filmer og bilder som viser grove seksuelle overgrep mot barn. Vi vil understreke at etterforskning av slike saker ofte vil kunne avdekke reelle overgrep. PF mener politiet må tildeles verktøy i takt med den teknologiske utviklingen for å kunne bekjempe de kriminelle effektivt på de arenaene de befinner seg, – i dette tilfellet i den digitale verden.»

Høringsinstansen argumenterer på denne bakgrunn for at det bør åpnes for bruk av kommunikasjonsavlytting i etterforskningen av saker etter straffeloven 1902 § 204 a (straffeloven § 311).

7.4.8.3 Departementets vurdering

Da adgangen til kommunikasjonsavlytting ble utvidet og knyttet til et generelt strafferammekrav ved lov 3. desember 1999 nr. 82, ble muligheten nevnt for å gjøre unntak fra dette strafferammekravet for blant annet befatning med overgrepsbilder av barn. Stortingets justiskomité uttalte i Innst. O. nr. 3 (1999–2000) punkt 7.3 side 7:

«[…] Komiteen er videre tilfreds med at unntaket for strafferammekravet ved narkotikalovbrudd opprettholdes, og ber departementet vurdere nøye om andre alvorlige lovbrudd i fremtiden bør gis lignende unntak, eller om det på et senere tidspunkt er naturlig å senke strafferammekravet. Dette gjelder bl.a. organisert kriminalitet som omfattende spritsmugling og distribusjon av barnepornografi.»

På bakgrunn av dette, samt høringsinnspillene fra Kripos og Politiets Fellesforbund, har departementet nå funnet grunn til å vurdere om det bør åpnes for kommunikasjonsavlytting etter straffeprosessloven § 216 a i saker om overgrepsbilder av barn.

Slikt materiale som er omfattet av § 311, utgjør gjerne en skildring av seksuelle overgrep mot barn. Straffebudet i straffeloven § 311 (straffeloven 1902 § 204 a) har til formål nettopp å beskytte barn mot de overgrepene som skjer ved produksjon av dette materialet.

Departementet er innforstått med at befatning med overgrepsbilder av barn må anses å være mindre alvorlig enn selve de underliggende overgrepene. Samtidig er det av betydning for produksjon av slikt materiale – og dermed også selve overgrepene – at det finnes en ervervsvillig målgruppe. Denne målgruppen skaper det nødvendige incitament for produksjonen av materialet og for de underliggende overgrepene. Etter departementets oppfatning må derfor tiltak for å bekjempe omsetning og annen befatning med overgrepsbilder av barn, også ses som tiltak for å bekjempe seksuelle overgrep mot barn.

De senere års utbredelse av internett har i betydelig grad lagt til rette for spredning av overgrepsbilder av barn. Internett utgjør i dag den primære distribusjonskanalen. Dette gjør det vanskelig for politiet å avdekke og etterforske saker om befatning med slikt materiale gjennom tradisjonelle etterforskningsmetoder som infiltrasjon og spaning. Som både Kripos og Politiets Fellesforbund anfører, er kommunikasjonsavlytting et av de mest målrettede og effektive etterforskningsverktøy når det gjelder kriminalitet som begås på internett. Hensett til dette – samt alvorligheten av de involverte lovbruddene – mener departementet at det nå bør åpnes for kommunikasjonsavlytting i saker om befatning med overgrepsbilder av barn. Departementet viser også til at slik metodebruk i ulik utstrekning er tillatt i både Danmark og Finland. Det foreslås også å åpne for hemmelig ransaking etter straffeprosessloven § 200 a, samt kameraovervåking på privat sted etter § 202 a i den her omtalte sakstypen, jf. nedenfor i kapitlene 10.4 og 12.6.

Departementet vil samtidig understreke at straffeloven § 311 omfatter handlinger med betydelig variasjon i alvorlighetsgrad. Eksempelvis vil produksjon og distribusjon av overgrepsbilder av barn normalt måtte anses mer alvorlig enn den rene besittelse. Adgangen til å benytte kommunikasjonsavlytting er først og fremst ment å gjelde de mer graverende forhold. Som alltid ellers må det vurderes ut ifra de konkrete omstendigheter hvorvidt vilkårene i straffeprosessloven § 216 a jf. § 170 a er oppfylt.

7.4.9 Forbund om ran

7.4.9.1 Gjeldende rett

Straffeloven § 329 (straffeloven 1902 § 269 nr. 1) rammer den som «den som inngår forbund med noen om å begå ran». Bestemmelsen rammer situasjonen der to eller flere personer inngår en avtale seg imellom om å begå et ran. Paragraf 329 er et eksempel på en bestemmelse som kriminaliserer en forberedende handling – det vil si en handling som i tid ligger forut for det straffbare forsøk. Forbrytelsen fullbyrdes ved at avtale inngås, slik at man ikke straffritt kan tre tilbake ved senere å oppgi planen.

Avtalen må bestå i et forbund om å begå «ran». Et ran er det å, med forsett om å skaffe seg eller andre en uberettiget vinning, øve vold mot en person, sette ham ute av stand til forsvar eller ved trusler fremkalle alvorlig frykt for vold mot noen, og derved bemektige seg en gjenstand som tilhører en annen, jf. § 327 første ledd bokstav a. Det samme gjelder det å ved slike midler tvinge noen til å handle slik at det medfører tap eller fare for tap for ham eller den han handler for, jf. § 327 første ledd bokstav b. Etter straffeloven § 328 kan et ran anses som grovt dersom det er brukt grov vold, truet med skytevåpen eller annet særlig farlig redskap, dersom ranet er nøye planlagt, foretatt overfor forsvarsløs person eller gjelder en betydelig verdi. Bestemmelsen om ransforbund skiller imidlertid ikke mellom simpelt og grovt ran.

Straffeloven § 329 er en videreføring av straffeloven 1902 § 269 nr. 1 i en noe endret språklig form. Bestemmelsen i § 269 nr. 2 om utrustning av skip for å begå ran, er ikke videreført.

Strafferammen for ransforbund etter straffeloven 1902 § 269 nr. 1 og straffeloven § 329 er fengsel inntil tre år. Dette tilfredsstiller ikke kravet om henholdsvis ti og fem års strafferamme i straffeprosessloven §§ 216 a og 216 b om kommunikasjonskontroll. Dersom lovbruddet kan knyttes til organisert kriminalitet, jf. straffeloven § 79 bokstav c (straffeloven 1902 § 60 a), vil imidlertid strafferammen forhøyes til inntil seks års fengsel. Det vil da kunne være adgang til å iverksette andre former for kommunikasjonskontroll enn avlytting, jf. straffeprosessloven § 216 b.

7.4.9.2 Metodekontrollutvalgets forslag

Metodekontrollutvalget vurderer i utredningen punkt 16.4.7 side 195 flg. om det er grunnlag for å utvide adgangen til kommunikasjonsavlytting etter straffeprosessloven § 216 a eller annen kommunikasjonskontroll etter § 216 b i saker som gjelder forbund om ran, eventuelt forbund om grovt ran. Utvalget finner imidlertid ikke å kunne tilrå en slik utvidelse. Standpunktet begrunnes med at den straffbare handling ikke anses å være tilstrekkelig alvorlig.

Utvalget legger stor vekt på at det allerede i dag er adgang til kommunikasjonskontroll etter straffeprosessloven § 216 b dersom forbundet inngår som ledd i aktivitetene til en organisert kriminell gruppe, jf. straffeloven 1902 § 60 a (straffeloven § 79 bokstav c). Videre er det etter straffeprosessloven § 222 d anledning til å anvende skjulte tvangsmidler – herunder både kommunikasjonsavlytting og annen kontroll av kommunikasjonsanlegg – for å avverge grove ran begått som ledd i aktivitetene til en organisert kriminell gruppe, jf. første ledd bokstav b. Etter utvalgets oppfatning er det særlig i disse tilfellene slik tvangsmiddelbruk vil være aktuell.

Utvalget kan heller ikke se at det er grunnlag for å gjøre en begrenset utvidelse til saker som gjelder forbund om grovt ran. Det pekes i den forbindelse på at verken straffeloven 1902 eller straffeloven skiller mellom forbund om simpelt eller grovt ran.

7.4.9.3 Høringsinstansenes syn

Riksadvokaten, Advokatforeningen og *Forsvarergruppen av 1977* støtter utvalgets vurderinger om adgangen til kommunikasjonskontroll ved mistanke om ransforbund. *Riksadvokaten* antar i den forbindelse at straffeprosessloven § 222 d om tvangsmiddelbruk i avvergende øyemed vil gi tilstrekkelig mulighet til å kunne avverge alvorlige ran.

Politidirektoratet, NAST, Kripos, Oslo politidistrikt, Søndre Buskerud politidistrikt og *Politiets Fellesforbund* går imot utvalgets forslag, og mener at tvangsmidlene som i dag er tilgjengelig, ikke strekker til.

Politiets Fellesforbund fremhever særlig brutaliteten og profesjonaliteten i ulike ran som har vært gjennomført de siste årene, og mener disse trekkene viser at kommunikasjonskontroll er nødvendig for å bekjempe ransmiljøene på en effektiv måte. Forbundet understreker at intensjonen med å utvide tvangsmiddeladgangen er å kunne avdekke planer om ran og deretter forhindre at disse blir gjennomført. Både *Politiets Fellesforbund* og *Søndre Buskerud politidistrikt* viser til erfaringer fra Sverige, der tendensen har gått i retning av flere grove ran. Høringsinstansene gir uttrykk for at norsk politi ønsker å stå best mulig rustet mot en mulig tilsvarende utvikling i Norge.

Søndre Buskerud politidistrikt mener at straffeloven 1902 § 269 om ransforbund (straffeloven § 329) i praksis begrenser politiets mulighet til å bruke kommunikasjonskontroll. Politidistriktet legger til grunn at dersom «det [er] grunn til å anta at flere personer deltar i planleggingen av ranet, vil de siktede rettslig sett befinne seg innenfor § 269 helt frem til selve ranshandlingen igangsettes». I denne perioden antas det at man er «avskåret fra å benytte kommunikasjonskontroll etter strpl § 216 a». Høringsinstansen mener at dersom straffeloven ikke hadde inneholdt en egen straffebestemmelse om forberedelse, ville adgangen til å iverksette kommunikasjonskontroll vært til stede på et tidligere tidspunkt. Synspunktet illustreres med et eksempel:

> «Søndre Buskerud politidistrikt og «Catch» etterforsket for noen år tilbake en sak om ran av verditransport der det ble benyttet kommunikasjonskontroll etter at et ran var gjennomført. Kontrollen avdekket planer om et nytt ran av samme type. Dette skapte etter hvert store problemer med etterforskningen, idet kommunikasjonskontrollen i stadig større grad avdekket ransplanlegging, og i mindre grad ga beviser for den forbrytelse som allerede var begått. Saken dokumenterte imidlertid godt det behovet en hadde for å kunne benyttet metoden, og hvilke problemer straffeloven § 269 skaper i det praktiske liv. Hadde man hatt tilsvarende situasjon i en narkotikasak er det ingen tvil om at kommunikasjonskontrollen ville kunne fortsette, idet det innkom informasjon om at et nytt straffbart forhold var under planlegging. Dette underbygger kun den allerede etablerte mistanken. I ranssaken ble situasjonen imidlertid motsatt, idet den informasjonen som innkom etter hvert svekket politiets mulighet til å benytte metoden. Dette til tross for at en hadde sikker informasjon om at et større ran var i anmarsj. Denne tildels uforståelige forskjellen mellom to meget alvorlige lovbestemmelser innebærer at man i politiet til tider nærmest ønsker seg straffelovens § 269 fjernet. Dette ville i langt større grad satt en i stand til å etterforske og avverge de grove ranssakene.»

Søndre Buskerud politidistrikt mener videre at det er lite tilfredsstillende at bruken av kommunikasjonskontroll for å avverge grove ranshandlinger forutsetter at handlingene kan knyttes til en organisert kriminell gruppe. Det påpekes at vilkårene i straffeloven 1902 § 60 a (straffeloven § 79 bokstav c) er strenge, og at det i en tidlig fase av etterforskningen kan være problematisk å fremskaffe bevis for gruppens organisering og deltakernes identitet, tilknytning, arbeidsoppgaver mv.

Oslo politidistrikt, med tilslutning fra *Politidirektoratet* og *Kripos*, foreslår at adgangen til kommunikasjonskontroll begrenses til saker som gjelder forbund om grovt ran.

7.4.9.4 Departementets vurdering

Ransforbund utgjør en alvorlig lovbruddstype, som kan ha potensielt store samfunnsskadelige konsekvenser dersom avtalen realiseres. Departementet understreker likevel at det først og fremst er selve ranet, og ikke den forutgående avtalen, som representerer den skadevoldende aktivitet. Dette må få betydning også i vurderingen av hvilke etterforskningsmetoder som skal være tilgjengelig ved de ulike lovbruddene.

Med en strafferamme på fengsel inntil fem år, kan straffeloven 1902 § 267 om ran danne grunnlag for bruk av kommunikasjonskontroll etter straffeprosessloven § 216 b. Det samme gjelder den tilsvarende bestemmelsen i straffeloven § 327, som har en strafferamme på seks år. Derimot er det ikke adgang til å benytte kommunikasjonsavlytting etter § 216 a, som krever en strafferamme på fengsel i ti år. Dersom ranet er foretatt som ledd i aktivitetene til en organisert kriminell gruppe, forhøyes imidlertid strafferammen for ran, jf. straffeloven 1902 § 60 a (straffeloven § 79 bokstav c). I slike tilfeller vil også kommunikasjonsavlytting etter straffeprosessloven § 216 a kunne benyttes, såfremt også de øvrige vilkår for slik metodebruk er oppfylt. Er det tale om grovt ran, er den øvre strafferamme fengsel inntil tolv år, jf. straffeloven 1902 § 268. I straffeloven er dette hevet til fengsel inntil 15 år. Den høye strafferammen oppfyller kravet til både kommunikasjonsavlytting etter straffeprosessloven § 216 a og til annen kontroll av kommunikasjonsanlegg etter § 216 b. Begge metoder vil følgelig

kunne benyttes ved mistanke om forsøk på eller fullbyrdelse av et grovt ran.

Søndre Buskerud politidistrikt anfører at bestemmelsen i straffeloven 1902 § 269 (straffeloven § 329) i realiteten begrenser adgangen til å benytte kommunikasjonskontroll i etterforskningen av ranshandlinger etter §§ 267 og 268 (straffeloven §§ 327 og 328). Departementet kan ikke følge politidistriktets resonnement på dette punkt. Bestemmelsen kriminaliserer en bestemt type forberedelseshandling, og medfører at straff kan ilegges *før* gjerningsmannen krysser grensen for straffbart forsøk. Det er ikke holdepunkter for at bestemmelsen er ment å skulle *flytte* grensen for hva som anses som forsøk på ran. Hvorvidt grensen er overskredet, må vurderes ut fra gjerningsbeskrivelsen i straffeloven §§ 327 og 328 (straffeloven 1902 §§ 267 og 268) sammenholdt med den alminnelige regel om straffbart forsøk i straffeloven § 16 (straffeloven 1902 § 49). Dette må gjelde også i relasjon til spørsmålet om tvangsmiddelbruk som følge av mistanke om (forsøk på) overtredelse av bestemmelsene om fullbyrdet ran.

I tillegg til adgangen til metodebruk i etterforskningssporet, kan både kommunikasjonsavlytting etter straffeprosessloven § 216 a og annen kommunikasjonskontroll etter § 216 b benyttes for å *avverge* en ranshandling. Dette gjelder etter straffeprosessloven § 222 d første ledd bokstav b når det er rimelig grunn til å tro at noen kommer til å begå en handling som rammes av straffeloven § 328, jf. straffeloven § 79 bokstav c (straffeloven 1902 § 268 annet ledd jf. § 267, jf. § 60 a) – altså et grovt ran som begås som ledd i aktivitetene til en organisert kriminell gruppe. Enkelte høringsinstanser har bemerket at kravet om kobling til en organisert kriminell gruppe i straffeprosessloven § 222 d vanskeliggjør bruken av skjulte etterforskningsmetoder for å avverge ran. Departementet vil i den forbindelse fremheve de endringer i straffeloven 1902 § 60 a som ble gjort ved lov 21. juni 2013 nr. 85. Ved lovendringen ble straffansvaret for organisert kriminalitet utvidet, og definisjonen av organisert kriminell gruppe justert slik at den også favner grupper med en flatere og løsere struktur, jf. Prop. 131 L (2012–2013) punkt 11 side 68 flg. Tilsvarende endringer ble gjort i straffeloven § 79 bokstav c. Departementet antar at endringene kan avhjelpe de problemer som høringsinstansene påpeker, og ønsker å avvente virkningene av disse endringene før en eventuell fornyet vurdering av spørsmålet om tvangsmiddelbruk.

På denne bakgrunn finner departementet ikke å ha tilstrekkelige holdepunkter for å anta at dagens tilgang på etterforskningsmetoder ved mistanke om ransforbund er utilstrekkelig. Dette gjelder også for saker om forbund om grovt ran. Departementet slutter seg følgelig til Metodekontrollutvalgets konklusjoner, og foreslår ikke noen generell adgang til kommunikasjonskontroll i saker om ransforbund.

7.4.10 Annen alvorlig profittmotivert kriminalitet

7.4.10.1 Metodekontrollutvalgets forslag og høringsinstansenes syn

Metodekontrollutvalget omtaler under overskriften «Politiets utfordringer: Trekk ved kriminalitetsutviklingen» enkelte lovbrudd som kan karakteriseres som alvorlig profittmotivert kriminalitet. Dette gjelder tradisjonell vinningskriminalitet som utpressing, ran og tyveri, som omtales i henholdsvis punkt 8.6.19 side 95 og punkt 8.6.20 side 96. Videre omtales økonomisk kriminalitet – herunder bedragerier, regnskapsovertredelser, korrupsjon, skatte- og avgiftskriminalitet, konkurransekriminalitet, verdipapirkriminalitet samt heleri og hvitvasking i punkt 8.6.21 side 96–99. Utvalget drøfter imidlertid ikke behovet for nye etterforskningsmetoder i denne sammenheng. Spørsmålet er likevel – i ulike former – tatt opp av enkelte høringsinstanser.

Oslo politidistrikt, med tilslutning fra *Politidirektoratet*, fremhever at omfanget av profittmotivert kriminalitet er stort, og at denne kriminalitetsformen utgjør et betydelig samfunnsproblem. For å bekjempe dette ønsker politidistriktet ytterligere virkemidler for å kunne sette seg i posisjon til å inndra utbyttet fra handlingene, noe som kan være en kraftfull incentivstyring som signaliserer at kriminaliteten ikke lønner seg. Politidistriktet mener en adgang til å benytte kommunikasjonskontroll ved mistanke om grovt heleri eller grov hvitvasking etter straffeloven 1902 § 317 fjerde ledd (straffeloven §§ 333 og 338) vil være et effektivt virkemiddel i så måte. Det uttales:

> «Primærforbrytelsene er ofte utført i samarbeid med flere andre, og ofte i en organisert kriminell gruppe, jfr. strl. § 60a. Utbyttet fordeles mellom medvirkerne, og den enkelte vil på egen hånd starte oppbygging av sin personlige økonomi. Etterforskningen av en uforklart formue vil da naturlig nok innrettes mot den enkelte som er, eller fremstår som, eier av de aktuelle formuesobjektene. Hvilke underliggende primærforbrytelser vedkommende har

> begått, herunder hvilke personer han eventuelt har samarbeidet med, vil politiet sjelden ha kunnskap om. Politiet vil således vanskelig kunne argumentere for at selve formuesoppbyggingen skjer som ledd i en organisert kriminell gruppe, jfr. strl. § 60a. Strafferammen i § 317 blir således en barriere for å starte skjult etterforsking med KK. Det er [uheldig], idet denne typen etterforsking er ønskelig sett ut fra målet om å ta bakmennene og å komme i inndragningsposisjon.»

Ved å bruke informasjon fra kommunikasjonskontroll kan man etter høringsinstansens syn blant annet utelukke legalt erverv av formuesobjekter og bevise eierforhold til ulike eiendeler.

Økokrim fremholder på sin side at etterforskningsmessige utfordringer taler for kommunikasjonskontroll i de mest alvorlige saker om verdipapirkriminalitet, innsidehandel og markedsmanipulasjon, jf. verdipapirhandelloven § 17-3 første ledd. Det vises til at slik kriminalitet er samfunnsskadelig, samtidig som den for de kriminelle representerer en svært lønnsom og forholdsvis enkel måte å tilegne seg en uberettiget andel av verdiene i verdipapirmarkedet på. Effektiv etterforskning og iretteføring er derfor avgjørende for å sikre tilliten til verdipapirmarkedet. Etter høringsinstansens syn vil kommunikasjonskontroll være et egnet virkemiddel for å oppnå en slik effektiv etterforskning:

> «De etterforskingsmessige problemene i slike saker følger blant annet av at kommunikasjonen mellom de innvidde *er* selve kriminaliteten. Mens kommunikasjon normalt er et *middel* for å begå en annen form for kriminalitet, vil innholdet i kommunikasjonen kunne være selv[e] kriminaliteten ved denne form for markedsmisbruk. I mange slike saker kan således oppgaven formuleres som å skulle bevise utover enhver rimelig tvil at det har vært en kommunikasjon mellom de impliserte med et bestemt og ulovlig innhold. Typisk for slike saker er at det ikke finnes noen fornærmede eller vitner, det er kun de mistenkte selv som kjenner innholdet i kommunikasjonen. Videre etterlater lovbruddene normalt ikke noen objektivt registrerbare spor, det er f eks ingenting som skiller et tilfelle av ulovlig innsidehandel fra en lovlig gjennomført transaksjon. Aktørene er som regel profesjonelle og evner å skjule sin aktivitet og sine spor for politiet. ØKOKRIM har erfart at særlig de mest alvorlige og best organiserte sakene er særdeles vanskelige å oppklare. I andre land har man derimot lykkes med å oppklare selv svært alvorlige og godt organiserte saker, men da med bruk av bl.a. kommunikasjonskontroll.»

Også *Kontrollutvalget for kommunikasjonskontroll* bemerker at det kan være behov for metodebruk også i saker med mindre enn ti års strafferamme, og nevner som eksempel alvorlig vinningskriminalitet.

NAST peker på at Norge i dag har et stort problem med vinningskriminelle bander fra utlandet, særlig fra Øst-Europa. I enkelte tilfeller blir norsk politi varslet om disse fra utenlandsk politi – typisk om at banden er på vei mot Norge fra et bestemt land. NAST fremholder at adgangen til metodebruk i slike tilfeller er for snever, ettersom den forutsetter at de mistenkte har krysset den nedre grense for forsøk på et lovbrudd av en viss alvorlighetsgrad. Det foreslås derfor å åpne for kommunikasjonskontroll ved overtredelse av straffeloven 1902 § 162 c om forbund om handling med minst tre års strafferamme som skal begås som ledd i aktivitetene til en organisert kriminell gruppe (straffeloven § 198).

Med hensyn til trygdebedrageri uttaler *Arbeidsdepartementet* generelt at antallet personer anmeldt for dette har økt de siste årene. De fleste av de anmeldte har begynt i ordinært arbeid eller utvidet et arbeidsforhold uten å oppgi det på meldekort til Arbeids- og velferdsetaten. Som følge av dette retter Arbeids- og velferdsetaten nå større oppmerksomhet mot avdekking av systematisk svindel.

7.4.10.2 Departementets vurdering

En rekke lovbrudd som kan karakteriseres som grov profittmotivert kriminalitet har etter gjeldende straffelovgivning en øvre strafferamme på fengsel i seks år. Dette gjelder blant annet grovt underslag etter straffeloven § 325 (straffeloven 1902 §§ 256 jf. 255), grovt tyveri etter § 322 (straffeloven 1902 §§ 258 jf. 257), grovt bedrageri etter § 372 (straffeloven 1902 §§ 271 jf. 270), grovt heleri etter § 333 eller grov hvitvasking etter § 338 (straffeloven 1902 § 317 fjerde ledd jf. første og annet ledd), grovt skattesvik etter § 379 (tidligere ligningsloven §§ 12-2 jf. 12-1) og innsidehandel og markedsmanipulasjon etter verdipapirhandelloven §§ 3-3 og 3-8, jf. § 17-3 første ledd. Med en strafferamme på seks år er det adgang til å benytte kommunikasjonskontroll etter straffeprosessloven § 216 b, men ikke avlytting av kommunikasjonsanlegg etter § 216 a i etterforskningen av

de nevnte lovbrudd. Er handlingen utøvet som ledd i aktivitetene til en organisert kriminell gruppe, forhøyes imidlertid den øvre strafferammen til fengsel inntil 12 år, jf. straffeloven § 79 bokstav c (11 år etter straffeloven 1902 § 60 a). I slike tilfeller vil det også være adgang til å benytte kommunikasjonsavlytting etter straffeprosessloven § 216 a, jf. vilkåret om ti års strafferamme eller mer i bestemmelsens første ledd bokstav a.

Departementet har merket seg at flere høringsinstanser mener det foreligger et behov for å utvide adgangen til metodebruk ved ulike forbrytelsestyper knyttet til alvorlig profittmotivert kriminalitet. Dette understøttes av flere trusselanalyser som viser at utviklingen i kriminalitetsbildet innen profittmotivert kriminalitet går i retning av større mobilitet, mer komplekse lovbrudd, profesjonalisering og internasjonalisering. Som også Metodekontrollutvalget bemerker i utredningen punkt 8.6.21 på side 98–99 er økonomisk kriminalitet og tradisjonell organisert kriminalitet knyttet tettere sammen enn tidligere, og organisert kriminalitet involveres i stadig større grad i legitim forretningsvirksomhet, der lovlig og ulovlig virksomhet drives side om side bak en fasade av komplekse selskapsstrukturer. Utvalget peker dessuten på at bruken av selskapsstrukturer hvor enhetene er registrert i flere ulike land og styres gjennom truster som opererer fra skatteparadiser, gir betydelige utfordringer for politiet. Dette gjør avdekking og oppklaring utfordrende. Departementet har stor forståelse for at de omtalte kriminalitetsformene kan by på betydelige etterforskningsmessige utfordringer og at en utvidet adgang til kommunikasjonskontroll kan synes som et egnet virkemiddel.

På samme tid finner departementet – på bakgrunn av *denne* høringen – ikke å ha tilstrekkelig grunnlag for å utvide adgangen til kommunikasjonskontroll i saker om profittmotivert kriminalitet. Det understrekes at kommunikasjonskontroll utgjør et særlig inngripende tiltak overfor dem som rammes, og at det derfor er grunn til å utvise varsomhet ved eventuelle utvidelser. Et oppdatert kunnskapsgrunnlag om kriminalitetsbildet og etterforskningsmessige behov i saker om profittmotivert kriminalitet er nødvendig for å vurdere utvidelse av metodebruken opp mot konsekvenser for personvernet. Det er iverksatt flere prosjekter som vil kunne gi et slikt kunnskapsgrunnlag. Departementet vil derfor avvente oppdatert informasjon om trusselbildet med tilhørende behovsvurdering før man tar stilling til om eventuelle lovforslag knyttet til utvidet metodebruk bør sendes på høring.

7.4.11 Oppfordring, rekruttering og opplæring til terrorlovbrudd

7.4.11.1 Gjeldende rett

Straffeloven § 136 gjelder oppfordring, rekruttering og opplæring til terrorhandlinger og terrorrelaterte handlinger. Bestemmelsen er en videreføring av straffeloven 1902 § 147 c. Bestemmelsen ble tilføyd ved lov 19. desember 2008 nr. 114, for at Norge skulle kunne ratifisere Europarådets konvensjon 16. mai 2005 om forebygging av terrorisme.

Paragraf 136 bokstav a til c rammer henholdsvis det å oppfordre, rekruttere eller gi opplæring til terrorhandlinger og terrorrelaterte handlinger. Hva som skal anses som en terrorhandling eller terrorrelatert handling fremgår av straffeloven §§ 138 til 144 (straffeloven 1902 § 147 a første eller tredje ledd, § 147 b første eller annet ledd). Særskilt for disse er at de er begått med terrorhensikt eller har særlig samfunnsskadelige virkninger.

Bokstav d var ny ved lov 21. juni 2013 nr. 85, og kriminaliserer mottakelse av terrortrening. Dette består etter bestemmelsen i å la seg lære opp i metoder eller teknikker som er særlig egnet til å utføre eller bidra til utførelsen av en handling som rammes av de nevnte bestemmelsene om terrorhandlinger og terrorrelaterte handlinger.

Strafferammen for alle alternativer er fengsel inntil seks år. Strafferammen gir følgelig grunnlag for bruk av kommunikasjonskontroll etter straffeprosessloven § 216 b. Det er derimot ikke adgang til å iverksette kommunikasjonsavlytting etter § 216 a, med mindre lovbruddet er utøvet som ledd i aktivitetene til en organisert kriminell gruppe, jf. straffeloven § 79 bokstav c (straffeloven 1902 § 60 a).

7.4.11.2 Forslaget i høringsnotatet

I høringsnotat 12. juli 2012 om kriminalisering av forberedelse til terrorhandling, utvidet adgang til tvangsmiddelbruk mv. punkt 2.5.2 side 38 vises det til et forslag fra PST om å utvide adgangen til å benytte tvangsmidler – herunder også kommunikasjonsavlytting – i saker om oppfordring, rekruttering og opplæring til terrorhandlinger etter straffeloven 1902 § 147 c (straffeloven § 136). Spørsmålet er ikke behandlet i Metodekontrollutvalgets utredning. Fra høringsnotatet hitsettes:

> «PST anfører at adgangen til å benytte tvangsmidler i saker om oppfordring, rekruttering og opplæring til terrorhandlinger er svært begren-

set, på grunn av den lave strafferammen på 6 år. PST har i dag ikke anledning til å benytte kommunikasjonskontroll annet enn ved innhenting av løpende trafikkdata etter straffeprosessloven § 216 b, og er således avskåret fra bruk av kommunikasjonsavlytting etter § 216 a. Slik kommunikasjonsavlytting kan bestå i å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke. Avlyttingsadgangen omfatter all informasjonsutveksling mellom kommunikasjonsanlegg, uavhengig av hvilken form eller hvilket innhold informasjonen måtte ha. Dermed omfattes i tillegg til samtaler, overføring av tekst (herunder e-post), bilde og film.

PST påpeker at de forhold som § 147 c skal ramme, hovedsakelig bedrives ved hjelp av telekommunikasjon og internett. Uten mulighet til å avlytte internettaktiviteter ved mistanke om overtredelse av bestemmelsen, vil PST heller ikke kunne fange opp forsøk på å rekruttere personer til terrorvirksomhet eller opplæring i å lage for eksempel bomber. PST anfører at hemmelig ransaking (§ 200 a) og dataavlesning også vil fremstå som egnede verktøy for å finne beviser for forhold som rammes av bestemmelsene på mistenktes datasystem.»

Departementet tok i høringsnotatet ikke nærmere stilling til forslaget fra PST, men la til grunn følgende (punkt 2.5.4 side 39):

«En utvidelse av adgangen til å benytte tvangsmidler forutsetter enten at strafferammen økes for slike lovbrudd, eller at straffebudet inntas uttrykkelig i de enkelte bestemmelsene om tvangsmidler. Tillatelse til å benytte enkelte tvangsmidler, herunder kommunikasjonsavlytting og skjult ransaking, forutsetter således at handlingen har en strafferamme på 10 år eller mer, eller at den kan subsumeres under de konkret oppregnede straffebudene i de ulike bestemmelsene.»

7.4.11.3 Høringsinstansenes syn

Flertallet av høringsinstansene som har kommentert forslaget om å utvide metodetilgangen i saker etter straffeloven 1902 § 147 c (straffeloven § 136), støtter forslaget uttrykkelig. Dette gjelder *Riksadvokaten*, *NAST*, *PST*, *Hordaland politidistrikt, Politijuristene* og *Politiets Fellesforbund*.

Nordre Buskerud politidistrikt har ingen konkrete merknader til spørsmålet, men uttaler generelt om forslagene i høringsnotatet at det er viktig å gi PST de virkemidler som de mener det er et saklig behov for. *Oslo statsadvokatembeter* har heller ingen konkrete merknader til forslaget, men bemerker generelt at forslag til reglene om tvangsmidler fremstår som velfunderte.

Riksadvokaten og *PST* viser til at bruk av skjulte tvangsmidler ofte vil være eneste reelle mulighet til å skaffe informasjon om overtredelser av straffeloven 1902 § 147 c (straffeloven § 136). PST fremhever blant annet at det viktigste beviskilden i slike saker er telekommunikasjon og internettaktiviteter, og at det uten adgang til utvidet tvangsbruk vil være vanskelig å avdekke slike lovbrudd:

«PST påpeker i vårt brev av 1. november 2011, at det er en kjensgjerning at de forhold som straffeloven § 147c skal ramme, hovedsakelig skjer ved hjelp av telekommunikasjon og internett. Straffeloven § 147c har en strafferamme på 6 år, noe som gir dette svært begrenset adgang til å benytte tvangsmidler. Når det ikke foreligger adgang til å avlytte internettaktiviteter ved mistanke om overtredelser av bestemmelsen, vil PST heller ikke kunne fange opp forsøk på å rekruttere personer til terrorvirksomhet eller opplæring i å lage for eksempel bomber.

Vi viser videre til at tvangsmidler som hemmelig ransaking og dataavlesing vil fremstå som egnede verktøy for å finne beviser for forhold som rammes av straffeloven § 147 c, på mistenktes datasystem.

Det er derfor vår vurdering at dersom bestemmelsen skal kunne fungere etter sin hensikt vil det være helt avgjørende at det gis utvidet adgang til å benytte tvangsmidler ved anvendelsen av denne.»

PST viste dessuten under høringen av Metodekontrollutvalgets utredning til at de miljøer hvor rekruttering og opplæring til terrorhandlinger foregår er lukkede miljøer:

«Det er PSTs vurdering at straffeloven § 147c (strafferamme på 6 år) bør utløse tvangsmiddelbruk på linje med PSTs øvrige straffebud. Etterforsking av saker hvor oppfordring, rekruttering og opplæring til terrorhandling er tema, vil være vanskelig uten å ha anledning til bruk av tvangsmidler. Det er PSTs vurdering at utvalgets begrunnelse for hvorfor noen straffe-

bud med strafferamme mindre enn 10 år kvalifiserer for tvangsmiddelbruk også gjelder for straffeloven § 147c. Det vises til at de miljøer hvor rekruttering og opplæring til terrorhandlinger foregår er lukkede miljøer[...].»

Også *Riksadvokaten* viser til at tradisjonell etterforskning, spaning og infiltrasjon vanskelig lar seg gjennomføre i de miljøer som er involvert i oppfordring, rekruttering og opplæring til terrorhandlinger.

PST peker dessuten på at det er begrensede muligheter for å benytte opplysninger innhentet ved avvergende etterforskning etter straffeprosessloven § 222 d – såkalt overskuddsinformasjon – i saker hvor det er mistanke om overtredelse av straffeloven 1902 § 147 a om terrorhandlinger (straffeloven §§ 131–134) som bevis i saker etter § 147 c (straffeloven § 136). PST utdyper dette synspunktet slik:

«Vi ser nå at de forslag som er sendt på høring er lagt på en lav strafferamme med lite metodebruk. Dette er utfordrende fordi man i disse sakene er avhengige av metoder. Videre avskjærer det vår mulighet til å anvende bevis innhentet i en avvergende etterforskning ved bruk av f eks romavlytting eller kommunikasjonskontroll, som bevis i disse sakene. Dette skyldes de restriktive reglene i Norge for bruk av overskuddsinformasjon hvor hovedregelen er at bevis innhentet ved bruk av en metode, eksempelvis kommunikasjonskontroll, ikke kan brukes som bevis for straffbare forhold som ikke i seg selv gir adgang til metoden.

Det er i dag et vanlig scenario at det foreligger grunn til å tro at noen kommer til å begå en terrorhandling eller inngå forbund om en slik handling. Det igangsettes så en avvergende etterforsking etter straffeprosessloven § 222 d (avvergende etterforsking), hvor en vil ha full metodeadgang, og hvor det f eks kan anvendes kommunikasjonskontroll (KK) og romavlytting. Slik reglene er i dag, er det kun hvis man tar ut tiltale for overtredelse av straffeloven § 147 a (terrorhandlinger) at alle opplysninger fra metodebruken i den avvergende etterforskingen kan brukes. Videre kan f eks KK-informasjon brukes for straffeloven § 147 b (terrorfinansiering). [...]

Det er PSTs erfaring at den viktigste beviskilde i terrorsakene er avlytting av kommunikasjon. Dette gjelder der flere er involvert og i saker om rekruttering, finansiering og trening. Det vil også være viktig mot soloterrorister f eks ved avdekking av anskaffelse av gjenstander og bruk av internett. I saker om oppfordring til terror kan det være avgjørende med tanke på å skaffe informasjon rundt hvem som f. eks. har fremsatt oppfordringen på internett. Dersom PST ikke kan bruke informasjon fra avlytting av kommunikasjon i disse sakene, vil de i praksis ofte være virkningsløse.

Vi registrer departementets uttalelse på side 50 i høringsnotatet om at bruk av overskuddsinformasjon vil bli nærmere drøftet i forbindelse med oppfølgningen av Metodekontrollutredningens utredning. Dette er positivt, men det er vår vurdering at enkelte grep bør kunne gjøres allerede nå.»

Politijuristene bemerker at rettssikkerhetsgarantier er viktigere enn en snever avgrensning av hvilke straffebud som skal gi anledning til å bruke metoden. Politijuristene uttaler i den forbindelse:

«[...] Det er lett å mene at det er vel som viktig med rettssikkerhetsgarantier ved bruk av metoder, som kontroll fra påtalemyndighet og domstol enn en snevrere avgrensning av hvilke straffebud som skal gi anledning til å benytte metoden. Vi mener at det er riktig og viktig at lovgiver har en vurdering av hvilke metoder som skal tillates ved etterforskning av hvilke straffebud. Men vi tillater oss likevel å peke på at rettstatsgarantier og rettssikkerhet ivaretas vel så godt igjennom rettsstatenes kontrollfunksjoner, de uavhengige kontrollørene som påtalemyndighet og domstol – og forsvarer/§ 100a-advokat – skal utgjøre. På denne bakgrunn er vi derfor åpne for utvidelser av bruk av tvangsmidler, dersom rettssikkerhetsgarantier og personvernhensyn kan ivaretas på en tilfredsstillende måte.»

Noen av høringsinstansene viser dessuten til at det er større adgang til å benytte skjulte etterforskningsmetoder ved enkelte andre lovbrudd med lavere strafferamme enn ved ulike former for forberedelse til terror. Dette gjelder blant annet mindre narkotikalovbrudd, som for eksempel overtredelse av straffeloven 1902 § 162 første ledd (straffeloven § 231). *PST* påpeker at det er liten grunn til å ha mindre bevismuligheter enn i disse sakene. PST viser også til at det er full metodeadgang i saker etter straffeloven 1902 § 91 a om flyktningespionasje til tross for at bestemmelsen har en strafferamme på to år (etter straffeloven § 126 tre år). *Politijuristene* fremhever at de mil-

jøer som er delaktig i overtredelser av straffeloven 1902 § 147 c (straffeloven § 136), er utilgjengelige på samme måte som de miljøer som befatter seg med narkotika:

> «De miljøer som PST har sin fokus rettet mot, er etter vår oppfatning utvilsomt like utilgjengelige som miljøer som befatter seg med narkotika mv (overtredelse av strl § 162), med de adganger som der er gitt til metodebruk. På et generelt grunnlag kan vi derfor mene at når det er åpnet for inngripende metodebruk på enkelte områder i Norge, typisk ved overtredelse av strl § 162, har man tatt et valg hva gjelder om norske myndigheter skal tillate metoden brukt. Når metoden er tillatt brukt, bør den også kunne brukes til å forsvare de verdier PST er satt til å forsvare.»

Politiets Fellesforbund uttaler generelt om forslagene i høringsnotatets del 1 og 2 (som omfatter forslaget om å utvide metodetilgangen i saker etter straffeloven 1902 § 147 c) at de balanserer hensynet til kriminalitetsbekjempelse og rettssikkerhetshensyn:

> «Vårt syn på utvidet adgang til tvangsmiddelbruk og til anonym vitneførsel er forankret i de overordnede prinsipper for rettssikkerhet sett opp i mot de behov som foreligger for å avdekke, oppklare og iretteføre kriminelle handlinger av den type det her er snakk om. Det vil uansett være slik at de prinsipielle rettssikkerhetshensyn må veie særdeles tungt. Videre ser vi også grunn til i en viss grad å vektlegge behovet for å samordne lovgivning med andre land med hensyn til arbeidet med å bekjempe denne type grenseoverskridende kriminalitet, som disse verktøy gir mulighet for.
>
> I vår vurdering av forslaget har vi kontinuerlig stilt oss spørsmålet hvorvidt strafferetten gir tilstrekkelig beskyttelse i forkant av at terror skjer? Videre har vi stilt oss spørsmålet hvorvidt lovverket er tilstrekkelig både når det gjelder forebyggendesporet og etterforskningssporet i forhold til terror. I vårt arbeid med disse spørsmålene har vi vurdert dil[e]m[m]aene mellom på den ene siden personvern og vern om fellesverdier opp i mot utvidet bruk av tvangsmidler og anonym vitneførsel til bruk i etterforskning. I vårt arbeid med høringen har vi også sett hen til det tidligere metodeutvalgets arbeid samt påpekinger fra metodekontrollutvalget.
>
> Politiets Fellesforbund har mot denne bakgrunn kommet frem til at vi må ha en sterkere lovgivning som gir myndighetene muligheter til å avdekke intensjoner ift terror og derigjennom svekke kapasiteten til potensielle terrorister. Vi mener at de lovendringer som foreslås i høringen balanserer forholdet mellom frihet og sikkerhet opp i mot de forventninger samfunnet har til politiet om å skape et tryggere samfunn.»

Hordaland politidistrikt påpeker at forslaget isolert vil redusere behovet for kriminalisering av forberedelser til terror.

NAST og *Politijuristene* mener prinsipalt at de foreslåtte endringene ikke bør skje gjennom tilpasning av de relevante tvangsmiddelhjemlene, men ved at strafferammen for saker etter straffeloven 1902 § 147 c (straffeloven § 136) bør økes. Politijuristene mener at straffverdigheten og skadepotensialet ved de handlinger som § 147 c omfatter, tilsier at strafferammen kan heves til mer enn ti år. NAST mener generelt at ulike former for forberedelse til terror bør ha en høyere strafferamme og at maksimumsstraffen etter § 147 c bør være minst ti år. Både NAST og Politijuristene mener imidlertid at straffeloven 1902 § 147 c bør inntas i de enkelte bestemmelsene om tvangsmidler dersom strafferammen ikke økes.

Noen av høringsinstansene har ikke kommentert forslaget om å utvide metodetilgangen i saker etter straffeloven 1092 § 147 c (straffeloven § 136) direkte, men mener generelt at behovet for forslagene om utvidet metodeadgang ikke er tilstrekkelig dokumentert. *Advokatforeningen* uttaler blant annet følgende:

> «Det er vanskelig å se at det skulle foreligge noe som skulle medføre at man bør gå bort fra de vurderinger som ble foretatt av Metodekontrollutvalget.»

Datatilsynet uttaler generelt om forslagene i del 2 og 3 av høringsnotatet:

> «Datatilsynet kan heller ikke se at departementet tilfredsstillende har utredet og dokumentert behovet for de øvrige lovforslagene (forslagets del 2 og 3).»

7.4.11.4 Departementets vurdering

Departementet går i proposisjonen her inn for å beholde det generelle strafferammekravet på ti år

for de mest inngripende tvangsmidlene, herunder kommunikasjonsavlytting, se punkt 6.1.4.

Enkelte høringsinstanser, deriblant NAST, har tatt til orde for å øke strafferammen for overtredelser av straffeloven 1902 § 147 c (straffeloven § 136), slik at det generelle strafferammekravet vil være oppfylt også for kommunikasjonsavlytting. Det generelle spørsmålet om hvorvidt straffebudenes strafferammer skal fastsettes med tanke på å kunne benytte bestemte tvangsmidler er drøftet i Ot.prp. nr. 90 (2003–2004) punkt 11.3.4, hvor departementet uttaler at:

> «[…] strafferammene som et utgangspunkt ikke skal fastsettes med henblikk på å gi adgang til bruk av straffeprosessuelle tvangs- og etterforskingsmidler.»

Behovet for å kunne ta i bruk hemmelige tvangsmidler må derfor løses ved at det eventuelt inntas en uttrykkelig henvisning til de relevante straffebudene i terrorkapitlet i bestemmelsene om de enkelte tvangsmidler, jf. Ot.prp. nr. 8 (2007–2008) punkt 8.5.4.4 side 173. Departementet holder fast ved disse synspunktene, og merker seg at både Riksadvokaten og PST under høringen har støttet en slik tilnærming. Spørsmålet er derfor om straffeloven § 136 (straffeloven 1902 § 147 c) bør legges til oppregningen av enkeltstraffebud i straffeprosessloven § 216 a første ledd bokstav b, slik at det blir adgang til kommunikasjonsavlytting ved mistanke om oppfordring, rekruttering eller opplæring til terror. Dette vil bero på en konkret vurdering av behovet for metoden i den aktuelle sakstypen.

PST mener det er behov for å bøte på problemene rundt metodeadgang og muligheten til å anvende materialet fra metoder som bevis. Ifølge PST skyldes problemet de restriktive reglene i Norge for bruk av overskuddsinformasjon, hvor hovedregelen er at materiale innhentet ved bruk av en metode, eksempelvis kommunikasjonskontroll, ikke kan brukes som bevis for straffbare forhold som ikke i seg selv gir adgang til metoden.

Ved lov 21. juni 2013 nr. 86, som trådte i kraft 13. september s.å., ble det gitt utvidet adgang til å bruke opplysninger fra kommunikasjonskontroll og romavlytting om andre straffbare forhold enn dem etterforskingsskrittet var ment å avdekke – såkalt «overskuddsinformasjon» – som bevis. Dette ble begrunnet med at et forbud mot bruk av overskuddsinformasjon som bevis for straffbare forhold som ikke i seg selv kunne ha begrunnet den aktuelle metodebruken, harmonerer dårlig med politiets generelle plikt til å forebygge og oppklare straffbare handlinger. Etter lovendringen skal overskuddsinformasjon kunne brukes som bevis såfremt det «etter sakens art og forholdene ellers ikke vil være et uforholdsmessig inngrep» og «oppklaring av saken uten bruk av overskuddsinformasjonen i vesentlig grad vil bli vanskeliggjort», jf. Prop. 147 L (2012–2013) kapittel 5 side 72–84 og kapittel 11.1 side 178–179. Departementet antar at endringen i noen grad vil kunne avhjelpe den situasjon PST beskriver.

Det kan imidlertid også anføres andre argumenter for at straffeloven § 136 om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger (straffeloven 1902 § 147 c) bør inntas i opplistingen av lovbrudd som gir adgang til kommunikasjonsavlytting. Flertallet av høringsinstansene som har kommentert forslaget om å utvide metodetilgangen i saker etter straffeloven 1902 § 147 c, støtter forslaget. Flere har pekt på at det foreligger et særlig behov for å kunne benytte slike skjulte tvangsmidler i de aktuelle sakene. Blant annet viser Riksadvokaten til at bruk av skjulte tvangsmidler ofte vil være eneste reelle mulighet til å skaffe informasjon om overtredelser. Departementet er enig med Riksadvokaten, og antar at tradisjonell etterforskning, spaning og infiltrasjon ofte kan være vanskelig å gjennomføre i de miljøer som er involvert i overtredelser av straffeloven § 136.

Departementet legger videre vekt på at forhold som rammes av § 136, ifølge PST i stor grad bedrives ved hjelp av telekommunikasjon og over internett. Uten mulighet til å avlytte internettaktiviteter ved mistanke om overtredelse av bestemmelsen, vil PST heller ikke kunne fange opp forsøk på å rekruttere personer til terrorvirksomhet eller opplæring i å lage for eksempel bomber. Kommunikasjonsavlytting – så vel som hemmelig ransaking og dataavlesing – fremstår som egnede verktøy for å finne bevis for forhold som rammes av bestemmelsen.

Terrorvirksomhet er en svært alvorlig kriminalitetsform, som ofte har forgreninger på tvers av landegrenser og som i stor grad rammer det sivile samfunnet. Gjennom den frykt og utrygghet terrorhandlinger skaper, rammer de dessuten bredere enn tap av menneskeliv og materielle skader. Utviklingen de senere årene viser at vi står overfor et mer skjerpet, fragmentert og uoversiktlig trusselbilde, jf. punkt 4.5 ovenfor.

Oppfordring, rekruttering eller opplæring til terrorhandlinger vil senere kunne avføde nettopp slike. Departementet er enig i at det på bakgrunn av disse hensyn er et behov for å kunne benytte inngripende tvangsmidler også i saker etter straffeloven § 136. Departementet ser ingen avgjø-

rende innvendinger som tilsier at det ikke skal kunne benyttes slike tvangsmidler i disse sakene.

På den bakgrunn foreslår departementet at det åpnes for bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a ved mistanke om overtredelse av straffeloven § 136, ved at det tas inn en henvisning til bestemmelsen i straffeprosessloven § 216 a første ledd bokstav b. Det samme foreslås for andre skjulte tvangsmidler hvor det i utgangspunktet kreves en strafferamme på fengsel inntil ti år, nærmere bestemt hemmelig ransaking etter § 200 a, skjult kameraovervåking på privat sted etter § 202 a annet ledd, personnær teknisk sporing etter § 202 c og dataavlesing etter ny § 216 o. Etter departementets oppfatning taler de hensyn som er nevnt ovenfor, for at politiet kan benytte også disse virkemidlene i etterforskningen av slike saker. Derimot finner en ikke at det er dokumentert et behov for å tillate et så inngripende tvangsmiddel som romavlytting, jf. også kapittel 8 nedenfor.

Hva gjelder spørsmålet de nevnte metodene også bør kunne benyttes for å *avverge* slike forbrytelser, vises til punkt 13.4.4.2 nedenfor.

7.5 Kommunikasjonskontroll knyttet til person

7.5.1 Gjeldende rett

I henhold til straffeprosessloven § 216 a tredje ledd kan kommunikasjonsavlytting bestå i å «avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke». I formuleringen «bestemte» kommunikasjonsanlegg ligger et krav om at anlegg som skal avlyttes må identifiseres i rettens kjennelse, jf. Ot.prp. nr. 64 (1998–99) punkt 23 side 157. Det er følgelig ikke adgang til å knytte tillatelsen direkte til den personen som skal avlyttes. Samme identifikasjonskrav følger av straffeprosessloven § 216 b annet ledd for andre former for kommunikasjonskontroll enn avlytting.

Dersom det er en fasttelefon eller telefaks som skal kontrolleres, kan anlegget identifiseres ved hjelp av telefonnummeret. Mobiltelefoner har i tillegg et såkalt IMEI-nummer (International Mobile Equipment Identity), som svarer til serienummeret på mobiltelefonen og er unikt for hvert enkelt apparat. Videre kan mobiltelefoner identifiseres ved hjelp av et IMSI-nummer (International Mobile Subscriber Identity), som angir abonnenten som er registrert på telefonens SIM-kort.

Datamaskiner i nettverk identifiseres ved hjelp av en nettverksadresse. På internett kan såkalte IP-adresser benyttes. En del maskiner, herunder de fleste private datamaskiner, får imidlertid tildelt en ny IP-adresse hver gang de kobler seg til internett. I slike tilfeller vil tillatelsen til kommunikasjonskontroll ikke kunne knyttes til IP-adressen, ettersom denne ikke er egnet til å identifisere en bestemt maskin.

7.5.2 Andre lands rett

I de andre nordiske land gjelder i all hovedsak det samme krav som etter norsk rett til identifisering av bestemte kommunikasjonsanlegg. *Svensk* og *finsk* rett tillater under ingen omstendighet at en tillatelse til kommunikasjonskontroll knyttes til person. I Sverige ble forslag om dette nylig forkastet i Prop. 2013/14:237 Hemliga tvångsmedel mot allvarliga brott, hvor det ble lagt til grunn at effektivitetsbehov ikke kan veie tyngre enn hensynet til at retten skal kjenne alle konkrete omstendigheter når den fatter sin beslutning. I punkt 6.2.5 side 97 uttales:

> «Det finns alltså en del som talar för att regleringen bör ändras för att bättre hantera situationer där nya platser eller adresser blir aktuella efter ett initialt domstolsbeslut om avlyssning eller övervakning. Samtidigt anser regeringen att integritets- och rättssäkerhetsskäl alltjämt talar för att lagstiftningen bör vara utformad på ett sådant sätt att beslutsfattaren kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen. Förutsättningarna för delar av den initiala prövningen – bl.a. tillämpningen av proportionalitetsprincipen – skulle försämras om åtgärden inte var bestämd till viss adress, plats eller liknande. Beslutsfattarens möjligheter att bedöma i vilken mån ett tillstånd behöver förenas med villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan skulle sannolikt också minska. Regeringen är därför nu inte beredd att ta bort kravet på att viss adress, utrustning eller plats ska anges i tvångsmedelsbeslutet. […]»

I *dansk rett* finnes en begrenset adgang til å iverksette såkalt inngrep i meddelelseshemmeligheten ved å angi en bestemt person (den mistenkte) som inngrepet retter seg mot. Adgangen er avgrenset til å gjelde i etterforskningen av visse alvorlige forbrytelser, jf. retsplejeloven § 783, stk. 2. Dette gjelder lovbrudd som nevnt i straffeloven kapittel 12 (forbrytelser mot statens selvstendig-

het og sikkerhet) og 13 (forbrytelser mot statsforfatningen og de øverste statsmyndigheter, terrorisme mv.), straffeloven § 123 (obstruksjon av rettsvesenet), § 180 (kvalifiserte former for ildpåsettelse), § 183, stk. 2 (kvalifisert forvoldelse av visse samfunnsskadelige forbrytelser), § 191 (alvorlig narkotikaforbrytelse), § 192 a (alvorlig overtredelse av våpenlovgivningen), § 228 (hallikvirksomhet), § 237 (drap), § 245 (legemsbeskadigelse), § 246 jf. § 245 (legemsbeskadigelse med døden eller alvorlig skade til følge), § 252, stk. 1 (kvalifiserte former for å utsette noens liv eller førlighet for fare), § 261, stk. 2 (grov frihetsberøvelse), § 262 a (menneskehandel) og § 288 (ran).

Dersom det gis tillatelse til inngrep i meddelelseshemmeligheten knyttet til person, skal politiet snarest mulig etter utløpet av tillatelsens varighet underrette retten om de telefonnumre som inngrepet har vært rettet mot og som ikke er angitt i kjennelsen. Underretningen skal angi bestemte grunner til å anta at det fra telefonnumrene gis meddelelser til eller fra den mistenkte. Hvis særlige forhold taler for det, skal underretning skje senest 24 timer etter at inngrepet er iverksatt. Retten underretter deretter den oppnevnte advokat, som kan kreve rettens prøving av inngrepets lovlighet. Burde inngrepet etter rettens oppfatning ikke vært foretatt, skal dette meddeles Justitsministeriet.

Bestemmelsen i retsplejeloven § 783, stk. 2 ble innført ved lov nr. 542 av 8. juni 2006 på bakgrunn av en rapport fra en interdepartemental arbeidsgruppe om «Det danske samfunds indsats og beredskab mod terror», avgitt 3. november 2005. I rapportens anbefaling nr. 26 ble det anbefalt å åpne for at inngrep i meddelelseshemmeligheten kan rettes mot en person, og ikke bare mot bestemte kommunikasjonsmidler. Anbefalingen ble særlig begrunnet i ressurshensyn (punkt 4.3.2 side 76):

> «Erfaringen viser, at en del mistænkte forsøger at sløre deres handlinger ved at anvende flere forskellige kommunikationsmidler/-apparater. Det kan f.eks. være forskellige mobiltelefoner eller SIMkort, som udskiftes løbende. Der erindres i den forbindelse om, at den tekniske udvikling gennem de senere år har betydet, at såvel antallet som tilgængeligheden af de til rådighed stående kommunikationsmidler er øget betydeligt.
>
> Hvis en mistænkt anvender flere forskellige kommunikationsmidler, skal der derfor indhentes en retskendelse for hvert enkelt kommunikationsmiddel. Det medfører, at der skal holdes et retsmøde hver gang med inddragelse af en dommer og forsvarer, samt at politiet skal forberede sagen forud for retsmødet.
>
> Hvis der skabes mulighed for, at retskendelsen vedrører personen og ikke kommunikationsmidlet, vil der kunne spares ressourcer både hos domstole og politi, hvilket også erfaringer fra udlandet har vist.»

Folketinget fulgte opp arbeidsgruppens tilråding, med visse innstrammende endringer.

Etter den *islandske* straffeprosessloven kan tillatelse til avlytting eller opptak av telekommunikasjon knyttes enten til et bestemt kommunikasjonsapparat eller til kommunikasjonsapparater som «tilhører en bestemt person eller han har rådighed over», jf. § 81 første punktum. Dersom tillatelsen knyttes til en person, skal rettens kjennelse angi «hvem [kommunikasjonsapparatet] tilhører eller hvem råder over det», jf. § 84, stk. 2. Vilkårene for kommunikasjonsavlytting knyttet til person er for øvrig de samme som for annen kommunikasjonskontroll (se punkt 7.3.4 ovenfor).

7.5.3 Metodekontrollutvalgets forslag

Metodekontrollutvalget vurderer i utredningen punkt 16.5 side 196 flg. hvorvidt retten bør kunne gi politiet tillatelse til kommunikasjonskontroll knyttet til en person generelt, uten krav om identifisering av et bestemt kommunikasjonsanlegg. Utvalget finner imidlertid ikke å kunne fremme et slikt forslag. Konklusjonen begrunnes med at ordningen ville gi politiet for vide fullmakter og svekke mulighetene til kontroll med bruken av kommunikasjonskontroll.

Utvalget vurderer videre om det bør innføres en regel etter modell av den danske retsplejeloven § 783, stk. 2. En slik regel vil etter utvalgets oppfatning ivareta rettsikkerhetsaspektene på en bedre måte, ved at informasjon om avlyttede telefonnumre formidles via domstolen til den offentlig oppnevnte advokaten, som kan bringe inngrepets lovlighet inn for retten. Etter utvalgets oppfatning har imidlertid den danske løsningen også klare svakheter. Ved at dommeren skal videreformidle relevante opplysninger til den oppnevnte advokaten, stilles dommeren i en etter norsk rett ukjent rolle. Utvalget setter spørsmålstegn ved at dommeren tildeles en plass i saksbehandlingen som ikke innebærer en kontrollfunksjon. Etter utvalgets mening legger dessuten ordningen i for stor grad kontrollfunksjonen til den oppnevnte advokaten. Dette står i motsetning til det alminnelige system, hvor påtalemyndigheten må fremme en

begjæring som retten tar stilling til etter å ha hørt advokatens innsigelser.

Utvalget ser at det er ressurskrevende at politiet må fremme nye begjæringer om kommunikasjonskontroll hver gang mistenkte bytter telefon eller SIM-kort. Etter utvalgets syn vil imidlertid påtalemyndighetens hastekompetanse kunne brukes for å utvide kontrollen til også å omfatte det eller de nye anleggene, slik at etterforskningen ikke blir skadelidende. Utvalget har i den forbindelse vurdert om det kan være grunn til å «samle opp» flere utvidelser foretatt ved bruk av hastekompetanse i en felles begjæring til retten etter en viss tidsperiode. Det konkluderer imidlertid med at en slik ordning i for stor grad vil svekke domstolens etterfølgende kontroll med påtalemyndighetens bruk av hastekompetansen.

7.5.4 Høringsinstansenes syn

Fornyings-, administrasjons- og kirkedepartementet, Oslo statsadvokatembeter, PST, Advokatforeningen og *Forsvarergruppen av 1977* støtter utvalgets vurderinger, og ønsker ikke at det åpnes for kommunikasjonskontroll knyttet til person. *Riksadvokaten* uttrykker å ha «en viss forståelse» for utvalgets konklusjon, mens *Oslo politidistrikt* for tiden ikke finner det hensiktsmessig å argumentere videre for endringer på dette punkt.

Politiets Fellesforbund er uenig med utvalget, og mener man bør kunne knytte en tillatelse til kommunikasjonskontroll til mistenkte som person og ikke bare til et konkret kommunikasjonsanlegg.

Kripos og *Søndre Buskerud politidistrikt* fremmer begge alternative forslag til utvalgets løsning. *Kripos* uttaler:

> «Dagens regelverk gir mulighet til å avlytte både mistenktes simkort og hans imeinummer (mobiltelefon). Ved kommunikasjonskontroll av simkort fremkommer det hvilken telefon (imei) simkortet sitter i. Avlyttingen er aktiv uavhengig av hvilken telefon mistenkte benytter. På samme måte vil en avlytting av imeinummer avdekke hvilket simkort som [er] knyttet til imeinummeret. Avlyttingen er aktiv uavhengig av hvilket simkort mistenkte benytter.
>
> På denne måten kan politiet registrere at mistenkte har byttet telefon via kommunikasjonskontroll av simkort, og at mistenkte har byttet simkort via kommunikasjonskontroll av imeinummer. Avlytting av simkort og imeinummer gir ikke identisk informasjon, eksempelvis vil ikke avlytting av imeinummer fange opp mistenktes bruk av sms. Det er viktig å avlytte alle simkort og imeinummer for å avdekke fremtidige bytter av telefoner og simkort.»

På denne bakgrunn foreslår Kripos at politiet gis mulighet til å begjære kommunikasjonskontroll på de SIM-kort og IMEI-nummer som avdekkes brukt via det enkelte kommunikasjonsanlegg. Etter høringsinstansens syn bør mistanken knyttes til en konkret opplysning om at mistenkte bytter telefoner og/eller SIM-kort regelmessig, og kontrollen som etableres bør avsluttes samtidig som kontrollen av det opprinnelige kommunikasjonsanlegget. Politiet bør dessuten straks innberette hver oppkopling til Riksadvokaten etter vanlige regler, sammen med en rapport om hvordan kommunikasjonsanlegget ble avdekket og med anmodningsskjemaet til nettleverandør.

Søndre Buskerud politidistrikt foreslår at man i stedet for å tillate kommunikasjonskontroll knyttet til person, senker terskelen for bruk av påtalemyndighetens hastekompetanse dersom det allerede foreligger en kjennelse om kommunikasjonskontroll. I dag skal påtalemyndighetens hastekompetanse bare benyttes dersom det er «stor fare» for at etterforskningen ellers vil lide. Etter politidistriktets syn vil problemene ved at man må vente på rettens behandling av nye begjæringer om kommunikasjonskontroll, avhjelpes ved at terskelen senkes. Ved en etterfølgende rettslig prøving vil dessuten rettssikkerhetshensyn bli ivaretatt.

Søndre Buskerud politidistrikt understreker videre at spørsmålet om kommunikasjonskontroll knyttet til person må ses i sammenheng med andre forslag i utvalgets utredning. Dette gjelder særlig forslaget om muntlige forhandlinger for hver enkelt begjæring om skjult tvangsmiddelbruk, samt forslaget om at samme oppnevnte advokat skal delta under behandlingen av alle begjæringer om tvangsmiddelbruk mot en bestemt mistenkt. Høringsinstansen fremholder:

> «Dersom man innfører denne ordningen, men samtidig ikke åpner for å knytte kommunikasjonskontrollen til person, vil systemet bli meget tungrodd og etterforskningen etter vårt syn tilnærmet umuliggjort. Bruker man en narkotikasak med fire mistenkte som eksempel, og legger til grunn at disse benytter to telefoner hver, vil det til en hver tid foregå avlytting av åtte telefoner. Dette er et forholdsvis normalt scenario i en mindre narkotikasak. Det er videre normal fremgangsmåte blant de krimi-

nelle at telefoner byttes ofte, særlig nær opptil den kriminelle handlingen, f.eks avhenting av et narkotikaparti. Legges det videre til grunn at alle fire mistenkte bytter ut en av telefonene daglig i en periode på fire dager, vil dette generere 16 rettsmøter i løpet av disse fire dagene. Samtlige rettsmøter skal etter utvalgets forslag berammes med sakens parter. Dette vil i realiteten ikke være praktisk gjennomførbart, i hvert fall ikke innenfor den kort[e] periode en har til rådighet før etterforskningen blir vesentlig skadelidende.

Dersom utvalgets forslag følges på alle punkter, vil det etter vårt syn ikke lenger være praktisk mulig å gjennomføre en kommunikasjonskontroll som ivaretar de strenge rettssikkerhetsgarantier som skal stilles til denne type etterforskning. Tapet av informasjon i påvente av at begjæringer blir behandlet av tingretten vil kunne bli stort. Dette blir enda mer omfattende dersom det må fremsettes ny begjæring hver gang en mistenkt bytter kommunikasjonsanlegg. Kommunikasjonskontrollen vil med en slik ordning kun inneholde bruddstykker av kommunikasjon mellom de mistenkte, noe som vil svekke både etterforskningen og mistenktes rettssikkerhet. Så lenge det gis tillatelse til kommunikasjonskontroll må en også sørge for at den de bevis som innhentes i størst mulig grad gir et helhetlig bilde av de handlinger den mistenkte gjør. Dette vil ikke være tilfellet dersom utvalgets forslag tas til følge på disse tre punktene.»

Etter politidistriktets syn må en derfor velge mellom de ulike forslagene. Dersom en ønsker obligatoriske rettsmøter og samme advokat for samtlige begjæringer, må en samtidig åpne for at kommunikasjonskontroll knyttes til person. Dersom en derimot ønsker å opprettholde systemet med at tillatelse knyttes til et bestemt kommunikasjonsanlegg, må forslaget om muntlige rettsmøter og samme forsvarer vike.

7.5.5 Departementets vurdering

I en del kriminelle miljøer er det ikke uvanlig at aktørene hyppig bytter telefon eller SIM-kort, især i tiden nært opp til gjennomføringen av en straffbar handling. Som følge av dette vil politiet – på grunn av identifikasjonskravet i straffeprosessloven §§ 216 a og 216 b – ofte måtte fremme et stort antall begjæringer om kommunikasjonskontroll i etterforskningen av en og samme mistenkt. Departementet har forståelse for at dette kan være tid- og ressurskrevende, og at en adgang til å knytte kommunikasjonskontrollen til en bestemt person vil kunne bidra til å effektivisere etterforskningen.

Departementet er imidlertid enig med utvalget i at ressurshensyn alene ikke kan tillegges avgjørende vekt. En har merket seg at flere høringsinstanser på politi- og påtalesiden også gir uttrykk for å støtte, eller ha forståelse for, et slikt syn. Kommunikasjonskontroll er inngripende overfor den eller dem som rammes, noe som tilsier at det må stilles strenge krav til kontroll. Dette av hensyn til mistenktes rettssikkerhet, men også for å ivareta interessene til eventuelle andre berørte personer. Dersom det åpnes for å knytte kommunikasjonskontrollen til mistenktes person, og ikke til et bestemt kommunikasjonsanlegg, får politiet en vid fullmakt til å iverksette kommunikasjonskontroll uten konkret rettslig prøving. Selv om det ikke er grunn til å tro at politiet ville misbruke en slik fullmakt, ønsker departementet å tilstrebe et system som i størst mulig grad forebygger misbruk. Ved å videreføre dagens ordning, sikres en grundig kontroll av all bruk av kommunikasjonskontroll, idet hver enkelt oppkopling vurderes og begrunnes av både påtalemyndighet og domstol.

Departementet antar at bruk av påtalemyndighetens hastekompetanse ofte vil være aktuell i situasjoner der den eller de mistenkte bytter telefon eller SIM-kort ofte. Dette kan bidra til å avhjelpe praktiske problemer som følger av at tillatelsen til kommunikasjonskontroll ikke kan knyttes til en bestemt person. En har merket seg at Søndre Buskerud politidistrikt mener terskelen for bruk av hastekompetansen er for høy og foreslår at terskelen senkes i saker hvor det allerede foreligger en kjennelse om bruk av kommunikasjonskontroll. Etter departementets oppfatning vil imidlertid en slik differensiering av vilkårene for bruk av hastekompetanse være rettsteknisk uheldig, og vil kunne bidra til å undergrave utgangspunktet om rettslig prøving.

Departementet er for øvrig enig med Søndre Buskerud politidistrikt i at de ulike forslagene i utvalgets utredning må avpasses og ses i sammenheng med hverandre. En ser også at et krav om muntlige forhandlinger forut for enhver ny oppkobling ville kunne vanskeliggjøre etterforskningen i situasjoner der mistenkte ofte bytter telefon eller SIM-kort. Som det fremgår av punkt 6.7.4 går departementet ikke inn for en hovedregel om muntlige forhandlinger ved rettens behandling av begjæringer om skjult tvangsmiddelbruk. Departementets forslag medfører følgelig ingen endring

i muligheten til hurtig behandling av nye begjæringer om kommunikasjonskontroll. En kan heller ikke se at forslaget om oppnevnelse av samme advokat skaper nevneverdige etterforskningsmessige problemer. Det vises til at regelen gjelder «så langt det er mulig», slik at eventuelle forsinkelser som kan skade etterforskningen kan gi grunnlag for oppnevnelse av en annen advokat. Departementet viser for så vidt til drøftelsen i punkt 6.6.2.4 ovenfor.

7.6 Kommunikasjonskontroll knyttet til tjeneste

Under høringen har enkelte høringsinstanser tatt opp spørsmålet om det bør åpnes for kommunikasjonskontroll knyttet til tjeneste. Problemstillingen er ikke drøftet i utvalgets utredning.

Kripos kommenterer at det kan konstateres et endret brukermønster ved at bruken beveger seg fra faste kommunikasjonsanlegg til tjenester med særskilte identifikatorer. Tjenester som Skype, Messenger, e-post og nettsamfunn (for eksempel Facebook) aksesseres i dag ved hjelp av brukernavn med tilhørende passord. Tilbyderne av disse tjenestene er vanligvis ikke de nettilbyderne politiet forholder seg til. I tillegg gir flere tilbydere av telefonitjenester sine brukere tilgang til tjenester via internett. Ifølge Kripos betyr dette at «dersom mistenkte benytter disse tjenestene via et annet nett enn sitt normale, eksempelvis en trådløs internettsone på en flyplass, vil ikke kommunikasjonen bli fanget opp til tross for at mistenkte benytter kommunikasjonstjenester politiet kjenner til at mistenkte disponerer». Kripos bemerker også at det i senere tid har skjedd en endring i hvor brukerne lagrer sine data, ettersom flere store selskaper tilbyr lagring av informasjon på sentrale steder. Dette gjør ifølge høringsinstansen at kun en begrenset del av mistenktes informasjon trenger å være lagret eller tilgjengelig på mistenktes egen datamaskin.

På denne bakgrunn foreslår Kripos at straffeprosessloven § 216 a endres slik at bestemmelsen også gir hjemmel for avlytting av mistenktes kommunikasjonstjenester. Høringsinstansen mener avlyttingen dermed kan bli mer målrettet og mindre inngripende, ved at den spisses direkte mot brukerens aktivitet. Dette vil angivelig også redusere mengden informasjon som samles inn som ikke er relevant for politiformål. Som mønster viser Kripos til svensk rett, som tillater kommunikasjonskontroll av «ett telefonnummer, en kod eller annen teleadress», samt finsk rett, som viser til «en viss teleanslutning, e-postadress eller någon annan sådan teleadress till eller från teleterminalutrustning gjennom ett sådant allmänt kommunikasjonsnät».

Også *NAST* mener at ordlyden i § 216 a tredje ledd bør endres slik at tillatelsen til avlytting kan knyttes til en bestemt kommunikasjonstjeneste. Embetet uttaler:

> «Poenget er at ett og samme fysiske anlegg kan ha flere brukerkontoer, og det kan være aktuelt å avlytte trafikken dem imellom, for eksempel mellom epostkonti på samme server. Mens en IP-adresse kan tilhøre serveren, identifiserer brukernavnet kontoen. Dermed bør brukernavnet være tilstrekkelig kriterium, og man taler da om bruk av en tjeneste, ikke et bestemt anlegg. I realiteten kan tilbyderen bytte anlegg (server) uten at det påvirker bruken, og politiets metoder må følge *kontoen*, ikke hvorfra den fysisk leveres til enhver tid.»

Departementet ser at en adgang til å knytte kommunikasjonskontrollen til en bestemt tjeneste, og ikke bare et bestemt kommunikasjonsanlegg, vil kunne avhjelpe enkelte av de problemer som oppstår som følge av at moderne kommunikasjonsteknologi i større grad er knyttet til tjenester enn til faste kommunikasjonsanlegg. En ser heller ikke bort fra at en slik adgang kan gjøre kontrollen mer målrettet og således mindre personvernkrenkende.

Ved å knytte tillatelsen til kommunikasjonskontroll til en bestemt tjeneste, vil imidlertid tjenesten kunne kontrolleres selv om mistenkte bytter til et annet kommunikasjonsanlegg enn det han opprinnelig benyttet. Dette skiller seg på grunnleggende punkter fra utgangspunktet i gjeldende rett om at kontrollen må knytte seg til «bestemte telefoner, datamaskiner eller andre anlegg for kommunikasjon», jf. også drøftelsen i punkt 7.5 ovenfor. Spørsmålet om å fravike dette utgangspunktet ved å tillate kommunikasjonskontroll knyttet til tjeneste er ikke behandlet av utvalget og er kun tatt opp av et lite antall høringsinstanser. På det nåværende tidspunkt finner departementet derfor ikke å ha tilstrekkelig grunnlag for å foreslå nye regler om kommunikasjonskontroll knyttet til tjeneste.

Departementet viser dessuten til forslaget om å åpne for dataavlesing, jf. proposisjonen kapittel 14. En antar at forslaget i noen grad vil avhjelpe de etterforskningsmessige utfordringene som høringsinstansene har påpekt som argumenterer for kommunikasjonskontroll knyttet til tjeneste.

Departementet ønsker derfor å avvente virkningene av denne endringen før det eventuelt foretas en fornyet utredning av behovet for kommunikasjonskontroll knyttet til tjeneste.

7.7 Kommunikasjonskontroll for å lokalisere kommunikasjonsanlegg

7.7.1 Gjeldende rett

7.7.1.1 Hjemler som gir politiet adgang til selv å innhente lokaliseringsdata

Etter straffeprosessloven §§ 202 b og 202 c kan politiet iverksette teknisk sporing for å klarlegge hvor den mistenkte eller bestemte gjenstander befinner seg. Teknisk sporing vil si at politiet plasserer elektronisk peileutstyr på et objekt for å lokalisere hvor objektet befinner seg. Metoden iverksettes uten at den tiltaket er rettet mot, gjøres kjent med det.

Mens § 202 b gjelder sporing av kjøretøy, gods eller andre gjenstander, gir § 202 c hjemmel for såkalt personnær teknisk sporing. Sistnevnte innebærer at teknisk peileutstyr plasseres i for eksempel klær eller bestemte gjenstander som den mistenkte bærer med seg, jf. § 202 c første ledd bokstav a. Med teknisk peileutstyr menes elektroniske signalsendere som kan festes til en gjenstand og brukes til å følge denne gjenstandens bevegelser, jf. Ot.prp. nr. 64 (1998–99) punkt 23 side 148. Plassering av peileutstyr i klær eller gjenstander som den mistenkte bærer med seg, vil kunne gjøre det mulig for politiet å motta kontinuerlig informasjon om vedkommendes bevegelser over en lengre periode. Dette fordrer imidlertid at politiet i forkant har kunnet feste peileutstyret til gjenstander som den mistenkte bærer.

Straffeprosessloven § 216 b gir hjemmel for annen kontroll av kommunikasjonsanlegg enn kommunikasjonsavlytting. Kontroll etter bestemmelsen kan bestå i å innstille eller avbryte overføring av kommunikasjon til eller fra et bestemt kommunikasjonsanlegg (annet ledd bokstav a), stenge anlegg for kommunikasjon (bokstav b), identifisere anlegg ved hjelp av teknisk utstyr (bokstav c), eller kreve trafikkdata utlevert fra eier eller tilbyder av nett eller tjeneste (bokstav d). Alternativet i bokstav c om identifisering av anlegg kom inn i ved endringslov 17. juni 2005 nr. 87, og åpner for at politiet kan bruke peileutstyr eller andre tekniske innretninger for å få tilgang til kommunikasjonsanleggets unike identitet. I praksis gjøres dette som regel ved bruk av en såkalt IMSI-catcher (mobil basestasjon). Fremgangsmåten er i Ot.prp. nr. 60 (2004–2005) punkt 8.5.2 side 109 beskrevet på følgende måte:

> «[…] I praksis skjer dette ved at politiet i en kort periode gjennomfører en teknisk observasjon av anlegget for å kartlegge påloggede identiteter. Etter å ha foretatt systematiske sammenligninger, for eksempel av hvilke identiteter som går igjen på to forskjellige steder hvor politiet vet at den mistenkte oppholder seg på bestemte tidspunkter, vil politiet som regel være i stand til å identifisere en eller flere kommunikasjonsenheter som den mistenkte antas å besitte.»

Identifisering av et kommunikasjonsanlegg vil ofte skje med sikte på å fremme begjæring om kommunikasjonsavlytting, men kan også anvendes på annen måte – for eksempel som grunnlag for begjæring om innsyn i abonnementsopplysninger.

Straffeprosessloven § 216 b annet ledd bokstav c var gjenstand for tolkning i en kjennelse fra Høyesteretts ankeutvalg inntatt i Rt. 2009 side 394. Det ble her reist spørsmål om bestemmelsen gir adgang til å iverksette kommunikasjonskontroll med sikte på å identifisere personen som bruker et bestemt kommunikasjonsanlegg, og ikke anlegget som sådan. Politiet hadde i saken fremsatt begjæring om kommunikasjonskontroll av en mobiltelefon som sto registrert på en annen person enn den politiet antok at disponerte telefonen. Formålet med kontrollen var å bringe på det rene identiteten til brukeren av telefonen – som var mistenkt for narkotikakriminalitet.

Både tingretten og lagmannsretten tok politiets begjæring til følge. Lagmannsretten tok utgangspunkt i at ordlyden i straffeprosessloven § 216 b annet ledd bokstav c ikke tar sikte på situasjoner hvor det er den mistenkte som skal identifiseres, men la større vekt på andre rettskildefaktorer. Retten fremhevet at tilfellet ligger nær lovens ordlyd, at reelle hensyn tilsier at kontrollen burde tillates, samt at lovgiver antakelig ville inkludert disse tilfellene dersom man var oppmerksom på problemstillingen.

Høyesteretts ankeutvalg opphevet enstemmig lagmannsrettens kjennelse på grunn av feil lovtolkning. Til tross for at ankeutvalget ikke var uenig i de hensyn lagmannsretten hadde pekt på, mente man at kravet om klar lovhjemmel måtte veie tyngre. Det ble vist til at hjemmelskravet på straffeprosessens område må stå særlig sterkt – både ut fra det generelle legalitetsprinsippet i norsk rett og lovkravet i EMK artikkel 8. Videre

viste retten til en uttalelse i Ot.prp. nr. 60 (2004–2005) punkt 8.5.2 side 109, hvor det heter:

> «Slik departementet oppfatter gjeldende rett, kan politiet ikke ta i bruk GSM-identifiseringssystemer uten lovhjemmel. Selv i situasjoner hvor de aktuelle anleggenes identitet kan fanges opp uten at kommunikasjon avlyttes, innebærer bruk av slike systemer et så vidt følbart inngrep for de som berøres av undersøkelsene, at det ikke bør åpnes for bruk av slikt utstyr før Stortinget har tatt stilling til spørsmålet.»

Ankeutvalget konkluderte på denne bakgrunn med at det etter gjeldende rett ikke er adgang til å iverksette kommunikasjonskontroll etter straffeprosessloven § 216 b med sikte på å avdekke brukerens identitet.

Bestemmelsen innebærer følgelig en viss adgang til å lokalisere mobiltelefoner og andre mobile kommunikasjonsanlegg. Bruken av virkemidlet er imidlertid begrenset til et visst formål – nærmere bestemt identifisering av anlegget. Metoden kan derimot ikke benyttes med sikte på å fastslå hvor kommunikasjonsanlegget – og dermed også den mistenkte – befinner seg, jf. Rt. 2009 side 394 og NOU 2009: 15 punkt 16.6 side 198–199.

7.7.1.2 Hjemler som gir adgang til å kreve utlevering av lokaliseringsdata

Opplysninger om et kommunikasjonsanleggs posisjon på et gitt tidspunkt kan kreves utlevert fra tilbyder av elektroniske kommunikasjonstjenester etter reglene om utleveringspålegg og beslag. Det følger av straffeprosessloven §§ 203 og 210 at ting som kan ha betydning som bevis, kan beslaglegges inntil det foreligger rettskraftig dom, eller retten kan pålegge besitteren å utlevere tingen. Elektronisk lagrede opplysninger er «ting» etter disse bestemmelsene, jf. Rt. 1992 side 904.

Dersom det er strengt nødvendig for etterforskningen i saken, kan utlevering og beslag skje uten at den som rammes blir gitt underretning eller ved at han underrettes først på et senere tidspunkt, jf. §§ 208 a og 210 a. En forutsetning er at noen med skjellig grunn mistenkes for en handling eller forsøk på handling som kan medføre høyere straff enn fengsel i 6 måneder.

Reglene om utleveringspålegg og beslag er begrenset av regler om vitneplikt, jf. § 204. I henhold til § 118 kan retten bare ta imot forklaring som et vitne kan gi uten å krenke taushetsplikt som påligger tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, dersom departementet samtykker. Samtykke kan bare nektes dersom åpenbaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jf. § 118 første ledd siste punktum. Samtykkekompetansen utøves av Nasjonal kommunikasjonsmyndighet (tidligere Post- og teletilsynet) i kraft av delegasjon, jf. vedtak 23. juni 1995 nr. 39.

Kommunikasjonsopplysninger kan ikke innhentes etter de nevnte bestemmelsene med virkning fremover i tid. Adgangen gjelder følgelig kun såkalte historiske data, jf. straffeprosessloven § 210 b siste ledd. Ønsker politiet en fortløpende utlevering av opplysninger om hvor et kommunikasjonsanlegg befinner seg når det benyttes til kommunikasjon, må dette skje etter reglene om kommunikasjonskontroll i § 216 b.

Straffeprosessloven § 216 b annet ledd bokstav d gir hjemmel for å innhente fra eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjonen, opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med et kommunikasjonsanlegg og andre data knyttet til kommunikasjon. Med «andre data knyttet til kommunikasjon» menes blant annet informasjon om en mobiltelefons geografiske posisjon idet en samtale finner sted, jf. Ot.prp. nr. 64 (1998–99) punkt 23 side 159. Ifølge § 216 b tredje ledd gjelder § 216 a fjerde ledd tilsvarende, slik at eier eller tilbyder av nett eller tjeneste kan pålegges å yte den bistand som er nødvendig ved gjennomføringen av kontrollen, jf. § 216 a fjerde ledd annet punktum. Ettersom opplysningene som kan kreves utlevert er data knyttet til kommunikasjon, synes utleveringsadgangen begrenset til opplysninger som genereres når det aktuelle anlegget faktisk benyttes til kommunikasjon.

7.7.2 Andre lands rett

7.7.2.1 Dansk rett

I Danmark fikk man ved lov nr. 542 av 8. juni 2006 en egen hjemmel for å pålegge tilbyder av telenett eller teletjeneste å utlevere posisjonsopplysninger for mobiltelefoner. Metoden – såkalt «teleobservation» – er ansett som en form for spaning («observation»), og er plassert i retsplejelovens bestemmelser om dette. Loven § 791 a, stk. 5 lyder slik:

> «Politiet kan fra udbydere af telenet eller teletjenester indhente oplysninger vedrørende lokaliseringen af en mobiltelefon, der antages at benyttes af en mistænkt (teleobservation), hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der kan medføre fængsel i 1 år og 6 måneder eller derover.»

Etter § 791 a, stk. 6 plikter tilbydere av telenett eller teletjenester å bistå politiet ved utførelsen av inngrepet, herunder ved å gi opplysninger som nevnt i stk. 5.

Retsplejelovens regler om teleobservasjon ble vedtatt i forbindelse med den såkalte «Terrorpakke II», etter anbefaling fra en tverrdepartemental arbeidsgruppe for terrorbekjempelse. I rapporten «Det danske samfunds indsats og beredskab mod terror» (oktober 2005) uttaler gruppen, jf. punkt 4.3.2 side 79:

> «Den nuværende teknik inden for mobiltelefoni giver mulighed for, at man via mastepositioner kan stedfæste, hvor en tændt mobiltelefon befinder sig, uanset om mobiltelefonen faktisk benyttes til kommunikation.
>
> Højesteret har i kendelse af 25. oktober 2002 fastslået, at et sådant fremadrettet indgreb må sidestilles med observation af personer, der befinder sig på et ikke frit tilgængeligt sted, da teleselskabernes videregivelse af positionsoplysninger i henhold til telekonkurrencelovens § 13, stk. 3, ikke kan anses for berettiget, medmindre videregivelse af positionsoplysningerne kan anses for hjemlet i retsplejelovens regler om strafprocessuelle tvangsindgreb eller videregivelse må sidestilles med et sådant indgreb.»

På denne bakgrunn anbefalte arbeidsgruppen at tilbydere av elektroniske kommunikasjonsnett og -tjenester skulle forpliktes til løpende utlevering av opplysninger om hvilke basestasjoner en påslått mobiltelefon er i kontakt med, og at tilbyderne skulle forpliktes å innrette sine tekniske systemer slik at de aktuelle inngrep er mulig. Justisministeriet sluttet seg til arbeidsgruppens anbefaling.

7.7.2.2 Svensk rett

Etter rättegångsbalken 27 kap. 19 § 1 mom. kan politiet iverksette såkalt hemmelig overvåking av elektronisk kommunikasjon, ved å innhente ulike former for informasjon om kommunikasjonsanlegg. Bestemmelsen ble endret ved lag (2012:281), da kravet om at kommunikasjonsanlegget faktisk var brukt til kommunikasjon, ble fjernet. Etter dette kan politiet blant annet hente inn historiske opplysninger om «vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område», jf. nr. 2. Om dette uttales i Prop. 2011/12:55 side 97 følgende:

> «En eller flera basstationstömningar sker ofta med avseende på platsen för ett grovt brott. För de brottsbekämpande myndigheterna är möjligheten till en sådan inledande åtgärd ofta central för att så snabbt som möjligt kunna identifiera misstänkta personer i utredningen. Regeringen delar utredningens bedömning att det är nödvändigt för effektiviteten i den brottsbekämpande verksamheten att möjligheten att genomföra basstationstömning finns kvar när bestämmelsen i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation, enligt vad som föreslagits i avsnitt 6.1, upphävs. Det är av samma skäl viktigt att det i brottsbekämpningen ges tillgång till uppgifter avseende t.ex. mobiltelefoner som är påslagna men som inte vid det aktuella tillfället har använts för kommunikation.»

Regjeringen uttalte samtidig at det er uten betydning fra et integritetssynspunkt om et mobilt kommunikasjonsanlegg blir brukt til kommunikasjon eller ikke. Åpningen for å innhente posisjonsopplysninger som ikke har tilknytning til kommunikasjon kunne derfor «inte anses medföra någon nämnvärd ökning av integritetsintrånget för den enskilde».

Bestemmelsen i 27 kap. 19 § 1 mom. gir videre hjemmel for å innhente sanntidsopplysninger om «i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits», jf. nr. 3. I den nevnte proposisjonen uttales om dette (side 98):

> «En inhämtning som innebär att de brottsbekämpande myndigheterna får möjlighet att följa hur en mobiltelefon förflyttas kommer att beröra betydligt färre personer men innebär samtidigt ett större integritetsintrång för den person som övervakningen avser. Möjligheten att kartlägga den enskilde och hans eller hennes förhållanden ökar. Denna form av kartläggning får enligt regeringens bedömning anses omfattas av tillämpningsområdet för den nya grundlagsbestämmelsen om stärkt skydd för den personliga integriteten (se närmare ovan). Mot bakgrund av de tydliga avgränsningar som

> regeringen föreslår för den nya regleringen om inhämtning bl.a. i fråga om syftet med inhämtningen och betydelsen av uppgifterna, blir dock tillämpningsområdet så snävt att nyttan av att införa en sådan möjlighet för de brottsbekämpande myndigheterna måste anses överväga det ökade integritetsintrång utvidgningen medför. Inhämtningsmöjligheten medför inte heller ett hot mot den fria åsiktsbildningen.»

Overvåking av elektronisk kommunikasjon kan skje ved etterforskning av lovbrudd med en minstestraff på seks måneders fengsel, jf. 19 § 3 mom. Det samme gjelder ved visse særskilt angitte straffebud, herunder datainnbrudd, befatning med barnepornografi av en viss alvorlighet, visse former for narkotikalovbrudd og smugling, samt visse former for særlig samfunnsfarlig kriminalitet. Forsøk, forberedelse eller forbund kan gi grunnlag for metodebruk såfremt slike handlinger i seg selv er straffbare. Dersom ingen med skjellig grunn kan mistenkes for lovbruddet, og formålet med metodebruken er å finne ut hvem som kan mistenkes, er vilkårene de samme som for kommunikasjonsavlytting, jf. 19 § 4 mom. jf. 20 § 2 mom. Det kreves da at lovbruddet har en minstestraff på to års fengsel eller mer, at det er tale om angitte former for særlig samfunnsfarlig kriminalitet eller at lovbruddets straffverdighet for øvrig overstiger to års fengsel, jf. 18 § 2 mom.

7.7.2.3 Finsk rett

Tvångsmedelslagen 10 kap. 10 § gjelder innhenting av basestasjonsopplysninger, som er definert som «information om teleadresser och teleterminalutrustning som redan är eller kommer att bli registrerade i ett telesystem via en viss basstation». Etter bestemmelsen kan politiet gis tillatelse til å innhente basestasjonsopplysninger for det antatte tidspunktet for et lovbrudd fra en basestasjon i nærheten av det antatte åstedet. Dersom det foreligger særlige grunner, kan tillatelse gis også for et annet tidspunkt eller et annet sted som er av betydning for etterforskningen av lovbruddet.

Tillatelse til innhenting av basestasjonsopplysninger kan gis på samme vilkår som såkalt «teleövervakning», som tilsvarer kommunikasjonskontroll hvor man ikke fanger opp innholdet i kommunikasjonen. Metoden kan benyttes i etterforskningen av lovbrudd med en strafferamme på minst fire års fengsel, samt ved visse andre særskilt angitte lovbrudd. Sistnevnte omfatter blant annet lovbrudd med minst to års strafferamme som er begått ved bruk av teleadresse eller teleterminalutstyr, datainnbrudd mv., visse former for seksuallovbrudd, narkotikalovbrudd og forberedelse til terror.

Tvångsmedelslagen 10 kap. 21 § gir hjemmel for teknisk sporing av ulike typer gjenstander. Med teknisk sporing forstås etter 1 mom. at «förflyttning av föremål, ämnen eller egendom spåras med hjälp av radiosändare som fästs eller som redan finns på objektet eller med hjälp av någon annan liknande teknisk anordning, metod eller programvara».

Bestemmelsen er søkt utformet på en teknologinøytral måte, for å sikre at ulikt utstyr og programvare – så vel som egenskaper som finnes hos gjenstanden som spores – kan benyttes. Om dette uttales i RP 222/2010 rd 295267 side 345:

> «I definitionen begränsas inte spårningsmetoderna på samma sätt som i 5 a kap. 1 § 1 mom. 3 c punkten i den gällande tvångsmedelslagen, utan teknisk spårning ska kunna utföras neutralt med avseende på tekniken, med olika tekniska anordningar, medier och programvaror. Dessutom nämns i definitionen för tydlighetens skull att egenskaper som redan finns hos föremål, ämnen eller egendom kan utnyttjas. Då utförs den tekniska spårningen antingen helt och hållet med hjälp av en egenskap som redan finns eller så kompletteras den på något sätt av förundersökningsmyndigheten. Som exempel kan nämnas att positioneringsutrustning som redan finns i ett fordon aktiveras i hemlighet för att genomföra teknisk spårning.»

Et annet eksempel kan trolig være bruk av posisjoneringsutstyr eller -program som finnes i et mobilt kommunikasjonsanlegg.

Teknisk sporing kan rettes mot objekter, gods eller eiendom som er gjenstand for en straffbar handling eller som den mistenkte antas å besitte eller anvende, dersom vedkommende er mistenkt for et lovbrudd med en strafferamme på minst ett års fengsel. Om formålet med sporingen er å følge hvordan en mistenkt forflytter seg ved at sporingsutstyret festes på vedkommendes klær eller på objekt vedkommende bærer med seg, er adgangen likevel begrenset til lovbrudd som opplistes i 16 § 3 mom. Dette innebærer at metoden kan anvendes i etterforskningen av lovbrudd med strafferamme på minst fire års fengsel, narkotikalovbrudd, forberedelse til terror samt grov tollovertredelse.

7.7.3 Metodekontrollutvalgets forslag

Spørsmålet om kommunikasjonskontroll med sikte på å avdekke mistenktes identitet eller oppholdssted drøftes av utvalget i utredningen punkt 16.6 side 198 flg. På bakgrunn av Høyesteretts ankeutvalgs klare vurdering av de reelle hensyn som gjør seg gjeldende og at lovgiver antakelig ville inkludert tilfellene dersom man var oppmerksom på problemstillingen, har utvalget kommet til at det bør åpnes for kommunikasjonskontroll etter straffeprosessloven § 216 b for å avdekke identiteten til personen (mistenkte) som bruker et bestemt anlegg. Identifisering av mistenkte hvor telefonnummeret er kjent vil i praksis for eksempel kunne skje ved bruk av et mobilt GSM–identifiseringssystem, såkalt IMSI–catcher, som vil kunne fange opp hvor den aktuelle telefonen befinner seg. Politiet vil da kunne være i stand til å finne ut hvor mistenkte befinner seg, og derigjennom identifisere mistenkte.

Metodekontrollutvalget bemerker samtidig at situasjonen også kan være at politiet vet hvem mistenkte er, men at trafikkdata om hvilke basestasjoner kommunikasjonsanlegget er koblet opp mot ikke gir sikre holdepunkter for *hvor* vedkommende oppholder seg. Problemstillingen kan oppstå i forbindelse med for eksempel pågripelse eller hvor det av andre grunner er nødvendig raskt å lokalisere og gripe inn overfor mistenkte, for eksempel i en gisselsituasjon. Utvalget mener at det i slike tilfeller bør være adgang til posisjonspeiling for å fastslå mistenktes oppholdssted ved hjelp av mobilt identifiseringssystem. Det foreslås derfor et uttrykkelig tillegg i straffeprosessloven § 216 b som tar sikte på denne typen situasjoner.

Etter utvalgets forslag skal de nevnte hjemlene gis i en egen bokstav i straffeprosessloven § 216 b annet ledd. Ny bokstav e foreslås å lyde:

> «Kontrollen kan gå ut på […] å identifisere personen som bruker et anlegg som nevnt i bokstav a, eller hvor vedkommende oppholder seg.»

7.7.4 Høringsinstansenes syn

Metodekontrollutvalgets forslag om kommunikasjonskontroll for å avdekke identitet eller oppholdssted får bred støtte i høringen. Av de som har uttalt seg om spørsmålet, støtter samtlige høringsinstanser Metodekontrollutvalgets forslag. Dette omfatter *Riksadvokaten, NAST, Oslo statsadvokatembeter, Kripos, Oslo politidistrikt, PST, Advokatforeningen* og *Forsvarergruppen av 1977*. Flere høringsinstanser peker på behovet for slik tvangsmiddelbruk og støtter utvalgets begrunnelse.

Advokatforeningen uttaler i den sammenheng:

> «Utvalget har i avsnitt 16.6 om kommunikasjonskontroll for å avdekke identitet eller oppholdssted, gått inn for at kontroll av kommunikasjonsanlegg etter straffeprosessloven § 216 b kan gjennomføres for å avdekke identiteten til personen (mistenkte) som bruker et bestemt anlegg. Advokatforeningen har etter omstendighetene ingen bemerkninger til dette lovendringsforslaget og finner utvalgets begrunnelse fyllestgjørende.»

Forsvarergruppen av 1977 har heller ikke innvendinger til utvalgets vurderinger hva gjelder avdekking av identitet eller oppholdssted.

Riksadvokaten er enig i utvalgets forslag om endring av straffeprosessloven § 216 b til å omfatte avdekking av identiteten og oppholdssted for en bruker av en bestemt telefon.

PST uttaler:

> «Når det gjelder utvalgets forslag om bruk av kommunikasjonskontroll for å avdekke identitet eller oppholdssted støtter PST dette. På linje med det ordinære politi vil også PST ha behov for å kunne bruke kommunikasjonskontroll for å [få] avdekket identitet eller oppholdssted.»

Kripos er enig i den foreslåtte endringen til straffeprosessloven § 216 b annet ledd og drøftelsen i tilknytning til dette, men understreker at bestemmelsen må gjøres så teknologinøytral som mulig. Av den grunn mener Kripos at det er fornuftig at det ikke er foreslått bruk av begrepet «ved hjelp av teknisk utstyr», slik det er i dagens bokstav c) i samme bestemmelse. Kripos peker videre på behovet for andre løsninger, som bruk av stille SMS:

> «For politiet er [det] en meget praktisk problemstilling da det pr i dag finnes tekniske løsninger for å sende «skjulte» tekstmeldinger til mistenkte, slik at dette genererer en basestasjonsoppføring i politiets KK-system. Etter Kripos' oppfatning vil en slik metode verken være kommunikasjonskontroll etter strpl §216a / §216b eller teknisk sporing etter strpl §202b / §202c etter dagens regler. Derimot vil det etter Kripos' oppfatning være posisjonspeiling etter den foreslåtte bestemmelsen i strpl §216b annet ledd.

Den aktuelle tekniske løsningen vil trolig ikke komme inn under begrepet «teknisk utstyr». Metoden bidrar til å lokalisere området mistenkte befinner seg i når det foretas kommunikasjonskontroll. Denne metoden er særs anvendelig når politiet må ha kontroll på flere mistenkte i en sak, og det ikke er praktisk gjennomførbart å spane mot alle objekter samtidig, eller i situasjoner hvor politiet mister kontroll med objektet det spanes mot. Politiet kan da generere basestasjonsopplysninger ved at det sendes en tekstmelding til mistenktes telefon, men hvor denne ikke er synlig for mistenkte.

Samme metodikk kan også benyttes når det ikke foretas kommunikasjonskontroll etter strpl § 216a, men da vil opplysningene være langt mer upresise slik løsningen fungerer i dag. Det vil gi opplysninger om hvorvidt mistenktes telefon er aktiv og i hvilket område den befinner seg. Dette området er langt mindre nøyaktig enn en basestasjonsopplysning. I disse tilfellene benyttes teleselskapenes nettverk ved hjelp av en ekstern teknisk løsning hvor det gjøres en forespørsel hvorvidt mistenktes telefon er aktiv. En vil da få svar hvorvidt telefonen er aktiv, hvilket telenett den befinner seg i og en omtrentlig posisjon (med lav nøyaktighetsgrad). Forespørselen genererer ingen kommunikasjon til mistenktes telefon, kun en nettverksforespørsel til teleselskapenes system.

Kripos foreslår at det presiseres i lovforslaget at en slik type posisjonspeiling omfattes av den nye bestemmelsen i strpl §216b annet ledd, ny bokstav e).»

NAST uttrykker en generell bekymring for at lovgiver mener det er påkrevet å regulere skritt for skritt hva som skal være formålet med bruk av eksisterende etterforskningsmetoder. Høringsinstansen uttaler:

«NAST støtter selvfølgelig forslaget om at reglene skal tilrettelegge for lokalisering av person, på grunn av det åpenbare behovet for dette. Men det synes å hefte svakheter ved at lovgiver mener det er påkrevet å regulere skritt for skritt hva som skal være *formålet* med informasjonsfangsten, og gjør det i tilknytning til *eksisterende spesifikke metoder,* i dette tilfellet kommunikasjonskontroll.

I dag, med utstrakt bruk av mobil trådløs kommunikasjonsteknologi, er det nokså selvsagt at opplysninger om elektronisk kommunikasjon (metadata) sier noe om *hvor* et kommunikasjonsanlegg er, og følgelig også noe om hvor en person er når anlegget brukes. Men slike opplysninger får en ikke bare ved å utnytte teknologi i forhold til kommunikasjonskontroll, det gjelder også for lagrede data. Ved IP-sporing kan man avdekke *den geografiske posisjonen* til en mistenkt på det tidspunkt vedkommende koblet seg opp til sin brukerkonto i nettet. Og dersom politiet har sendt et rapporteringsprogram til kontoen, kan det gi *varsel* til politiet når oppkobling skjer, slik at tilslag, f.eks. med tanke på pågripelse, kan skje.

Det relevante skillet synes å gå mellom *aktiv og passiv* anskaffelse av lokaliseringsdata. Med«aktiv» menes at politiet anskaffer dataene på egen hånd, og man er da i praksis henvist til bruk av teknisk utstyr av fysisk art som en IMSI-catcher, eller tjenester som politiet anvender selv, for eksempel bruk av et rapporteringsprogram som nevnt, eller som kjøpes av en tilbyder, for eksempel «silent SMS». Den «passive» metoden gjelder utlevering av trafikk- og lokaliseringsdata m.v. fra tilbyder. Også slike data sier noe om posisjon, men er registrert som ledd i vanlig tjenesteyting.»

Oslo politidistrikt bemerker at det man ved bruk av teknisk utstyr kan avdekke, er den geografiske posisjonen til et kommunikasjonsanlegg. Oppnår man en presis lokalisering av kommunikasjonsanlegget, vil man deretter kunne identifisere brukeren av anlegget. Formålet med bestemmelsen vil dermed etter politidistriktets forståelse være å kunne lokalisere et bestemt mobilt kommunikasjonsanlegg, først og fremst mobiltelefon. I tråd med dette foreslår høringsinstansen at bestemmelsen utformes slik:

«… å fastslå den geografiske posisjon til anlegg som nevnt i bokstav a ved hjelp av teknisk utstyr.»

Oslo politidistrikt mener dessuten at det er mest naturlig å innta den foreslåtte bestemmelsen i § 216 annet ledd bokstav d, og at det som i dag er bokstav d blir bokstav e. Bokstav c og d vil da gjelde henholdsvis identifisering og lokalisering ved hjelp av teknisk utstyr, og det er naturlig at disse nevnes i sammenheng. *NAST* mener i stedet at den foreslåtte bestemmelsen systematisk hører hjemme i straffeprosesslovens kapittel om teknisk sporing.

7.7.5 Departementets vurdering

7.7.5.1 Kort om fremgangsmåter for lokalisering av mobile enheter

Når det kommuniseres ved hjelp av mobilnettet, etterlates elektroniske spor som i kortere eller lengre tidsrom lagres hos nett- og tjenestetilbydere. Blant informasjonen som lagres er såkalte trafikkdata, som er opplysninger om den geografiske plasseringen til et mobilt kommunikasjonsanlegg idet kommunikasjon finner sted. For mobiltelefoner fremkommer trafikkdata først og fremst i form av opplysninger om basestasjonstilknytning – det vil si om hvilken basestasjon (mobilmast) telefonen har benyttet til å kommunisere.

Mobilnettet holder imidlertid også oversikt over hvor påslåtte mobilanlegg befinner seg når de ikke er i bruk til kommunikasjon. Dette er nødvendig for å vite hvilken basestasjon signalene skal sendes til når anlegget blir kalt opp. Nett- og tjenestetilbydere mottar derfor kontinuerlig såkalte signaleringsdata, som kan forstås som «data som genereres mellom terminalen og tilgjengelig basestasjon og angir terminalens geografiske plassering når den er slått på, uten at trafikkdata formidles», jf. ekomforskriften § 7-2 første ledd annet punktum.

En basestasjon er en radiosender som fungerer som bindeledd mellom det mobile kommunikasjonsanlegget og telefonsentralen. Dekningsområdet for en basestasjon kan variere betydelig avhengig av hvor basestasjonen er plassert. I tettbygde strøk, hvor basestasjonene står tett, vil hver mast gjerne ha en radius på noen hundre meter, mens dekningsområdet i mindre befolkede områder kan være flere mil. Dette medfører at nøyaktighetsgraden på lokaliseringsdata som innhentes fra basestasjonene, vil være forskjellig avhengig av hvor den aktuelle basestasjonen befinner seg.

Det finnes i dag flere ulike tekniske løsninger for lokalisering av mobile kommunikasjonsanlegg ved hjelp av basestasjonsopplysninger. For det første er det mulig å benytte spesielle typer teknisk utstyr – eksempelvis en såkalt IMSI-catcher. IMSI-catcheren fungerer som en mobil basestasjon som henter inn kortnummer (IMSI) og apparatnummer (IMEI) for alle mobilanleggene som befinner seg innenfor dens dekningsradius. Ettersom dekningsområdet for IMSI-catcheren er konfigurerbart, vil denne fremgangsmåten kunne gi opplysninger av høyere nøyaktighetsgrad enn «vanlige» basestasjonsopplysninger. Fremgangsmåten er imidlertid ressurskrevende, ettersom IMSI-catcheren manuelt må transporteres til og opereres fra et sted i nærheten av mobilanlegget som skal lokaliseres. Etter forslaget fremsatt av Metodekontrollutvalget, vil politiet kunne benytte IMSI-catcher eller annet teknisk utstyr for å lokalisere en mistenkt i en straffesak.

For det andre kan «vanlige» basestasjonsopplysninger begjæres utlevert fra nett- eller tjenestetilbyder. Her vil nøyaktighetsgraden på opplysningene avhenge av størrelsen på dekningsområdet for den aktuelle basestasjonen. Ettersom tilbyderne regelmessig mottar både trafikk- og signaleringsdata, vil fremgangsmåten gjerne være mindre ressurskrevende enn bruk av eksternt teknisk utstyr. Mens trafikkdata i dag kan kreves utlevert etter straffeprosessloven § 216 b annet ledd bokstav d, har politiet ingen klar hjemmel for å kreve utlevering av data som ikke er «knyttet til kommunikasjon» – herunder signaleringsdata.

I tillegg til lokalisering som skjer via mobilnettet, finnes det lokaliseringsløsninger som benytter GPS (Global Positioning System) og lignende systemer. GPS er en satellittbasert lokaliseringsteknologi som benyttes utendørs, og som i hovedsak ikke fungerer inne. GPS-lokalisering kan for eksempel skje ved at det installeres en programvare på et mobilanlegg, som kontinuerlig sender informasjon om anleggets posisjon til en tjener på internett. GPS-opplysninger vil normalt være mer nøyaktige enn basestasjonsopplysninger som innhentes via mobilnettet.

7.7.5.2 Lokalisering ved hjelp av politiets eget utstyr

Politiet har ofte behov for på en effektiv måte å kunne lokalisere en mistenkt i en straffesak. Slike opplysninger kan være nødvendige eksempelvis for å foreta pågripelse, eller for å finne frem til andre impliserte, finne utbytte osv. Rent faktisk kan signaler fra mobiltelefoner eller andre mobile kommunikasjonsanlegg være et effektivt hjelpemiddel for å lokalisere en mistenkt. Dagens lovhjemler gir imidlertid politiet kun en begrenset mulighet til å nyttiggjøre seg disse signalene.

Metodekontrollutvalget har foreslått en utvidelse av politiets adgang til å benytte kommunikasjonskontroll for å lokalisere en mistenkt i en straffesak. Etter forslaget til ny bokstav e i straffeprosessloven § 216 b annet ledd skal kommunikasjonskontroll kunne iverksettes for «å identifisere personen som bruker et [kommunikasjonsanlegg], eller hvor vedkommende oppholder seg». Ifølge merknaden til den foreslåtte bestemmelsen vil dette i praksis kunne skje for eksempel «ved bruk av et mobilt GSM-identifiseringssystem, som vil kunne fange opp hvor den aktuelle telefonen

befinner seg. Politiet vil da kunne være i stand til å finne ut hvor mistenkte befinner seg, og derigjennom eventuelt også identifisere mistenkte.»

Departementet har vanskelig å se hvordan det lar seg gjøre i praksis å *identifisere* brukeren av et kommunikasjonsanlegg ved hjelp av kommunikasjonskontroll. Opplysninger om brukerens identitet og oppholdssted vil kunne oppnås ved en kombinasjon av kunnskap om kommunikasjonsanleggets posisjon, at brukeren befinner seg i umiddelbar nærhet til kommunikasjonsanlegget, samt bruk av ordinære etterforskningsmetoder som spaning. Departementet antar derfor at utvalget har ment å foreslå en adgang til kommunikasjonskontroll for å *lokalisere* et bestemt kommunikasjonsanlegg. En antar videre at høringsinstansene har forstått utvalget på denne måten, og således har avgitt sine uttalelser ut ifra dette.

Departementet er enig i at kommunikasjonskontroll etter straffeprosessloven § 216 b bør kunne benyttes til å lokalisere et bestemt kommunikasjonsanlegg. I kombinasjon med andre etterforskningsmetoder vil slik metodebruk kunne gi politiet informasjon om mistenktes identitet og oppholdssted, som kan ha avgjørende betydning ved for eksempel pågripelser eller i politiets arbeid med å avdekke bakmenn og deltakere i kriminelle miljøer. Lokaliseringen av kommunikasjonsanlegget vil således kunne brukes for å identifisere personen som bruker det, uavhengig av om anlegget, typisk en mobiltelefon, står registrert på en annen person enn den politiet antar disponerer telefonen. Departementet kan heller ikke se at kommunikasjonskontroll for å lokalisere et kommunikasjonsanlegg har særskilte trekk som gjør det betenkelig å åpne for slik metodebruk. Avveiningen av de hensyn som gjør seg gjeldende stiller seg på mange måter tilsvarende som for annen kommunikasjonskontroll etter straffeprosessloven § 216 b annet ledd bokstav c.

Metodekontrollutvalgets foreslåtte bestemmelse sier ikke noe om hvilke virkemidler politiet kan benytte, men kun hva slags informasjon som kan innhentes. Dette skiller seg fra de øvrige alternativene i § 216 b annet ledd, som i større grad angir *hva* politiet kan foreta seg. Det kan stilles spørsmål om den foreslåtte bestemmelsen tilfredsstiller lovkravet på straffeprosessens område.

Metodekontrollutvalget har foreslått at politiets adgang til å lokalisere et kommunikasjonsanlegg reguleres i en ny bokstav e i straffeprosessloven § 216 b annet ledd. Departementet er av den oppfatning at lokalisering av et kommunikasjonsanlegg har en naturlig forbindelse til det å identifisere et kommunikasjonsanlegg. Hjemlene for de to virkemidlene bør derfor plasseres i tilknytning til hverandre. Det foreslås følgelig at lokalisering av kommunikasjonsanlegg inkorporeres i § 216 b annet ledd bokstav c.

Bestemmelsen vil gi politiet adgang til å benytte eget teknisk utstyr for å fastslå hvor et mobilt kommunikasjonsanlegg befinner seg. Dette kan være en IMSI-catcher, men også annet teknisk utstyr som er egnet til å innhente lokaliseringsopplysninger. Derimot er bestemmelsen ikke ment å gi grunnlag for bruk av ulike typer programvare for å lokalisere mobilanlegg. Dette fremgår ved bruken av begrepet «utstyr», som etter en alminnelig forståelse neppe omfatter programvare. Det vil dermed ikke være adgang til for eksempel å installere et rapporteringsprogram på mistenktes mobiltelefon, som løpende sender informasjon om telefonens GPS-koordinater.

Departementet er for øvrig ikke enig med Det nasjonale statsadvokatembetet i at metoden det her er tale om bør flyttes til kapitlet om teknisk sporing. Selv om lokalisering av et bestemt kommunikasjonsanlegg kan ha visse likhetstrekk med teknisk peiling, er det likevel en form for kommunikasjonskontroll som naturlig hører hjemme i kapitlet om kommunikasjonskontroll, jf. punkt 7.7.5.5 nedenfor.

7.7.5.3 Utlevering av lokaliseringsdata fra nett- og tjenestetilbydere

På bakgrunn av innspill i forbindelse med høringen av Metodekontrollutvalgets utredning, synes det å være behov for å supplere adgangen til å benytte eget teknisk utstyr for å lokalisere mobilanlegg med en enklere og mindre ressurskrevende fremgangsmåte for lokalisering. Under høringen av Metodekontrollutvalgets utredning har flere høringsinstanser på politi- og påtalesiden tatt til orde for at utvalgets forslag går for kort og ikke dekker politiets behov. Foranlediget av disse høringsuttalelsene, samt senere henvendelser i forbindelse med oppfølgingen av utredningen, har departementet sett grunn til å foreslå at politiet også skal kunne få utlevert lokaliseringsdata fra nett- og tjenestetilbydere. Det vises også til NOU 2015: 13 «Digital sårbarhet – sikkert samfunn» side 117, der utvalget gir uttrykk for at det er behov for å avklare hjemmelsgrunnlaget for regulering av tilgang til signaleringsdata.

Som det fremgår ovenfor, mottar nett- og tjenestetilbydere jevnlig lokaliseringsdata som sier noe om hvor et bestemt mobilanlegg – og dermed også anleggets bruker – befinner seg. Politiets adgang til å nyttiggjøre seg disse opplysningene

er i dag begrenset av kravet om at informasjonen må være «knyttet til kommunikasjon», jf. straffeprosessloven § 216 b annet ledd bokstav d. Det er vanskelig å se at personvernhensyn kan begrunne et markant skille i politiets adgang til informasjonsinnhenting basert på om mobilanlegget rent faktisk har vært benyttet til kommunikasjon. En mistenkt i en straffesak kan neppe sies å ha en mer berettiget interesse i at politiet ikke vet hvor han befinner seg når han ikke kommuniserer via et mobilanlegg, enn når han bruker anlegget til kommunikasjon.

Ikke-kommunikasjonsrelaterte lokaliseringsopplysninger kan dessuten allerede i dag innhentes ved bruk av teknisk sporing etter straffeprosessloven § 202 c. Dette forutsetter imidlertid at peileutstyr i forkant festes på mistenktes klær eller lignende, noe som kan sies å øke graden av inngripen. Det kan hevdes at inngrepet reduseres dersom man i stedet kan innhente lokaliseringsopplysninger ved hjelp av et mobilanlegg som mistenkte uansett bærer med seg.

Sammenlignet med informasjonsinnhenting ved hjelp av eget teknisk utstyr, har innhenting av opplysninger fra nett- og tjenestetilbyder flere fordeler. For det første er det i utgangspunktet tale om lokaliseringsdata som uansett innhentes av tilbyder, slik at det vil være ressursbesparende at opplysningene hentes direkte herfra. For det andre vil det ved denne fremgangsmåten være lavere risiko for at informasjonsinnhentingen påvirker kommunikasjonsnettet, noe som kan være tilfellet ved bruk av for eksempel IMSI-catcher, som «omdirigerer» telesignalene for å kunne fange opp relevante opplysninger.

På denne bakgrunn foreslås en endring i straffeprosessloven § 216 b annet ledd nåværende bokstav d, som gjør at det ikke lenger skal være noen forutsetning for å kunne kreve utlevert opplysninger fra nett- eller tjenestetilbyder, at opplysningene kan knyttes til kommunikasjon. Bestemmelsen vil gi anledning til å innhente historiske lokaliseringsopplysninger, så vel som opplysninger i sanntid. Forslaget er i tråd med de utvidelser som ble gjort i dansk og svensk rett i henholdsvis 2006 og 2012.

7.7.5.4 Bruk av stille SMS

I forbindelse med og i forlengelsen av høringen av Metodekontrollutvalgets utredning, har departementet også mottatt henvendelser angående bruk av såkalt stille SMS. Stille SMS innebærer at det over mobilnettet sendes en melding som ikke er synlig på mottakerens mobilanlegg, men som likevel genererer trafikk – og dermed basestasjonsopplysninger – som kan brukes til å lokalisere det aktuelle anlegget. Stille SMS vil generere oppslag i nett- og tjenestetilbydernes systemer, som politiet kan kreve utlevert etter straffeprosessloven § 216 b annet ledd bokstav d.

Det finnes i dag tekniske løsninger for å sende «skjulte» tekstmeldinger til mistenkte. Fremgangsmåten kan sammenlignes med at politiet ringer til mistenkte fra et skjult telefonnummer og deretter legger på, utelukkende for at oppkoblingen skal generere trafikkdata som kan brukes i etterforskningen. Fremgangsmåten brukes som etterforskningsverktøy i flere andre europeiske land, blant annet Tyskland.

Fremgangsmåten er i dag ikke lovregulert. I brev fra Riksadvokaten 30. mai 2014 gis det uttrykk for at politiet «utvilsomt [har] behov for å kunne sende stille SMS i visse saker», og det anmodes om at departementet vurderer spørsmålet om lovfesting av metoden. Riksadvokaten viser til at en uttrykkelig lovforankring kan forhindre at det i enkeltsaker blir stilt spørsmål om legalitetsprinsippet eller EMK artikkel 8 er gått for nær, samt til behovet for åpenhet om hvilke metoder politiet kan benytte seg av.

I kraft av den alminnelige handlefrihet kan politiet iverksette en rekke etterforskningstiltak uten særskilt hjemmel i lov. Det å ringe eller sende en ordinær SMS til en mistenkt i en straffesak vil være et slikt tiltak. Det kan imidlertid være noe mer tvilsomt om politiet i kraft av den alminnelige handlefrihet kan sende SMS-er når dette skjer *uten at mottakeren har mulighet til å få vite om det*. Videre vil bruk av stille SMS normalt forutsette bistand fra nett- eller tjenestetilbyder, noe som neppe kan kreves uten særskilt lovhjemmel. Departementet er kjent med at minst én av eierne av mobilnettene i Norge har stengt muligheten for å sende stille SMS til sine abonnenter. Hensett til det strenge hjemmelskravet på straffeprosessens område, er det under enhver omstendighet å foretrekke at en bruk av stille SMS har klart grunnlag i lov. Departementet foreslår at slik lovhjemmel plasseres i straffeprosessloven § 216 b annet ledd ny bokstav e.

7.7.5.5 Nærmere om vilkårene

Lokalisering av mobile kommunikasjonsanlegg har likhetstrekk med både kommunikasjonskontroll etter straffeprosessloven § 216 b og teknisk sporing etter § 202 c. Det kan anføres at hjemmelen tematisk passer bedre inn i straffeprosessloven § 202 c om personnær teknisk sporing,

ettersom resultatet av metodebruken ofte vil være den samme – at man kan følge den mistenktes bevegelser over tid. Mens opplysningene som innhentes ligner dem man får ved teknisk sporing, nemlig kontinuerlig informasjon om mistenktes bevegelser, er imidlertid selve fremgangsmåten som benyttes tett knyttet til kommunikasjonsanlegget og dets egenskaper.

Lokaliseringen av mobile kommunikasjonsanlegg kan gjennomføres enten ved at politiet benytter eget teknisk utstyr (såkalte IMSI-catchere) eller ved at teletilbyder får plikt til å utlevere opplysninger til politiet. Slike fremgangsmåter ligner de eksisterende former for kommunikasjonskontroll etter bestemmelsene i henholdsvis straffeprosessloven § 216 b annet ledd bokstav c og d. Dette trekker i retning av at det er naturlig at en eventuell utvidet hjemmel for lokalisering plasseres her. En plassering i straffeprosessloven § 202 c vil dessuten medføre at lokalisering i utgangspunktet kun kan skje ved mistanke om lovbrudd med minst ti års strafferamme. Dette vil ikke dekke politiets praktiske behov.

Departementet foreslår en endring straffeprosessloven § 216 b annet ledd bokstav d, som gjør at det ikke lenger skal være noen forutsetning for å kunne kreve utlevert opplysninger fra nett- eller tjenestetilbyder at opplysningene kan knyttes til kommunikasjon. En slik bestemmelse vil gi anledning til å innhente historiske lokaliseringsopplysninger, så vel som opplysninger i sanntid. Dette er i tråd med de utvidelser som ble gjort i dansk og svensk rett i henholdsvis 2006 og 2012.

Etter forslaget skal lokalisering kunne skje på samme vilkår som andre former for kommunikasjonskontroll som ikke fanger opp innholdet i mistenktes kommunikasjon. Dette innebærer at etterforskningen må gjelde lovbrudd med en strafferamme på minst fem års fengsel, eventuelt visse særskilt oppregnede lovbrudd. I tillegg kan tillatelse bare gis dersom det må antas at tiltaket vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort, jf. § 216 c første ledd. Som ved all tvangsmiddelbruk må tiltaket være forholdsmessig, jf. § 170 a. De prosessuelle vilkår vil ellers være de samme som ved bruk av kommunikasjonskontroll. Bruken vil dessuten være underlagt kontroll fra Kontrollutvalget for kommunikasjonskontroll.

At forslagene inkorporeres i straffeprosessloven § 216 b, medfører at vilkårene blir mindre strenge enn det som gjelder for teknisk sporing etter § 202 c. Dette kan synes inkonsistent, all den tid informasjonen som innhentes i stor grad er den samme som for personnær teknisk sporing. Fremgangsmåtene skiller seg imidlertid klart fra hverandre ved at teknisk sporing krever at peileutstyr fysisk festes på mistenktes klær eller lignende, mens forslagene her gjør nytte av et kommunikasjonsanlegg som mistenkte selv bærer med seg. Dette bidrar til å gjøre metoden mindre inngripende enn personnær teknisk sporing, og begrunner etter departementets oppfatning lempeligere vilkår for bruk.

7.7.5.6 Bistandsplikt og kostnadsfordeling

Ved bruk av kommunikasjonskontroll påhviler det nett- og tjenestetilbydere en bistands- og tilretteleggingsplikt. Ifølge straffeprosessloven § 216 a fjerde ledd annet punktum kan politiet pålegge eier eller tilbyder av nett eller tjeneste «å yte den bistand som er nødvendig ved gjennomføringen av [kontrollen]». Bestemmelsen gjelder tilsvarende ved kommunikasjonskontroll etter straffeprosessloven § 216 b, jf. bestemmelsen tredje ledd. Det følger videre av ekomloven § 2-8 første ledd at tilbyder av elektronisk kommunikasjonsnett eller -tjeneste plikter å «tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres». Primært gjelder dette politiets adgang til kommunikasjonskontroll.

De nevnte bestemmelsene vil gjelde tilsvarende ved innhenting av lokaliseringsdata fra nett- eller tjenestetilbyder etter forslaget her. Det samme gjelder ved bruk av stille SMS.

Et særlig spørsmål gjelder hvorvidt de nevnte bestemmelsene gjør at nett- og tjenestetilbydere – etter pålegg fra politiet – plikter å konfigurere sine systemer slik at de mottar lokaliseringsdata hyppigere eller med høyere nøyaktighetsgrad enn de ellers ville gjort. Etter departementets oppfatning kan bestemmelsene ikke tolkes så vidt. Tilbyderne vil dermed ha plikt til å bistå politiet med å hente ut informasjon som finnes i deres systemer, men ikke til å iverksette selvstendige tiltak for å innhente mer informasjon eller andre typer informasjon. Det er imidlertid uten betydning hvor i tilbydernes systemer de aktuelle opplysningene finnes.

Det understrekes videre at forslaget her ikke i seg selv pålegger tilbyderne noen plikt til å lagre lokaliseringsdata ut over det tidsrom som er nødvendig for egne formål.

Etter ekomloven § 2-8 annet ledd skal tilbyders driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten «dekkes av staten for de merkostnader som følger av disse tjenestene». I praksis dekkes kostnadene i henhold til avtaler inngått mellom politiet og den enkelte tjenestetilbyder.

Ettersom forslaget ikke pålegger tilbyderne å konfigurere sine systemer på bestemte måter, legger departementet til grunn at merkostnadene som skal dekkes av politiet i første rekke er kostnader knyttet til utlevering av data. Øvrige driftskostnader er ikke å anse som merkostnader og ligger derfor utenfor det som skal dekkes av staten.

8 Romavlytting

8.1 Gjeldende rett

Bestemmelsen om romavlytting i straffeprosessloven § 216 m ble innført ved lov 17. juni 2005 nr. 87. Det kontroversielle spørsmålet om man skulle åpne for romavlytting var forut for dette vurdert i flere ulike sammenhenger – med ulike resultater, se nærmere Ot.prp. nr. 60 (2004–2005) punkt 7.4 til 7.6 side 83 flg. Når man til slutt fant det berettiget å åpne for metoden, var dette særlig begrunnet i endringer i kriminalitets- og trusselsituasjonen, som hadde gitt et større behov for å verne seg mot terrorhandlinger og organiserte kriminelle grupper. Samtidig ble det understreket at det er begrenset hvor langt samfunnet kan gå i å tillate romavlytting og andre inngripende metoder, uten at mange vil oppfatte prisen – i form av inngrep i den personlige sfære – som for høy, jf. Ot.prp. nr. 60 (2004–2005) side 96 flg.

Straffeprosesslovens romavlyttingsbegrep er negativt avgrenset og omfatter alle former for hemmelig avlytting ved tekniske midler som ikke er kommunikasjonsavlytting etter § 216 a. Romavlytting vil normalt foregå ved at det plasseres mikrofoner, sendere eller opptaksutstyr på et sted hvor mistenkte antas å ville oppholde seg. Den kan imidlertid også gjennomføres ved hjelp av retningsmikrofoner eller annet utstyr som kan benyttes på avstand, jf. Ot.prp. nr. 60 (2004–2005) punkt 7.2 side 81. Avlytting som skjer uten bruk av tekniske hjelpemidler – for eksempel når en polititjenestemann lytter fra et naborom eller gjennom et åpent vindu – er derimot ikke å anse som romavlytting, jf. samme dokument side 82.

Straffeprosessloven § 216 m opererer ikke med et generelt strafferammekrav, men knytter adgangen til romavlytting til visse særskilt angitte lovbrudd. Tillatelse til å benytte metoden kan etter første ledd bokstav a gis ved skjellig grunn til mistanke om terrorhandling eller trusler om å begå terrorhandling etter straffeloven §§ 131 eller 134 (straffeloven 1902 § 147 a første eller tredje ledd). Det samme gjelder etter bokstav b ved forsettlig drap, grovt ran samt særlig grov narkotikaovertredelse, dersom handlingene samtidig kan knyttes til aktivitetene til en organisert kriminell gruppe etter straffeloven §§ 232 annet ledd, 275 eller 328, jf. straffeloven § 79 bokstav c (straffeloven 1902 §§ 233, 268 annet ledd jf. 267 og 162 tredje ledd, jf. 60 a). Til sist kan tillatelse etter bokstav c gis i etterforskning av drap som er utført som ledd i motarbeiding av rettsvesenet etter straffeloven §§ 275 jf. 157 eller 275 jf. 159 (straffeloven 1902 § 233, jf. § 132 a).

Ved siden av det omtalte kriminalitetskravet, oppstiller straffeprosessloven § 216 m tredje ledd enkelte materielle tilleggsvilkår for bruk av romavlytting. Etter bestemmelsen kan tillatelse bare gis dersom det må antas at romavlytting vil være av vesentlig betydning for å oppklare saken (indikasjonskravet), og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort (subsidiaritetskravet). Kravene suppleres av det alminnelige forholdsmessighetsprinsippet i straffeprosessloven § 170 a.

Tillatelse til romavlytting kan bare gis for sted hvor det må antas at den mistenkte vil oppholde seg, jf. straffeprosessloven § 216 m fjerde ledd. Dette kan være både et privat rom og et offentlig sted. Gjelder det avlytting av offentlig sted eller annet sted som er tilgjengelig for et større antall personer, kan tillatelse likevel bare gis når det foreligger «særlige grunner». Det samme gjelder ved avlytting av sted hvor advokat, lege, prest eller andre erfaringsmessig fører samtaler av svært fortrolig art eller av redaksjonslokale eller tilsvarende sted hvor redaktør eller journalist fører samtaler av yrkesmessig art, såfremt vedkommende ikke selv er mistenkt i saken. Avlyttingen skal i alle tilfeller innrettes slik at den i minst mulig grad fanger opp samtaler hvor den mistenkte ikke er part. Sistnevnte vilkår, samt kravet om «særlige grunner» ved avlytting av offentlig sted, ble lagt til av Stortingets justiskomité for å ivareta intensjonen om i størst mulig grad å hindre at uskyldige tredjepersoner avlyttes, jf. Innst. O. nr. 113 (2004–2005) punkt 7.2 side 25–26.

Dersom det er et lukket rom som skal avlyttes, kan politiet måtte bryte seg inn for å plassere utstyr som er nødvendig for å gjennomføre avlyttingen. Det følger av § 216 m femte ledd at en tillatelse til romavlytting også gir politiet rett til å

foreta innbrudd for å plassere eller fjerne utstyr, med mindre retten har bestemt noe annet.

Tillatelse til å iverksette romavlytting gis som hovedregel av retten for inntil to uker av gangen, jf. § 216 m siste ledd. For øvrig er de personelle og prosessuelle reglene for kommunikasjonskontroll i straffeprosessloven §§ 216 d til 216 k gitt tilsvarende anvendelse for romavlytting. Dette medfører blant annet at påtalemyndigheten har hastekompetanse dersom det ved opphold er stor fare for at etterforskningen vil lide, at overskuddsinformasjon på nærmere fastsatte vilkår skal slettes, at bruken av romavlytting kontrolleres av Kontrollutvalget for kommunikasjonskontroll samt at personer som har befatning med avlyttingen er underlagt særskilt taushetsplikt. For en nærmere omtale av reglene vises til proposisjonen punkt 7.1.4.

8.2 Folkerettslige forpliktelser

Politiets bruk av romavlytting utgjør et inngrep etter EMK artikkel 8, som beskytter retten til respekt for privatliv, familieliv, hjem og korrespondanse. Beskyttelsen gjelder selvsagt i det private hjem, men vil etter EMDs praksis også kunne omfatte samtaler som finner sted i for eksempel et kontorlokale eller en fengselscelle. Etter omstendighetene vil det også kunne foreligge et inngrep dersom samtalen som avlyttes finner sted i det offentlige rom, jf. *P.G. og J.H. mot Storbritannia* 25. september 2001 (sak 44787/98) avsnitt 56–57. Sentralt i vurderingen står i så fall de involvertes rimelige forventning om privatliv i den aktuelle konteksten.

Retten til respekt for privatlivet er ikke absolutt. Etter artikkel 8 nr. 2 kan det gjøres inngrep i rettigheten såfremt dette skjer med hjemmel i lov og er nødvendig i et demokratisk samfunn av hensyn til visse nærmere angitte formål. I den konkrete vurderingen av om vilkårene er oppfylt, har EMD i stor grad inntatt samme tilnærming som i saker om kommunikasjonsavlytting, jf. blant annet *Vetter mot Frankrike* 31. mai 2005 (sak 59842/00) avsnitt 26. Det vises derfor til redegjørelsen i punkt 7.2 ovenfor.

8.3 Andre lands rett

Den *danske* hjemmelen for romavlytting finnes i retsplejeloven § 780, stk. 1, nr. 2, som gir politiet adgang til å «aflytte andre samtaler eller udtalelser ved hjælp af et apparat». Slikt inngrep kan i hendhold til § 781 bare foretas dersom det er bestemte grunner til å anta at det på den aktuelle måten gis meddelelser til eller fra en mistenkt, og inngrepet kan antas å være av avgjørende betydning for etterforskningen av visse typer lovbrudd. Dette gjelder alle lovbrudd med en strafferamme på fengsel i seks år eller mer, i tillegg til enkelte særskilt angitte lovbrudd. Herunder omfattes forsettlig overtredelse av straffeloven kapittel 12 (forbrytelser mot statens selvstendighet og sikkerhet) og kapittel 13 (forbrytelser mot statsforfatningen og de øverste statsmyndigheter, terrorisme mv.), og overtredelse av straffebud om blant annet befrielse fra fengsel og bistand til rømning, straffunndragelse, bevisforspillelse, unndragelse fra militærtjeneste, hallikvirksomhet, overgrepsbilder av barn, trusler på livet, utpressing og menneskesmugling. Det er likevel et vilkår at etterforskningen gjelder lovbrudd som har medført eller kan medføre fare for menneskers liv eller velferd eller for betydelige samfunnsverdier, jf. retsplejeloven § 781, stk. 5.

Romavlytting kan ikke benyttes dersom dette etter omstendighetene ville utgjøre et uforholdsmessig inngrep, jf. retsplejeloven § 782, stk. 1. Etter § 782, stk. 2 kan avlytting heller ikke rettes mot prester, leger, forsvarere, rettsmeglere eller advokater, i den utstrekning disse er fritatt fra å avgi forklaring som vitne. Tillatelse til romavlytting kan i alle tilfelle gis for inntil fire uker av gangen og beslutningen treffes av retten, jf. § 783.

I *Sverige* fremgikk reglene om romavlytting inntil nylig av den tidsbegrensede lag (2007:978) om hemlig rumsavlyssning. Ved lag (2014:1419) ble reguleringen gjort permanent og innlemmet i rättegångsbalken, jf. Prop. 2013/14:237 punkt 9.2 side 164 flg.

Romavlytting er nå definert i rättegångsbalken 27 kap. 20 d § 1 mom. som avlytting eller opptak som gjøres i hemmelighet med et teknisk hjelpemiddel som er ment å gjengi lyd, og som gjelder tale i enerom, samtale mellom andre eller forhandlinger i møter eller andre sammenkomster som offentligheten ikke har tilgang til. Bestemmelsen 2 mom. angir kriminalitetskravet. Det fremgår her at romavlytting kan brukes i etterforskningen av lovbrudd med en minstestraff på fengsel i fire år eller mer, spionasje, eller lovbrudd som nevnt i 3 § i lov om forretningshemmeligheter, dersom det er grunn til å tro at handlingen er begått på oppdrag for eller med støtte fra fremmed makt eller av noen som har handlet på vegne av fremmed makt og det kan antas at lovbruddet ikke bare fører til bøter. Forsøk, forberedelse og forbund er omfattet dersom slike handlinger i seg

selv er straffbare. I tillegg kan metoden brukes dersom det etter omstendighetene kan antas at lovbruddets straffverdighet vil overstige fengsel i fire år, og saken gjelder menneskehandel, voldtekt, grov seksuell tvang, voldtekt mot barn, grovt seksuelt overgrep mot barn, grov utnyttelse av barn for seksuell posering, grov hallikvirksomhet, grov utpressing, grov barnepornografi, grovt angrep på rettsvesenet, grov narkotikaforbrytelse eller grov narkotikasmugling. Forsøk, forberedelse og forbund er omfattet dersom slike handlinger i seg selv er straffbare og deres straffverdighet overstiger fengsel i fire år. I tillegg til at det må foreligge skjellig mistanke om et av de her nevnte lovbrudd, er det krav om at romavlytting er av «synnerlig vikt» for etterforskningen, jf. rättegångsbalken 27 kap. 20 e § 1 mom.

I henhold til 20 e § 2 mom. kan romavlytting bare skje på sted hvor det finnes «särskild anledning» til å anta at den mistenkte kommer til å oppholde seg. I annen bolig enn mistenktes kan romavlytting bare skje dersom det er «synnerlig anledning» til å tro at mistenkte vil oppholde seg der. Videre nevner bestemmelsen 3 mom. en rekke steder som ikke kan avlyttes, herunder lokaler som benyttes til virksomhet omfattet av taushetsplikt etter tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller som benyttes av advokater, leger og annet helsepersonell, prester mv. Avlytting kan heller ikke skje av ytringer som ville være omfattet av rättegångsbalkens vitneforbuds- eller vitnefritaksregler, jf. 22 §. Tillatelse til bruk av romavlytting gis i alle tilfeller av retten, jf. 21 §. Tillatelsen kan ikke gjelde for et tidsrom lenger enn det som er nødvendig, og kan ikke overstige én måned fra beslutningsdagen. Tillatelsen skal angi hvilket sted den gjelder. Dersom det også gis tillatelse til å foreta innbrudd etter 25 a § for å installere nødvendig utstyr, skal dette angis særskilt.

I *Finland* varierer vilkårene for såkalt teknisk avlyssning med hvilket sted som skal avlyttes. Er det tale om sted som ikke benyttes som beboelsesrom, kan avlytting iverksettes ved skjellig grunn til mistanke om lovbrudd med en øvre strafferamme på minst fire års fengsel, samt narkotikalovbrudd, forberedelse til lovbrudd som begås i terrorhensikt eller grovt tollrapporteringslovbrudd, jf. tvångsmedelslagen 10 kap. 16 § 2 mom. Det samme gjelder for avlytting av fengselsceller og lignende.

Adgang til avlytting av beboelsesrom er ikke knyttet til noe generelt strafferammekrav, men begrenset til å gjelde ved visse særskilt oppregnede alvorlige lovbrudd, jf. tvångsmedelslagen 10 kap. 17 §. De aktuelle lovbrudd omfatter blant annet folkemord, spionasje, forræderi, grov seksuell utnyttelse av barn, drap, grov menneskehandel, grovt ran, grov sabotasje, terrorisme og grov narkotikakriminalitet.

Teknisk avlytting kan bare gjelde sted hvor den mistenkte sannsynligvis befinner seg. Gjelder det avlytting av bolig eller avlytting som rettes mot en frihetsberøvet, treffes beslutning av retten, jf. 10 kap. 18 § 1 mom. Annen avlytting kan ifølge 2 mom. besluttes av arrestasjonsbemyndiget tjenestemann. Beslutningen kan i alle tilfelle treffes for maksimalt en måned av gangen, jf. 3 mom.

8.4 Kriminalitetskravet – koblingen til bestemmelsen om organisert kriminalitet

8.4.1 Metodekontrollutvalgets forslag

Adgangen til å bruke romavlytting i norsk rett ble innført ved lov 17. juni 2005 nr. 87. Metodekontrollutvalget mener generelt at lovendringene har vært praktisert for lite og i for kort tid til at det er mulig å underlegge dem en reell og helhetlig evaluering, jf. utredningen punkt 17.4.1 side 203. På grunn av dette, samt det forhold at utvalget ikke har fått innsyn i saksdokumenter underlagt taushetsplikt, anbefaler utvalget en evaluering av romavlyttingsreglene på et senere tidspunkt.

Utvalget peker likevel på at aktører fra politiet og påtalemyndigheten mener anvendelsesområdet for romavlytting er for snevert (punkt 17.4.3 side 204). Dette skyldes særlig at anvendelsen av straffeprosessloven § 216 m første ledd bokstav b er koblet til straffeloven 1902 § 60 a om organisert kriminalitet (straffeloven § 79 bokstav c). Utvalget uttrykker forståelse for at koblingen til § 60 a er utfordrende for politiet og påtalemyndigheten, men finner ikke å kunne foreslå utvidelser i metodens anvendelsesområde. Begrunnelsen er det manglende evalueringsgrunnlaget, samt at utvalget ikke har sett det som sin oppgave å overprøve de rettspolitiske vurderinger som ble gjort i forbindelse med lovendringene i 2005.

8.4.2 Høringsinstansenes syn

De høringsinstansene som har uttalt seg om spørsmålet, har ulike oppfatninger om koblingen mellom kriminalitetskravet ved romavlytting og straffeloven 1902 § 60 a (straffeloven § 79 bokstav c). *Riksadvokaten* påpeker at straffebudene som er oppregnet i § 216 m gjelder meget alvorlige straff-

bare handlinger, uavhengig av om kriminaliteten kan betegnes som organisert. Det anføres særlig at det gir liten mening at tilgangen til en etterforskningsmetode for å oppklare drap skal være avhengig av tilknytning til organisert kriminalitet. Embetet mener offerperspektivet her synes å ha kommet i bakgrunnen.

Også *Oslo statsadvokatembeter* og *Oslo politidistrikt* mener at straffebudene som er oppregnet i straffeprosessloven § 216 m er så vidt graverende at de i seg selv kan begrunne romavlytting, uavhengig av tilknytning til organisert kriminalitet. *Oslo politidistrikt* uttaler:

> «De oppregnede straffebud er i seg selv såpass grove forbrytelser at det synes unødvendig med et krav om at det i tillegg også må være mistanke om overtredelse av 60a. Eksempelvis bør forsettlig drap alene være tilstrekkelig for å kunne benytte romavlytting. Det samme gjelder for grovt ran og særlig grove narkotikaforbrytelser. For drap kan det etter politiets syn ikke aksepteres at slike forbrytelser forblir uoppklart som følge av manglende metodetilgang.»

Både *Oslo statsadvokatembeter* og *Oslo politidistrikt* peker samtidig på praktiske problemer ved at adgangen til tvangsmiddelbruk er knyttet til straffeloven 1902 § 60 a. Høringsinstansene mener at bestemmelsen er upresis og fremholder at det ofte kan være vanskelig å fastslå om vilkårene er oppfylt i en innledende fase av etterforskningen.

Også *Politidirektoratet* viser til at koblingen til straffeloven 1902 § 60 a kan være en praktisk vanskelig terskel for anvendelse av romavlytting og mener det bør vurderes å gjøre endringer som kan avbøte dette. På grunn av den relativt begrensede erfaringen med metoden, vil høringsinstansen imidlertid per i dag ikke tilrå endringer i dens anvendelsesområde.

Advokatforeningen viser på sin side til det prinsipielt betenkelige ved å tillate inngripende tvangsmidler og advarer mot en situasjon hvor spørsmålet som reises ikke handler om tvangsmidlets inngripende effekt, men snarere om hvorvidt det er tid for nye utvidelser. Foreningen slutter seg derfor til utvalgets konklusjon om ikke å foreslå utvidelser i anvendelsesområdet for romavlytting. *Forsvarergruppen av 1977* understreker at de strenge vilkårene i straffeprosessloven § 216 m er utformet slik for at bruken av romavlytting skal være restriktiv og er enig i at metodens anvendelsesområde ikke bør endres.

8.4.3 Departementets vurdering

Departementet vil innledningsvis understreke at romavlytting representerer ett 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 overvåking. Metoden kan etter departementets oppfatning derfor bare forsvares på områder hvor det er svært viktig med effektiv etterforskning og bare hvor det er grunn til å tro at avlytting vil kunne gi opplysninger av sentral betydning for etterforskningen. Det er følgelig grunn til å utvise stor tilbakeholdenhet med – og kreve gode begrunnelser for – en eventuell utvidelse av anvendelsesområdet for romavlytting.

Etter straffeprosessloven § 216 m første ledd bokstav b kan romavlytting i dag benyttes i etterforskningen av saker som gjelder forsettlig drap, grovt ran og særlig grov narkotikaovertredelse. En forutsetning for å kunne benytte metoden er likevel at lovbruddet samtidig kan knyttes til straffeloven § 79 bokstav c om organisert kriminalitet (straffeloven 1902 § 60 a). Bestemmelsen kommer til anvendelse dersom den straffbare handlingen er utøvet «som ledd i aktivitetene til en organisert kriminell gruppe». Med organisert kriminell gruppe menes et samarbeid mellom tre eller flere personer som har som et hovedformål å begå en handling som kan straffes med fengsel i minst tre år, eller som går ut på at en ikke ubetydelig del av aktivitetene består i å begå slike handlinger, jf. § 79 bokstav c annet ledd (§ 60 a annet ledd).

Bakgrunnen for at man begrenset adgangen til romavlytting til å gjelde ved organisert kriminalitet, var de særlige etterforskningsmessige utfordringer slik kriminalitet medfører. Fra Ot.prp. nr. 60 (2004–2005) punkt 7.7.2 side 100–101 hitsettes:

> «Stadig flere drap begås under forhold og i miljøer som gjør det vanskelig å nå frem med tradisjonelle etterforskingsmetoder […]. Her er det et klart og dokumentert behov for å åpne for romavlytting, som etter departementets syn veier tyngre enn de hensynene som taler mot slik avlytting. Dette stiller seg annerledes i forhold til drap som begås utenfor de organiserte kriminelle miljøene. Slike drap begås ofte i affekt, og vanskelighetene med å nå frem med tradisjonelle etterforskingsmetoder er ikke så store som hvor etterforskingen retter seg mot en organisert kriminell gruppe. Behovet for å romavlytte er derfor gjennomgående ikke like

stort, og risikoen for at avlyttingen vil ramme uskyldige eller utenforstående, er ofte langt større.»

På bakgrunn av innspill i høringsrunden har departementet nå funnet grunn til å vurdere på nytt hvorvidt kravet om tilknytning til organisert kriminalitet er berettiget.

Tilbakemeldinger fra instanser på politi- og påtalesiden indikerer at det kan være vanskelig på et tidlig stadium i etterforskningen å påvise sannsynlighetsovervekt for at den straffbare handlingen er begått som ledd i organisert kriminalitet. Dette gjør at koblingen til straffeloven § 79 bokstav c (straffeloven 1902 § 60 a) fremstår som et avgrensningskriterium som kan være utfordrende å bruke. Departementet har forståelse for disse innvendingene og for betydningen av at vilkårene for skjult tvangsmiddelbruk er utformet på en måte som gjør metodene praktisk anvendelige.

Departementet vil imidlertid fremheve at det ved lov 21. juni 2013 nr. 85 ble gjort endringer i straffeloven 1902 § 60 a, som kan ha betydning for anvendelsen av bestemmelsen også som grunnlag for tvangsmiddelbruk. Anvendelsesområdet for § 60 a ble med dette utvidet, blant annet gjennom en mer vidtrekkende definisjon av hva som skal anses som en organisert kriminell gruppe. Definisjonen favner nå grupper med en flatere og løsere struktur enn tidligere. Videre er det gjort endringer for å hindre at bestemmelsen avgrenses til samarbeid hvor deltakerne er profesjonelle kriminelle, og det er ikke lenger nødvendig at samarbeidet utelukkende eller i det vesentligste består av å begå alvorlig kriminalitet. Tilsvarende endringer er gjort i straffeloven § 79 bokstav c. Det vises til Prop. 131 L (2012–2013) punkt 11 side 68 flg. Etter departementets oppfatning vil endringene trolig gjøre det lettere å sannsynliggjøre overtredelse av bestemmelsen om organisert kriminalitet på et tidligere stadium i etterforskningen, og dermed kunne avhjelpe enkelte av de praktiske problemene høringsinstansene har pekt på.

Samtidig har departementet forståelse for de høringsinstansene som fremhever at alvorlighetsgraden ved lovbruddene som er oppregnet i straffeprosessloven § 216 m første ledd bokstav b er svært høy – uavhengig av om de kan knyttes til organisert kriminalitet. Lovbruddene som nevnes – forsettlig drap, grovt ran og særlig alvorlig narkotikaforbrytelse – er i seg selv handlinger med et betydelig skadepotensial. Dette gjelder i særdeleshet for drap, der hensynet til ofrene og de etterlatte tilsier at politiet gjør alle mulige bestrebelser for å oppklare saken. Dette legges blant annet til grunn i Riksadvokatens årlige rundskriv om mål og prioriteringer i straffesaksbehandlingen, hvor det fremgår at drap er en av de aller høyest prioriterte forbrytelsestypene. Dette taler for at politiet også gis tilstrekkelige virkemidler i etterforskningen av drapssaker.

Kriminalitetskravet for bruk av romavlytting etter straffeprosessloven § 216 m er i dag det samme som for bruk av tvangsmidler i avvergende øyemed etter straffeprosessloven § 222 d første ledd. Som det fremgår av proposisjonen punkt 13.4.3.4 foreslår departementet å fjerne kravet om tilknytning til organisert kriminalitet ved bruk av tvangsmidler – herunder også romavlytting – for å avverge drap. Bakgrunnen for dette er særlig hensynet til offeret. Selv om departementet ser at offerperspektivet kommer i en noe annen stilling når man kan *avverge* et drap enn når det er tale om å *etterforske* et allerede begått drap, mener man at en del av de samme hensyn gjør seg gjeldende også her. Således kan det anføres at forsettlig drap er en så alvorlig og uopprettelig krenkelse av menneskelivet, at det vil stride mot den allmenne rettsoppfatning dersom manglende metodetilgang skal være det som står i veien for oppklaring. Dette stiller seg annerledes for grovt ran og særlig grove narkotikaforbrytelser, hvor interessene som krenkes er av en annen karakter.

Departementet er enig med høringsinstansene som påpeker at hensynet til offeret vil være det samme uavhengig av hvorvidt et drap kan knyttes til aktivitetene til en organisert kriminell gruppe. På denne bakgrunn har departementet kommet til at forsettlig drap i seg selv bør kunne danne grunnlag for bruk av romavlytting. Det foreslås derfor at vilkåret om tilknytning til organisert kriminalitet fjernes for metoden ved drap. Ved grovt ran og særlig grov narkotikaovertredelse mener departementet derimot at kravet bør opprettholdes.

8.5 Kontroll og notoritet

Som det fremgår av punkt 8.1 ovenfor, er prosessuelle regler som gjelder for kommunikasjonskontroll i stor grad gitt anvendelse også ved bruk av romavlytting. Dette fremgår ved at straffeprosessloven §§ 216 d til 216 k «gjelder tilsvarende» for romavlytting, jf. § 216 m siste ledd. Dette innebærer blant annet at politiets metodebruk er gjenstand for kontroll fra Kontrollutvalget for kommunikasjonskontroll, jf. straffeprosessloven § 216 h. Det er videre lagt til grunn at reglene i kommuni-

kasjonskontrollforskriften kommer til anvendelse, slik at forskriftens kontrollregime også gjelder ved romavlytting. Dette innebærer at det blant annet stilles krav til protokollføring og innrapportering til Riksadvokaten. I tillegg til reglene i forskriften har Riksadvokaten 5. juni 2009 (RA–2009–44) gitt egne retningslinjer om romavlytting. Retningslinjene inneholder veiledning for dokumentasjon og loggføring, om hvordan innhentet materiale skal håndteres, om når avlytting skal kobles på og fra, samt om ansvar for at retningslinjene iakttas.

Metodekontrollutvalget viser i utredningen punkt 17.4.5 side 204–205 til Riksadvokatens retningslinjer og er positiv til disse. Det mener samtidig at retningslinjene bør fastsettes som forskrift, slik som for kommunikasjonskontroll. Utvalget har imidlertid ikke sett det som sin oppgave å komme med forslag til en slik forskrift.

Under høringsrunden er det kun *Riksadvokaten* som har uttalt seg om hvorvidt retningslinjer for bruk av romavlytting bør fastsettes som forskrift. Embetet har forståelse for utvalgets synspunkt om at regler om bruk av romavlytting bør gis i forskrifts form, fordi dette i større grad vil sikre notoritet rundt regelverket og gi større rettskildemessig tyngde og forankring. Riksadvokaten mener likevel det kan være hensiktsmessig å vinne noe erfaring med gjeldende retningslinjer før en tar opp dette arbeidet.

Departementet støtter Riksadvokaten i at det er hensiktsmessig at erfaring med praktiseringen av gjeldende retningslinjer bør danne grunnlag for et eventuelt forskriftsarbeid. Departementet vil løpende vurdere behovet for å forskriftsfeste egne regler om romavlytting og vil se dette i sammenheng med kommunikasjonskontrollforskriften. En finner imidlertid ikke at det i nærværende proposisjon bør fremmes forslag om slike regler.

8.6 Tilretteleggingsplikt og samarbeid med nettleverandørene

Ved bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a er netteiere og tjenestetilbydere gitt en plikt til å samarbeide med politiet. Dette følger av § 216 a fjerde ledd annet punktum, hvoretter «[p]olitiet kan pålegge eier eller tilbyder av nett eller tjeneste å yte den bistand som er nødvendig ved gjennomføringen av avlyttingen». Noen tilsvarende plikt til bistand følger ikke av straffeprosessloven § 216 m om romavlytting.

Metodekontrollutvalget bemerker i utredningen punkt 17.4.6 side 205 at romavlytting kan foregå på flere måter, blant annet ved å overføre lyd via fastlinjenettet eller via mobilnettet. Dette forutsetter et nært og godt samarbeid med nettleverandørene. Ifølge utvalget er det på denne bakgrunn reist spørsmål om tjenesteleverandørene bør lovpålegges en plikt til å samarbeide med politiet når romavlytting skjer via teletjenester. Utvalget finner imidlertid ikke å ha grunnlag for å vurdere behovet for formalisering av en slik tilretteleggingsplikt.

Oslo politidistrikt fremholder i sin høringsuttalelse at den teknologiske utviklingen gjør at det i visse tilfelle er viktig med en tilretteleggingsplikt for nettleverandørene. Høringsinstansen viser til straffeprosessloven § 216 a fjerde ledd annet punktum og gir uttrykk for at en tilsvarende bestemmelse bør være naturlig også for romavlytting. Ingen av de øvrige høringsinstansene har kommentert spørsmålet.

Etter departementets syn gir Metodekontrollutvalgets utredning og den etterfølgende høringen ikke grunnlag for å konstatere et behov for å formalisere en tilretteleggingsplikt for nettleverandørene. I motsetning til ved kommunikasjonskontroll er politiet normalt ikke avhengig av en utenforstående tjenestetilbyder, men kan etablere romavlytting ved hjelp av eget utstyr. Departementet vil følgelig på det nåværende tidspunkt ikke fremme lovforslag om en tilsvarende tilretteleggingsplikt som etter straffeprosessloven § 216 a fjerde ledd annet punktum. En ser imidlertid ikke bort fra at den teknologiske utviklingen i fremtiden vil føre til at romavlytting gjennomføres på andre måter enn i dag, slik at eksterne aktørers medvirkning i større grad blir påkrevet. Det kan i så fall oppstå behov for en fornyet vurdering av spørsmålet på et senere tidspunkt.

8.7 Ambulerende romavlytting

Det følger av straffeprosessloven § 216 m fjerde ledd at tillatelse til romavlytting kan gis for «sted hvor det må antas at den mistenkte vil oppholde seg». Tillatelsen knyttes følgelig til et mer eller mindre presist angitt «sted» og ikke til personen som skal avlyttes (mistenkte). *Metodekontrollutvalget* viser i utredningen punkt 17.4.7 til et møte med PST, hvor organet fremmet forslag om å innføre såkalt ambulerende romavlytting. Dette innebærer at en mikrofon blir plassert på mistenkte, typisk på klærne eller gjenstander vedkommende har på seg eller med seg. Selv om ambulerende

avlytting vil kunne gi et noe bedre vern av tredjepersoner, vil utvalget ikke tilrå en slik adgang. Årsaken er at det personvernmessige inngrepet overfor mistenkte blir for stort. Utvalget kan heller ikke se at ambulerende romavlytting vil være gjennomførbart i praksis, ettersom mistenkte gjerne vil skifte klær eller legge igjen gjenstander.

Det er få høringsinstanser som har uttalt seg om spørsmålet om ambulerende romavlytting. *Advokatforeningen* er enig med utvalget i at forslaget fra PST ikke kan anbefales og begrunner dette i at det personvernmessige inngrepet er for stort. Også *Oslo statsadvokatembeter* slutter seg til utvalgets synspunkter.

Departementet vil understreke at enhver form for romavlytting utgjør et meget inngripende tiltak overfor den eller de som avlyttes. Graden av personnærhet og inngripen øker betraktelig dersom det blir tale om å feste avlyttingsutstyret på mistenkes person, klær eller gjenstander vedkommende bærer med seg. Departementet ser at såkalt ambulerende avlytting vil kunne bidra til at tredjepersoners personvern i noe mindre grad blir krenket. Metoden er imidlertid av en så inngripende karakter overfor den som avlyttes, at den krever en fyllestgjørende begrunnelse. Departementet kan ikke se at høringen gir tilstrekkelig grunnlag for å overprøve Metodekontrollutvalgets vurderinger på dette punkt. En vil derfor på det nåværende tidspunkt ikke fremme forslag om å åpne for ambulerende romavlytting.

9 Teknisk sporing

Straffeprosessloven §§ 202 b og 202 c hjemler bruk av teknisk sporing, som er plassering av teknisk peileutstyr på et objekt for å lokalisere hvor objektet befinner seg. Med teknisk peileutstyr menes elektroniske signalsendere som kan festes til et objekt for å følge dets bevegelser. Sendere som kan overføre lyd eller bilde, omfattes ikke.

Straffeprosessloven § 202 b regulerer plassering av sendere på kjøretøy, gods eller andre gjenstander. Slik metodebruk kan iverksettes dersom noen med skjellig grunn mistenkes for handling eller forsøk på handling som kan medføre fengsel i fem år eller mer, eller som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum eller 198 (straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90 om forbrytelser mot rikets sikkerhet eller § 162 c om forbund om alvorlige straffbare handlinger som ledd i organisert kriminalitet). Det er påtalemyndigheten som har kompetanse til å beslutte teknisk sporing etter § 202 b.

Straffeprosessloven § 202 c regulerer såkalt personnær teknisk sporing, som er av mer inngripende art enn sporing etter § 202 b. Politiet kan etter § 202 c plassere peileutstyr i klær eller gjenstander som den mistenkte bærer på seg, eller i veske eller annen håndbagasje som den mistenkte bærer med seg. Det er likevel ikke adgang til å plassere sendere på den mistenktes kropp. Grunnvilkåret for personnær teknisk sporing etter § 202 c er at noen med skjellig grunn mistenkes for en handling eller forsøk på handling som kan medføre fengsel i ti år eller mer, eller som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129 eller 136 a (straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90, 104 a første ledd annet punktum, 104 a annet ledd jf. første ledd annet punktum eller 147 d), eller eksportkontrolloven § 5. I tillegg stilles det krav om at teknisk sporing må antas å være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort, jf. § 202 c annet ledd første punktum. Det er retten som har kompetanse til å beslutte teknisk sporing etter § 202 c, likevel slik at påtalemyndigheten er gitt hastekompetanse når det er fare ved opphold.

Bruken av teknisk sporing etter straffeprosessloven §§ 202 b og 202 c må ikke være uforholdsmessig etter den generelle bestemmelsen i § 170 a.

Metodekontrollutvalget foreslår å utvide adgangen til teknisk sporing til å gjelde saker om grov ulovlig våpenomsetning, jf. bestemmelser som frem til 1. oktober 2015 stod i våpenloven § 33 annet ledd. Utvalget påpeker at slik metodebruk ikke er tillatt, ettersom strafferammen ikke tilfredsstiller kravet i straffeprosessloven §§ 202 b og 202 c om henholdsvis fem og ti års strafferamme. Ved ikraftsetting av ny straffelov ville dette endres. Grov ulovlig våpenomsetning ville da rammes av straffeloven § 191, som har en øvre strafferamme på seks års fengsel. Kunne lovbruddet knyttes til aktivitetene til en organisert kriminell gruppe, ville strafferammen heves til inntil 12 års fengsel, jf. straffeloven § 79 bokstav c. I vurderingen av strafferammen tok departementet «noe hensyn til» behovet for å anvende ekstraordinære etterforskningsmetoder, jf. Ot.prp. nr. 8 (2007–2008) Om lov om endringer i straffeloven 20. mai 2005 nr. 28 mv. punkt 10.10.3 side 255 flg.

Utvalget foreslår å åpne for teknisk sporing etter straffeprosessloven § 202 b ved mistanke om overtredelse av våpenloven § 33 annet ledd. Personnær teknisk sporing etter § 202 c foreslås tillatt dersom handlingen også kan knyttes til aktivitetene til en organisert kriminell gruppe, jf. straffeloven 1902 § 60 a (straffeloven § 79 bokstav c). Forslaget innebar en forskuttering av den metodetilgang som politiet uansett ville få ved ikraftsettingen av straffeloven. Et flertall av *høringsinstansene* har uttrykt støtte til utvalgets forslag.

I høringen har *Oslo politidistrikt* tatt til orde for en ytterligere utvidelse av adgangen til teknisk sporing, ved å innta en henvisning til straffeloven 1902 § 269 nr. 1 om ransforbund (straffeloven § 329) i straffeprosessloven §§ 202 b og 202 c. *Riksadvokaten* og *Oslo politidistrikt* foreslår dessuten at straffeloven 1902 § 223 første ledd om frihetsberøvelse (straffeloven § 254) legges til oppregningen i straffeprosessloven § 202 c – på samme måte som i § 216 a om kommunikasjons-

avlytting, jf. punkt 7.4.6.2 ovenfor. Etter høringsinstansens syn bør politiet i slike saker kunne bruke skjulte metoder for å bringe på det rene hvor den bortførte og gjerningsmannen befinner seg – for at vedkommende skal kunne befris så raskt som mulig og for å sikre bevis.

Ettersom straffeloven trådte i kraft 1. oktober 2015, finner departementet at det ikke er behov for å gjøre endringer i metodetilgangen i saker om ulovlig grov våpenomsetning slik utvalget foreslår. Derimot foreslår departementet å åpne for personnær teknisk sporing etter straffeprosessloven § 202 c i saker om frihetsberøvelse, se begrunnelsen i punkt 7.4.6.3, og i saker om oppfordring, rekruttering og opplæring til terror, jf. punkt 7.4.11.4 ovenfor. Hva gjelder forslaget fra Oslo politidistrikt om å utvide sporingsadgangen til å omfatte mistanke om ransforbund, bemerkes at det allerede i dag vil være adgang til å benytte en rekke ulike etterforskningsmetoder – herunder også teknisk sporing – for å etterforske fullbyrdede ranshandlinger. Departementet kan ikke se at det gjennom høringen er godtgjort et konkret behov for ytterligere metodetilgang også ved forbund om ran. Det vises for så vidt til drøftelsen i punkt 7.4.9.4 ovenfor.

10 Utleveringspålegg, ransaking, beslag, postbeslag og postkontroll

10.1 Innledning

Ved lov 3. desember 1999 nr. 82 ble det blant annet innført regler om utsatt underretning ved ransaking, beslag og utleveringspålegg. Det ble videre innført regler om utleveringspålegg fremover i tid. I tillegg ble det innført regler om hastekompetanse. Hastekompetanse er behandlet under punkt 6.4, og utsatt underretning under punkt 6.10, herunder drøftelser av Metodekontrollutvalgets forslag til endringer.

10.2 Utleveringspålegg

Etter gjeldende rett kan besitteren av en ting som antas å ha betydning som bevis, pålegges å utlevere denne, jf. straffeprosessloven § 210 første ledd. Utleveringspålegg kan utferdiges i alle sakstyper, men kan ikke rettes mot personer som er fritatt for vitneplikt eller mot mistenkte selv.

Utleveringspålegg skal besluttes av retten. Politiet har imidlertid hastekompetanse etter § 210 annet ledd. Politiets beslutning skal snarest mulig forelegges for retten for godkjennelse.

Mistenkte skal underrettes om at det er fattet beslutning om utleveringspålegg, jf. straffeprosessloven § 53 første ledd, jf. § 52 annet ledd. Dersom det er strengt nødvendig for etterforskningen i saken at underretning ikke gis, kan retten på nærmere vilkår treffe kjennelse om utsatt underretning, jf. § 210 a, se punkt 6.10.1.

Metodekontrollutvalget foreslår ingen innholdsmessige endringer i reglene om utleveringspålegg. Utvalget foreslår imidlertid å rette opp i en inkurie i straffeprosessloven § 210, jf. utredningen punkt 19.2.1 side 210:

> «Det følger av annet ledd første punktum at ordre fra påtalemyndigheten kan tre i stedet for «kjennelse» av retten. Det stilles ikke opp noe formkrav til rettens avgjørelse i første ledd, og før lovendringen var det vanlig å treffe avgjørelsen som formløs beslutning. Formkravet ble ikke berørt nærmere i motivene til lovendringen, og beror formodentlig på en inkurie.»

Utvalget foreslår at bestemmelsen endres slik at det klart fremgår at rettens avgjørelse kan treffes som formløs beslutning.

Metodekontrollutvalget gir uttrykk for at et utleveringspålegg «[ikke] gir politiet rett til å beholde den utleverte tingen. I så fall må det treffes beslutning om beslag, jf. straffeprosessloven §§ 203 eller 211.». Det vises til utredningen punkt 19.2.1 side 211.

Oslo politidistrikt, *Riksadvokaten* og *Økokrim* er uenige i dette synspunktet. *Riksadvokaten* uttaler:

> «Når politiet etter utleveringspålegg fra retten har fått overlevert den aktuelle tingen, er det etter riksadvokatens syn unødvendig i tillegg å måtte treffe beslutning om beslag.»

Departementet mener det ikke er nødvendig med beslutning om beslag når politiet etter utleveringspålegg har fått overlevert tingen. Beslag og utleveringspålegg er to alternative metoder. Utleveringspålegg er et supplement til beslag i situasjoner der politiet ikke er i posisjon til å ta tingen. Vurderingstemaene for utleveringspålegg og beslag er sammenfallende, nemlig at det må dreie seg om ting som «antas å ha betydning som bevis». Når retten først har foretatt denne vurderingen for utleveringspålegg av en ting, vil det ikke være påkrevd at politiet gjør vurderingen på ny for beslag av tingen.

Departementet viser til NOU 2004: 6 punkt 7.11.1 side 114, der Politimetodeutvalget uttaler:

> «I Rt. 1997 side 470 omhandles sak hvor NetCom AS i medhold av straffeprosessloven § 210, jf § 205 og § 118 annet ledd ble pålagt å utlevere trafikkdata. Her anvendes beslag i tillegg til utleveringspålegg. Men det er unødvendig når politiet vil få besittelsen i kraft av utleveringspålegget.»

Departementet viser videre til Johs Andenæs, Norsk straffeprosess samlet utgave ved Tor-Geir Myhrer (4. utgave, Oslo 2009) side 324, der det samme fremgår forutsetningsvis:

> «I stedet for å treffe beslutning om beslag av en ting kan påtalemyndigheten i visse tilfeller etter § 210 be retten om å gi besitteren pålegg om utlevering (…).»

Departementet legger etter dette til grunn at når politiet har fått rettens beslutning om utleveringspålegg, må det være tilstrekkelig til å beholde tingen.

Departementet foreslår at den språklige inkurien i straffeprosessloven § 210 annet ledd første punktum rettes. Paragraf 210 første ledd stiller ikke opp noe formkrav til rettens avgjørelse om utleveringspålegg, og det har vært vanlig å treffe avgjørelsen som formløs beslutning, se Bjerke/Keiserud/Sæther, Straffeprosessloven kommentarutgave Bind I (4. utgave, Oslo 2011) side 726 og Rt. 2000 side 1236. Av § 210 annet ledd første punktum følger imidlertid forutsetningsvis at rettens avgjørelse skal treffes ved kjennelse. Ordet kjennelse kom inn i lovteksten ved lov 3. desember 1999 nr. 82 uten at formkravet ble berørt i forarbeidene. Det legges til grunn at ordet kjennelse ble brukt ved en språklig inkurie, og at beslutnings form er tilstrekkelig.

10.3 Utleveringspålegg fremover i tid

Etter straffeprosessloven § 210 b første ledd kan retten ved kjennelse pålegge den som i fremtiden vil få besittelse av en ting som antas å ha betydning som bevis, å utlevere tingen til politiet straks den mottas. Vilkårene er strengere enn etter alminnelig utleveringspålegg. For utleveringspålegg fremover i tid gjelder et skjerpet kriminalitetskrav, idet slikt pålegg bare kan gis når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i fem år eller mer eller for overtredelse av straffeloven §§ 121, 123, 125, 126 eller 127 jf. 123 i kapittel 17 om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser (straffeloven 1902 kapittel 8 om forbrytelser mot statens selvstendighet og sikkerhet).

Utleveringspålegg fremover i tid kan bare gis for et bestemt tidsrom som ikke må være lenger enn strengt nødvendig, og ikke mer enn fire uker av gangen, jf. § 210 b annet ledd. Påtalemyndigheten er ikke gitt hastekompetanse. Retten kan ved kjennelse beslutte utsatt underretning til den mistenkte dersom det er strengt nødvendig for etterforskningen, jf. straffeprosessloven § 210 c første ledd.

Både *Metodekontrollutvalget* og *PST* foreslår å åpne for bruk av utleveringspålegg fremover i tid som ledd i PSTs forebyggende virksomhet. Dette er behandlet i punkt 13.5.5.4 om tvangsmiddelbruk i forebyggende øyemed. For øvrig foreslås ingen endringer i reglene om utleveringspålegg fremover i tid og ingen høringsinstanser ber om endringer. Reglene nevnes her for helhetens skyld og fordi de er av betydning ved øvrige vurderinger.

10.4 Ransaking

Ransaking av bolig, rom eller oppbevaringssted kan foretas ved skjellig grunn til mistanke om en handling som kan medføre frihetsstraff, jf. straffeprosessloven § 192 første ledd. Formålet må være å iverksette pågripelse, søke etter bevis eller søke etter ting som kan beslaglegges eller som det kan tas heftelse i. Ransaking kan også på visse vilkår foretas hos andre enn mistenkte, jf. § 192 tredje ledd. Straffeprosessloven §§ 193 og 194 hjemler razzia av hus eller rom. Ransaking av person er hjemlet i § 195. Det er retten som kan beslutte ransaking, jf. § 197 første ledd, men i noen situasjoner kan påtalemyndigheten eller politiet beslutte ransaking, jf. § 197 annet ledd og § 198. Hvis det foreligger skriftlig samtykke til ransakingen, kan ransakingen skje uten beslutning fra retten. Etter straffeprosessloven § 200 a første ledd kan retten ved kjennelse beslutte at ransaking kan settes i verk uten underretning til mistenkte eller andre, se punkt 6.10.1.

Metodekontrollutvalget foreslår ingen endringer i reglene om ransaking. Utvalget gir imidlertid uttrykk for at «[p]olitiet [bare] kan beholde ting de finner under en ransaking dersom det fattes beslutning om beslag etter straffeprosessloven §§ 203 eller 211», jf. utredningen punkt 19.2.3 side 212.

Riksadvokaten er ikke fullt ut enig i dette og mener at det bare kreves beslutning om beslag dersom besitteren ikke utleverer gjenstanden frivillig.

Riksadvokaten og *Oslo politidistrikt* foreslår dessuten at straffeloven 1902 § 223 første ledd om frihetsberøvelse (straffeloven § 254) skal gi grunnlag for bruk av kommunikasjonsavlytting etter straffeprosessloven § 216 a, jf. punkt 7.4.6. Det samme foreslås for enkelte andre skjulte

tvangsmidler, herunder hemmelig ransaking etter straffeprosessloven § 200 a, dersom det åpnes for dette. Bakgrunnen er at situasjoner som involverer frihetsberøvelse kan være høyst alvorlige og dramatiske, for eksempel fordi det er grunn til å frykte for den bortførtes liv. Etter høringsinstansenes syn bør politiet i slike situasjoner kunne bruke skjulte metoder for å bringe på det rene hvor den bortførte og gjerningsmannen befinner seg. Dette for at vedkommende skal kunne befris så raskt som mulig og for å sikre bevis.

D e p a r t e m e n t e t slutter seg til Riksadvokatens innvending og mener at straffeprosessloven § 205 må leses slik at det ikke kreves beslutning om beslag der besitteren utleverer ting frivillig. Da kan beslaget skje formløst som ledd i etterforskningen, jf. Johs Andenæs, Norsk straffeprosess samlet utgave ved Tor-Geir Myhrer (4. utgave, Oslo 2009) side 319. Dette vil også gjelde for ransaking, slik at det ikke kreves beslutning om beslag når besitteren utleverer ting frivillig etter ransaking. Politiet må imidlertid lage en opptegnelse over hva som er beslaglagt, jf. § 207 første ledd.

Departementet foreslår dessuten å åpne for hemmelig ransaking etter straffeprosessloven § 200 a ved etterforskning av offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, frihetsberøvelse, menneskehandel, grov menneskesmugling og overgrepsbilder av barn – forutsatt at øvrige vilkår for slik metodebruk er oppfylt. Behovet for tvangsmidler kan begrunnes på samme måte som for kommunikasjonskontroll, jf. punktene 7.4.3.4, 7.4.4.4, 7.4.6.3, 7.4.8.3 og 7.4.11.4 ovenfor. Hemmelig ransaking vil kunne være hensiktsmessig der politiet for eksempel ønsker å ransake en pc eller et datasystem for å avdekke overgrepsbilder uten at den mistenkte blir underrettet om dette. Det samme gjelder ved etterforskning av grov menneskesmugling og menneskehandel, der det for eksempel kan være behov for å ransake lokaler som antas å bli brukt til oppbevaring av ofre for slike lovbrudd, uten at bakmennene blir varslet om dette.

10.5 Beslag

Ting som antas å ha betydning som bevis, kan beslaglegges inntil rettskraftig dom foreligger i saken, jf. straffeprosessloven § 203 første ledd. Det kreves ikke en bestemt mistenkt. Det er lagt til grunn at det må foreligge skjellig grunn til mistanke om en straffbar handling, selv om lovens ordlyd ikke inneholder noe slikt krav, jf. Rt. 2000 side 577 og Johs Andenæs, Norsk straffeprosess samlet utgave ved Tor-Geir Myhrer (4. utgave, Oslo 2009) side 316.

Utgangspunktet er at beslag besluttes av påtalemyndigheten, jf. straffeprosessloven § 205 første ledd. Dersom påtalemyndigheten finner at det foreligger særlige grunner, kan spørsmålet bringes inn for retten, jf. § 205 annet ledd. Enhver som rammes av beslaget kan dessuten kreve spørsmålet om opprettholdelse brakt inn for retten, jf. § 208 første ledd. Bestemmelsen om formell beslutning i § 205 første ledd gjelder ikke når besitteren frivillig utleverer tingen, se punkt 10.4 om ransaking.

Etter straffeprosessloven § 208 a første ledd kan retten ved kjennelse beslutte at underretning om beslag til den mistenkte eller andre kan utsettes.

Metodekontrollutvalget foreslår ingen endringer i reglene om beslag, og heller ingen *høringsinstanser* ber om endringer. Reglene nevnes her fordi de er av betydning for øvrige vurderinger, herunder av reglene om postbeslag.

10.6 Postbeslag

10.6.1 Gjeldende rett

Straffeprosessloven §§ 211 og 212 har særregler om postbeslag, det vil si beslag av «[b]rev, telegram eller annen sending som besittes av en postoperatør eller en tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste», jf. § 211 første ledd. Postbeslag kan foretas dersom sendingen vil kunne beslaglegges hos mottakeren etter reglene i §§ 203 og 204. Sendingen må dermed antas å ha betydning som bevis, jf. § 203 første ledd, og beslag kan bare skje så fremt ikke innholdet i sendingen omfattes av unntakene fra vitneplikten i §§ 117–121 og 124–125, jf. § 204 første ledd. Dette vil for eksempel gjelde sendinger fra og til lege og advokat. Men er vilkårene for postbeslag ellers til stede, kan sendingen beslaglegges hos operatør uavhengig av operatørens taushetsplikt. Dette inngrepet i det som tradisjonelt har vært betegnet som posthemmeligheten, er kompensert ved at det for postbeslag er et vilkår at det foreligger mistanke om handling som etter loven kan medføre straff av fengsel i mer enn 6 måneder.

Postbeslag besluttes av retten ved kjennelse. Er det fare ved opphold, kan påtalemyndigheten gi pålegg om at sendinger skal holdes tilbake inntil rettens kjennelse foreligger, men ikke ut over en uke. Postbeslag kan som hovedregel bare åpnes og gjennomses av dommeren, som avgjør hva som

eventuelt har «betydning i saken», jf. § 212. Det som har betydning overlates til påtalemyndigheten, mens resten sendes videre til mottaker. Mottaker og avsender skal underrettes om hva som er åpnet og som holdes under beslag, så fremt det kan skje uten skade for etterforskningen.

Ved lov 3. desember 1999 nr. 82 ble det vedtatt tilføyelser i § 212 om at retten, i saker om rikets sikkerhet, kan overlate til politiet å åpne og gjennomse sendingen dersom særlige grunner tilsier det. Det ble også vedtatt at i slike saker kan underretning også unnlates av hensyn til etterforskningen av andre saker om overtredelser som angår rikets sikkerhet. Endringene, som må ses i sammenheng med samtidig opphevelse av loven om postkontroll i saker om rikets sikkerhet, er ikke trådt i kraft.

Det særlige vernet om posthemmeligheten har sin parallell i EMK artikkel 8, som omfatter vernet om korrespondanse. Vernet etter EMK artikkel 8 er ikke absolutt. Men hvis det er tale om et inngrep etter artikkel 8 nr. 1, må vilkårene i unntaksbestemmelsen i artikkel 8 nr. 2 være oppfylt. Det innebærer at inngrepet må ha hjemmel i lov, det må ha et relevant formål og det må være nødvendig i et demokratisk samfunn.

Ordlyden tilsier at beslagshjemmelen i § 211 gjelder for enkeltsendinger og slik sett skiller seg fra postkontroll etter lov 24. juni 1915 nr. 5 om kontroll med post- og telegrafforsendelser og med telefonsamtaler, som hjemler fortløpende kontroll av post, se NOU 2004: 6 punkt 7.8.4.3 side 108.

Sendingen må besittes av postoperatør eller tilbyder. Det vil si at den må være underveis fra avsender til mottaker. Ved vanlige postsendinger opphører operatørens besittelse når posten er kommet frem til mottakeren, typisk til hans postkasse eller postboks. Fra dette tidspunktet gjelder de alminnelige beslagsreglene, og § 211 kan ikke lenger brukes som hjemmel.

Ordlyden indikerer at § 211 også hjemler postbeslag av e-post, jf. også NOU 2004: 6 punkt 7.8.4.3 side 108. I rettspraksis har postbeslagsreglenes anvendelse på e-postsendinger budt på tvil, særlig sett hen til når sendingen kan sies å være i tjenestetilbyderens besittelse.

I RG 1998 side 1155 kom Borgarting lagmannsrett, under tvil, til at det var naturlig å gi postbeslagsreglene tilsvarende anvendelse på e-post, mens bestemmelsen om utleveringspålegg i § 210 jf. § 203 ikke ble ansett som tilstrekkelig hjemmel for beslag av e-post. Lagmannsretten uttalte at «[i]nntil posten er hentet opp og fjernet av mottakeren er det naturlig å anse E-posten for å være i tjenesteformidlerens besittelse, […].».

I Borgarting lagmannsretts kjennelse i RG 2008 side 1477 heter det at «[e]n sending i lovens forstand må etter lagmannsrettens syn i prinsippet omfatte elektronisk formidlet post». Det ble imidlertid lagt til grunn at e-post bare er i tjenestetilbyderens besittelse i det korte tidsrommet, normalt bare noen sekunder, fra e-posten sendes til den kommer frem til mottakerens innboks. Fra dette tidspunktet kan mottakeren råde over e-posten ved å lese, slette, videresende eller lagre den, mens tjenestetilbyder ikke har slik rådighet. Retten slo fast at beslag av e-posten i det korte tidsrommet fra den sendes til den kommer frem til mottakers innboks må skje med hjemmel i § 211, mens beslag etter dette tidspunkt må skje etter de alminnelige beslagsreglene.

I saken Frostating lagmannsretts kjennelse 20. juli 2015 (LF-2015-111129) hadde politiet bedt om utlevering av innholdet i e-postadressen A@ntebb.no, herunder e-post lagret i innboks/utboks/utkast, kontaktregister, adresser og annen informasjon tilknyttet kontoen, back-up-logger tilknyttet kontoen og trafikkdata. I saken ble det dissens 2-1.

Rettens mindretall mente at postbeslagsregelen i § 211 gjelder både sendinger som er underveis til mottaker, og sendinger som er kommet frem. Det avgjørende er om formidleren er i besittelse av sendingen, for eksempel som sikkerhetskopi. Mindretallet konkluderte med at beslag burde behandles etter den strenge spesialbestemmelsen i § 211, og ikke etter den alminnelige regel i § 210. Mindretallet kunne ikke se at det med gjeldende straffeprosesslov var gode grunner til å vurdere e-poster annerledes enn brev etter de relevante bestemmelsene. De reelle hensynene, herunder å verne betroelser, var like sterke. Det kunne heller ikke være avgjørende at saksbehandlingen etter § 211 ble mer arbeidskrevende enn etter den smidigere § 210.

Rettens flertall støttet seg på kjennelsen fra 2008 og uttalte:

> «Det spesielle med e-poster, i motsetning til brev, er at de kan være i avsenders, tilbyders og mottakers besittelse samtidig. E-post kan dessuten være sikkerhetskopiert og fortsatt være i tilbyders besittelse.
>
> […] I denne avgjørelsen legges til grunn at tilbyder besitter e-posten inntil den er kommet frem til mottakers innboks. Fysisk vil e-posten være lagret på tilbyders e-postserver, men mottaker vil ha full rådighet over denne ved å lese, slette, videresende eller lagre e-posten.

En slik forståelse innebærer at reglene i straffeprosessloven § 211 får sterkt begrenset betydning for utleveringspålegg av e-poster. Det er kun i de få sekund når e-posten er på vei fra avsender til den har nådd mottakers innboks, at beslag etter § 211 er aktuelt.

Flertallets oppfatning er at regelen om postbeslag i § 211 retter seg mot sendinger som er under formidling. Det er unaturlig å si at e-poster som er kommet frem til mottakers innboks er «sendinger». E-postene er da mottatt. At tilbyder også kan ha tilgang til materialet ved at det er lagret på dennes server, kan ikke ses å være avgjørende. Poenget er at på det tidspunkt er det ikke noen sending lenger, men lagret, eventuelt slettet materiale. Det er heller ikke snakk om ulik forståelse av besittelsesbegrepet i § 210 og § 211, slik flertallet ser det. Besittelsen er i § 211 knyttet opp til «sending» og ikke til mottatt e-post. I det siste tilfellet er det § 210 som er aktuelt. Begjæringen om utlevering må likevel rettes mot tilbyder fordi opplysningene er lagret på dennes server og utlevering krever bistand fra tilbyderen.

Utleveringsbegjæringen omfatter også mer enn mottatte og sendte e-poster. Den omfatter e-post lagret i utkast, kontaktregister, adresser og annen informasjon tilknyttet kontoen og trafikkdata. Dette kan neppe kategoriseres som «sendinger» og kan ikke ses å omfattes av reglene i § 211.»

Flertallet uttalte at de spesielle reglene for postoperatører ikke syntes å være godt tilpasset dagens samfunn med utstrakt bruk av e-post. Flertallet påpekte at bestemmelsene i §§ 211 og 212 er forslått opphevet av Metodekontrollutvalget, jf. NOU 2009: 15 kapittel 19 side 213-215, hvor det vises til at domstolens rolle som kontrollør av e-postbeslag fremstår som svært uhensiktsmessig. Etter dette kom flertallet til at det var riktig å anvende straffeprosessloven § 210 som hjemmel for utleveringspålegget, og anken ble forkastet.

10.6.2 Metodekontrollutvalgets forslag

Metodekontrollutvalget foreslår at særreglene om postbeslag i straffeprosessloven §§ 211 og 212 oppheves. Utvalget antar at postbeslag stort sett benyttes når politiet ikke ønsker å underrette mistenkte, men at dette behovet nå dekkes av reglene om utsatt underretning ved beslag og utleveringspålegg. Utvalget viser i sin argumentasjon for opphevelse av postbeslagsreglene til at når det aksepteres at politiet kan beslaglegge brev hos mistenkte uten at vedkommende underrettes og uten at det gjelder særlige regler om gjennomsyn, må det aksepteres at dette også gjøres hos operatøren. Det vises til utredningen punkt 19.3 side 214:

«Med tanke på at man i lov 3. desember 1999 nr. 82 fikk regler som åpner for utsatt underretning ved utleveringspålegg, ransaking og beslag, på samme vilkår som for postbeslag (fengsel i mer enn seks måneder), fremstår reglene i §§ 211 og 212 etter utvalgets mening i dag som overflødige. Når det aksepteres at politiet kan beslaglegge brev hos mistenkte uten at vedkommende underrettes og uten at det gjelder særlige regler om gjennomsyn, må det etter utvalgets syn aksepteres at dette også kan gjøres hos operatør.»

I utredningen vises det også til at de fleste postbeslag i dag vil gjelde e-post. Dersom man legger til grunn at e-postbeslag skal følge de alminnelige reglene om utlevering og beslag, jf. RG 2008 side 1477, blir anvendelsesområdet for §§ 211 og 212, ifølge utvalget, svært begrenset. Skulle e-postbeslag følge reglene om postbeslag, innvender utvalget at en ordning hvor dommeren må gå gjennom all e-postkorrespondanse for å sortere ut det som er av betydning for politiet, fremstår som svært uhensiktsmessig.

10.6.3 Høringsinstansenes syn

Norsk forening for kriminalreform (KROM) er uenig med utvalget i at bestemmelsene bør oppheves, og det uttales:

«Utvalget foreslår å oppheve strpl. §§ 211 og 212 med henvisning til at de har et begrenset anvendelsesområde, dårlig tilpasset dagens moderne samfunn og uhensiktsmessig fordi domstolen må gjennomgå posten og sortere ut det som tilsynelatende er relevant for politiet. KROM er av den oppfatning at bestemmelsene ikke bør oppheves, men være fanebestemmelser i forhold til håndtering av informasjon politiet ikke skal ha tilgang på. Det må være domstolen og ikke politiet som ivaretar rettssikkerheten. KROM er av den oppfatning at denne tilnærmingen også bør gjelde beslag som innhentes ved bruk av skjulte etterforskningsmetoder og kommunikasjonskontroll herunder overskuddsinformasjon og der hvor samtalepartneren er beskyttet mot vitneplikt, med mer.»

Advokatforeningen og *Politidirektoratet* har ikke merknader til utvalgets kapittel 19 om utleveringspålegg, ransaking, beslag, postbeslag og postkontroll. *Oslo statsadvokatembeter* er enig i utvalgets synspunkter og forslag. Også *Oslo politidistrikt* støtter utvalget i at postbeslag bør vurderes etter de gjeldende reglene om beslag.

PST uttaler:

> «En konsekvens av forslagene om opphevelse av straffeprosessloven §§ 211 og 212 samt loven om postbeslag, er at PSTs adgang til å bruke tvangsmidler innsnevres noe. Av den grunn foreslår utvalget at det i straffeprosessloven § 210b åpnes for at PST i forebyggende øyemed kan anvende utleveringspålegg fremover i tid.
>
> PST støtter utvalgets forslag. Særlig ser vi forslaget om at det i straffeprosessloven § 210b åpnes for at PST i forebyggende øyemed kan anvende utleveringspålegg fremover i tid, som positivt. En slik adgang vil bidra til viktig informasjon i forebyggende saker og forslaget fremstår som både nødvendig og nyttig.»

10.6.4 Departementets vurdering

Mye av den korrespondansen som tidligere foregikk per post, sendes nå elektronisk. Hvor lenge en e-post kan anses å være i nett- og tjenestetilbyders besittelse og dermed vil kunne beslaglegges med hjemmel i § 211 om postbeslag, har som nevnt vært omdiskutert.

I korte trekk er spørsmålet om politiets krav på informasjon fra nett- og tjenestetilbyder om mistenktes e-postkonto skal kunne hjemles i reglene om utleveringspålegg (straffeprosessloven § 210) eller den strengere regelen om postbeslag (straffeprosessloven § 211). Det er ubestridt at e-post som er kommet frem til mottaker og lastet ned av denne, kan kreves utlevert med utleveringspålegg mot mottaker. Spørsmålet er imidlertid om postbeslagsregelen er riktig hjemmel for krav mot nett- og tjenestetilbyder.

Det er avsagt tre lagmannsrettskjennelser i noe ulik retning om spørsmålet. I den første (RG 1998 side 1155) fant retten under tvil at reglene om postbeslag i § 211 måtte legges til grunn, inntil e-posten er hentet opp av mottaker. I den andre kjennelsen (RG 2008 side 1477) mente retten at opplysninger lagret på siktedes e-postkonti bare er å anse som «sending» som besittes av teletilbyder inntil den er kommet frem til mottaker, og at riktig tvangsmiddel etter dette er § 210 om utleveringspålegg. I den siste saken (LF-2015-111129) støttet flertallet seg på kjennelsen fra 2008 og fant at e-poster som er kommet frem til mottakers innboks, uavhengig av om de er lastet ned lokalt, skal kreves utlevert ved utleveringspålegg, da de ikke lenger er å anse som sending omfattet av postbeslagsregelen. Det ble også slått fast at adresselister og kontakter etc. ikke kan anses som sendinger, og således må kreves etter utleveringspåleggsbestemmelsen.

Kjernen i de to første kjennelsene var om skjæringstidspunktet for når en e-post opphører å være en sending etter postbeslagsregelen, skal være når den er kommet frem til mottakers innboks, eller når den er lastet ned til dennes lokale server. Her skiller den tredje kjennelsen seg ut fra de øvrige, da mindretallet mente at § 211 både gjelder sendinger som er underveis til mottaker, og sendinger som er kommet frem, enten de er lastet ned eller ikke. Mindretallet la til grunn at det avgjørende var om formidleren er i besittelse av sendingen, for eksempel som sikkerhetskopi.

Departementet peker på at tanken bak reglene om postbeslag er at dersom beslag lovlig kan skje hos mottaker, bør man kunne foregripe beslaget ved å ta beslag *under forsendelsen*, eksempelvis om det er fare for at mottakeren vil ødelegge eller på annen måte fjerne forsendelsen etter å ha mottatt den. Det forutsettes altså at beslaget er en «sending», og departementet mener at det ikke er naturlig å si at e-poster som er kommet frem til mottakers innboks er «sendinger» i § 211 sin forstand. E-postene er da mottatt av adressaten. At tilbyder også kan ha tilgang til materialet ved at det er lagret på dennes server, kan ikke ses å være avgjørende. På det tidspunkt er det ikke noen sending lenger, men lagret informasjon som eventuelt kan kreves utlevert etter reglene om utleveringspålegg i § 210.

Det er heller ikke riktig at dersom mindretallets tolkning i LF-2015-111129 av § 211 legges til grunn, vil e-post likestilles med ordinær post. Tvert imot vil en slik forståelse gi et sterkere vern for e-poster enn for annen post, ved at det ikke tas hensyn til at sendingen faktisk er kommet frem til mottaker. Departementet bemerker at e-post som er kommet frem til mottaker, utvilsomt kan beslaglegges hos mistenkte eller andre etter de alminnelige reglene i § 210, og dette bør gjelde tilsvarende overfor nett- og tjenestetilbyder.

Etter dette legges det til grunn at postbeslagsreglene er praktisk lite anvendelige for beslag av e-postsendinger, da postbeslag bare kan gjøres gjeldende i de få sekundene e-posten er på vei fra avsender til den har nådd mottakers innboks.

Departementet kan ikke utelukke at postbeslag fremdeles vil kunne være aktuelt for ordinær post, for eksempel der en postsending inneholder narkotika. Både politiet og tollmyndighetene har gitt uttrykk for at salg av syntetiske narkotiske stoffer over internett er et økende problem, og antall narkotikabeslag på flyplasser og postterminaler har økt kraftig. Selv om mye fanges opp av Tollvesenet allerede på Oslo Lufthavn med hjemmel i tolloven kapittel 16, legger departementet til grunn at også politiet vil kunne ha behov for å foreta beslag i postsendinger. Departementet mener derfor at postbeslag fortsatt kan være anvendelig for andre sendinger enn e-post. Korrespondanse som besittes av postoperatør vil imidlertid, i fravær av spesialreglene om postbeslag, kunne beslaglegges hos eller pålegges utlevert av operatøren med hjemmel i de alminnelige reglene om beslag og utleveringspålegg, eventuelt i kombinasjon med utsatt underretning til mistenkte.

Departementet vil bemerke at dersom spesialreglene om postbeslag oppheves, vil beslag hos eller utlevering fra operatør bare kunne skje etter opphevelse av operatørens taushetsplikt. Årsaken er at reglene om utleveringspålegg og beslag er begrenset av regler om vitneplikt, jf. straffeprosessloven §§ 204 og 210. Postoperatørens taushetsplikt følger av § 30 i lov om posttjenester (postloven), som trådte i kraft 1. januar 2016. Taushetsplikten er i utgangspunktet til hinder for beslag, utleveringspålegg og utleveringspålegg fremover i tid, jf. straffeprosessloven § 204 første ledd første punktum, § 210 første ledd første punktum og § 210 b første ledd jf. § 118 første ledd. Uten postbeslagsreglene vil dermed opphevelse av taushetsplikten være nødvendig for beslag hos eller utlevering fra operatør.

Nett- og tjenestetilbydere har i utgangspunktet taushetsplikt etter ekomloven § 2-9. I henhold til straffeprosessloven § 118 kan retten bare ta imot forklaring som et vitne ikke kan gi uten å krenke taushetsplikt som påligger tilbyder av tilgang til elektronisk kommunikasjonsnett eller elektronisk kommunikasjonstjeneste, dersom departementet samtykker. Samtykkekompetansen utøves av Nasjonal kommunikasjonsmyndighet (tidligere Post- og teletilsynet, heretter kalt NKOM) i kraft av delegasjon, jf. vedtak 23. juni 1995 nr. 39. Samtykke kan bare nektes dersom åpenbaringen vil kunne «utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold», jf. § 118 første ledd siste punktum. Straffeprosessloven § 118 åpner dessuten for at retten i visse tilfeller kan overprøve en nektelse av å gi samtykke.

I Metodekontrollutvalgets utredning punkt 19.2.5 side 213 uttales:

> «Lagmannsrettsavgjørelsen fra 2008 innebærer at politiet bare vil kunne få tilgang til innholdet i e-post dersom Post- og teletilsynet opphever teletilbyderens taushetsplikt etter ekomloven, ettersom unntaket i §§ 203, jf. 204 og 210 for opplysninger som et vitne vil kunne nekte å forklare seg om gjelder tilsvarende her. Som et resultat av avgjørelsen har Post- og teletilsynet begynt å behandle slike begjæringer, og tilsynet har overfor utvalget gitt uttrykk for at det har registrert en økende interesse for slike innholdsdata fra påtalemyndighetens side. Til nå har tilsynet imidlertid aldri funnet grunnlag for å frita noen tilbyder for taushetsplikten om innholdet i e-post. Ifølge tilsynet skyldes dette at de har fått lite dokumentasjon på hva slikt innsyn faktisk vil åpenbare, og at de sterke personvernhensyn som ligger til grunn for reglene i §§ 211 og 212 om post under forsendelse, også gjør seg gjeldende i forhold til e-postkonti.»

Departementet bemerker at det er grunn til å være noe mer imøtekommende når det gjelder politiets utleveringspålegg etter den siste kjennelsen (LF-2015-111129). NKOM var ankepart i den aktuelle saken og anførte blant annet at reelle grunner talte for at riktig beslagshjemmel var § 211, da det var tale om utlevering av mye større mengder informasjon enn ordinær post. NKOM mente at et slikt inngrep burde hjemles i den bestemmelsen som i størst mulig grad ivaretar respekt for kommunikasjon. Denne argumentasjonen førte ikke frem. Det er likevel verdt å merke seg at en av NKOMs innvendinger var at det ved et utleveringspålegg ikke vil være oversikt over hvilken kommunikasjon som utleveres i motsetning til etter fremgangsmåten i § 211. Departementet mener det kan stilles spørsmål om politiet i noe større grad kan presisere hvilken informasjon som antas å ha betydning som bevis, jf. § 210. Det vises til Bjerke/Keiserud/Sæther, Straffeprosessloven kommentarutgave Bind I (4. utgave, Oslo 2011) side 725, der det heter:

> «[…] Et vilkår for plikt til fremleggelse er at kravet – og pålegget – er slik spesifisert og konkretisert at det er mulig for den som skal fremlegge tingen, f.eks. et dokument, å vite hva han skal fremlegge, jf. Rt. 1997 s. 266, se også RG 2009 s. 705 (Borgarting lagmannsrett). Utleve-

> ringspålegg forutsetter på samme måte som beslag at tingen kan identifiseres. Dersom dette ikke er mulig, må påtalemyndigheten gå veien om ransaking, jf. *Andenæs/Myhrer*, Norsk straffeprosess s. 324.»

I den siste kjennelsen (LF-2015-111129) ble tjenestetilbyder pålagt, uhindret av sin taushetsplikt, å utlevere til politiet innholdet av en konkret e-postadresse, herunder e-post lagret i innboks, utboks og utkast, kontaktregister, adresser, annen informasjon tilknyttet kontoen, back-up-logger tilknyttet kontoen og trafikkdata, jf. straffeprosessloven § 203 og § 204 jf. § 210. Pålegget gjaldt hele perioden fra e-postkontoen ble opprettet til pålegget ble gjennomført. Det synes å være lagt til grunn at så lenge det dreier seg om én konkret e-postadresse, er kravet tilstrekkelig presisert og begrenset. Det kan imidlertid ikke utelukkes at politiet i den konkrete sak har mulighet til å avgrense utleveringspålegget ytterligere, for eksempel ved å vise til aktuelle avsendere, mottakere eller grupper av personer som er av særlig interesse. Departementet forstår likevel at en slik konkretisering i andre saker kan være vanskelig eller umulig, dersom formålet med å be om all kommunikasjon nettopp er å avdekke hvem det kommuniseres med. Ved å måtte begrense utleveringspålegget til kommunikasjon med kjente personer, vil politiet være avskåret fra å oppdage nye spor, noe som vil være lite hensiktsmessig. Departementet vil understreke at det i rettspraksis ikke er stilt krav om at dokumentbeslag kan knyttes til enkelte nærmere angitte dokumenter. Det må bero på en konkret og praktisk vurdering hvor langt man kan gå i å godta en kollektiv angivelse av dokumenter, jf. Rt. 1981 side 1199, Rt. 1992 side 898 og Rt. 1995 side 1831. Departementet utelukker imidlertid ikke at pålegget kan avgrenses på andre måter, for eksempel ved å vise til et nærmere angitt tidsrom, fremfor at det bes om «samtlige e-poster siden e-postkontoen ble opprettet».

Departementet vil understreke at også informasjon i utkast, kontaktregister, adresser etc. kan begjæres utlevert etter § 210. Det vises til betraktninger i Bjerke/Keiserud/Sæther, Straffeprosessloven kommentarutgave Bind I (4. utgave, Oslo 2011) side 725, der det heter:

> «Om en ting kan antas å ha betydning som bevis, må avgjøres etter en konkret vurdering. En rimelig mulighet er nok. Om en ting, f.eks. en navneliste, kan lede til opplysninger om andre bevis i saken, f.eks. om vitner i saken, må også dette etter omstendighetene kunne gi grunnlag for et utleveringspålegg når disse opplysningene kan antas å ha betydning for etterforskningen, se også Ot.prp. nr. 64 (1998-99) s. 153 (til § 210b).»

Departementet antar at dersom utleveringsbegjæringer konkretiseres i tråd med ovennevnte, vil det også være mulig for NKOM å ta stilling til om utleveringen av informasjonen vil kunne «utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold», jf. § 118 første ledd siste punktum.

Departementet bemerker at hensynet til vern av konfidensiell informasjon, for eksempel korrespondanse med advokat, lege, prest etc., er ivaretatt gjennom bevisforbudsbestemmelsen i straffeprosessloven § 119, jf. § 210 første ledd første punktum i.f., der det fremgår at adgangen til å pålegge utlevering er knyttet til vitneplikten. Dersom det blant tingene som er pålagt utlevert, anføres å være noe som vedkommende kan nekte å vitne om, skal materialet oversendes retten som etter en gjennomgåelse beslutter hva politiet har adgang til å beholde. Dette følger av en analogisk anvendelse av straffeprosessloven § 205 tredje ledd siste punktum, jf. Bruce og Haugland, Skjulte tvangsmidler (Oslo 2014) side 158 og Rt. 1986 side 1149. Saken gjaldt spørsmål om beslag i et pengeskap hos siktede som ble anført å inneholde fortrolig korrespondanse mellom ham og hans forsvarer. Høyesteretts kjæremålsutvalg slo fast at dokumenter som besitteren før eller under ransakingen hevder er unntatt fra beslag etter § 204 («dokumenter eller annet hvis innhold et vitne kan nekte å forklare seg om etter §§ 117-121 og 124-125»), ikke kan gjennomgås av politiet ved ransakingen. I Rt. 2000 side 531 slo Høyesterett fast at en journalists rett til å nekte å oppgi en kilde, jf. straffeprosessloven § 125, medfører begrensninger i adgangen til å ta beslag, jf. hovedregelen i straffeprosessloven § 204 og behandlingsreglene i straffeprosessloven § 205 tredje ledd.

Avgjørelsen fra 1986 er noe modifisert gjennom Rt. 1995 side 1831, som gjaldt beslag i opptegnelser, journalmateriale og regnskapsmateriale hos en bedragerisiktet lege og andre leger i kontorfellesskap, der Kjæremålsutvalget tillot politiet å foreta en utsortering av dokumenter. Utvalget påpekte at avgjørelsen fra 1986 fremsto «som særlig knyttet til situasjoner hvor taushetspliktsbestemmelsene tar sikte på å beskytte mot innsyn nettopp fra politiets side». Det ble vist til forarbeidene, jf. NUT 1969: 3 Innstilling om rettergangsmåten i straffesaker fra Straffeprosesslovkomiteen side 256, der komiteen uttaler:

> «[…] Ved ransaking må politiet kunne undersøke papirer i den utstrekning det er nødvendig for å skaffe grunnlag for skjønnet over hvilke papirer som bør beslaglegges […], og i så fall er det ikke til å unngå at politiet også kan komme til å gjennomse papirer som det ikke er adgang til å beslaglegge. Det vesentligste vil således i alle tilfelle måtte være lovens begrensning av beslagsadgangen.».

Der besitteren påberoper seg taushetspliktsregler som tar sikte på å beskytte mot innsyn nettopp fra politiets side, som korrespondanse med advokat, gjelder imidlertid et totalforbud mot politiets gjennomgåelse, og retten må forestå gjennomgåelsen av hele materialet. De dokumentene som etter rettens vurdering ikke er underlagt beslagsforbud, skal utleveres påtalemyndigheten for vurdering og beslutning om beslag, jf. Rt. 2011 side 296 og Bruce og Haugland, Skjulte tvangsmidler (Oslo 2014) side 150. Prosedyrene for gjennomgåelse av slikt materiale er de samme ved utleveringspålegg som ved beslag, jf. Bruce og Haugland, Skjulte tvangsmidler (Oslo 2014) side 158.

Denne reguleringen tilfredsstiller etter departementets syn de krav som kan utledes av EMDs praksis om EMK artikkel 8, jf. forutsetningsvis Rt. 2015 side 81. Saken gjaldt materiale innhentet ved kommunikasjonskontroll, herunder samtaler med advokat. Høyesterett understreket i avsnitt 18 at kommunikasjonskontroll og beslag er underlagt ulike regelsett, og forsvarerens anførsel om at materiale innhentet ved kommunikasjonskontroll måtte behandles på samme måte som materiale innhentet ved beslag, jf. § 204 jf. § 205 tredje ledd, førte ikke frem. Høyesterett fant imidlertid at dersom det på forhånd er klart at materialet inneholder telefonsamtaler som faller inn under straffeprosessloven § 119, skal påtalemyndigheten uten videre sørge for at de blir sortert ut og slettet, jf. straffeprosessloven § 216 g bokstav b, uten adgang til å påbegynne gjennomhøring av dem. Høyesterett fant videre at det følger av de prinsipper som kan utledes av EMDs praksis, at en gjennomhøring av samtaler påtalemyndigheten vet – eller ved gjennomgåelsen blir klar over – at er med en advokat, men hvor det er usikkert om det dreier seg om en klientsamtale som faller inn under straffeprosessloven § 119, rammes av Grunnloven § 102 og EMK artikkel 8, jf. forutsetningen i *Kopp mot Sveits* 25. mars 1998 (Sak 23224/94). Høyesterett uttalte i avsnitt 28:

> «Dette innebærer at påtalemyndigheten i de tilfellene jeg drøfter, må slette samtalene med mindre det etableres en ordning som på dette punktet er i samsvar med EMK artikkel 8. Forsvareren har subsidiært anført at samtalene i slike tilfeller må sendes tingretten for gjennomgang uten at politiet på forhånd har gjennomgått disse. En slik praksis vil sikre at eventuelle samtaler som omfattes av straffeprosessloven § 119, tas ut av materialet og slettes. Eventuelle samtaler som ikke er vernet, returneres påtalemyndigheten. En slik ordning vil etter mitt syn tilfredsstille kravene i EMK artikkel 8. […]»

Departementet mener at uttalelsen forutsetningsvis bekrefter at reguleringen om domstolsgjennomgåelse ved beslag av materiale som antas å være underlagt bevisforbudsreglene, tilfredsstiller de krav som kan utledes av EMDs praksis.

Prosedyren med rettens gjennomgåelse gjelder også ved databeslag, jf. Rt. 2013 side 968. Høyesterett uttalte her at politiet i forbindelse med beslag hadde lovlig adgang til å speilkopiere en harddisk som inneholdt elektronisk lagret skriftlig materiale, til tross for advokaters taushetsplikt, jf. straffeprosessloven § 204, jf. § 119. Politiet hadde imidlertid ikke anledning til å beholde speilkopien av advokatens harddisk, som umiddelbart skulle ha vært oversendt tingretten uten noen form for gjennomgåelse eller grovsortering fra politiets side, jf. straffeprosessloven § 205 tredje ledd. Tingretten kunne likevel ha innhentet bistand fra en uavhengig sakkyndig, dersom den ikke selv ønsket å gjennomføre søkingen.

Det bemerkes at den sistnevnte saken gjaldt beslag av materiale hos en advokat, hvor det er en presumpsjon for at det beslaglagte materialet er underlagt taushetsplikt, jf. avsnitt 30 i kjennelsen, som det også henvises til i Rt. 2015 side 81 avsnitt 19. Departementet mener at politiets adgang til å foreta en grovsortering kan være større i saker hvor en slik presumpsjon ikke foreligger, jf. Straffeprosesslovkomiteens betraktninger i NUT 1969: 3 Innstilling om rettergangsmåten i straffesaker fra Straffeprosesslovkomiteen side 256. Høyesterett legger i Rt. 2013 side 968 vekt på at hensynet til fortrolig kommunikasjon mellom en advokat og hans klient nyter et sterkt vern, jf. avsnitt 37. Dette fremgår også av Rt. 2015 side 1456 avsnitt 21. Selv om nett- og tjenestetilbydere er underlagt taushetsplikt, kan taushetspliktsbestemmelsene neppe sies å ta sikte på å beskytte mot innsyn nettopp fra politiets side, og det er heller ingen presumpsjon for at e-postkontoen vil inneholde konfidensiell informasjon som korrespondanse med advokat. Dette tilsier at politiet i større grad kan tillates å foreta en grovsortering av materialet som mottas. Under

enhver omstendighet legger departementet til grunn at dersom politiet har rettet pålegg om utlevering av opplysninger knyttet til en konkret e-postadresse mot nett- og tjenestetilbyder og mottatt slikt materiale, og det deretter fremgår av avsender- eller mottakerfeltet eller på annen måte at opplysningene vil kunne være underlagt bevisforbud, må dette materialet oversendes domstolen uten ytterligere gjennomgåelse.

Da hensynet til vern av konfidensiell informasjon er ivaretatt ved beslag og utleveringspålegg, fordi retten her skal forestå gjennomgåelsen av materialet, finner departementet at det ikke er behov for det særskilte vern som postbeslagsreglene knesetter. Departementet støtter etter dette Metodekontrollutvalget i at særreglene om postbeslag i straffeprosessloven §§ 211 og 212 kan oppheves.

10.7 Postkontroll i saker om rikets sikkerhet

10.7.1 Gjeldende rett

Lov 24. juni 1915 nr. 5 åpner for kontroll med post- og telegrafforsendelser og med telefonsamtaler «når dette antas påkrevd av hensyn til rikets sikkerhet», jf. § 1 første ledd. Utenfor krigstid må det dreie seg om mistanke om overtredelse av nærmere angitte bestemmelser, herunder lov om forsvarshemmeligheter og straffeloven 1902 kapittel 8, 9, 12, 13 og 14. Forskrift 18. august 1960 nr. 2 om kontroll med post- og telegramforsendelser § 1 utvider lovens anvendelsesområde. Etter forskriften kreves grunn til mistanke for at slike straffbare handlinger er begått.

Postkontroll innebærer at politiet i et bestemt tidsrom får tillatelse til å undersøke alle brev til og fra mistenkte, og skiller seg på denne måten fra reglene om utleveringspålegg, beslag og postbeslag.

Postkontroll krever tillatelse fra retten, men påtalemyndigheten er gitt hastekompetanse i særlig påtrengende tilfeller, jf. forskriften § 1 første og annet ledd.

Reglene om postkontroll i saker om rikets sikkerhet ble foreslått opphevet av Sikkerhetsutvalget i NOU 1993: 3 og av Metodeutvalget i NOU 1997: 15. Departementet sluttet seg til forslaget om opphevelse i Ot.prp. nr. 64 (1998–99), men foreslo særregler i straffeprosessloven § 212 for saker om rikets sikkerhet. Postkontrolloven ble opphevet samtidig som de foreslåtte endringene i straffeprosessloven ble vedtatt ved lov 3. desember 1999 nr. 82. Ifølge kongelig resolusjon av samme dato skulle opphevelsen av postkontrolloven og de foreslåtte endringene i § 212 foreløpig ikke tre i kraft. Endringene har fremdeles ikke trådt i kraft.

De vedtatte endringene av § 212 innebærer to tilføyelser, første ledd nytt annet punktum og annet ledd nytt femte punktum, og er særregler for saker om rikets sikkerhet.

Den første lovendringen innebærer at retten, i saker om rikets sikkerhet, kan overlate til politiet å åpne og gjennomse sendingen uten at det foreligger samtykke fra avsender. «Beslutter retten å overlate til politiet å åpne og gjennomse posten, må den kunne stille visse vilkår, for eksempel om at en polititjenestemann med særlig kunnskap om kodespråk skal gjennomføre kontrollen», jf. Ot.prp. nr. 64 (1998–99) side 154.

Gjeldende § 212 annet ledd åpner for at underretning til mottaker og avsender om hva som er åpnet og om hva som holdes i beslag, kan unnlates eller utsettes hvis slik underretning kan skade etterforskningen. Her siktes det til etterforskningen i den saken som mistanken gjelder, ikke andre saker. Den andre endringen av § 212 innebærer at underretning i saker om rikets sikkerhet også kan unnlates eller utsettes av hensyn til etterforskningen i *andre* saker om rikets sikkerhet. «Unntaksbestemmelsen vil først og fremst ha betydning i forhold til saker som har nær tilknytning til den saken postkontrollen [postbeslag er omtalt som postkontroll] gjelder. Det er for eksempel snakk om den samme person, den samme terrorgruppe eller det samme lands etterretningsorganisasjon i begge tilfeller», jf. Ot.prp. nr. 64 (1998–99) punkt 23 side 154.

10.7.2 Metodekontrollutvalgets forslag

Utvalget bemerker at det er uheldig at Stortingets beslutning om opphevelse av postkontrolloven, samt endringene i straffeprosessloven § 212, ikke er trådt i kraft, se utredningen punkt 19.3.2 side 214. Utvalget går ut ifra at grunnen er at man har oppdaget at loven om postkontroll har et anvendelsesområde som går ut over reglene om postbeslag, og viser til at loven hjemler fortløpende kontroll, har et lavere mistankekrav enn postbeslagsreglene, ikke gir mistenkte krav på underretning og foreskriver en enklere beslutningsprosess. Utvalget har vurdert om reglene om postkontroll likevel ikke burde oppheves, eventuelt om det bør gjøres andre endringer i straffeprosessloven. Det vises til at Politiets sikkerhetstjeneste har opplyst at de i dag ikke bruker hjemmelen for postkontroll i saker om rikets sikkerhet,

særlig fordi PST ikke ønsker å bruke en lov som er opphevet. PSTs behov er etter det opplyste dekket gjennom reglene om utleveringspålegg, postbeslag og utleveringspålegg fremover i tid. På denne bakgrunn foreslår Metodekontrollutvalget at opphevelsen av loven om postkontroll i saker om rikets sikkerhet settes i kraft.

Ettersom PSTs adgang til å bruke tvangsmidler innsnevres noe dersom reglene om postbeslag og postkontroll oppheves, forslår utvalget å åpne for bruk av utleveringspålegg fremover i tid etter straffeprosessloven § 210 b som ledd i PSTs forebyggende virksomhet, se punkt 13.5.5.4.

10.7.3 Høringsinstansenes syn

Advokatforeningen og *Politidirektoratet* har ingen merknader til utvalgets forslag om ikraftsettelse av opphevelsen. *PST* og *Oslo statsadvokatembeter* støtter forslaget.

PST uttaler:

> «Utvalget foreslår at opphevelsen av lov om postkontroll bør tre i kraft umiddelbart. PSTs behov dekkes i hovedsak gjennom reglene om utleveringspålegg, postbeslag og utleveringspålegg fremover i tid, og PST bruker i dag ikke bestemmelsene om postkontroll i saker om rikets sikkerhet.
>
> En konsekvens av forslagene om opphevelse av straffeprosessloven §§ 211 og 212 samt loven om postbeslag, er at PSTs adgang til å bruke tvangsmidler innsnevres noe. Av den grunn foreslår utvalget at det i straffeprosessloven § 210b åpnes for at PST i forebyggende øyemed kan anvende utleveringspålegg fremover i tid.
>
> PST støtter utvalgets forslag. Særlig ser vi forslaget om at det i straffeprosessloven § 210 b åpnes for at PST i forebyggende øyemed kan anvende utleveringspålegg fremover i tid, som positivt. En slik adgang vil bidra til viktig informasjon i forebyggende saker og forslaget fremstår som både nødvendig og nyttig.»

Riksadvokaten har ingen avgjørende innvendinger til at straffeprosessloven § 210 b om fremtidig utleveringspålegg inntas i oppregningen i politiloven § 17 d.

10.7.4 Departementets vurdering

Departementet foreslår, i tråd med Metodekontrollutvalgets forslag, at opphevelsen av loven ikraftsettes. Behovet for postkontroll i saker om rikets sikkerhet må søkes dekket gjennom bestemmelsene om beslag, utleveringspålegg og utleveringspålegg fremover i tid.

Departementet mener det ikke er behov for et separat regelsett om postkontroll i saker om rikets sikkerhet. Reglene i straffeprosessloven bør dekke behovet for slik kontroll, jf. vurderingene i Ot.prp. nr. 64 (1998–99) punkt 8.2.5 side 41 og punkt 9.5 side 89. Ved å samle reglene i straffeprosessloven, vil systemet bli mer oversiktlig. Departementet viser videre til at loven ble vedtatt opphevet i 1999, og at det har gått mange år uten at postkontroll har blitt benyttet. PST har overfor Metodekontrollutvalget opplyst at de i dag ikke bruker hjemmelen for postkontroll i saker om rikets sikkerhet, og at PSTs behov er dekket gjennom de øvrige tvangsmiddelbestemmelsene i straffeprosessloven.

Når det gjelder spørsmålet om det skal åpnes for utleveringspålegg fremover i tid i forebyggende øyemed med hjemmel i politiloven § 17 d, støtter departementet utvalget og PST, se punkt 13.5.5.4.

11 Innhenting av trafikkdata

11.1 Innledning

11.1.1 Begrepsbruk

Trafikkdata er i Metodekontrollutvalgets utredning definert som «opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med et bestemt kommunikasjonsanlegg, og andre data knyttet til kommunikasjon». Definisjonen sondrer ikke mellom trafikkdata og såkalte lokaliseringsdata. Med lokaliseringsdata menes opplysninger om hvilke telefoner eller annet kommunikasjonsutstyr som innenfor et nærmere geografisk område har vært satt i forbindelse med bestemte telefoner eller kommunikasjonsutstyr. Ved lovendringer tilknyttet gjennomføring av datalagrinsdirektivet skilles det mellom trafikk- og lokaliseringsdata, all den tid innhenting av lokaliseringsdata representerer et større inngrep i personvernet enn innhenting av trafikkdata. I det følgende gjennomføres derfor et slikt skille. Der utvalget eller høringsinstansene bruker begrepet «trafikkdata» i den videre betydning begrepet hadde før, vil det bli presisert at også lokaliseringsdata er omfattet.

Verken trafikk- eller lokaliseringsdata omfatter opplysninger om innholdet i kommunikasjonen.

11.1.2 Datalagringsdirektivet

11.1.2.1 Kort om direktivet

Datalagringsdirektivet (2006/24/EF) ble vedtatt 15. mars 2006. Kjernen i direktivet er en plikt for ekomtilbydere til å lagre all trafikkdata i en viss periode. Formålet er å kunne benytte dette i arbeidet med kriminalitetsbekjempelse. Gjennomføringsfristen for medlemsstatene ble satt til 15. september 2007. Datalagringsdirektivet er ikke innlemmet i EØS-avtalen fordi Island ikke har godtatt det. Innholdet i direktivet ble like fullt gjennomført i norsk rett ved lov 11. april 2011 nr. 11 (heretter kalt lagringsloven), som omfatter endringer i ekomloven og straffeprosessloven. Loven er ikke i kraft. Hovedgrunnen til dette er arbeidet med en modell for fordeling av kostnader mellom ekomtilbydere og politiet. En lovproposisjon med de nødvendige lovendringene skulle etter planen vært lagt frem for Stortinget vårsesjonen 2014.

EU-domstolen i storkammer avsa 8. april 2014 dom i sakene C-293/12 og C-594/12, der EUs datalagringsdirektiv (2006/24) ble kjent ugyldig som stridende mot EU-charteret 2000 artikkel 7 og 8 om retten til privatliv og personvern. Direktivet ble funnet å være mer inngripende i retten til privatliv og personvern enn det som ble ansett som nødvendig for å ivareta allmenne interesser eller andres rettigheter.

EU-charteret er ikke bindende for Norge. De nevnte bestemmelsene i charteret fremstår imidlertid som en oppdatert versjon av EMK artikkel 8, og det er også i dommen trukket paralleller til denne og EMD-avgjørelser om personvern. EMK er gjort til en del av norsk rett ved menneskerettsloven, med forrang overfor annen norsk lov. Retten til personvern og privatliv er også gitt et grunnlovsvern ved ny § 102 i Grunnloven. For norsk retts vedkommende blir det spørsmål om hvorvidt lagringsloven slik den nå lyder er forenlig med EMK artikkel 8 i lys av dommen fra EU-domstolen, samt Grunnloven § 102. En slik vurdering vil imidlertid ikke foretas i den foreliggende proposisjonen. Spørsmålene er vurdert i en ekstern utredning, se nærmere omtale i punkt 11.4. Drøftelsen nedenfor vil begrenses til Metodekontrollutvalgets forslag om lovendringer.

11.1.2.2 Metodekontrollutvalgets avgrensning mot direktivet

I vurderingen av reglene om innhenting av trafikkdata, avgrenser Metodekontrollutvalget mot en nærmere vurdering av EUs datalagringsdirektiv. Utvalget viser til at direktivet ikke sier noe om hvilke vilkår som skal gjelde for politiets tilgang til trafikkdata, og dermed ikke berører utvalgets vurderinger direkte, jf. punkt 20.4 side 219.

Departementet la frem forslag til hvordan EUs datalagringsdirektiv kunne gjennomføres i norsk rett i Prop. 49 L (2010–2011) Endringer i ekom-

loven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett). Under Stortingets behandling ble de prosessuelle og materielle vilkår for politiets tilgang til trafikkdata og lokaliseringsdata skjerpet på flere punkter, jf. Innst. 275 L (2010–2011). Dette var av hensyn til personvernet. Gjennomføring av datalagringsdirektivet i norsk rett vil således få direkte betydning for politiets innhenting av trafikkdata under etterforskningen.

Et spørsmål for departementet har derfor vært om det at utvalget ikke har behandlet forholdet til datalagringsdirektivet, gjør at det er enkelte sider ved berøringsflaten mellom metodekontroll og datalagringsdirektivet som ikke har vært gjenstand for høring. Departementet kan imidlertid ikke se at det er tilfellet. Spørsmålene som ikke direkte var gjenstand for høring i forbindelse med Metodekontrollutvalgets utredning, gjelder forhold som ble drøftet under høringen av datalagringsdirektivet og som Stortinget siden har tatt stilling til gjennom Lovvedtak 46 (2010–2011), jf. lov 15. april 2011 nr. 11. Det gjelder spørsmålet om materielle vilkår for innhenting, om lagringstid og om påtalemyndighetens hastekompetanse. Domstolskontroll og spørsmålet om å frata Nasjonal kommunikasjonsmyndighet (tidligere Post- og teletilsynet) oppgaven med å frita for taushetsplikt ved innhenting av trafikk- og lokaliseringsdata, ble drøftet i begge høringsrunder.

Lovendringene i tilknytning til datalagringsdirektivet følger i stor utstrekning opp forslagene til Metodekontrollutvalget. Departementet ser derfor ikke behov for en utførlig gjennomgåelse av utvalgets forslag, men vil likevel kort omtale forslagene og klargjøre på hvilken måte de gjennomføres. Som følge av de mellomliggende lovendringer som ledd i gjennomføringen av datalagringsdirektivet, er *høringsinstansenes* merknader til utvalgets forslag lite treffende, og vil ikke bli behandlet nærmere i det følgende.

11.2 Rettstilstanden inntil lovendringer tilknyttet datalagringsdirektivet trer i kraft

Lovendringene i tilknytning til datalagringsdirektivet var opprinnelig ventet å tre i kraft 1. juli 2014. EU-domstolens avgjørelse 8. april 2014 har imidlertid påvirket dette.

Politiet har i dag, før lovendringen i tilknytning til datalagringsdirektivet trer i kraft, flere og til dels overlappende hjemmelsgrunnlag for innhenting av historiske trafikk- og lokaliseringsdata under etterforskningen. Innhenting kan skje der teletilbyderne utleverer dataene frivillig, eller gjennom reglene om beslag og utleveringspålegg, jf. straffeprosessloven §§ 203 og 210, dersom de antas å ha betydning som bevis. Forutsetningen er i alle tilfeller at Nasjonal kommunikasjonsmyndighet (tidligere Post- og teletilsynet) opphever teletilbydernes taushetsplikt. Tilsynet har delegert kompetanse fra Samferdselsdepartementet. Utleveringspålegg avgjøres som hovedregel av retten, jf. straffeprosessloven § 210 første ledd, mens beslag besluttes av påtalemyndigheten dersom trafikkdataene ikke utleveres frivillig, jf. § 205 første ledd første punktum.

Etter straffeprosessloven § 215 a kan påtalemyndigheten som ledd i etterforskningen gi pålegg om sikring av elektronisk lagrede data – sikringspålegg. Dette gjelder både trafikkdata og innholdsdata, herunder filer med lyd, bilder eller tekst.

Innhenting av historiske data kan dessuten skje med hjemmel i straffeprosessloven § 216 b om kommunikasjonskontroll. Annet ledd bokstav d gir hjemmel for å innhente data knyttet til kommunikasjon. For det første omfattes opplysninger om hvilke kommunikasjonsanlegg som har kommunisert med et bestemt annet anlegg. Dette kan for eksempel være teleselskapenes registreringer av samtaler til og fra en telefon eller loggen over kommunikasjonen til og fra en datamaskin. Videre omfattes andre data knyttet til kommunikasjonen. Dette inkluderer blant annet opplysninger om samtalenes varighet, mobiltelefoners geografiske plassering idet samtalene finner sted og hvem som var logget inn på en datamaskin på det tidspunkt maskinen ble benyttet til kommunikasjon, jf. merknader til bestemmelsen i Ot.prp. nr. 64 (1998–99) kapittel 23. Regelen gir både adgang til å pålegge utlevering av historiske data, og til å gi pålegget virkning fremover i tid. Bestemmelsen stiller krav om skjellig grunn til mistanke, og mistanken må rette seg mot handling som kan medføre fengselsstraff i fem år eller mer. Alternativt må mistanken gjelde en eller flere handlinger som rammes av straffebudene opplistet i bestemmelsens første ledd bokstav b. Det kreves som hovedregel rettens kjennelse for å innhente data, jf. § 216 b første ledd.

For en nærmere redegjørelse av rettstilstanden for innhenting av trafikkdata forut for ikrafttredelse av lovendringene, vises til utvalgets utredning side 216–218 og Prop. 49 L (2010–2011) punkt 12.1. Nedenfor vil rettstilstanden etter lovendringen beskrives nærmere.

11.3 Hvordan er Metodekontroll-utvalgets forslag gjennomført?

11.3.1 Hjemmelsgrunnlag for innhenting av trafikk- og lokaliseringsdata

11.3.1.1 Metodekontrollutvalgets forslag

Metodekontrollutvalget ønsker et mer enhetlig regelverk om utlevering av trafikkdata og mener at hensynet til personvern og rettssikkerhet for den opplysningene gjelder, tilsier at utlevering bare bør kunne skje etter reglene om tvangsmidler. Utvalget mener det bør åpnes for utlevering av trafikkdata bare dersom det foreligger beslutning om utleveringspålegg etter § 210, eventuelt med utsatt underretning etter § 210 a, samt at det fortsatt skal kunne skje med hjemmel i § 216 b.

11.3.1.2 Departementets vurdering

Det er klart forutsatt i Prop. 49 L (2010–2011) at § 210 ikke lenger gir hjemmel for å innhente trafikk- og lokaliseringsdata. Forslaget er derfor ikke lenger aktuelt, og departementet finner ikke grunn til å behandle dette nærmere. Departementet bemerker imidlertid at utvalgets intensjon om et mer enhetlig regelverk og bedre personvern synes å være ivaretatt gjennom de nye bestemmelsene om utlevering av trafikk- og lokaliseringsdata i §§ 210 b og 210 c.

For utlevering av historiske, personspesifikke *trafikkdata* er hovedregelen nedfelt i straffeprosessloven § 210 b. Bestemmelsen er ny som følge av datalagringsdirektivet, og oppstiller flere vilkår for innhenting. For det første kreves det skjellig grunn til mistanke. Dernest er det lovfestet et strafferammekrav, alternativt et kriminalitetskrav med opplisting av spesifikke lovbrudd. Etter § 210 b bokstav a må mistanken gjelde handlinger som kan medføre fengsel i fire år eller mer. I Prop. 49 L (2010–2011) punkt 12.6 begrunnes strafferammekravet slik:

> «Et vilkår om krav til strafferamme på fire år eller mer reflekterer etter departementets vurdering den graden av inngrep i personvernet som innhenting av data representerer.»

Der det er grunn til å tro at handlingen er utøvet som ledd i aktivitetene til en organisert kriminell gruppe, er strafferammekravet fengsel i tre år eller mer, jf. § 210 b bokstav b. Alternativt kan innhenting skje der kriminalitetskravet etter henvisningene i § 210 b bokstav c er oppfylt.

Innhenting av *lokaliseringsdata* er regulert i straffeprosessloven § 210 c. Den gjelder datasøk i et bestemt område, for eksempel all trafikk på Egertorget lørdag kl. 23.00. Adgangen til å innhente lokaliseringsdata er snevrere enn for trafikkdata. I Prop. 49 L (2010–2011) punkt 12.6 begrunnes forskjellen med at basestasjonssøk er «mer inngripende i forhold til personvernet, blant annet fordi man da får med seg mye overskuddsinformasjon.» Strafferammekravet i bokstav a er derfor satt til fengsel i fem år eller mer. Oppregningen i bokstav c er dessuten søkt avgrenset til handlinger som basestasjonssøk antas å være særskilt nyttig i etterforskningen av. Etter § 210 c bokstav b er strafferammekravet senket til fengsel i tre år eller mer der det er grunn til å tro at handlingen er utøvet som ledd i aktivitetene til en organisert kriminell gruppe.

For trafikk- og lokaliseringsdata gjelder i tillegg et fellesvilkår om at opplysningene må antas å være av vesentlig betydning for etterforskningen. Innhentingen må for øvrig være forholdsmessig etter straffeprosessloven § 170 a.

Politiet og retten kan ikke innhente opplysninger om trafikk- og lokaliseringsdata gjennom vitneprov i større utstrekning enn det som følger av §§ 210 b og 210 c. Dette er fastsatt i ny § 118 a. Bestemmelsen er begrunnet i omgåelseshensyn.

Ut over lovendringene i tilknytning til datalagringsdirektivet, videreføres hjemmelsgrunnlaget i straffeprosessloven § 216 b annet ledd bokstav d for innhenting av trafikkdata.

Dersom kunden samtykker og opphever taushetsplikten, kan teletilbydere utlevere opplysninger om kundens teletrafikk. Dette forutsetter imidlertid at kunden gis kjennskap til begjæringen, og anses derfor lite praktisk.

Straffeprosessloven § 222 d og politiloven § 17 d åpner dessuten for innhenting av trafikkdata i avvergende og forebyggende øyemed. Politiet vil også kunne innhente trafikkdata med hjemmel i den ulovfestede regelen om nødrett.

11.3.2 Domstolsbehandling

Utvalget går inn for obligatorisk domstolsbehandling ved utlevering av trafikkdata, herunder lokaliseringsdata, begrunnet i hensynet til de berørtes rettssikkerhet.

Departementet bemerker at domstolskontroll med innhenting av data anses å være en sentral rettsikkerhetsgaranti. Både innhenting av trafikkdata og lokaliseringsdata krever etter lovendringen rettens kjennelse. Utvalgets forslag er

således gjennomført i straffeprosessloven §§ 210 b og 210.

Retten skal i utgangspunktet sørge for at den som blir rammet snarest mulig blir kjent med kjennelsen, jf. straffeprosessloven § 52 annet ledd. Fra dette utgangspunktet følger et unntak der utsatt underretning om innhenting av data etter §§ 210 b og 210 c er «strengt nødvendig» for etterforskningen, jf. § 210 d.

Om utsatt underretning uttalte departementet følgende i Prop. 49 L (2010–2011) punkt 12.6:

> «Slik utsatt underretning kan være særlig aktuelt i de tilfellene hvor dataene søkes innhentet i en tidlig fase av etterforskningen og før det er foretatt noen pågripelse. Blir den som i slike tilfeller rammes, klar over utleveringspålegget, kan det ofte miste mye av sin effekt. Videre etterforskning, eksempelvis ransaking og beslag, kan dessuten bli vanskeliggjort.»

For å bøte på manglende kontradiksjon i slike tilfeller, plikter retten å oppnevne offentlig advokat for mistenkte, jf. straffeprosessloven § 100 a første ledd første punktum.

Det fremgår ikke eksplisitt av utredningen om Metodekontrollutvalget ønsker å videreføre ordningen med å gi påtalemyndigheten hastekompetanse med etterfølgende domstolskontroll. Denne løsningen er uansett videreført med lovendringene som følge av datalagringsdirektivet, jf. straffeprosessloven §§ 210 b fjerde ledd og § 210 c annet ledd.

11.3.3 Taushetsplikt

Som en konsekvens av kompetanseoverføringen til domstolene, foreslår *utvalget* å frata Post- og teletilsynet (nå Nasjonal kommunikasjonsmyndighet) oppgaven med å gi politiet tilgang til trafikkdata. Utvalget ønsker å gå bort fra den ordningen at tilsynet må vurdere opphevelse av taushetsplikten.

Departementet bemerker at også dette forslaget er i samsvar med senere lovendringer, jf. ekomloven § 2-9. Det rettslige utgangspunktet er at trafikk- og lokaliseringsdata er underlagt taushetsplikt. Taushetsplikten gjelder innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger, jf. ekomloven § 2-9 første ledd.

Fra dette utgangspunktet gjelder to unntak. Taushetsplikten er for det første ikke til hinder for at såkalte abonnementsopplysninger gis til påtalemyndigheten eller politiet, eller annen myndighet i medhold av lov, jf. ekomloven § 2-9 tredje ledd. Dette unntaket gjaldt også forut for gjennomføringen av datalagringsdirektivet.

Det andre unntaket følger av ekomloven § 2-9 nytt femte ledd. Her heter det at taushetsplikten ikke er til hinder for at trafikk- og lokaliseringsdata utleveres til politi og påtalemyndighet i medhold av straffeprosessloven §§ 210 b, 210 c, 216 b eller 222 d, til Politiets sikkerhetstjeneste i medhold av politiloven § 17 d eller til Finanstilsynet i medhold av verdipapirhandelloven § 15-3 annet ledd nr. 3. Innhenting av data forutsetter således ikke lenger Nasjonal kommunikasjonsmyndighets opphevelse av taushetsplikten.

Metodekontrollutvalget går inn for å kunne straffe teletilbydere som bryter taushetsplikt etter politiloven § 17 f, jf. straffeloven 1902 § 121 (straffeloven § 209). Forslaget er i tråd med lovendringene som følge av datalagringsdirektivet. Politiet kan pålegge teletilbyderne taushetsplikt med hjemmel i politiregisterloven § 35 første ledd første punktum og politiloven § 17 f tredje ledd. Overtredelse av slik taushetsplikt kan straffes etter straffeloven 1902 § 121 (straffeloven § 209), så sant vedkommende er gjort oppmerksom på dette.

11.4 Departementets avsluttende bemerkninger

Metodekontrollutvalgets forslag er i all hovedsak fulgt opp ved vedtakelsen av lov 15. april 2011 nr. 11 om gjennomføring av datalagringsdirektivet. Departementet finner på nåværende tidspunkt ikke grunn til å foreta endringer i reglene om utlevering av trafikk- og lokaliseringsdata. Bestemmelsene må vurderes samlet med øvrige lovendringer i tilknytning til datalagringsdirektivet, herunder lagringsplikten, i lys av EU-domstolens avgjørelse 8. april 2014. På oppdrag fra Samferdselsdepartementet og Justis- og beredskapsdepartementet har Hans Petter Graver, professor og dekan ved Universitetet i Oslo, og advokat Henning Harborg utredet om de norske reglene om datalagring er i overenstemmelse med EMK etter EU-domstolens opphevelse av datalagringsdirektivet. Utredningen konkluderer med at det er tvilsomt om den norske lagringsloven vil la seg forene med EMK, særlig sett hen til kravet til begrunnelse og dokumentasjon av nødvendigheten av å lagre data. Videre ser utrederne utfordringer med å skille ut taushetsbelagt informasjon til og fra sjelesørgere, helsepersonell, presse, advokater mv. før materialet utleveres. Konklusjonene i utred-

ningen er ikke til hinder for videreføring av dagens regime for lagring og utlevering til politiet av data fra elektronisk kommunikasjon som ekomtilbyderne lagrer for egne formål. Utredningen ble avgitt 1. oktober 2015 og er til behandling i departementene.

12 Skjult kameraovervåking

12.1 Gjeldende rett

Politiets adgang til å iverksette skjult kameraovervåking i etterforskningsøyemed reguleres av straffeprosessloven § 202 a. Bestemmelsen ble tatt inn i straffeprosessloven ved lov 15. mars 1991 nr. 5 på bakgrunn av innføringen av straffeloven 1902 § 390 b, som satte et generelt forbud mot skjult kameraovervåking på offentlig sted. Sistnevnte bestemmelse er senere erstattet av personopplysningsloven § 40 om varslingsplikt ved kameraovervåking på offentlig sted eller sted hvor en begrenset krets av personer ferdes jevnlig.

Politiet kan iverksette skjult kameraovervåking på offentlig sted når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger som kan medføre høyere straff enn fengsel i seks måneder, jf. straffeprosessloven § 202 a første ledd. Det er ikke noe vilkår at mistanken kan rettes mot en eller flere bestemte personer. Overvåking vil følgelig kunne iverksettes for eksempel der politiet har mistanke om at det på et bestemt sted foregår hyppig omsetning av narkotika eller tyvegods, men uten at mistanken kan rettes mot noen identifisert person, jf. Ot.prp. nr. 56 (1989–90) punkt 12 side 60. Det er heller ikke noe krav om at den straffbare handlingen er begått eller begås på offentlig sted.

I tillegg til kriminalitetskravet, er det et vilkår for å iverksette kameraovervåking at slik overvåking vil være av vesentlig betydning for etterforskningen. Dette såkalte indikasjonskravet forutsetter at overvåkingen på en kvalifisert måte vil være til hjelp for å avdekke de straffbare forholdene, sikre bevis osv. Det er imidlertid ikke nødvendig at skjult kameraovervåking er den eneste mulige etterforskningsmetode i saken, jf. Ot.prp. nr. 56 (1989–90) punkt 12 side 60.

Skjult kameraovervåking på offentlig sted vil nødvendigvis ramme ikke bare den eller de som begår de straffbare handlinger, men også andre personer som måtte ferdes på stedet. Hvorvidt skjult kameraovervåking skal kunne iverksettes vil derfor bero på en avveining av på den ene side hensynet til en effektiv etterforskning og på den annen side hensynet til integriteten til dem som ferdes på stedet, jf. Ot.prp. nr. 56 (1989–90) punkt 4.3 side 36. Dette avgjøres etter en konkret vurdering, hvor det særlig skal legges vekt på alvorlighetsgraden av den straffbare handlingen, hvorvidt det foreligger alternative etterforskningsmetoder, hvor beferdet stedet er osv., jf. Ot.prp. nr. 56 (1989–90) punkt 12 side 60.

Beslutning om bruk av skjult kameraovervåking på offentlig sted treffes av retten, og tillatelse gis for et bestemt tidsrom som ikke må være lengre enn strengt nødvendig og høyst fire uker, jf. straffeprosessloven § 202 a annet ledd. Beslutningen treffes uten at den mistenkte eller den som beslutningen ellers rammer gis adgang til å uttale seg, og beslutningen blir ikke meddelt dem, jf. tredje ledd.

Straffeprosessloven § 202 a gjelder kun for overvåking som skjer på offentlig sted. Begrepet «offentlig sted» skal forstås på samme måte som etter straffeloven § 10 (straffeloven 1902 § 7 første ledd), og omfatter «et sted bestemt for alminnelig ferdsel eller et sted der allmennheten ferdes». At et område er privat eid, utelukker ikke at det kan regnes som et offentlig sted. Således vil begrepet kunne omfatte for eksempel en butikk eller et handlesenter, eller en privateid vei eller lignende som er alminnelig beferdet. Straffeprosessloven § 202 a regulerer ikke kameraovervåking utenfor offentlig sted, slik som i privat bolig eller på annet privat sted. Politiet har følgelig ingen hjemmel til å iverksette slik overvåking. Skjult kameraovervåking på privat sted vil etter omstendighetene kunne rammes av straffeloven § 266 om hensynsløs atferd (straffeloven 1902 § 390 a) og således være straffbart.

Straffeprosessloven § 202 a benytter i dag begrepet «fjernsynsovervåking», som skal forstås i samsvar med reglene i personopplysningloven kapittel VII. Ved lov 20. april 2012 nr. 18 ble terminologien i personopplysningsloven endret, og loven benytter nå begrepet «kameraovervåking». «Kameraovervåking» er i personopplysningsloven § 36 første ledd definert som vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende over-

våkingskamera eller annet lignende utstyr som er fastmontert. Som kameraovervåking anses både overvåking med og uten mulighet for opptak av lyd- og bildemateriale. Definisjonen omfatter også utstyr som lett kan forveksles med en ekte kameraløsning – såkalte dummy-kameraer. Ulike former for overvåking på offentlig sted som faller utenfor denne definisjonen, er antatt å kunne foretas av politiet uten særskilt lovhjemmel, jf. Ot.prp. nr. 56 (1989–90) punkt 12 side 60. Dette gjelder for eksempel overvåking i form av manuell spaning med kikkert eller lignende, eller overvåking ved hjelp av tekniske hjelpemidler, men som ikke har en vedvarende eller regelmessig gjentatt karakter.

12.2 Andre lands rett

I *Danmark* er skjult kameraovervåking av personer som befinner seg på fritt tilgjengelig sted, ikke ansett som et straffeprosessuelt tvangsmiddel. Metoden er derfor ikke særskilt lovregulert, og politiets bruk av den kun underlagt et alminnelig forholdsmessighetskrav, jf. bet. 1298/1995 punkt 5.3.2.2 side 123 flg. Derimot er såkalt «observation» av personer som befinner seg på et ikke fritt tilgjengelig sted, regulert i retsplejeloven (LBK nr 1139 af 24/09/2013) § 791 a. Bestemmelsen oppstiller ulike krav avhengig av hva slags utstyr som benyttes og hvor den som observeres oppholder seg. Etter § 791 a, stk. 1 kan politiet foreta fotografering eller iakttakelse ved hjelp av kikkert eller annet apparat, såfremt dette må antas å være av vesentlig betydning for etterforskningen og denne gjelder lovbrudd som etter loven kan medføre fengselsstraff. Observasjon ved hjelp av fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat er reservert for lovbrudd som kan medføre fengsel i ett år og seks måneder eller mer, jf. stk. 2.

Observasjon av personer som befinner seg i bolig eller annet husrom, ved hjelp av fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat, eller ved hjelp av apparat som anvendes i boligen eller husrommet, er regulert i § 791 a, stk. 3. Det kreves her bestemte grunner til å anta at bevis i saken kan oppnås ved inngrepet, samt at inngrepet må antas å være av avgjørende betydning for etterforskningen. Metoden kan bare benyttes ved lovbrudd som kan medføre fengsel i seks år eller mer, forsettlig overtredelse av straffeloven kapittel 12 (forbrytelser mot statens selvstendighet og sikkerhet) eller 13 (forbrytelser mot statsforfatningen og de øverste statsmyndigheter, terrorisme mv.), befrielse fra fengsel, bistand til rømning, unndragelse fra militærtjeneste, omfattende samfunnsskadelig driftsforstyrrelse, trusler, utpressing og menneskesmugling. Lovbruddet må i tillegg ha medført eller kunne medføre fare for menneskers liv eller velferd eller for betydelige samfunnsverdier.

Observasjon av et ikke fritt tilgjengelig sted som den som påstår å være fornærmet har rådighet over, er ikke omfattet av reglene i bestemmelsen, såfremt den påstått fornærmede har gitt skriftlig samtykke til overvåkingen, jf. stk. 4. Alle former for observasjon er underlagt et generelt forholdsmessighetskrav, jf. stk. 7.

Avgjørelse om bruk av observasjon ved hjelp av fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat treffes av retten ved kjennelse, jf. § 791 a, stk. 8, jf. § 783, stk. 1. Kjennelsen skal angi hvilket sted tillatelsen gjelder. Politiet er gitt hastekompetanse, jf. § 783, stk. 4.

I *Sverige* er politiets adgang til bruk av hemmelig kameraovervåking regulert i rättegångsbalken 27 kap. 20 a til 20 c §§. Metoden innebærer at fjernstyrte tv-kameraer, andra optisk-elektroniske instrumenter eller sammenlignbart utstyr benyttes til optisk personovervåking i etterforskningsøyemed, uten at det opplyses om overvåkingen, jf. 20 a § 1 mom.

Grunnvilkåret for at hemmelig kameraovervåking kan iverksettes er at etterforskningen gjelder et lovbrudd med minstestraff på to års fengsel eller mer, eller visse former for særlig samfunnsfarlig kriminalitet, jf. 20 a § 2 mom. Det samme gjelder ved forsøk på, forberedelse til eller forbund om slikt lovbrudd. Adgangen gjelder også ved andre typer lovbrudd dersom det etter omstendighetene kan antas at lovbruddets straffverdighet overstiger fengsel i to år. Dersom dette kriminalitetskravet er oppfylt, er hemmelig kameraovervåking tillatt i to tilfelle. Det første gjelder dersom noen med skjellig grunn er mistenkt for lovbruddet, og overvåkingen gjelder et sted der det mistenkte kan antas å ville oppholde seg, jf. 20 b §. Dersom ingen bestemt person kan mistenkes for lovbruddet, kan kameraovervåking iverksettes for å overvåke stedet hvor lovbruddet ble begått eller nære omgivelser til dette, såfremt formålet med overvåkingen er å avdekke hvem som med skjellig grunn kan mistenkes for lovbruddet, jf. 20 c §. For begge tilfeller gjelder at avgjørelsen om å iverksette kameraovervåking må være av «synnerlig vikt» for etterforskningen.

Beslutning om å iverksette hemmelig kameraovervåking treffes etter 21 § av retten på begjæring fra påtalemyndigheten. Påtalemyndigheten er gitt hastekompetanse, jf. 21 a §. Rettens beslutning skal angi tidsrommet for tillatelsen, som ikke kan være lenger enn det som er nødvendig og ikke overstige én måned. Beslutningen skal angi hvilket sted tillatelsen gjelder.

Etter den *finske* tvångsmedelslagen 10 kap. 19 § forstås med såkalt «optisk observation» at man iakttar eller gjør opptak av en mistenkt eller av et område eller sted med kamera eller annet utplassert utstyr, metoder eller programvare. Observasjonen kan under ingen omstendighet rettes mot husrom som brukes som permanent bolig, jf. 10 kap. 19 § 2 mom. Derimot kan observasjonen rettes mot mistenkte som befinner seg utenfor husrom som brukes som permanent bolig og mot mistenkte som er frihetsberøvet på grunn av lovbrudd. Observasjonen kan rettes mot et rom eller et annet sted den mistenkte med sannsynlighet kan antas å befinne seg eller besøke.

Vilkårene for å iverksette optisk observasjon varierer med stedet observasjonen rettes mot. Observasjon av såkalte «hemfridsskyddade platser» eller av personer som er frihetsberøvet på grunn av lovbrudd, kan bare foretas ved mistanke om lovbrudd som kan medføre fengsel i fire år eller mer, narkotikalovbrudd, forberedelse til terrorhandling, eller grovt tollrapporteringslovbrudd, jf. 10 kap. 19 § 3 mom. jf. 16 § 3 mom. Beslutning fattes av retten, jf. 20 § 1 mom. «Hemfridsskyddade platser» omfatter etter strafflagen 24 kap. 11 § boliger, fritidsboliger og øvrige rom som er beregnet til bolig, slik som hotellrom, telt, husvogner og fartøyer som kan bebos, trappeoppganger i bolighus, samt gårder som utgjør beboernes private område og de bygninger som er fast forbundet med slike gårder.

For annen optisk observasjon kreves at mistanken gjelder lovbrudd som kan medføre fengsel i minst ett år. Beslutning kan i slike tilfeller fattes av en arrestasjonsbemyndiget tjenestemann, jf. tvångsmedelslagen 10 kap. 20 § 2 mom. Tillatelse gis i alle tilfelle for høyst en måned av gangen.

12.3 Folkerettslige forpliktelser

EMK artikkel 8 nr. 1 beskytter retten til respekt for privatliv, familieliv, hjem og korrespondanse. I kjerneområdet for bestemmelsen ligger den enkeltes rett til å bli vernet mot inngrep i sitt private hjem. Det er derfor klart at skjult kameraovervåking rettet mot private hjem vil utgjøre et inngrep i artikkel 8. Begrepene privatliv og hjem er i praksis tolket relativt vidt og omfatter trolig også privat område som direkte tilstøter et privat hjem – for eksempel en trappeoppgang. Vernet kan også omfatte forretningslokaler, jf. for eksempel *Niemietz mot Tyskland* 16. desember 1992 (sak 13710/88).

For overvåking som skjer *utenfor* det private hjem, er beskyttelsen etter artikkel 8 svakere. EMD har imidlertid anerkjent at det eksisterer et område for interaksjon mellom mennesker som faller inn under privatlivsbegrepet, selv om den foregår på offentlig sted. Hvorvidt det foreligger et inngrep i en slik kontekst vil bero på en konkret vurdering, hvor blant annet de berørtes forventning om å få være i fred står sentralt. I en sak om hemmelig avlytting, *P.G. og J.H. mot Storbritannia* 25. september 2001 (sak 44787/98), uttaler domstolen (avsnitt 57):

> «There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor.»

Det er slått fast i flere saker at monitorering av offentlig tilgjengelig sted ved bruk av sikkerhetskameraer uten opptaksmulighet, ikke utgjør et inngrep i artikkel 8, jf. blant annet *Herbecq mot Belgia* 14. januar 1998 (sak 32200/96). Kommisjonen bemerket i avgjørelsen at «the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person». På grunnlag av dette måtte alt som kunne observeres på stedet betraktes som offentlig opptreden («public behaviour»). Det samme følger av *Perry mot Storbritannia* 17. juli 2003 (sak 63737/00), hvor EMD konstaterte at «the normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention» (avsnitt 40).

Dersom bruken av sikkerhetskameraer går ut over det som kan anses som rimelig og forutsigbart, kan imidlertid vurderingen bli en annen. I Perry-saken var saksforholdet at klageren var mistenkt for en rekke væpnede ran i biler. Da ved-

kommende ikke ønsket å la seg fotografere med sikte på vitnekonfrontasjon, ble fastmonterte sikkerhetskameraer på politistasjonen brukt for å innhente videoopptak av mistenkte. Dette ble gjort ved at et sikkerhetskamera som var i kontinuerlig drift ble justert for å sikre at det fanget opp bilder av den mistenkte. Etter domstolens oppfatning var dette noe annet enn ordinær bruk av sikkerhetskameraer – ettersom kameraet med hensikt hadde blitt manipulert for å fange opp bilder av klageren, samt fordi opptaket ble vist for vitner og senere lagt frem under den offentlige rettssaken mot klageren. Det forelå derfor et inngrep i artikkel 8 (avsnitt 41–42).

I motsetning til ved synlig bruk av sikkerhetskameraer, vil politiets bruk av skjult kameraovervåking til etterforskningsformål normalt ikke være kjent for dem som rammes. Slik overvåking vil dermed ikke ha den samme grad av forutberegnelighet som bruk av synlige kameraer. Til dette kommer at opptakene – i motsetning til ved ren monitorering – blir lagret for å kunne brukes i videre etterforskning og strafforfølgning. Dette øker tiltakets inngripende karakter. Det vises til følgende uttalelse i den tidligere nevnte saken *P.G. og J.H. mot Storbritannia* (avsnitt 57):

> «A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method […].»

Uttalelsen indikerer at det er av vesentlig betydning hvorvidt opptakene som gjøres lagres med tanke på videre systematisk bruk. På denne bakgrunn er det grunn til å tro at politiets bruk av skjult kameraovervåking etter omstendighetene vil utgjøre et inngrep i artikkel 8 – også når overvåkingen skjer på et offentlig sted.

Inngrep som her nevnt kan bare skje på de vilkår som er angitt i EMK artikkel 8 nr. 2. Det følger av bestemmelsen at inngrepet må ha hjemmel i lov og være nødvendig i et demokratisk samfunn av hensyn til visse særskilt angitte formål. Som legitime formål regnes blant annet å forebygge og bekjempe uorden eller kriminalitet. I tillegg til at det må foreligge formell lovhjemmel, innebærer lovkravet at hjemmelen må være tilgjengelig for dem som rammes, samt være formulert på en måte som gjør disse i stand til å forutse lovens konsekvenser, jf. for eksempel *Kopp mot Sveits* 25. mars 1998 (sak 23224/94) avsnitt 55. Ettersom en adgang til å iverksette hemmelig overvåking representerer en særskilt fare for misbruk, må det dessuten finnes adekvate og effektive sikkerhetsmekanismer, jf. for eksempel *Klass m.fl. mot Tyskland* 6. september 1978 (sak 5029/71) avsnitt 50. Som slike sikkerhetsmekanismer regnes blant annet krav om rettslig kontroll med myndighetenes bruk av overvåkingstiltak, jf. *Klass*-saken avsnitt 55.

12.4 Begrepet kameraovervåking

Dagens regel om «skjult fjernsynsovervåking» i straffeprosessloven § 202 a speiler forbudet mot skjult kameraovervåking på offentlig sted i personopplysningsloven § 40. Forbudet skal forstås i samsvar med personopplysningsloven § 36 første ledd, som fikk sin nåværende utforming ved lov 20. april 2012 nr. 18. Ved nevnte lovendring ble begrepet «fjernsynsovervåking» erstattet med «kameraovervåking», og kameraovervåkingsbegrepet for øvrig søkt modernisert og gjort mer teknologinøytralt. Definisjonen av kameraovervåking i personopplysningsloven § 36 første ledd lyder nå slik:

> «Med kameraovervåking menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert. Som kameraovervåking anses både overvåking med og uten mulighet for opptak av lyd- og bildemateriale. Det samme gjelder utstyr som lett kan forveksles med en ekte kameraløsning.»

Under høringen har *Oslo politidistrikt*, med tilslutning fra *Politidirektoratet*, etterlyst en definisjon av kameraovervåkingsbegrepet inntatt i straffeprosessloven § 202 a. Høringsinstansene mener en slik definisjon bør fremgå av bestemmelsen selv, og ikke gjennom en henvisning til personopplysningsloven.

Departementet slutter seg til høringsinstansenes forslag, og går inn for at definisjonen av kameraovervåking skal fremgå uttrykkelig av straffeprosessloven § 202 a. Dette

vil klargjøre hvilke tiltak politiet kan iverksette i medhold av bestemmelsen og forenkle rettsanvendelsen. Hensynet til sammenheng i lovverket tilsier at definisjonen formuleres på samme måte som i personopplysningsloven. Det antas imidlertid at personopplysningsloven § 36 første ledd siste punktum, som omfatter «utstyr som lett kan forveksles med en ekte kameraløsning», ikke vil være relevant for etterforskningsformål. Dette punktum foreslås følgelig unntatt fra definisjonen i straffeprosessloven § 202 a.

12.5 Skjult kameraovervåking fra offentlig sted mot privat sted

12.5.1 Metodekontrollutvalgets forslag

Straffeprosessloven § 202 a gir som nevnt politiet, på nærmere vilkår, anledning til å iverksette skjult kameraovervåking «på offentlig sted». Metodekontrollutvalget uttaler at det i underrettspraksis er gitt tillatelse til å iverksette skjult kameraovervåking etter straffeprosessloven § 202 a også fra offentlig sted mot privat sted – et inngangsparti, jf. utredningen punkt 21.1 side 222 samt punkt 21.4.2 side 224. Etter utvalgets syn åpner straffeprosessloven § 202 a neppe for slik overvåking. Utvalget finner imidlertid at det bør være slik adgang, og foreslår derfor å gjøre det klart at kameraovervåking fra offentlig sted mot privat sted kan finne sted på samme vilkår som overvåking på offentlig sted. Utvalget viser i punkt 21.4.2 til at de samme steder vil kunne observeres av politiet i kraft av den alminnelige handlefrihet:

> «Utvalget finner ikke tungtveiende grunner til at politiet ikke bør ha anledning til å gjennomføre fjernsynsovervåking mot et privat sted, typisk et inngangsparti, når dette skjer som ledd i etterforskingen, og hvor politiet etter den alminnelige handlefriheten vil ha adgang til å observere det samme stedet. Utvalget er oppmerksom på at fjernsynsovervåking vil være et mer vedvarende inngrep, men finner dette ikke avgjørende.»

Metodekontrollutvalget foreslår følgelig at det presiseres i straffeprosessloven § 202 a at politiet har adgang til å iverksette skjult kameraovervåking fra offentlig sted mot privat sted.

12.5.2 Høringsinstansenes syn

Fornyings-, administrasjons- og kirkedepartementet, Politidirektoratet, Riksadvokaten, Kripos, Økokrim, Oslo statsadvokatembeter, Oslo politidistrikt, Telemark politidistrikt, Politiets sikkerhetstjeneste, Norges politilederlag og *Politiets Fellesforbund* støtter Metodekontrollutvalgets forslag. *Advokatforeningen, Forsvarergruppen av 1977* og *Norsk forening for kriminal reform (KROM)* tar avstand fra forslaget.

Fornyings-, administrasjons- og kirkedepartementet poengterer at det her er tale om bruk av skjult kamera rettet mot steder som politiet også ellers vil kunne observere eller overvåke manuelt. Departementet legger likevel til grunn at slik overvåking er mer inngripende enn overvåking av offentlig sted, ettersom den er rettet mot en eller flere konkrete personer. I tillegg vil de fleste ha en forventning om å være mindre iakttatt på privat enn på offentlig sted. Departementet fremhever imidlertid den potensielle effektiviseringsgevinsten ved å tillate slik overvåking, og mener den bør kunne tillates i kombinasjon med streng domstolskontroll:

> «[…] Det er klart at kameraovervåking vil være mer effektivt, og gi mer håndfast informasjon enn manuell overvåking. Samtidig vil det gi mulighet til i ettertid å gå tilbake i opptakene og se på detaljer eller episoder som ikke ville blitt oppfattet ved manuell overvåking. Overvåking vil også kunne vare over lengre tid når den skjer med kamera enn om den skal gjennomføres manuelt. Integritetsinngrepet er derfor større ved kameraovervåking enn ved manuell overvåking. FAD er likevel enig med utvalget i at skjult kameraovervåking av privat sted fra offentlig sted vil innebære en betydelig ressurseffektivisering. Dette, sammenholdt med streng domsstolskontroll for bruk av metoden, tilsier at tiltaket bør kunne tillates.»

Økokrim antar at adgangen til å overvåke fra offentlig mot privat sted vil kunne bli særlig viktig i miljøsaker, ved at den muliggjør filming av for eksempel en jakthytte eller et jakttårn.

12.5.3 Departementets vurdering

Departementet kan i det vesentlige tiltre utvalgets vurderinger når det gjelder skjult kameraovervåking på eller fra offentlig sted. Departementet mener således at dagens regel om skjult kameraovervåking på offentlig sted bør videreføres, og at politiet på samme vilkår bør ha adgang til å iverksette skjult kameraovervåking fra offentlig sted mot privat sted. Det vises til at dette er områder politiet allerede i dag kan observere ved manuell

spaning, og hvor de som ferdes ikke kan ha noen forventning om ikke å bli iakttatt. At det er av betydning hvorvidt det som overvåkes kan observeres av enhver som er til stede, er også lagt til grunn i praksis fra EMD, jf. omtalen i punkt 12.3 ovenfor. Departementet er innforstått med at kameraovervåking utgjør et større inngrep enn manuell observasjon, men har ikke funnet dette avgjørende.

Bruk av skjult kameraovervåking i etterforskningen vil kunne gi mer detaljert og håndfast informasjon enn manuell overvåking av de samme områdene. Adgang til å iverksette slik overvåking fra offentlig mot privat sted vil videre kunne medføre bedre utnyttelse av politiressurser, ved at automatiske hjelpemidler i visse tilfeller kan benyttes i stedet for operativt personell. Overvåkingen vil for eksempel kunne rette seg mot inngangsparti, gårdsrom, hage mv. som er synlig fra offentlig sted. Departementet finner likevel grunn til å understreke at overvåkingen ikke bør kunne innrettes slik at den fanger opp aktivitet som finner sted i private hjem, selv om dette skulle være synlig fra offentlig sted. En slik form for overvåking ville ha karakter av omgåelse av forbudet mot skjult kameraovervåking av private hjem som følger av departementets forslag, jf. punkt 12.6 nedenfor.

12.6 Skjult kameraovervåking på privat sted

12.6.1 Metodekontrollutvalgets forslag

Metodekontrollutvalget går inn for å utvide politiets adgang til å iverksette skjult kameraovervåking til også å gjelde på privat sted, unntatt i privat bolig, jf. utredningen punkt 21.4.3 side 224–225. Utvalget legger til grunn at skjult kameraovervåking på privat sted som utgangspunkt må anses som et større inngrep enn overvåking på offentlig sted. Det mener likevel at man ikke kan forvente å bevege seg helt fritt uten å bli observert av andre på privat sted, for eksempel i en bakgård eller et portrom. Utvalget finner det imidlertid klart at skjult kameraovervåking i privat bolig ikke under noen omstendighet bør tillates.

Som et argument for å tillate kameraovervåking på privat sted legger utvalget særlig vekt på at kameraovervåking vil kunne benyttes i kombinasjon med andre skjulte tvangsmidler, og gjøre disse mer målrettet og således mindre inngripende overfor dem som rammes, se følgende uttalelse i utredningen punkt 21.4.3:

> «Det er særlig i kombinasjon med romavlytting utvalget mener fjernsynsovervåking av privat sted har sin berettigelse. Romavlytting vil som oftest også ramme tredjepersoner, ettersom politiet ikke alltid vil ha oversikt over om mistenkte er til stede eller ikke. Dette er etter utvalgets syn uheldig av hensyn til tredjepersonenes personverninteresser. Ved å kombinere romavlytting med fjernsynsovervåking kan politiet målrette avlyttingen ved å skru på og av avlyttingsutstyret etter om mistenkte er til stede eller ikke. På denne måten vil personvernkrenkelsene overfor tredjepersoner reduseres.»

Utvalget viser videre til at bruk av kameraovervåking i kombinasjon med romavlytting vil kunne redusere politiets ressursbruk. Det legger til grunn at selv om skjult kameraovervåking på privat sted særlig har sin berettigelse i kombinasjon med romavlytting, kan det ikke utelukkes at et slikt tvangsmiddel vil være hensiktsmessig også i kombinasjon med andre tvangsmidler eller i andre sammenhenger.

På denne bakgrunn går Metodekontrollutvalget inn for at skjult kameraovervåking på privat sted, unntatt i privat bolig, bør kunne skje på strenge vilkår og etter tillatelse fra retten. Etter forslaget skal slik overvåking kunne skje ved etterforskning av de samme straffbare handlinger som kommunikasjonsavlytting etter straffeprosessloven § 216 a. Det foreslås videre krav om at overvåkingen må antas å være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort.

12.6.2 Høringsinstansenes syn

Fornyings-, administrasjons- og kirkedepartementet, Politidirektoratet, Riksadvokaten, Kripos, Økokrim, Oslo statsadvokatembeter, Oslo politidistrikt, Politiets sikkerhetstjeneste, Norges politilederlag og *Politiets Fellesforbund* støtter Metodekontrollutvalgets forslag. Også *Telemark politidistrikt* støtter utvalgets forslag, men mener det går for kort. *Advokatforeningen, Forsvarergruppen av 1977* og *KROM* tar avstand fra forslaget.

Advokatforeningen understreker de prinsipielle betenkeligheter ved å tillate økt bruk av skjult overvåking og kontroll av enkeltindividers aktivitet innenfor den private sfære, og motsetter seg at etterforskningsbehov her gis forrang.

Forsvarergruppen av 1977 påpeker at kameraovervåking er et svært inngripende tiltak overfor mistenkte, men i enda større grad overfor tredjepersoner. Gruppen peker på misbruksfaren, samt en frykt for uthuling av respekten for enkeltperso-

ners integritet ved bruk av denne type virkemidler. Gruppen er heller ikke enig i at politiets mulighet til å oppnå tilnærmet det samme ved vanlig spaning, er et argument for å tillate metoden:

> «Enhver må ta høyde for — utenfor husets/leilighetens fire vegger — at man kan bli observert av andre mennesker i nærheten, også om man er på privat sted. Imidlertid er det nok de færreste som holder det som påregnelig at en kan bli filmet i sin egen trappeoppgang, og det gjøres en antagelse fra vår side om at mange ville opplevd dette som svært krenkende.
>
> At politiet vil kunne ha mulighet til å observere mange av de samme bevegelser ved vanlig spaning, er etter vår oppfatning vesentlig annerledes enn å lagre menneskers bevegelser på film over lengre tid, potensielt til gjennomsyn for vesentlig flere enn spanerne selv, og ikke et argument for at fjernsynsovervåkning på privat sted bør kunne tillates. Snarere er det et argument for at man fortsetter å bruke de tradisjonelle metoder på dette feltet, og slik unngår de ideelle kostnadene som slik overvåkning vil medføre, selv om dette nok medfører større økonomiske kostnader.»

På samme måte er *KROM* av den oppfatning at selv om man ikke kan forvente å bevege seg helt fritt uten å bli observert av andre på private steder, er filming en integritetskrenkelse av en helt annen karakter. *KROM* kan heller ikke følge utvalget i at skjult kameraovervåking av privat sted vil redusere behovet for romavlytting.

Kripos, med tilslutning fra *Politidirektoratet*, er derimot enig i utvalgets vurderinger om at skjult kameraovervåking på privat sted vil være aktuelt i tilknytning til blant annet romavlytting. Høringsinstansen peker videre på at metoden også vil være aktuell i andre tilfeller:

> «Kripos er også enig i at skjult fjernsynsovervåking er en egnet metode i andre tilfeller enn som støtte for romavlytting. Eksempelvis egner den seg meget godt når politiet avdekker narkotikadepoter som oppbevares i fellesområder i boligkomplekser. Regelmessig får politiet kunnskap om narkotika som er gjemt i slike områder og det er behov for å knytte mistenkte til narkotikabeslaget. Utfordringen er at det er vanskelig å foreta spaning i slike områder, og det er usikkert når mistenkte vil dukke opp. En egnet fremgangsmåte vil være å erstatte narkotikaen med en lignende pakning og etablere fjernsynsovervåking for bevissikring. Tilsvarende kan man tenke seg om andre viktige bevismidler som er gjemt på privatområde, eksempelvis ransutstyr, penger, drapsvåpen mv.»

Høringsinstansen fremhever også at målrettet kameraovervåking av konkrete steder på privat område kan ivareta hensynet til tredjepersoner bedre enn eksempelvis overvåking av et inngangsparti av en boligblokk, hvor alle som går inn eller ut vil bli filmet.

Telemark politidistrikt mener forslaget går for kort, og argumenterer for at adgangen til å kameraovervåke privat sted også bør omfatte privat bolig:

> «Begrunnelsen for å gi en slik anledning til fjernsynsovervåking er blant annet å effektivisere romavlytting og gjøre slik avlytting mer presis. Denne begrunnelsen tilsier ingen slik begrensning som utvalget foreslår. På de samme vilkår som for kommunikasjonskontroll, eventuelt de vilkår som gjelder for romavlytting, bør det være adgang til skjult fjernsynsovervåking også av beboelsesrom.»

Politidirektoratet kan på sin side ikke se at det foreligger tilstrekkelig tungtveiende grunner til å tillate kameraovervåking i privat bolig.

Oslo politidistrikt, med tilslutning fra *Politidirektoratet*, understreker viktigheten av å angi anvendelsesområdet for den foreslåtte bestemmelsen tydelig. Høringsinstansen har samtidig innspill til forståelsen av begrepet «privat bolig»:

> «Med dette som utgangspunkt vil det likevel oppstå en del grensetilfeller. Hva med et hotellrom som leies for kort tid, eller fengselscelle, lugar el. Som heller ikke er naturlig omtale som privat bolig. Bortsett fra fengselsceller vil disse stedene bare brukes for et kortere tidsrom. Vi antar derfor at dette ikke kan anses som "privat bolig" (med mulig unntak for celle), men er samtidig innforstått med at skjult fjernsynsovervåkning i slike tilfeller lett kan bli ansett for å være et uforholdsmessig inngrep.»

Politidistriktet peker også på problemer knyttet til såkalte dekkleiligheter:

> «Et særlig praktisk tilfelle er de såkalte "dekkleiligheter" som kriminelle ofte benytter seg av. De er gjerne innredet og utstyrt som en "privat

bolig", men de brukes hovedsakelig til å planlegge straffbare handlinger, som oppbevaringssted for narkotika, tyvegods, redskaper og utstyr for bruk ved straffbare handlinger, gjemmested for mistenkte eller etterlyste personer etc. Det kan tenkes at noen av de som eier/leier leiligheten overnatter på stedet fra tid til annen, men at den for øvrig ikke benyttes av noen som ordinære bolig. Vi antar at slike leiligheter ikke faller inn under forbudet mot skjult fjernsynsovervåkning.»

Enkelte høringsinstanser uttaler seg mer konkret om vilkårene for bruk av skjult kameraovervåking på privat sted. *Oslo politidistrikt*, med tilslutning fra *Politidirektoratet*, slutter seg til utvalgets forslag, og anser det som et riktig utgangspunkt å tillate slik overvåking i samme type saker som kommunikasjonsavlytting. *Forsvarergruppen av 1977* og *KROM* kritiserer forslaget, som innebærer at skjult kameraovervåking på privat sted også kan foretas ved etterforskning av simple narkotikaovertredelser etter straffeloven 1902 § 162 første ledd (straffeloven § 231). *KROM* uttaler:

«Utvalgets lovforslag innebærer at det kan fjernsynsovervåkes på privat sted også for simple narkotikaforbrytelser. Etter KROMs syn åpnes det med dette for alt for inngripende skjulte etterforskningsskritt overfor en allerede stigmatisert gruppe og for en enorm mengde uskyldige tredjepersoner som er på vei hjem eller på besøk hos venner og kjente. Dette er etter KROMs syn helt uakseptabelt.»

Heller ikke *Forsvarergruppen av 1977* mener at alvorlighetsgraden i straffeloven 1902 § 162 første ledd (straffeloven § 231) kan forsvare bruk av skjult kameraovervåking på privat sted. Dersom forslaget om skjult kameraovervåking på privat sted blir tatt til følge, fremmer gruppen derfor forslag om å unnta simple narkotikaovertredelser.

NRK fremholder at dersom utvalgets forslag skal aksepteres, bør det nedlegges forbud mot å foreta kameraovervåking av eller mot redaksjonslokaler. Det vises til at slik overvåking vil kunne vise hvilke personer som har vært i kontakt med pressen og dermed kunne avsløre dens kilder. Under enhver omstendighet mener høringsinstansen at de samme begrensninger som gjelder for kommunikasjonskontroll og romavlytting, også bør gjelde for skjult kameraovervåking.

12.6.3 Departementets vurdering

12.6.3.1 Bør det åpnes for skjult kameraovervåking på privat sted?

Departementet går i punkt 12.1.5.3 ovenfor inn for at skjult kameraovervåking av privat sted som kan observeres fra offentlig sted, bør tillates. Spørsmålet her er om slik overvåking også bør tillates på privat sted som *ikke* er synlig fra offentlig sted. Etter departementets syn er overvåking av områder som ikke kan ses fra offentlig tilgjengelig sted, vesentlig mer inngripende enn overvåking av sted som kan observeres av enhver. Som Metodekontrollutvalget påpeker, er det likevel ikke slik at man her kan forvente å bevege seg fritt, helt uten å bli iakttatt av andre mennesker. Eksempelvis vil fellesarealer som bakgård, portrom, loft og kjeller regulært være beferdet av naboer, gjester mv., som kan overvære eventuell aktivitet på stedet.

En adgang til å iverksette skjult kameraovervåking antas å kunne være av etterforskningsmessig betydning når politiet får kunnskap om narkotika, våpen, utstyr mv. som oppbevares på steder hvor det er vanskelig å foreta spaning. Dette gjelder for eksempel når man finner slike gjenstander i fellesområder i bygårder som ikke er offentlig tilgjengelig. Ved å iverksette skjult kameraovervåking på stedet vil politiet kunne observere personer som oppsøker gjenstandene, og dermed lettere kunne knytte mistenkte til funnet.

Som Metodekontrollutvalget påpeker, vil skjult kameraovervåking på privat sted dessuten kunne være et effektivt virkemiddel i kombinasjon med andre skjulte tvangsmidler. Dette gjelder eksempelvis romavlytting eller kommunikasjonskontroll. Ved bruk av romavlytting alene kan det være nødvendig å lytte på samtalene til tredjepersoner selv om mistenkte ikke er til stede, for å kunne fastslå om vedkommende er der. Ved å kameraovervåke for eksempel inngangspartiet til lokalet som avlyttes, vil man kunne klargjøre om mistenkte på et bestemt tidspunkt befinner seg i lokalet. Dermed vil romavlyttingen kunne skrus av og på ettersom hvorvidt mistenkte er til stede, slik at utenforstående tredjepersoner i mindre grad rammes av avlyttingen. Departementet antar derfor at kameraovervåkingen vil kunne bidra til å gjøre bruken av romavlytting mer målrettet og således mindre inngripende. En slik bruk vil videre kunne redusere behovet for manuell spaning i forbindelse med bruk av romavlytting, og således føre til besparelser i politiressurser.

Departementet går på denne bakgrunn inn for at politiet, på strenge vilkår, bør gis adgang til å iverksette skjult kameraovervåking på visse pri-

vate steder. På grunn av de sterke personvernhensyn som gjør seg gjeldende, er departementet samtidig enig med utvalget i at adgangen til å iverksette skjult kameraovervåking ikke bør omfatte private hjem. Det er ikke vanskelig å argumentere for at også denne typen overvåking kunne utgjøre et effektivt virkemiddel i etterforskningen. Dette må imidlertid stilles opp mot den tungtveiende interesse hver enkelt har i å ha et område innenfor husets fire vegger hvor man kan få være helt i fred. Dette ligger i kjerneområdet for de verdier som er beskyttet av EMK artikkel 8 og Grunnloven § 102. De samme hensyn ligger også til grunn for forbudet mot ransaking av private hjem i forebyggende øyemed etter politiloven § 17 d annet ledd siste punktum.

Hvorvidt noe skal anses som privat bolig, og derfor ikke kan kameraovervåkes, må bero på om begrunnelsen for en sterkere beskyttelse gjør seg gjeldende. Her vil rekkevidden av Grunnloven § 102 kunne tjene som rettesnor. Således vil husværets art ikke i seg selv være avgjørende, slik at eksempelvis en hytte, husbåt eller campingbil omfattes av forbudet, dersom den benyttes som noens permanente bolig. Derimot antas unntaket normalt ikke å gjelde for steder hvor personer oppholder seg over kortere tidsrom, slik som fritidsboliger, hotellrom, kontorlokaler og lignende. Det legges likevel til grunn at personverninteresser i slike tilfeller vil kunne gjøre seg gjeldende i varierende grad, avhengig av stedets karakter og bruk. Dette vil etter omstendighetene kunne komme inn som et viktig moment i forholdsmessighetsvurderingen etter straffeprosessloven § 170 a.

Departementet legger til grunn at såkalte dekkboliger vanligvis ikke er å anse som et privat hjem, og derfor ikke vil falle inn under unntaket. Dette er steder som er innredet for å se ut som et privat hjem, men som i realiteten brukes til å planlegge kriminelle handlinger, skjule mistenkte, oppbevare utstyr og utbytte mv. Personer som oppholder seg her vil følgelig sjelden ha noen beskyttelsesverdig interesse i ikke å bli utsatt for skjult kameraovervåking. Departementet er innforstått med at det vil kunne by på visse bevisproblemer å avgjøre hvorvidt noe som ser ut som et privat hjem, i realiteten er en dekkbolig. Særlig gjelder dette på et tidlig stadium i etterforskningen. Videre vil det trolig kunne være en uklar grense mellom faktiske dekkboliger og steder som brukes som alminnelig bolig, men som også fungerer som åsted for planlegging av kriminelle handlinger, skjulested for mistenkte eller lignende. Det vil her være opp til retten, gjennom en alminnelig bevisvurdering, å avgjøre hvorvidt det aktuelle husværet er å anse som et privat hjem og dermed omfattes av unntaket. I den sammenheng er det sentralt at avgjørelse om skjult kameraovervåking av privat sted treffes ved kjennelse, med de krav til begrunnelse dette stiller, jf. punkt 12.7 nedenfor.

12.6.3.2 Ved hvilke lovbrudd bør metoden kunne benyttes?

Metodekontrollutvalget foreslår at skjult kameraovervåking på privat sted skal kunne iverksettes i samme typer saker som kan gi grunnlag for kommunikasjonsavlytting etter straffeprosessloven § 216 a. Dette innebærer at metoden som utgangspunkt kan benyttes i etterforskningen av alle lovbrudd som har en strafferamme på fengsel i ti år eller mer. Departementet anser dette for å være et riktig utgangspunkt, som sikrer at en så vidt inngripende etterforskningsmetode bare kan benyttes i saker som gjelder alvorlig kriminalitet.

Utvalgets forslag innebærer videre at skjult kameraovervåking på privat sted – i likhet med kommunikasjonsavlytting – også kan benyttes i etterforskningen av visse særskilt angitte lovbrudd med lavere strafferamme enn fengsel i ti år. Forslaget medfører at skjult kameraovervåking på privat sted blant annet kan benyttes ved enkelte overtredelser av straffeloven 1902 kapittel 8 om forbrytelser mot statens selvstendighet og sikkerhet og kapittel 9 om forbrytelser mot Norges statsforfatning og statsoverhode (straffeloven kapittel 17), samt ved narkotikaovertredelser, grov menneskesmugling og forsettlig eller uaktsom overtredelse av eksportkontrolloven. Departementet er enig i at dette er lovbrudd som på grunn av sine samfunnsskadelige konsekvenser eller særlige etterforskningsmessige utfordringer, kan forsvare en adgang til også å kunne iverksette skjult kameraovervåking på privat sted.

Som det fremgår av proposisjonen kapittel 7, foreslår departementet å utvide adgangen til å iverksette kommunikasjonsavlytting etter straffeprosessloven § 216 a i noe større grad enn det som følger av utvalgets forslag. Etter forslaget skal kommunikasjonsavlytting kunne benyttes i etterforskningen av saker om overgrepsbilder av barn etter straffeloven § 311 (straffeloven 1902 § 204 a), frihetsberøvelse etter §§ 254 (straffeloven 1902 § 223) og simpel menneskehandel etter § 257 (straffeloven 1902 § 224), samt om grov menneskesmugling etter utlendingsloven § 108 femte ledd. Etter departementets oppfatning tilsier de samme hensyn som begrunner bruk av kommunikasjonsavlytting i disse sakstypene, at politiet også bør kunne

iverksette skjult kameraovervåking på privat sted. Det vises for så vidt til drøftelsen i punkt 7.4, hvor kriminalitetskravet er inngående behandlet.

12.6.3.3 Øvrige vilkår

I tillegg til kravet om skjellig grunn til mistanke om at det er begått en handling av en viss alvorlighetsgrad, foreslår departementet at skjult kameraovervåking på privat sted bare skal kunne benyttes dersom det må antas at dette vil være av vesentlig betydning for å oppklare saken (indikasjonskrav). Kravet innebærer at det må antas at overvåkingen på en kvalifisert måte vil være til hjelp for å avdekke de straffbare forholdene, sikre bevis osv. Det foreslås videre at metoden bare skal kunne benyttes dersom oppklaring ellers i vesentlig grad vil bli vanskeliggjort (subsidiaritetskrav). Tilsvarende vilkår gjelder også for andre inngripende etterforskningsmetoder, som for eksempel personnær teknisk sporing etter straffeprosessloven § 202 c, kommunikasjonsavlytting etter § 216 a eller annen kommunikasjonskontroll etter § 216 b og romavlytting etter § 216 m.

Departementet har videre merket seg NRKs merknader knyttet til skjult kameraovervåking av redaksjonslokaler, og er enig i at pressens kildevern bør hensyntas ved utformingen av reglene om skjult kameraovervåking på privat sted. Ved lov 21. juni 2013 nr. 86 ble straffeprosessloven §§ 216 c og 216 m endret, for å sikre at reglene om kommunikasjonskontroll og romavlytting respekterer pressens rett til kildevern. Det ble der innført et krav om særlige grunner for å tillate kommunikasjonskontroll overfor redaktører og journalister, og for å tillate romavlytting av redaksjonslokaler eller tilsvarende. Etter departementets syn bør samme begrensning gjelde i relasjon til skjult kameraovervåking av redaksjonslokale eller tilsvarende sted hvor redaktør eller journalist fører samtaler av yrkesmessig art. Det vises for så vidt til begrunnelsen gitt i Prop. 147 L (2012–2013) punkt 8 side 133 flg.

12.7 Formelle krav

Etter gjeldende rett treffes rettens avgjørelse om iverksettelse av skjult kameraovervåking på offentlig sted etter straffeprosessloven § 202 a ved beslutning. Metodekontrollutvalgets forslag til ny utforming av § 202 a medfører at avgjørelse om skjult kameraovervåking skal skje ved kjennelse, både ved overvåking på eller fra offentlig sted og overvåking på privat sted. Endringen er ikke nærmere kommentert.

Oslo politidistrikt, med tilslutning fra *Politidirektoratet*, mener rettens avgjørelse om skjult kameraovervåking på eller fra offentlig sted fremdeles bør skje ved beslutning:

> «En begjæring til retten etter bestemmelsens første ledd bør, som i dag, behandles som kontorforretning. Denne fremgangsmåten har vært benyttet siden bestemmelsen ble innført ved lov 15. mars 1991 nr. 5, og vi kan ikke se at det er fremkommet vektige argumenter. Den mer omstendelige behandlingen med rettsmøte, oppnevning av advokat i medhold av § 100a m.v. savner etter vår mening tilstrekkelig begrunnelse. Når det gjelder eventuell oppnevning av 100a-advokat bemerkes at det ikke er et krav om noen bestemt mistenkt, for å kunne treffe beslutning etter dagens 202a (utkastet 202a, 1. ledd). Det kan være at politiet begjærer tillatelse til overvåkning av en offentlig plass hvor det er mistanke om at det omsettes narkotika eller tyvegods. I slike tilfeller vil det ikke være noen mistenkt som § 100a-advokaten kan representere.»

D e p a r t e m e n t e t har vurdert hvorvidt avgjørelser om skjult kameraovervåking *på eller fra offentlig sted* skal treffes ved kjennelse, slik det følger av utvalgets forslag. Dette er den alminnelige ordning ved de fleste andre typer skjulte tvangsmidler, slik som for eksempel personnær teknisk sporing etter straffeprosessloven § 202 c, kommunikasjonskontroll etter § 216 a eller § 216 b og romavlytting etter § 216 m. Disse tvangsmidlene skiller seg imidlertid fra skjult kameraovervåking på eller fra offentlig sted ved at det for sistnevnte ikke er krav om at mistanken skal rette seg mot en eller flere bestemte personer. Ettersom overvåkingen skjer på sted som kan iakttas av enhver, må metoden også anses mindre inngripende enn andre skjulte tvangsmidler som er nevnt her. På denne bakgrunn er departementet enig med Oslo politidistrikt i at det er forsvarlig at tillatelse til å iverksette skjult kameraovervåking på eller fra offentlig sted også i fremtiden gis ved formløs beslutning.

Adgangen til å iverksette skjult kameraovervåking *på privat sted* er ny og utgjør et mer inngripende tiltak enn overvåking på offentlig sted. Dette tilsier etter departementets vurdering at metoden kombineres med sterke rettssikkerhetsgarantier. Departementet tiltrer derfor utvalgets forslag om at avgjørelser om skjult kameraovervåking på privat sted skal fattes ved kjennelse. I motsetning til ved formløs beslutning, er det krav

om at kjennelser skal begrunnes, jf. straffeprosessloven § 52. Dette synliggjør at avgjørelsen er fattet på korrekt grunnlag og representerer således en viktig rettssikkerhetsgaranti.

Som en ytterligere rettssikkerhetsgaranti foreslår departementet at det i saker om skjult kameraovervåking på privat sted, skal oppnevnes offentlig advokat for den mistenkte. Dette gjøres ved at det inntas en henvisning til den relevante bestemmelsen i straffeprosessloven § 100 a. Advokaten skal ivareta den mistenktes interesser i forbindelse med rettens behandling av begjæringen. En tilsvarende regel finnes for andre typer skjulte tvangsmidler, herunder hemmelig ransaking etter § 200 a, teknisk sporing etter § 202 c, kommunikasjonskontroll etter § 216 a eller § 216 b og romavlytting etter § 216 m. Det vises for øvrig til punkt 6.6.7.

12.8 Hastekompetanse

I henhold til Metodekontrollutvalgets forslag skal kompetansen til å tillate skjult kameraovervåking både på eller fra offentlig sted og på privat sted, tilligge retten. Dette er i samsvar med det som følger av dagens regel om kameraovervåking på offentlig sted i straffeprosessloven § 202 a. Det samme er hovedregelen ved bruk av de fleste andre typer skjulte tvangsmidler.

Metodekontrollutvalget har ikke drøftet behovet for å gi påtalemyndigheten hastekompetanse. Flere høringsinstanser, herunder *Politidirektoratet, Riksadvokaten, Kripos* og *Oslo politidistrikt*, etterlyser imidlertid en slik kompetanse. *Riksadvokaten* illustrerer behovet med situasjonen der politiet for eksempel finner et parti narkotika i forbindelse med en hemmelig ransaking. I slike tilfeller vil mye kunne skje ved depotet innen man har rettens kjennelse.

Under henvisning til dagens bestemmelse bemerker *Kripos* og *Oslo politidistrikt* at man nå håndterer hastesituasjoner ved at kun «vedvarende» kameraovervåking anses å kreve rettens tillatelse. *Oslo politidistrikt*, med tilslutning fra *Politidirektoratet*, uttaler:

> «§ 202a — slik den lyder i dag — har ingen hastebestemmelse. Med en utvidelse av bestemmelsen som foreslått av utvalget, bør det gis en hastebestemmelse på samme måte som ved §§ 200a, 216a, m.fl. Dagens bestemmelse regulerer som nevnt kun «vedvarende» fjernsynsovervåkning, slik at overvåkning som pågår i et kortere tidsrom, ikke kan anses som «vedvarende», og således falle utenfor det som reguleres i bestemmelsen. Dette har så langt avhjulpet det problemet som oppstår når det haster å få satt i gang overvåkingen.»

D e p a r t e m e n t e t er enig med de høringsinstansene som har uttalt seg i at det er behov for å gi påtalemyndigheten hastekompetanse til å iverksette skjult kameraovervåking. Som Riksadvokaten påpeker kan dette for eksempel være aktuelt i saker hvor man i forbindelse med en ransaking finner et parti narkotika eller lignende, og derfor ønsker å iverksette kameraovervåking umiddelbart. Likeledes kan det tenkes at et behov for å iverksette skjult kameraovervåking oppstår utenom kontortid, i helg eller på helligdag, når man ikke har mulighet til å innhente rettens samtykke.

Etter departementets syn bør påtalemyndighetens kompetanse fremgå uttrykkelig av loven, hva gjelder både overvåking på eller fra offentlig sted og overvåking på privat sted. Dette harmonerer også med løsningen ved andre typer skjulte tvangsmidler, slik som teknisk sporing etter straffeprosessloven § 202 c, kommunikasjonskontroll etter straffeprosessloven § 216 a eller § 216 b og romavlytting etter straffeprosessloven § 216 m. Det foreslås derfor at påtalemyndigheten gis kompetanse til å beslutte skjult kameraovervåking i tilfeller hvor det ved opphold er stor fare for at etterforskningen vil lide, etter mønster av straffeprosessloven § 216 d.

12.9 Innbruddshjemmel

Metodekontrollutvalget konkluderer i sin utredning med at det vil være nødvendig for politiet med en innbruddshjemmel for å bruke skjult kameraovervåking på privat sted. Det vises til at selv om det i prinsippet kan innhentes samtykke fra for eksempel gårdeier, styret i et borettslag eller lignende, vil hensynet til diskresjon rundt tvangsmiddelbruken her stå sentralt. Utvalget går derfor inn for at politiet gis hjemmel til å foreta innbrudd for å plassere nødvendig utstyr for å kunne gjennomføre overvåkingen.

Politidirektoratet, Riksadvokaten, Kripos og *Oslo politidistrikt* støtter uttrykkelig forslaget om en innbruddshjemmel i straffeprosessloven § 202 a. De to sistnevnte påpeker imidlertid at en slik innbruddsadgang synes uteglemt i utformingen av bestemmelsen.

D e p a r t e m e n t e t slutter seg til de vurderinger Metodekontrollutvalget har gjort om behovet for innbruddshjemmel i straffeprosessloven § 202 a. Etter hva departementet kan se, er utval-

gets konklusjon på dette punktet likevel ikke reflektert i den foreslåtte lovbestemmelsen. Det foreslås derfor at en slik hjemmel uttrykkelig inntas, etter mønster av straffeprosessloven § 216 m femte ledd.

12.10 Underretningsplikt

I proposisjonen her punkt 6.10 foreslås å gjennomføre en enhetlig regulering av plikten til underretning ved bruk av skjulte tvangsmidler. Av hensyn til konsekvens i regelverket, bør reglene om skjult kameraovervåking etter departementets syn utformes i tråd med dette.

Etter gjeldende rett foreligger ingen underretningsplikt ved bruk av skjult kameraovervåking på offentlig sted etter straffeprosessloven § 202 a. Etter departementets syn er det heller ikke hensiktsmessig å innføre underretningsplikt ved overvåking *på eller fra offentlig sted*. Det vises til at slik overvåking kan iverksettes selv om det ikke foreligger mistanke mot en eller flere bestemte personer. Overvåkingen vil dessuten potensielt kunne ramme en stor gruppe individer, som ofte kan være vanskelig å identifisere. Som påpekt under punkt 6.10.2.4, vil en plikt til å underrette enhver som rammes av metodebruken i slike tilfeller være meget ressurskrevende for politiet og ikke gi noen klar personvernmessig gevinst.

I henhold til forslaget om skjult kameraovervåking *på privat sted* kan metoden benyttes når «noen med skjellig grunn mistenkes» for en handling av en viss alvorlighet. Følgelig kan slik overvåking bare iverksettes når mistanken er rettet mot en eller flere bestemte personer. Metodens inngripende karakter tilsier her at det er større grunn til at mistenkte i ettertid underrettes om overvåkingen. Departementet finner derfor at mistenkte som hovedregel bør underrettes om bruk av skjult kameraovervåking på privat sted. Videre bør underretning også gis til den som har rådigheten over det aktuelle stedet, når dette er en annen enn den mistenkte.

Det vises for øvrig til proposisjonen punkt 6.10.

12.11 Skjult kameraovervåking i avvergende og forebyggende øyemed

Metodekontrollutvalget fremholder i utredningen punkt 21.4.5 side 225 at de hensyn som taler for å tillate skjult kameraovervåking fra offentlig mot privat sted, samt på privat sted unntatt privat bolig, gjør seg gjeldende også der politiet søker å avverge eller forebygge alvorlige straffbare handlinger. En adgang til bruk i avvergende og forebyggende øyemed gjelder allerede i dag for skjult kameraovervåking på offentlig sted, jf. straffeprosessloven § 222 d og politiloven § 17 d, som begge viser til straffeprosessloven § 202 a. Ettersom utvalget ikke vil åpne for overvåking i privat bolig, kan det ikke se at tvangsmiddelbruken vil komme i konflikt med Grunnloven § 102.

KROM er uenig med utvalget i at private steder som trappeoppgang, kjellerrom og loft i sameie faller utenfor det Grunnloven § 102 er ment å beskytte. KROM kan ikke se at det er grunn til å forskjellsbehandle dem som bor i enebolig og dem som bor i sameie eller borettslag, når det gjelder hva som hører til deres hus. Ingen andre høringsinstanser har uttalt seg om adgangen til å benytte skjult kameraovervåking i avvergende og forebyggende øyemed.

Departementet kan i det vesentlige slutte seg til utvalgets vurderinger når det gjelder skjult kameraovervåking i avvergende og forebyggende øyemed. En mener således at det bør være adgang til overvåking både på eller fra offentlig sted og på privat sted som ikke er privat hjem, også for å forebygge eller avverge alvorlige straffbare handlinger. Departementet finner at slik tvangsmiddelbruk ikke vil være i strid med Grunnloven § 102, og peker særlig på at overvåkingen under ingen omstendighet kan rettes mot private hjem.

Som følge av metodens inngripende karakter finner departementet imidlertid at det i tillegg til de alminnelige vilkår bør kreves «særlige grunner» for å iverksette skjult kameraovervåking *på privat sted* for å forebygge eller avverge en straffbar handling. Et tilsvarende krav gjelder allerede i dag ved bruk av hemmelig ransaking etter straffeprosessloven § 200 a, personnær teknisk sporing etter § 202 c, kommunikasjonsavlytting etter § 216 a og romavlytting etter § 216 m, jf. henholdsvis straffeprosessloven § 222 d tredje ledd annet punktum og politiloven § 17 d annet ledd annet punktum. Det foreslås derfor at straffeprosessloven § 202 a annet ledd om skjult kameraovervåking på privat sted legges til i opplistingen i de to sistnevnte bestemmelsene.

Det vises for øvrig til proposisjonen kapittel 13, hvor vilkårene for skjult metodebruk i forebyggende og avvergende øyemed behandles i nærmere detalj.

13 Tvangsmiddelbruk i avvergende og forebyggende øyemed

13.1 Innledning

De fleste reglene om bruk av skjulte tvangsmidler krever at det er skjellig grunn til å tro at det begås eller er begått et lovbrudd av en viss alvorlighetsgrad. Ved lov 17. juni 2005 nr. 87 ble imidlertid politiet gitt adgang til å anvende skjulte tvangsmidler for å innhente informasjon med sikte på å *avverge* bestemte former for organisert og annen alvorlig kriminalitet, jf. straffeprosessloven § 222 d. Samtidig ble det innført en hjemmel i politiloven § 17 d til å bruke tvangsmidler for å *forebygge* kriminalitet. Skillet mellom forebyggende og avvergende metodebruk knytter seg til grensedragningen mellom generell forebyggende virksomhet og strafferettslig etterforskning. Forskjellen i begrepsbruk markerer at en – når metodebruken skjer som ledd i etterforskning – i tid gjerne befinner seg nærmere handlingen som søkes forhindret, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.1 side 60.

Departementet understreket at PST, i likhet med politiet for øvrig, som utgangspunkt og hovedregel bare skal kunne ta i bruk tvangsmidler etter at etterforskning er satt i verk, jf. Ot.prp. nr. 60 (2004–2005) punkt 9.3.6.4 side 124. I hovedsak foreslo derfor departementet at PSTs behov for økt bruk av tvangsmidler skulle dekkes ved å åpne for avvergende bruk av tvangsmidler som ledd i etterforskning, jf. straffeprosessloven § 222 d. For å dekke PSTs behov for økt metodetilgang på en tilfredsstillende måte, var det imidlertid nødvendig å senke mistankekravet ytterligere for noen få straffbare forhold. Fordi slik tvangsmiddelbruk skjer utenfor etterforskning, foreslo departementet å plassere hjemmelen i politiloven som en ny § 17 d. Dersom en sak begynner som en sak om forebygging, og på et tidspunkt går over i etterforskning, må den fortsatte bruken av tvangsmidler hjemles i straffeprosessloven, og tillatelse fra retten må innhentes på ny etter reglene i den loven.

13.2 Internasjonale forpliktelser

Bruk av tvangsmidler i avvergende og forebyggende øyemed reguleres i hovedsak av de samme internasjonale forpliktelsene som bruk av tvangsmidler i oppklaringssammenheng. Særlig relevant er retten til privatliv, vernet i blant annet FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 17 og Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8. På samme måte som bruk av tvangsmidler i etterforskningsøyemed, vil bruk av tvangsmidler i avvergende og forebyggende øyemed kunne utgjøre inngrep i denne rettigheten.

SP artikkel 17 verner mot «vilkårlige eller ulovlige» inngrep. FNs menneskerettighetskomité har på generelt grunnlag uttalt at inngrep må være basert på relevant og detaljert lovgivning for ikke å stride med konvensjonen.

SP artikkel 17 er ikke ansett å gå lenger enn EMK artikkel 8. Etter EMK artikkel 8 vil inngrepet være i overensstemmelse med konvensjonen dersom de tre vilkårene i artikkel 8 (2) er oppfylt: Tvangsmiddelbruken må være i «samsvar med loven», forfølge et legitimt formål og bli ansett «nødvendig i et demokratisk samfunn».

Det første vilkåret inneholder to elementer: Det må eksistere et rettslig grunnlag i nasjonal rett, og hjemmelen må være tilstrekkelig tilgjengelig og klar til at borgeren kan forutse sin rettsstilling, jf. punkt 5.2 ovenfor. Ved bruk av tvangsmidler har EMD lagt vekt på at nasjonal rett må inneholde rettssikkerhetsgarantier som verner mot vilkårlig maktutøvelse.

Et eksempel på dette er *Gillan og Quinton mot Storbritannia,* 12. januar 2010 (nr. 4158/05). Saken dreide seg om bestemmelser i den britiske terrorlovgivningen som ga britiske politikonstabler vid kompetanse til å stoppe og ransake personer i det offentlige rom uten noe spesielt krav til mistanke. EMD anså ransakingen som et inngrep i retten til privatliv og konkluderte med at inngrepet ikke var «i samsvar med loven». Dette til tross for at tvangsmiddelbruken hadde grunnlag i nasjonal lov og at det var gitt en detaljert beskrivelser av hvordan ransakingen skulle foregå.

Begrunnelsen var at kompetansen verken var tilstrekkelig begrenset eller underlagt tilstrekkelige rettssikkerhetsgarantier til å forhindre misbruk (avsnitt 87). Det forelå dermed en krenkelse av konvensjonen.

Når det gjelder vilkåret om at inngrepet må forfølge et legitimt formål, nevner artikkel 8 (2) eksplisitt flere av hensynene bak behovet for avvergende og forebyggende tiltak. Disse er «den nasjonale sikkerhet», «offentlige trygghet», «å forebygge uorden eller kriminalitet» («prevention of disorder or crime») og «å beskytte andres rettigheter og friheter». Det kan ikke være tvil om at politiets og PSTs arbeid for å forhindre og forebygge alvorlig kriminalitet omfattes av formålet. Hovedinntrykket er at domstolen i liten grad prøver angitte formålsangivelser, se *Leander mot Sverige* (sak 9248/81) avsnitt 49.

Det tredje vilkåret er at inngrepet må være «necessary in a democratic society», jf. artikkel 8 (2). Det må vurderes hvorvidt midlene som ble brukt var forholdsmessige sett i forhold til det legitime formålet. Det må i den forbindelse foretas en avveining mellom individets interesse etter artikkel 8 (1) og statens behov for å avverge eller forebygge kriminell aktivitet etter artikkel 8 (2). Se som eksempel *Murray mot Storbritannia,* 28. oktober 1994 (sak 14310/88) (storkammer) avsnitt 90 og 91. Saken gjaldt arrestasjonen av en kvinne som var mistenkt for å ha bidratt til finansiering av våpen til det amerikanske IRA. EMD uttalte følgende:

> «[…] the responsibility of an elected government in a democratic society to protect its citizens and its institutions against the threats posed by organised terrorism and the special problems involved in the arrest and detention of persons suspected of terrorist-linked offences […] These two factors affect the fair balance that is to be struck between the exercise by the individual of the right guaranteed to him or her under paragraph 1 of Article 8 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) for the State to take effective measures for the prevention of terrorist crimes (see, mutatis mutandis, the above-mentioned Klass and Others judgment, p. 28, para. 59).»

Klass m.fl. mot Tyskland, 6. september 1978 (nr. 5029/71) (plenum) dreide seg om fem tyske advokater som klaget på tysk lovgivning som ga myndighetene kompetanse til å overvåke deres post- og telefonkorrespondanse, uten plikt til å informere om overvåkningen etterpå. EMD uttalte (avsnitt 59):

> «The Court agrees with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention.»

Domstolen prøver i liten grad statenes vurdering av hvilke metoder som bør tillates for å bekjempe alvorlig kriminalitet. Statene er i så måte gitt en nokså vid skjønnsmargin. Likevel står ikke statene helt fritt, jf. *Klass m.fl. mot Tyskland* (avsnitt 49):

> «As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. […]
>
> Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.»

Statene har altså en skjønnsmargin i valg av ulike metoder for å ivareta offentlig sikkerhet, og dette omfatter bruk av tvangsmidler i avvergende og forebyggende øyemed. EMD har ikke avvist slik bruk av tvangsmidler i seg selv, se for eksempel *Gillan og Quinton mot Storbritannia* vist til ovenfor. Samtidig prøver domstolen nokså inngående om kompetansehjemlene er tilstrekkelig forutsigbare og tilgjengelige, herunder om det er etablert betryggende rettssikkerhetsgarantier.

Europarådet vedtok 11. juli 2002 retningslinjer for kampen mot terrorisme innenfor rammen av menneskerettighetene («Guidelines on human rights and the fight against terrorism»). Retningslinjens fortale understreker at terrorisme undergraver menneskerettigheter og demokrati, og at statene har plikt til å beskytte personer innenfor deres jurisdiksjon mot terrorisme (punkt I). Dette bygger blant annet på at EMD i *Osman mot Storbritannia*, 28. oktober 1998 (nr. 23452/94) (storkammer) avsnitt 115 tolket EMK artikkel 2 slik at bestemmelsen «in certain well-defined circumstances» påla statene en positiv forpliktelse til å

iverksette preventive tiltak for å beskytte ett individ fra et annet individs kriminelle handlinger. Retningslinjene vektlegger videre at også antiterror-tiltak må ha et presist lovgrunnlag og verken være vilkårlige eller diskriminerende (punkt III og II). Når det gjelder tiltak som griper inn i privatlivet til individer, fremhever retningslinjene at det må være mulig å prøve lovligheten av tiltakene for en domstol (punkt VI).

13.3 Andre lands rett

13.3.1 Svensk rett

I Sverige er utgangspunktet at bruk av skjulte tvangsmidler krever at det pågår etterforskning («förundersökning»), og i de fleste tilfelle forutsettes også at det foreligger skjellig grunn til mistanke mot personen som tvangsmiddelbruken retter seg mot, jf. Rättergångsbalken (1942:740) 27 kap. Det finnes imidlertid to egne lover som muliggjør bruk av skjulte tvangsmidler i avvergende og forebyggende øyemed. Dette er *lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott* og *lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*. Etter disse lovene er det ikke krav om at etterforskning pågår. Det finnes for øvrig enkelte bestemmelser som har til hensikt å forhindre lovbrudd i *lagen (1991:572) om särskild utlänningskontroll*, men denne kan kun legges til grunn i meget spesielle situasjoner og vil ikke behandles nærmere her.

Loven fra 2007 regulerer bruk av hemmelig avlytting av elektronisk kommunikasjon, hemmelig overvåking av elektronisk kommunikasjon, hemmelig kameraovervåking og postkontroll for å forhindre lovbrudd, jf. 1 § og 4 §. Derimot kan hemmelig romavlytting ikke anvendes i preventivt øyemed.

Det var tidligere krav om «särskild anledning att anta» at en person kommer til å utøve kriminell virksomhet som omfatter visse angitte lovbrudd. Det stiltes ikke krav til mistanke om et konkret lovbrudd, men etter praksis krevdes vanligvis en noenlunde konkretisert gjerning. Ved lovendring 9. desember 2014 ble vilkåret endret, slik at det nå er krav om «påtaglig risk för att» en person kommer til å utøve slik kriminell virksomhet. Dette ble blant annet begrunnet med at den dagjeldende ordlyd som regel forutsatte en noenlunde konkretisert gjerning, og at dette var å drive konkretiseringskravet for langt. I flere saker kunne en rekke ulike scenarier være tenkbare, og vilkåret burde derfor erstattes med et krav om risikobedømmelse, jf. Prop. 2013/14:237 side 105 flg. Denne skal være grunnet på faktiske omstendigheter, for eksempel uttalelser, trusler eller andre handlinger, og det er ikke tilstrekkelig med spekulasjoner eller allmenn bedømmelse. At det ikke lenger stilles krav om en spesifikk gjerning kan i enkelte saker forventes å medføre en noe lempeligere bruk av tvangsmidler i forebyggende øyemed, jf. proposisjonen side 107. Endringen trådte i kraft 1. januar 2015, og samtidig ble den tidsbegrensede loven gjort permanent, i tråd med forslag i betenkningen *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44), jf. SFS 2014:1422.

For at tvangsmiddelbruken skal kunne tillates må den kriminelle virksomheten innbefatte slikt lovbrudd:

1. sabotasje,
2. mordbrann, allmenfarlig ødeleggelse, kapring, sjø-, luftfarts- eller flyplassabotasje,
3. opprør, væpnet trussel mot lovlig orden, lovbrudd mot medborgerlig frihet,
4. høyforræderi, krigsstiftelse, spionasje, grov uautorisert befatning med hemmelige opplysninger, grov ulovlig etterretningsvirksomhet,
5. forretningsspionasje,
6. terrorlovbrudd, grov terrorfinansiering, grovt brudd på loven om straff for offentlig oppfordring, rekruttering og opptrening til terrorlovbrudd og annen særlig alvorlig kriminalitet,
7. mord, drap, grov mishandling, kidnapping, ulovlig frihetsberøvelse, om hensikten er å påvirke offentlig organ eller journalister til å gjøre eller unnlate en handling eller å hevne en handling.

Tvangsmiddelet må dessuten være av vesentlig betydning for å forhindre slik kriminalitet, jf. 5 §. Dette innebærer at det stilles et kvalitetskrav til de opplysninger tvangsmiddelet kan gi, samt at tvangsmiddelbruken er nødvendig. Det gjelder videre et proporsjonalitetskrav.

Beslutning om bruk av tvangsmidler i avvergende øyemed treffes av Stockholms tingrett, etter begjæring fra påtalemyndigheten. I visse saker vil et offentlig ombud utpekes av retten for å ivareta integritetsinteresser. Påtalemyndigheten kan fatte beslutning om tvangsmiddelbruk i hastesaker, der det å gå til retten ville innebære en forsinkelse av vesentlig betydning for mulighetene til å forhindre den kriminelle virksomheten, jf. 6 a §.

Loven av 2012 regulerer vilkårene for at politiet, Säkerhetspolisen og tollverket skal kunne innhente overvåkingsopplysninger om elektro-

nisk kommunikasjon i sin etterretningsvirksomhet. Den opprinnelig tidsbegrensede loven ble, i tråd med forslag i betenkningen *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44), gjort permanent fra 1. januar 2015, jf. SFS 2014:1422.

De overvåkingsopplysninger som kan innhentes er opplysninger om meddelelser som i et elektronisk kommunikasjonsnett er overført til eller fra et telefonnummer eller annen adresse (men ikke innholdet i meddelelsen), hvilke elektroniske kommunikasjonsutrustninger som har befunnet seg innen et visst geografisk område, eller i hvilket geografisk område en viss elektronisk kommunikasjonsutrustning befinner eller har befunnet seg. Til forskjell fra 2007-loven gjelder det ikke et krav om at tvangsmiddelbruken retter seg mot en konkret person. Politiet kan for eksempel undersøke hvilke mobiltelefoner som har befunnet seg i et visst område ved et visst tidspunkt.

Et vilkår, ved siden av proporsjonalitets- og behovsprinsippet, er at innhentingen er av særskilt betydning for å forebygge, forhindre eller oppdage kriminell virksomhet av angitt type, jf. 2 §. Videre er det krav at den kriminelle virksomheten som tvangsmiddelbruken retter seg mot gjelder lovbrudd som har en minimumsstraff på to år. Innhenting er imidlertid også tillatt ved visse særskilt angitte samfunnsfarlige lovbrudd innen Säkerhetspolisens ansvarsområde med en lavere minimumsstraff enn to år, jf. 3 §. Dette gjelder:

1. sabotasje,
2. kapring, sjø-, luftfarts- eller flyplassabotasje,
3. lovbrudd mot medborgerlig frihet,
4. spionasje, grov uautorisert befatning med hemmelige opplysninger og grov ulovlig etterretningsvirksomhet,
5. grov terrorfinansiering, grovt brudd på loven om straff for offentlig oppfordring, rekruttering og opptrening til terrorlovbrudd og annen særlig alvorlig kriminalitet.

Beslutning fattes av de kriminalitetsbekjempende myndigheter, som skal underrette Säkerhets- och integritetsskyddsnämnden om beslutningen, jf. 4 § og 6 §. Tillatelse fra domstolen kreves først dersom opplysningene siden skal anvendes i en etterforskning, jf. 9 §.

13.3.2 Finsk rett

I Finland ble ny Polislag 872/2011 sanksjonert 22. juli 2011. Loven trådte i kraft 1. januar 2014. Det følger av 1 kap. 1 § at bruk av tvangsmidler i forbindelse med etterforskning av lovbrudd reguleres av den nye Tvångsmedelslagen (806/2011), som trådte i kraft samme dag. Derimot reguleres bruken av hemmelige metoder for innhenting av informasjon med formål å forhindre, avsløre eller avverge risikoen for lovbrudd av ny Polislag 5. kap. Metodene omfatter blant annet teleavlytting, teleovervåking, innhenting av basestasjonsopplysninger, systematisk observasjon, fordekt innhenting av informasjon, teknisk avlytting (romavlytting) og optisk observasjon.

Med forhindring av lovbrudd menes handlinger som skal forhindre lovbrudd, forsøk på lovbrudd og forberedelse til lovbrudd, når det ut fra iakttagelser av, eller annen informasjon om, en persons virksomhet finnes grunn til å anta at personen kommer til å gjøre seg skyldig i lovbrudd, samt handlinger som skal avbryte allerede påbegynte lovbrudd eller begrense skadevirkningen av lovbrudd, jf. 5. kap 1 §.

Videre er det en generell forutsetning for bruk av hemmelige metoder for innhenting av informasjon at man med metoden kan antas å få informasjon som behøves for å forhindre, avsløre eller avverge risikoen for lovbrudd. Metoden må dessuten antas å være av vesentlig vekt for å kunne forhindre eller avsløre et lovbrudd, jf. 2 §. Utover dette finnes det særvilkår for bruk av de enkelte tvangsmidler i de påfølgende bestemmelsene, herunder kriminalitetskrav (strafferamme, eventuelt særskilt oppregnede straffebud), krav om hvilken myndighet som kan fatte beslutning, samt om tillatelsens varighet.

For eksempel kan politiet i henhold til 5 § gis tillatelse til teleavlytting for å forhindre lovbrudd dersom personen avlyttingen vil rette seg mot på grunn av ytringer, trusler eller opptreden med grunn kan antas å gjøre seg skyldig i et av følgende lovbrudd: lovbrudd mot Finlands suverenitet, krigsstiftelse, landsforræderi, spionasje, avsløring av statshemmeligheter, ulovlig etterretningsvirksomhet, særskilte lovbrudd med terrorhensikt, forberedelse til terrorhandlinger, å lede en terroristgruppe, å fremme en terroristgruppes virksomhet, å gi terroropplæring, rekruttering til terror og finansiering av terror. Videre kan det gis tillatelse til teleavlytting dersom det er nødvendig for å avverge en alvorlig fare som umiddelbart truer liv og helse. Beslutning om bruk av teleavlytting treffes av retten, etter begjæring fra politiet, jf. 7 §. Tillatelse gis for inntil en måned av gangen.

Videre kan politiet etter 8 § for å forhindre lovbrudd gis tillatelse til teleovervåking av en teleadresse eller teleterminalutrustning som innehas eller anvendes av en person som på grunn av ytringer, trusler, opptreden eller annet med grunn

kan antas å gjøre seg skyldig i et av følgende lovbrudd: Lovbrudd der strengeste straff er fengsel i minst fire år, lovbrudd som begås ved bruk av teleadresse eller teleterminalutrustning og der strengeste straff er fengsel i minst to år, utnyttelse av personer til sexhandel, hallikvirksomhet, narkotikalovbrudd, forberedelse til lovbrudd som begås med terrorhensikt eller grove tollovbrudd. Videre kan det gis tillatelse til teleovervåking dersom det er nødvendig at dette utføres umiddelbart for å avverge en fare som truer liv og helse. Liknende vilkår gjelder ved innhenting av basestasjonsopplysninger, jf. 12 §. Beslutning om bruk av teleavlytting eller innhenting av basestasjonsopplysninger treffes av retten, etter begjæring fra politiet, jf. 10 § og 12 §. Tillatelse til bruk av teleavlytting gis for inntil en måned av gangen. Politiet har på nærmere vilkår hastekompetanse, men spørsmålet skal i så tilfelle bringes inn for retten snarest mulig og senest innen 24 timer.

I henhold til 17 § kan politiet gis tillatelse til teknisk avlytting (herunder romavlytting) for å forhindre lovbrudd dersom personen avlyttingen vil rette seg mot på grunn av ytringer, trusler eller opptreden med grunn kan antas å gjøre seg skyldig i lovbrudd der strafferammen er fengsel i minst fire år, narkotikalovbrudd, forberedelse til lovbrudd med terrorhensikt og grove tollovbrudd. Avlyttingen kan utføres slik at den rettes mot sted som den mistenkte med sannsynlighet kan antas å befinne seg på eller besøke, samt i fengselsceller og lignende. Slik avlytting kan imidlertid ikke rettes mot fast bopel, jf. 17 § 2 mom. Det gjøres imidlertid unntak fra sistnevnte bestemmelse der det er nødvendig for at en politiaksjon trygt skal kunne gjennomføres eller dersom det kan avverge en overhengende fare som truer liv eller helse til den som gjenomfører aksjonen eller til den som skal pågripes eller beskyttes.

13.3.3 Dansk rett

Politiets adgang til å foreta inngrep i meddelelseshemmeligheten, overvåking, dataavlesing og forstyrrelse eller avbrytelse av radio- eller telekommunikasjon er regulert i retsplejelovens kapitel 71.

Etter reglene i dette kapittelet kan politiet, når visse vilkår vedrørende blant annet kriminalitetens grovhet er oppfylt, for eksempel avlytte telefonsamtaler eller foreta romavlytting, jf. retsplejelovens § 780, stk. 1, nr. 1 og 2, og foreta fotografering eller overvåking ved hjelp av kikkert eller annet apparat av personer som befinner seg på et ikke fritt tilgjengelig sted, jf. retsplejelovens § 791 a. Det bemerkes at politiets fotografering eller overvåking av personer som befinner seg på et fritt tilgjengelig sted *ikke* anses som et tvangsinngrep.

Ses det bort fra retsplejelovens § 791 c, som gir politiet adgang til å forstyrre eller avbryte radio- og telekommunikasjon i et område med henblikk på å *forebygge* visse former for særlig grov kriminalitet, herunder terrorisme, er det et krav for å anvende de tvangsinngrepene som er nevnt i retsplejelovens kapitel 71 at politiet har mistanke om at et straffbart forhold som forfølges av det offentlige *er begått*.

Det kreves ikke at det straffbare forhold er *fullbyrdet*. Politiet har dermed også adgang til å foreta inngrep i meddelelseshemmeligheten mv. som ledd i etterforskning av et *straffbart forsøk*, hvis betingelsene for det for øvrig er oppfylt.

Dansk rett åpner generelt for å straffe forsøkshandlinger i et videre omfang enn etter norsk rett. Ifølge straffeloven § 21 rammes «handlinger, som sigter til at fremme eller bevirke udførelsen af en forbrydelse», når denne ikke fullbyrdes, som forsøk. Forsøk er straffbart fra de første forberedende handlinger, dersom det foreligger fullbyrdelsesforsett. Det innebærer at politiet kan foreta etterforskning, og etter omstendighetene tvangsinngrep, så snart en gjerningsmann har begynt å forberede en forbrytelse som er undergitt offentlig påtale. Som et eksempel på politiets anvendelse av tvangsinngrep ved etterforskning av et straffbart forsøk, kan det vises til en dom fra Vestre Landsret avsagt 16. mai 2007 og gjengitt i Tidsskrift for Kriminalret 2007 side 593.

I denne saken hadde en anonym informant henvendt seg til SKAT (som har ansvaret for oppkreving av toll, skatter, avgifter og gjeld til det offentlige i Danmark) og opplyst at en person A sammen med andre ville begå et ran av en pengetransport fra SKAT på en nærmere angitt dato. Påtalemyndigheten begjærte avlyttingstillatelse av en telefon som tilhørte A, noe byretten tillot. Retten anførte blant annet at mistanken om at A sammen med andre var i ferd med å planlegge et ran av en pengetransport fra SKAT var underbygget av opplysningene fra den anonyme informanten, men også av foreliggende opplysninger om hvor og når det ble transportert særlig mye penger fra SKAT. Retten fant at det var bestemte grunner til å anta at det ved bruk av As telefon ble gitt meddelelser til eller fra en person som var mistenkt for å planlegge et ran. Landsretten stadfestet byrettens avgjørelse.

Reglene i retsplejeloven gjelder også for Politiets Efterretningstjenestes etterforskning, jf. § 6 i

lov nr. 604 12. juni 2013 om Politiets Efterretningstjeneste (PET). Det som er nevnt ovenfor får også anvendelse på Politiets Efterretningstjenestes adgang til å bruke de tvangsinngrep som er nevnt i retsplejelovens kapitel 71.

13.3.4 Islandsk rett

Reglene om hemmelige tvangsmidler finnes i straffeprocessloven kapitel 11 om telefonavlytting og andre tilsvarende inngrep, jf. §§ 80 til 85. Metodene omfatter blant annet telefonavlytting, kommunikasjonsavlytting og -opptak, lydopptak, kameraovervåking, observasjon, samt teknisk sporing av bil og på person.

Det er en forutsetning at inngrepet skjer under etterforskningen av en sak. Videre må inngrepet antas å gi opplysninger som anses for å være av vesentlig betydning for etterforskningen. For kommunikasjonskontroll og kommunikasjonsavlytting eller -opptak er det dessuten et vilkår at saken gjelder lovbrudd som kan straffes med fengsel i åtte år eller mer, eller at vektige samfunnsinteresser eller private interesser gjør det påkrevet. Beslutning om slike inngrep treffes av retten ved kjennelse for en periode på inntil fire uker av gangen.

Island har ikke spesielle regler om bruk av hemmelige tvangsmidler i avvergende eller forebyggende øyemed. Tvangsmidler kan altså bare benyttes under etterforskning, og dette forutsetter at det er «rimelig formodning om, at et strafbart forhold er begået», jf. straffeprocessloven 7. kapitel § 52. Forsøk er imidlertid straffbart, jf. straffeloven 3. kapitel § 20, og dette betyr at også forberedelser av lovbrudd etterforskes. Et vilkår er at det foreligger en «handling, der fremmer eller bevirker udførelsen af en forbrydelse». Det er mulig å få domstolsavgjørelse om bruk av tvangsmidler ved etterforskningen av forsøkshandlingen, og i slik forstand kan det sies at hemmelige tvangsmidler også benyttes for å hindre at den endelige forbrytelsen begås.

13.4 Tvangsmiddelbruk i avvergende øyemed

13.4.1 Innsnevring av de alminnelige vilkår

13.4.1.1 Gjeldende rett

13.4.1.1.1 Grunnvilkåret – som ledd i etterforskning

Det fremgår av § 222 d at tvangsmiddelbruk i avvergende øyemed må skje *som ledd i etterforskning*. Da utvalget stiller spørsmål om etterforskningsbegrepet er tilstrekkelig klart, finner departementet grunn til å presisere innholdet nærmere.

Det avgjørende for om etterforskning skal innledes er om det er «rimelig grunn til å undersøke om det foreligger straffbart forhold», jf. § 224 første ledd. Justisdepartementet uttalte i Ot.prp. nr. 60 (2004–2005) punkt 4.5.2 side 42 at grensen mellom etterforskning og annen politivirksomhet bør trekkes opp med utgangspunkt i retningslinjene i Riksadvokatens rundskriv nr. 3/1999 (Etterforsking). Rundskrivet kan langt på vei sies å være et resultat av den såkalte Furre-saken, jf. «Riksadvokatens gjennomgang av overvåkningstjenestens henvendelser til tyske myndigheter om opplysninger fra Stasi-arkivene» 29. april 1997. Her kom skillet mellom etterforskning og forebygging på spissen. Avgrensningen av etterforskningsbegrepet har særlig betydning for hvem som har ansvar og instruksjonsmyndighet – Riksadvokaten eller Justisdepartementet – og hvilke regler som gjelder for virksomheten – straffeprosessloven og påtaleinstruksen eller politiloven og forvaltningsloven. En av de klare konklusjonene en kunne trekke av Furre-saken, var at det var påtalemyndigheten ledet av Riksadvokaten som hadde ansvaret for den virksomheten som betegnes som etterforskning, og at Justisdepartementet ikke skulle instruere i enkeltsaker.

Det følger av rundskrivet at en virksomhet er å anse som etterforskning hvis siktemålet er å avklare om et straffbart forhold finner eller har funnet sted. Særlige spørsmål oppstår når politiets virksomhet har flere formål, for eksempel at politiet samtidig som det undersøker om et straffbart forhold er begått, forsøker å stanse eller avverge nye straffbare forhold. I Ot.prp. nr. 60 (2004–2005) punkt 4.5.2 side 42–43 slås det fast at dersom det først er åpnet etterforskning, vil politiets bruk av tvangsmidler måtte anses som del av etterforskningen, selv om hovedformålet i en bestemt situasjon er å stanse eller avverge en straffbar handling, noe som ble presisert i § 226 første ledd bokstav c ved endringslov 17. juni 2005 nr. 87. Dette er blitt mer praktisk etter hvert som flere handlinger er gjort straffbare på forberedelsesstadiet, jf. for eksempel straffeloven §§ 131 tredje ledd, 133, 136 og 136 a (straffeloven 1902 §§ 147 a fjerde og femte ledd, 147 c og 147 d).

I juridisk teori synes enkelte forfattere å legge til grunn at § 226 første ledd bokstav c innebærer en betydelig utvidelse av politiets og påtalemyndighetens kompetanse til å foreta etterforskning, og det skilles mellom etterforskning med oppklaringsformål «når det er rimelig grunn til å undersøke om det foreligger straffbart forhold» etter

§ 224 første ledd og «preventiv» etterforskning etter § 226 første ledd bokstav c, jf. Jo Hov, Rettergang II (Oslo, 2010) side 721. Tilføyelsen av § 226 første ledd bokstav c var imidlertid ikke ment å virke inn på forståelsen av § 224 om når etterforskning skal iverksettes, jf. merknad til bestemmelsen i Ot.prp. nr. 60 (2004–2005) side 151. Regelen i § 226 første ledd bokstav c angir kun et legitimt etterforskningsformål som gir grunnlag for informasjonsinnhenting etter at det er satt i verk etterforskning, jf. Riksadvokatens høringsuttalelse inntatt i Ot.prp. nr. 60 (2004–2005) punkt 4.4 side 38–39. Vilkårene for å sette i gang etterforskning etter § 224 må således være til stede.

Etterforskning kan iverksettes når det er «rimelig grunn til å undersøke» om det foreligger et straffbart forhold. Riksadvokaten angir tre sentrale momenter i den skjønnsmessige vurderingen som denne standarden åpner for, jf. rundskrivet punkt 3, nærmere bestemt *sannsynlighet*, *proporsjonalitet* og *saklighet*. I denne vurderingen inngår en bedømmelse av graden av sannsynlighet eller mulighet for at det foreligger et straffbart forhold. Hvilken sannsynlighet som bør kreves, vil særlig variere med hvor alvorlig det mulige lovbruddet er. Om dette heter det i Ot.prp. nr. 60 (2004–2005) punkt 4.5.3 side 43–44:

> «At det ikke oppstilles noe mistankekrav for å iverksette etterforsking, betyr uansett ikke at politiet står fritt til å foreta etterforskingsskritt. Sannsynligheten for at det er begått en straffbar handling fremheves også i riksadvokatens rundskriv nr. 3/1999 som ett av tre sentrale momenter i vurderingen av om det er «rimelig grunn» til å foreta etterforsking, jf straffeprosessloven § 224. Dersom det dreier seg om mindre alvorlige straffbare handlinger, bør det derfor stilles krav om en viss sannsynlighet om at den straffbare handlingen begås eller er begått før etterforsking iverksettes, i hvert fall om etterforskingen vil rette seg mot en bestemt person. På den annen side må etterforsking kunne iverksettes på grunnlag av opplysninger om at noen er i ferd med å begå eller har begått en svært alvorlig straffbar handling, selv om sannsynligheten for at det er hold i opplysningene er meget liten. Etter departementets syn er dette en fornuftig avveining av de krysssende hensynene som gjør seg gjeldende på området. [...]»

Det vil således kunne være grunnlag for å iverksette etterforskning både i situasjonen der det er rimelig grunn til å undersøke om et lovbrudd *er begått*, *begås* og der noe er *i ferd med å begås* – det siste dersom handlingen er av svært alvorlig karakter, slik at proporsjonalitetsvurderingen tilsier at det kreves en lavere sannsynlighetsgrad. I Bjerke/Keiserud/Sæther, Straffeprosessloven kommentarutgave Bind II (4. utgave, Oslo 2011) side 829 innlemmes også den siste situasjonen, jf. også Auglend, Mæland mfl., Politirett (Oslo 1998) side 296, der det legges til grunn at man er i etterforskning dersom forebyggende virksomhet går over i en konkret fase ved at det avdekkes opplysninger om at bestemte straffbare handlinger planlegges utført.

13.4.1.1.2 Nærmere om sammenhengen mellom lovbrudd som gir grunnlag for etterforskning og lovbruddet som søkes avverget

Som oftest vil det lovbrudd som gir grunnlag for etterforskning være et annet lovbrudd enn det som den skjulte metodebruken har til hensikt å avverge. Et typisk eksempel er at det er rimelig grunn til å undersøke om det er begått en straffbar forberedelseshandling, samtidig som det planlegges å begå en mer alvorlig straffbar handling som nevnt i § 222 d. Mer presist kan det være rimelig grunn til å undersøke om noen har inngått forbund om å begå terrorhandling, jf. straffeloven 1902 § 147 a fjerde jf. første ledd (straffeloven §§ 133 første ledd jf. 131), eller satt seg i besittelse av sprengstoff, jf. straffeloven 1902 § 161 (straffeloven § 190), og som ledd i denne etterforskningen kan det så bli aktuelt å avverge selve terrorhandlingen, jf. straffeloven 1902 § 147 a (straffeloven § 131).

Det er imidlertid ikke oppstilt noe krav om tilknytning mellom forholdet som gir grunnlag for å iverksette etterforskning og forholdet som søkes avverget, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.2.4 side 67. Tvangsmidler vil dermed kunne brukes i avvergende øyemed i alle tilfeller hvor det allerede er innledet etterforskning mot en person og det kommer frem opplysninger om at det planlegges en straffbar handling som nevnt i § 222 d.

Det stilles heller ikke noe uttrykkelig krav om at det er samme person som er gjenstand for den opprinnelige etterforskningen, som planlegger å begå den straffbare handlingen som ønskes avverget. Men uttrykket «som ledd i etterforsking» tilsier at personen som etterforskes og personen som et skjult tvangsmiddel retter seg mot, begge har en viss tilknytning til saken som etterforskes. Det vil for eksempel kunne brukes tvangsmidler i avvergende øyemed hvor det er innledet etter-

forskning mot en person i et kriminelt miljø, og det viser seg at andre personer i samme miljø planlegger en straffbar handling som nevnt i bestemmelsen.

Det er heller ikke noe vilkår at det allerede er innledet etterforskning – verken på person- eller saksnivå – når en får holdepunkter for at noen kommer til å begå en handling som rammes av et av straffebudene som er regnet opp i § 222 d. Som det fremgår av Ot.prp. nr. 60 (2004–2005) punkt 4.5.3 side 44 vil det – «når det først er grunnlag for å anvende tvangsmidler med hjemmel i den nye § 222 d – normalt også […] være grunn til å mistenke noen for å ha begått en straffbar forberedelseshandling». Særlig aktuell er trolig straffeloven § 198 (straffeloven 1902 § 162 c), som setter straff for den som inngår forbund med noen om å begå en straffbar handling som ledd i virksomheten til en organisert kriminell gruppe. Dersom det foreligger informasjon som gir rimelig grunn til å tro at noen kommer til å begå en terrorhandling, vil det særlig kunne være rimelig grunn til å undersøke om straffeloven § 131 tredje ledd (straffeloven 1902 § 147 a femte ledd) er overtrådt.

Et neste spørsmål er om det – dersom det er åpnet etterforskning fordi en har fått signaler om at noe alvorlig er i ferd med å begås – vil kunne tas i bruk tvangsmidler etter § 222 d for å avverge *samme* handling. Eller sagt på en annen måte: Er det nødvendig at det dreier seg om avverging av et *annet* straffbart forhold enn det som lå til grunn for at etterforskning ble iverksatt? I Bjerke/Keiserud/Sæther: Straffeprosessloven kommentarutgave Bind II (4. utgave, Oslo 2011) side 794 gis det uttrykk for at det må være rimelig grunn til å undersøke om det foreligger et annet straffbart forhold enn det som den skjulte metodebruken har til hensikt å avverge. Det synes å forutsette at selv i saker der hovedformålet med etterforskningen er å avverge en straffbar handling, må det altså også være grunn til å tro at det allerede foreligger et annet straffbart forhold. I kommentarutgaven på side 795 heter det videre:

> «Hvor stor selvstendig betydning vilkåret om igangsatt etterforsking har, vil for en stor del bero på hva slags straffbar handling som søkes avverget. Er det holdepunkter for at noen vil komme til å begå en terrorhandling, vil det som regel også være rimelig grunn til å undersøke om en (annen) straffbar handling er begått, ettersom handlinger som forbereder terrorhandlinger i vid utstrekning er kriminalisert. Dette kan stille seg annerledes for enkelte av de andre lovbruddene som kan avverges med hjemmel i § 222d, for eksempel organisert grov narkotikaforbrytelse, der det ikke er like «nødvendig» å bryte andre straffebestemmelser først.»

Spørsmålet kommer ikke så ofte på spissen, siden de fleste forberedelseshandlinger til de alvorlige lovbruddene som ramses opp i § 222 d første ledd selv er kriminalisert. Det vil derfor være grunnlag for å undersøke om det foreligger et annet lovbrudd, for eksempel at det er inngått forbund om terror eller drap etc. For enkelte av straffebudene som er regnet opp i § 222 d annet ledd, er det imidlertid ikke like opplagt at det – fordi det er grunn til å tro at noen kommer til å begå en slik straffbar handling – normalt også vil være rimelig grunn til å undersøke om det allerede foreligger et annet straffbart forhold.

Departementet vil imidlertid her slå fast at det etter gjeldende rett *ikke* kan oppstilles noe krav om at det må foreligge et annet straffbart forhold enn det som den skjulte metodebruken har til hensikt å avverge. Et slikt krav kan ikke utledes av ordlyden i § 222 d – «som ledd i etterforsking» – og det finnes heller ikke klare holdepunkter for en slik forståelse i forarbeidene. Tvert i mot er det uttalelser der som kan tas til inntekt for motsatt syn, blant i Ot.prp. nr. 60 (2004–2005) punkt 6.2.4, der det heter:

> «Hovedformålet med den nye § 222 d er å gi politiet et klart lovmessig grunnlag for å anvende selv de mest inngripende etterforskingsmetodene i saker hvor dagens hjemler for bruk av tvangsmidler ikke er anvendelige, men hvor det er av stor betydning å avverge en straffbar handling. For departementet har det vært særlig viktig å gjøre politiet bedre i stand til å avdekke planer om forbrytelser som vil kunne ha uopprettelige skadevirkninger, for derved å stå bedre rustet til å avverge forbrytelsene. Åpenbare eksempler er terroraksjoner av den art som i de senere år har funnet sted i New York, i Madrid og på Bali. I slike situasjoner er det viktigste å avverge selve handlingen. Dersom en aksjon av denne typen først er gjennomført, er dødsfall og omfattende menneskelige lidelser ofte ikke til å unngå.»

Det er nærliggende å anta at formuleringen i rettsteorien beror på en misforståelse og skyldes det faktum at etterforskning *typisk* iverksettes fordi et lovbrudd antas å være begått, slik at det naturlig dreier seg om andre forhold. Men dette stiller seg annerledes i situasjonen der politiet, uavhengig av

pågående etterforskning, har fått tips om fremtidig alvorlig kriminalitet og det således er rimelig grunn til å undersøke om noe kan være i ferd med å begås.

13.4.1.2 Utvalgets forslag

Et samlet utvalg mener at det er behov for å klargjøre og foreta en viss innsnevring av de alminnelige vilkårene for avvergende tvangsmiddelbruk etter § 222 d, jf. utredningen punkt 22.3.1 side 231. Dette begrunnes blant annet med at bestemmelsen gir hjemmel for vidtgående inngrep i enkeltmenneskers personvern. I slike tilfeller stiller EMK artikkel 8 nr. 2 et kvalifisert krav til inngrepets hjemmelsgrunnlag. Lovgiver bør dessuten uansett tilstrebe at inngrepshjemler blir formulert så klart som mulig. Som avgrensningskriterium foreslår utvalget et vilkår om at det som ledd i forberedelsen til den handling som søkes avverget, allerede er begått en straffbar handling. Utvalget uttaler at dette samtidig vil kunne avhjelpe de problemene som bestemmelsen, etter utvalgets flertalls oppfatning, reiser med hensyn til Grunnloven § 102, se kapittel 5.1.

Mens det er tydelig angitt i § 222 d hvilke straffbare handlinger som kan søkes avverget ved hjelp av tvangsmiddelbruk, er tilleggsvilkåret «som ledd i etterforsking» etter utvalgets syn ikke klart nok til å fungere som avgrensingskriterium for bruk av skjulte tvangsmidler. Utvalget viser til at det de senere årene har vært omdiskutert hva som ligger i begrepet etterforskning. Selv om det har skjedd en viss avklaring av dette spørsmålet, mener utvalget det bør stilles mer presise vilkår for å bruke skjulte tvangsmidler enn det som kreves for å åpne etterforskning. Utvalget er av den oppfatning at det reelle behovet for tvangsmidler i avvergende øyemed er størst og mest berettiget i tilfeller der det allerede i forbindelse med forberedelsen av den handling som søkes avverget er foretatt en straffbar handling.

I utvalgets merknad til den foreslåtte bestemmelse heter det:

> «Den viktigste endringen er at det skal kreves rimelig grunn til å tro at noen som ledd i forberedelsen av den handling som søkes avverget allerede har foretatt en straffbar handling som kan medføre fengselsstraff. Sammenlignet med det nåværende vilkåret «som ledd i etterforskning» stilles dermed et tydeligere krav til konkret mistanke om en straffbar handling og et tydeligere krav til sammenheng mellom denne og den forbrytelsen som søkes avverget. Fordi bruk av tvangsmidler på dette grunnlaget nødvendigvis vil skje som ledd i etterforsking, slik dette begrepet er definert i straffeprosessloven § 224, trenger dette ikke lenger sies uttrykkelig i lovteksten.»

Utvalget anfører at det er ønskelig å kreve en tydeligere tilknytning mellom den begåtte og den planlagte, straffbare handlingen. Utvalget mener det er særlig praktisk at det er mistanke om at noen allerede har avtalt å begå en alvorlig forbrytelse, siden det å inngå et såkalt «forbund» er straffbart ved de fleste av de forbrytelsestypene som straffeprosessloven § 222 d gir hjemmel for å avverge. Det uttales i den sammenheng:

> «Vilkåret om at den straffbare handling som anses begått må være foretatt «som ledd i forberedelsen av» den forbrytelse som søkes avverget, medfører et tydeligere krav til sammenheng mellom det som allerede er gjort og det som forventes å skje i fremtiden. En slik sammenheng vil være til stede der det er rimelig grunn til å tro at noen har utført den straffbare handlingen med forsett om enten alene, sammen med andre eller ved hjelp av andre å fullføre en slik alvorlig forbrytelse som i medhold av § 222d kan søkes avverget. Dette vil typisk være tilfellet der et såkalt formelt forberedelsesdelikt antas å være overtrådt. Det vil si tilfeller der det aktuelle straffebudet er formulert slik at det tydelig går frem at det dreier seg om forberedelse til en annen (og mer alvorlig) forbrytelse. Et typisk eksempel er straffeloven § 233 a om «å inngå forbund med noen om å begå en handling som nevnt i § 231 eller § 233». Et annet eksempel er anskaffelse av skytevåpen eller sprengstoff i den hensikt å begå en forbrytelse som nevnt i § 222d, jf. straffeloven § 161.»

Det bør etter utvalgets syn ikke stilles krav om at det straffebud som allerede er overtrådt formelt sett fremstår som et forberedelsesdelikt. Det avgjørende bør være om den straffbare handling etter gjerningspersonenes forsett inngår som ledd i forberedelsen av den svært alvorlige handlingen som politiet søker å avverge. I merknaden uttaler utvalget:

> «Vilkåret «som ledd i forberedelsen av» vil imidlertid også kunne være oppfylt der den regel som antas overtrådt fremstår som et helt selvstendig straffebud, for eksempel tyveri av et våpen eller et annet redskap. I slike tilfeller vil

> det avgjørende være om denne straffbare handling etter gjerningspersonens forsett antas å inngå som ledd i forberedelsen av en slik alvorlig forbrytelse som nevnes i § 222d første eller annet ledd. Det betyr at det må foretas en konkret vurdering av hva som på tidspunktet for den straffbare handling har vært den eller de aktuelle personene sine videre planer. En slik vurdering vil ha mye til felles med den bedømmelsen av personens gjennomføringsplan som må foretas der det er tvil om forsøkets nedre grense er passert. Det innebærer at vilkåret ikke vil være oppfylt dersom fullbyrdelsesforsettet med hensyn til den forbrytelse som søkes avverget først inntrer etter at den begåtte forbrytelse er avsluttet. Gjerningspersonen begynner for eksempel å forberede en terrorhandling og finner ut at han vil gjøre bruk av en gjenstand som han tidligere har stjålet (uten å ha terrorplaner). I et slikt tilfelle er det ikke tilstrekkelig nær sammenheng mellom tyveriet og den forbrytelse som søkes avverget.»

Utvalgets flertall uttaler at forslaget samtidig vil kunne avhjelpe de problemene som bestemmelsen i dag reiser i relasjon til Grunnloven § 102, se kapittel 5.1. Utvalgets flertall viser til at både Høgberg/Stub og Husabø har kommet til at § 222 d er for vid til å tilfredsstille unntaket for «kriminelle Tilfælde» i Grunnloven § 102. Det anføres at vilkåret om at bruken av tvangsmiddelet må skje «som ledd i etterforsking» ikke stiller et tilstrekkelig mistankekrav og heller ikke et tilstrekkelig krav til sammenheng mellom den straffbare handling det må være mistanke om er begått og den straffbare handling som søkes avverget.

13.4.1.3 Høringsinstansenes syn

Flertallet av de høringsinstanser som har uttalt seg om utvalgets forslag om klargjøring av vilkårene for bruk av tvangsmidler i avvergende øyemed, gir sin tilslutning til forslaget.

Datatilsynet støtter utvalgets vurdering om at det må legges til grunn at Grunnloven § 102 er til hinder for ransaking og romavlytting i private hjem, i avvergende og forebyggende øyemed. Også *Norsk forening for kriminalreform (KROM)* slutter seg til flertallets vurdering på dette punkt, men er likevel uenig i flertallets vurdering av mistankekravet, jf. nedenfor i punkt 13.4.2.3.

Advokatforeningen støtter det samlede utvalgs forslag til innsnevring og presisering av straffeprosessloven § 222 d om bruk av tvangsmidler i avvergende øyemed, men tar ikke eksplisitt stilling til om bestemmelsen går lenger enn det Grunnloven § 102 tillater. Heller ikke uttalelsen fra *Forsvarergruppen av 1977* berører dette spørsmålet uttrykkelig, men også her tiltres i utgangspunktet anbefalingen om å klargjøre og foreta en viss innsnevring av de alminnelige vilkår for bruk av bestemmelsen.

Oslo politidistrikt er enig i at den nye utformingen av bestemmelsen gjør den klarere enn slik den lyder i dag. Dette gjelder særlig med hensyn til vilkåret om at tvangsmiddelbruken må skje som ledd i etterforskning.

Oslo statsadvokatembeter sier seg enig i flertallets vurderinger, men gir samtidig uttrykk for at utvalget i for liten grad har vektlagt de legislative hensyn som bør være sentrale i dag. Statsadvokatembetet uttaler i den sammenheng blant annet følgende:

> «Den reelle begrunnelse må være at individene skal ha et materielt vern for sitt privatliv og at dette må være utgangspunktet ved fortolkningen. Dette prinsipp er også uttrykt i E.M.K. art 8, som fastslår at alle har krav på respekt for sitt privatliv, familieliv og korrespondanse. Et tilvarende utgangspunkt har man lagt til grunn for forståelsen av 4. grunnlovstillegg i den amerikanske forfatning. Dette innebærer rimeligvis ikke at dette vernet kan være absolutt. En slik løsning vil gjøre håndhevning av lovgivningen ganske umulig.
>
> Ordlyden i Grunnloven § 102 forbyr ransakning av hus bortsett fra slike som skjer i forbindelse med straffesaker. Det sier seg selv at en nesten 200 år gammel og meget knapt formulert grunnlovstekst ikke kan fortolkes strengt etter ordlyden. Dette gjelder særlig fordi det knapt finnes forarbeider, og om slike skulle finnes må de ha nokså begrenset vekt når de skal anvendes i forhold til dagens virkelighet. Som ellers ved fortolkning av grunnlovens bestemmelser må tolkningen baseres på en avveining av ulike og delvis motstridende hensyn. Ved forståelsen av Grunnloven § 102 blir det forholdet mellom hensynet til privatlivets fred og samfunnets behov, for å sikre en rimelig effektiv etterlevelse av lovgivingen, som bør være det sentrale element i tolkningen.»

PST uttaler at utvalgets forslag på dette punkt i hovedsak er i overensstemmelse med den praksis som over tid har vært fulgt i PST, og at PST således isolert sett ikke har innvendinger til forslaget om å klargjøre vilkårene. PST tar imidlertid ikke

uttrykkelig stilling til spørsmålet om grunnlovsstrid og uttaler følgende:

> «PST legger til grunn at Stortinget ved behandlingen av endringen av politiloven § 17d og straffeprosessloven § 222d i 2005, foretok en grundig vurdering nå av alle spørsmål knyttet til endringene. PST finner det vanskelig å foreta en ny vurdering nå kun basert på en ny teoretisk gjennomgang av det samme kildemateriale lovgiver den gang hadde tilgang til. Vi finner i tillegg at grunnlovmessigheten av eksisterende lovgivning vanskelig kan være gjenstand for en alminnelig høring. Vi finner det derfor riktig å overlate vurderingen av dette spørsmålet til departementets lovavdeling, eventuelt avgjørelse av Høyesterett.»

PST har i ettertid uttrykt uro overfor departementet over de snevre rammene som utvalgets forslag setter, og at det ligger flere hindringer her som kan gjøre det vanskelig for PST å kunne avverge alvorlige lovbrudd. Også *Det nasjonale statsadvokatembetet* har gitt uttrykk for slik uro i ettertid.

Riksadvokaten og *Østfold politidistrikt* sier seg uenig i flertallets fortolkning av Grunnloven § 102. Riksadvokaten legger, i likhet med utvalgets mindretall, til grunn at bruk av tvangsmidler i avvergende eller forebyggende øyemed omfattes av uttrykket «i kriminelle Tilfælde». Riksadvokaten gir uttrykk for at flertallets fortolkning av dette uttrykket har nokså usikker rettskildemessig støtte, og viser blant annet til at ordlyden i § 102 ikke synes å være til hinder for at bestemmelsen tolkes slik at det er nok at de aktuelle undersøkelsene tar sikte på å forebygge eller avverge kriminalitet:

> «Preposisjonsbruken (i kriminelle tilfeller) kan således forstås som en rent tematisk henvisning til kriminalitetsbekjempelse, uten at det innebærer et særskilt krav om at grensen for det straffbare må være overtrådt. Etter riksadvokatens syn bør en være tilbakeholden med å innfortolke skranker i Grunnloven som etter alt å dømme lå utenfor intensjonsdybden hos Eidsvollsfedrene ved valg av formulering, og som ordlyden på ingen måte tvinger til. Ikke minst gjelder det ved bedømmelsen av typetilfeller grunnlovskonsipistene neppe hadde i tankene.»

Riksadvokaten kan heller ikke se at de hensyn som gjør seg gjeldende tilsier at det bør innfortolkes et krav om at det allerede må være begått straffbare handlinger:

> «Det ser ut til å være ubestridt at Grunnloven § 102 tar sikte på å verne mot *vilkårlige* og *uforholdsmessige* inngrep i borgernes hjem. De krav som dermed må stilles til saklighet, sannsynlighet og forholdsmessighet, kan vanskelig sies å være uløselig knyttet til om straffbare handlinger allerede er begått, blir begått eller vil bli begått: Det kan foreligge sikre holdepunkter for at en alvorlig straffbar handling vil bli begått, uten at en har indikasjoner på at noe straffbart allerede har funnet sted. Den forståelse som er lagt til grunn av utvalgsflertallet, innebærer at grunnlovsvernet i stor grad avhenger av hvorvidt forberedelseshandlinger er gjort straffbare – et i prinsippet rent formelt kriterium. En slik forståelse kan skape et uheldig press i retning av å kriminalisere forberedelseshandlinger i større grad enn det som måtte være ønskelig ut fra strafferettslige overveielser. Et beslektet hensyn er at en streng forståelse av grunnloven på dette punkt – med en tilsvarende begrensning av hjemmelsgrunnlaget for avvergende (og forebyggende) metodebruk – vil kunne ha som en nokså påregnelig konsekvens at det oppstår situasjoner hvor en tvinges til å gjøre bruk av nødrett. Det er selvsagt ikke heldig.
>
> Heller ikke faren for *feiltreff* kan stille seg prinsipielt og systematisk forskjellig for forebyggende, avvergende og oppklarende virksomhet. Selv om begåtte og fremtidige hendelser prinsipielt kan sies å ha ulik status, stilles man i det praktiske liv for begge typer bedømmelsessituasjoner overfor fragmentert informasjon av vekslende karakter, og der fremgangsmåten for å ta stilling ikke er vesentlig forskjellig for bevisvurderinger og prognoser. Vurderingenes treffsikkerhet avhenger mer av hvilke krav som stilles til informasjonens kvalitet og sannsynlighetsgrad enn av om vurderingstemaet er hendelser i fortid eller fremtid.
>
> Det er videre ikke opplagt at faren for misbruk – i betydningen metodebruk uten at vilkårene er oppfylt eller med et annet reelt siktemål enn det som er anført som begrunnelse – er større ved undersøkelser rettet mot straffbare handlinger under oppseiling enn ved tilsvarende undersøkelser rettet mot allerede begått kriminalitet. Formentlig har det større betydning hvilke krav som stilles til objektive holdepunkter for mistanke, samt hvilke regler som gjelder for bruk av den informasjon som innhentes.»

Riksadvokaten støtter ikke en innsnevring av adgangen til avvergende metodebruk på en slik

måte som utvalget foreslår. Det er etter Riksadvokatens oppfatning ikke hensiktsmessig å fjerne henvisningen til at tvangsmiddelbruken må skje «som ledd i etterforsking» og sette inn et vilkår om at det «er rimelig grunn til å tro» at det «som ledd i forberedelsen allerede er begått en straffbar handling som kan medføre fengselsstraff». Riksadvokaten mener det er pedagogisk gunstig å beholde begrepet, på grunn av det grunnleggende skille mellom etterforskning og forebygging. Det uttales i den sammenheng:

> «Ved at vilkåret om at tvangsmiddelbruken skal skje som ledd i etterforsking er fremhevet i § 222d understrekes det grunnleggende skille mellom avvergeetterforsking i medhold av straffeprosessloven under påtalemyndighetens ledelse og ansvar og bruk av forebyggende metoder i medhold av politiloven. Da bestemmelsene i § 222d og politiloven §§ 17d-17f ble innført var dette et sentralt poeng, jf. Ot.prp. nr. 60 (2004–2005) side 57-59 og Innst. O nr. 113 (2004–2005) side 34. Det kan også vises til riksadvokatens rundskriv nr. 4/2007 om etterforskingskompetanse og påtaleansvar i PST. Det er pedagogisk gunstig at det grunnleggende skille mellom etterforsking og forebygging understrekes ved en uttrykkelig henvisning i lovteksten til at avvergetiltakene etter § 222d må skje som ledd i etterforsking.»

Riksadvokaten avviser videre at det er usikkerhet om forståelsen av etterforskningsbegrepet:

> «Selv om det er riktig at etterforskingsbegrepet har vært «omdiskutert» (side 231 annen spalte), er grensedragningen mellom etterforsking og forebygging – og betydningen av dette – godt beskrevet gjennom rundskriv herfra, departementets uttrykkelige tilslutning til riksadvokatens rundskriv i Ot.prp. nr. 60 (2004–2005) og avgjørelsene i Rt 2008 side1575 og Rt 2009 side 1075. Det er i dag ingen usikkerhet om forståelsen av etterforskingsbegrepet.»

Riksadvokaten slår fast at innskjerpingen i utvalgets forslag består i at det ikke lenger skal være nok at det er rimelig grunn til å undersøke *om* en straffbar handling er begått; det må være rimelig grunn å tro *at* en slik handling er begått, og uttaler:

> «Riksadvokaten har vanskelig for å se hvorfor man i et tilfelle der det er rimelig grunn til å tro at et drap eller en terroraksjon vil bli begått, skal kunne gjøre bruk av avvergende metoder dersom det i forbindelse med planleggingen er holdepunkter for at det er begått et tyveri eller inngått et straffbart forbund, men ikke dersom en har pålitelig informasjoner om at en person som handler på egenhånd vil begå alvorlig kriminalitet, og det så langt ikke er konkret informasjon om at noe straffbart har passert. Det kan se ut til å være en forutsetning for forslaget at (relativt lav grad av) mistanke om at det er begått en (nokså bagatellmessig) straffbar handling som ledd i planleggingen av et alvorlig lovbrudd, utgjør et særlig sikkert holdepunkt for om det vil bli begått en alvorlig straffbar handling. En er i sterk tvil om grunnlaget for slike antagelser.»

Etter Riksadvokatens syn dreier forslaget på en uheldig måte oppmerksomheten fra det vesentlige spørsmålet om hvilke holdepunkter man har for at noe alvorlig er i gjære, til det mindre sentrale tema om den strafferettslige vurderingen av de forhold som har ledet frem til den avvergingssituasjon man står overfor. Det er nok så at straffbare handlinger som del av forberedelsene til alvorlig kriminalitet gjennomgående vil være en viktig indikator for gjennomføringsvilje og kapasitet hos de som antas å være i ferd med å begå alvorlige straffbare handlinger. Men det vil ikke nødvendigvis alltid være slik, og kravet til at vilkårene for etterforskning foreligger, er etter Riksadvokatens syn et relevant, fleksibelt og tilstrekkelig kriterium for avvergende metodebruk ved siden av kravet om at det må være rimelig grunn til å tro at noen kommer til å begå en alvorlig straffbar handling.

13.4.1.4 Departementets vurdering

13.4.1.4.1 Innledning

Departementet konstaterer at et samlet utvalg mener at det er behov for å klargjøre og foreta en viss innsnevring av de alminnelige vilkårene for avvergende tvangsmiddelbruk etter § 222 d. Det er imidlertid bare flertallet, medlemmene Dalseide, Elden, Husabø, Nylund, Schartum og Schou, som delvis begrunner dette med at bestemmelsen, slik den er formulert i dag, er grunnlovsstridig.

Departementet finner grunn til først å knytte noen kommentarer isolert til hensiktsmessigheten av å innsnevre, og behovet for å klargjøre, de alminnelige vilkårene for bruk av tvangsmidler i avvergende øyemed. Dette fordi et samlet utvalg mener en slik klargjøring, uavhengig av grunnlov-

svurderingen, er nødvendig. Deretter vil de eventuelle konstitusjonelle skranker behandles.

Departementet vil innledningsvis bemerke at en innsnevring som foreslått av utvalget, vil ha betydning for et stort antall saker der Grunnloven under enhver omstendighet ikke blir utfordret. Dette fordi innsnevringen er foreslått å gjelde generelt for *all tvangsmiddelbruk i avvergende øyemed*, og således også for andre tvangsmidler enn ransaking og romavlytting i privat bolig. Selv om en legger til grunn flertallets syn om at et tydeligere krav til konkret mistanke er nødvendig av hensyn til Grunnloven ved romavlytting eller ransaking av private hjem, gjelder ikke dette tilsvarende ved bruk av de øvrige tvangsmidler, for eksempel ved kommunikasjonskontroll, eller dersom romavlytting eller ransaking foretas andre steder enn i private hjem.

13.4.1.4.2 Er det hensiktsmessig å innsnevre de alminnelige vilkår?

Departementet mener at det er mest hensiktsmessig å videreføre bestemmelsens alminnelige vilkår uendret. Departementet har lagt vekt på at Metodekontrollutvalgets forslag vil innebære en *betydelig innskrenking* av politiets adgang til å benytte tvangsmidler for å avverge alvorlig kriminalitet. Det bemerkes i den sammenheng at det kan settes spørsmålstegn ved om høringsinstansene faktisk har forstått rekkevidden av utvalgets endringsforslag.

Innskjerpingen i utvalgets forslag består for det første i at det ikke lenger vil være nok med rimelig grunn til å undersøke om det «foreligger» en straffbar handling, det må være rimelig grunn til å tro *at det allerede er begått* en slik handling. Som nevnt ovenfor under punkt 13.4.1.1 rommer uttrykket «foreligger» i straffeprosessloven § 224 første ledd ikke bare handlinger som er begått, men også handlinger som *begås* eller *er i ferd med å begås*. Departementet støtter Riksadvokaten i at forslaget på en uheldig måte dreier oppmerksomheten fra det vesentlige spørsmålet om hvilke holdepunkter man har for at noe alvorlig er i gjære, til det mindre sentrale tema om den strafferettslige vurderingen av de forhold som har ledet frem til den avvergingssituasjon man står overfor. Det synes vilkårlig dersom det avgjørende for tvangsmiddelbruken skal være hvorvidt et konkret, kanskje bagatellmessig lovbrudd, som for eksempel et tyveri, allerede er begått.

Utvalget anfører at etterforskningsbegrepet ikke er tilstrekkelig klart, selv etter Riksadvokatens rundskriv og departementets uttrykkelige tilslutning til dette i Ot.prp. nr. 60 (2004–2005). Av den grunn har departementet i punkt 13.4.1.1 om gjeldende rett funnet grunn til å presisere det nærmere innholdet i etterforskningsbegrepet. Departementet mener, i motsetning til utvalget, at etterforskningsbegrepet er tilstrekkelig klart til å fungere som et avgrensingskriterium for avvergende metodebruk.

Det kan synes som om etterforskningsbegrepet i sin tid ble inntatt av pedagogiske grunner for å tydeliggjøre grensen mellom bruk av tvangsmidler i forebyggende og avvergende øyemed, og det kan anføres at den selvstendige betydningen som vilkår er begrenset. Departementet mener likevel at det er pedagogisk gunstig å beholde en uttrykkelig henvisning i lovteksten til at avvergetiltakene etter § 222 d må skje *som ledd i etterforskning*. Slik tydeliggjøres det grunnleggende skillet mellom bruk av tvangsmidler i avvergende øyemed under påtalemyndighetens ledelse og ansvar i medhold av straffeprosessloven, og bruk av forebyggende metoder under Justisdepartementets ansvar i medhold av politiloven. En gjennomføring av utvalgets endringsforslag vil innebære et brudd med det gjeldende, etablerte og velkjente system.

Videre foreslår utvalget at adgangen til å bruke tvangsmidler i avvergende øyemed begrenses til de tilfeller hvor det er *sammenheng* mellom et opprinnelig lovbrudd og det lovbrudd som søkes avverget. Spørsmålet om det, på grunn av faren for misbruk, burde oppstilles et krav om sammenheng mellom forholdet som gir grunnlag for å iverksette etterforskning og forholdet som søkes avverget, ble drøftet og avvist i Ot.prp. nr. 60 (2004–2005), jf. punkt 6.2.4 side 67. Dette ble begrunnet med at når bestemmelsen nå var gitt en målrettet utforming med et strengt kriminalitetskrav, så var behovet for å innta et slikt uttrykkelig krav om sammenheng i loven mindre. Dette skyldtes at det så godt som alltid ville være grunnlag for å iverksette etterforskning, for eksempel for å undersøke om noen har inngått forbund med sikte på å begå en slik alvorlig handling. Departementet opprettholder konklusjonen, men med en annen begrunnelse.

Departementet mener at det vil kunne gi uheldige utslag å begrense adgangen til å bruke tvangsmidler i avvergende øyemed til der det er sammenheng mellom et opprinnelig lovbrudd og det lovbrudd som søkes avverget. Samfunnets interesse av å beskytte seg mot alvorlige straffbare handlinger, og behovet for å benytte tvangsmidler for å avverge disse, er ikke nødvendigvis mindre selv om de to handlinger ikke er relatert

til hverandre. Det vil for eksempel i praksis ofte kunne være behov for bruk av tvangsmidler i avvergende øyemed i tilfeller hvor det er innledet etterforskning på person- eller saksnivå og hvor det fremkommer opplysninger som gir grunn til å tro at noen innenfor samme miljø vil begå tilsvarende eller andre straffbare handlinger, uten at det er grunn til å undersøke om det allerede er begått en straffbar handling som ledd i forberedelsene til disse handlingene. Dessuten vil det i praksis være svært vanskelig å påvise en konkret sammenheng, noe som vil kunne gjøre det nærmest umulig for politiet å sikre borgerne mot alvorlig kriminalitet.

Departementet har videre søkt å klargjøre at det etter gjeldende rett ikke kan oppstilles krav om at etterforskning allerede er innledet eller kan innledes i sak om et *annet* lovbrudd. Det er således tilstrekkelig at det er grunnlag for etterforskning og behov for å benytte tvangsmidler for å avverge *samme* handling. Departementet mener det verken er eller bør være avgjørende for tvangsmiddeladgangen hvorvidt etterforskning allerede er innledet eller kan innledes i sak om et annet lovbrudd. I så tilfelle nærmest tvinges politiet til å konstruere et hendelsesforløp der et forberedelseslovbrudd foreligger, for slik å kunne avverge «hovedlovbruddet». Som Riksadvokaten peker på kan den forståelse som er lagt til grunn av utvalgsflertallet, også skape et uheldig press i retning av å kriminalisere forberedelseshandlinger i større grad enn det som måtte være ønskelig ut fra strafferettslige overveielser. For enkelte av straffebudene som er regnet opp i § 222 d annet ledd, er det heller ikke like opplagt at det – fordi det er grunn til å tro at noen kommer til å begå en slik straffbar handling – normalt også vil være rimelig grunn til å undersøke om det allerede foreligger et annet straffbart forhold. Dersom vilkåret om tilknytning til organisert kriminalitet fjernes for drap, jf. punkt 13.4.3.4 nedenfor, så vil det for eksempel kunne være vanskelig å påvise grunnlag for å iverksette etterforskning om forbund mot drap, for så å benytte tvangsmidler for å avverge selve drapet.

Utvalgets endringsforslag synes også unødig strengt, og det kan heller ikke utelukkes at begrensningene vil kunne føre til at nødrett oftere vil benyttes som hjemmelsgrunnlag for avvergende inngrep. En slik dreining i den rettslige forankringen av bruk av tvangsmidler i avvergende øyemed er etter departementets syn uheldig. Ved nødrett treffes beslutningen på grunnlag av mindre faste kriterier og det skjer ingen domstolskontroll, heller ikke etterfølgende, av beslutningen.

Departementet konkluderer etter dette med at det *ikke er hensiktsmessig* å innskrenke adgangen til bruk av tvangsmidler i avvergende øyemed på en slik måte Metodekontrollutvalget foreslår.

13.4.1.4.3 Gjør konstitusjonelle skranker det nødvendig å innskrenke de alminnelige vilkår og adgangen til å bruke tvangsmidler i avvergende øyemed?

Departementet går nå over til å drøfte om Grunnloven gjør det nødvendig å innskrenke adgangen til å benytte tvangsmidler i avvergende øyemed.

Metodekontrollutvalgets flertall slutter seg til hovedtrekkene i betenkningene fra Husabø og Høgberg/Stub, og finner at enkelte av dagens lovtillatte metoder er i strid med Grunnloven § 102, slik den da lød. Både Husabø og Høgberg/Stub legger til grunn at unntaket for «kriminelle Tilfælde» bare kommer til anvendelse der det allerede er begått en straffbar handling. Videre konkluderer både Husabø og Høgberg/Stub med at forbudet mot «Hus-inkvisisjoner» ikke bare omfatter ransaking, men også romavlytting og visse former for dataavlesing, nærmere bestemt innbrudd for å montere dataavlesingsutstyr. Hjemmelen for hemmelig ransaking og romavlytting i avvergende øyemed etter straffeprosessloven § 222 d anses å stå i et tvilsomt forhold til Grunnloven § 102, for så vidt gjelder inngrep i private hjem.

Departementet legger til grunn at § 102 første ledd annet punktum gir et absolutt vern mot inngrep som er å anse som «husransakelse», med unntak av når dette gjøres «i kriminelle tilfeller». Det er ikke tvilsomt at ransaking i private boliger er å anse som «husransakelse». Når det gjelder romavlytting og innbrudd ved dataavlesing, er det mer usikkert om tvangsmidlene omfattes av begrepet «husransakelse». Det er argumenter som trekker i retning av å anse slike metoder for å falle utenfor. For det første er en slik tolkning forenlig med ordlyden i annet punktum, som nå altså er endret fra «husinkvisisjon» til det snevrere uttrykket «husransakelse». For det annet er det mindre behov for en vid tolking av «husransakelse» etter grunnlovsreformen i 2014, idet et mer generelt formulert grunnlovsvern nå følger av § 102 første ledd første punktum. På den annen side kan det legges vekt på den generelle intensjonen til Stortinget ved språkrevisjonen, nemlig at det ikke var meningen å forskyve innholdet. Mot dette kan det imidlertid innvendes at også den tidligere rettstilstanden og rekkevidden av begrepet

husinkvisisjon var uklar. Likevel kan det hevdes at formålet med det opprinnelige forbudet mot husinkvisisjon var å verne om den private sfære, som både ransaking, romavlytting og innbrudd vil gjøre inngrep i. Rettstilstanden må etter dette sies å være usikker.

Dersom begrepet «husransakelse» tolkes utvidende, slik at det omfatter både romavlytting og innbrudd i tillegg til ransaking, blir det neste spørsmålet hvorvidt det kan sies å foreligge «kriminelle tilfeller» i avvergingssituasjonen. Som nevnt i punkt 5.1.3 ovenfor, legger departementet til grunn at det av formuleringen «kriminelle tilfeller» ikke kan utledes et krav om at det allerede må være foretatt en straffbar handling. Den fortolkningen som utvalgets flertall legger til grunn har nokså usikker forankring i de tungtveiende rettskildene. Departementet finner at flertallets avveining av hensynet til å verne om borgernes hjem på den ene siden og hensynet til kriminalitetsbekjempelse på den annen side, er mangelfull. Utvalgets vurdering av disse motstridende hensynene kan i ytterste konsekvens føre til at politiet mister noen av de virkemidler som er nødvendig for å avverge alvorlig kriminalitet, med den følge at liv kan gå tapt. Rettskildesituasjonen har på dette punktet dessuten endret seg etter at utvalget avga sin vurdering, særlig sett hen til de grunnlovsendringer som ble vedtatt våren 2014. Grunnloven § 93 og § 102 annet ledd gir nå statens myndigheter en plikt til å beskytte retten til liv og til å verne om den personlige integritet, herunder den enkeltes fysiske integritet.

Selv om det av formuleringen «kriminelle tilfeller» ikke kan utledes et krav om at en straffbar handling allerede må være begått, understreker departementet likevel at adgangen til å foreta inngrep i hjemmet for å forhindre fremtidig kriminalitet ikke er ubegrenset. For tiltak som ikke er å anse som «husransakelse» etter Grunnloven § 102 første ledd annet punktum, vil vurderingen av grunnlovsmessigheten skje etter normen i § 102 første ledd første punktum. Ved vurderingen må det tas stilling til om slik metodebruk ivaretar legitime formål og om den er forholdsmessig. Departementet legger til grunn at vurderingstemaet vil være det samme for tiltak som er å anse som husransakelse etter annet punktum, *dersom disse benyttes «i kriminelle tilfeller»* og således ikke rammes av den trolig absolutte forbudsregelen i annet punktum.

De konstitusjonelle skranker for adgangen til å benytte tvangsmidler må altså vurderes etter bestemmelsen i Grunnloven § 102 første ledd første punktum, som nedsetter et generelt vern for privatlivets fred og er utformet som en individuell rettighet for den enkelte borger. Det er på det rene at bestemmelsen ikke gir en udelt rett til privatliv, jf. flertallets merknader (representanter fra Høyre, FrP og Ap) i Kontroll- og konstitusjonskomiteens innstilling, se Innst. 186 S (2013–2014). Vurderingen av om en bestemt metodebruk er forholdsmessig etter § 102 vil være nokså sammenfallende med vurderingen etter EMK artikkel 8 nr. 2. Den innebærer at lovgiver, og i siste instans domstolene, må foreta en avveining mellom individets behov for beskyttelse mot inntrengning i privatsfæren på den ene siden og de legitime samfunnsbehovene som begrunner inngrepet på den andre siden. I Høyesteretts dom 29. januar 2015 inntatt i Rt. 2015 side 93 (avsnitt 60) uttales følgende om denne vurderingen:

> «Til forskjell fra SP artikkel 17 og EMK artikkel 8, inneholder Grunnloven § 102 ingen anvisning på om det overhodet kan gjøres lovlige begrensninger i privat- og familielivet. Men grunnlovsvernet kan ikke være – og er heller ikke – absolutt. I tråd med de folkerettslige bestemmelsene som var mønster for denne delen av § 102, vil det være tillatt å gripe inn i rettighetene etter første ledd første punktum dersom tiltaket har tilstrekkelig *hjemmel*, forfølger et *legitimt formål* og er *forholdsmessig*, jf. Rt-2014–1105 avsnitt 28. Forholdsmessighetsvurderingen må ha for øye balansen mellom de beskyttede individuelle interessene på den ene siden og de legitime samfunnsbehovene som begrunner tiltaket på den andre.»

EMK artikkel 8 nr. 2 åpner for at inngrep kan rettferdiggjøres dersom det har hjemmel i lov, ivaretar nærmere angitte formål og er nødvendig i et demokratisk samfunn for å oppfylle ett eller flere legitime formål, jf. punkt 5.2 ovenfor. Når det gjelder vilkåret om at inngrepet må forfølge et legitimt formål, nevner artikkel 8 nr. 2 eksplisitt flere av hensynene bak behovet for avvergende og forebyggende tiltak. Disse er «den nasjonale sikkerhet», «offentlige trygghet», «å forebygge uorden eller kriminalitet» og «å beskytte andres rettigheter og friheter». Det kan ikke være tvil om at politiets og PSTs arbeid for å forhindre og forebygge alvorlig kriminalitet omfattes av formålet. Videre må en eventuell lovgivning være tilstrekkelig forutsigbar. Det er også av betydning hvilke rettssikkerhetsgarantier som foreligger, særlig i form av domstolskontroll. Det kan legges til at en etter EMK har lagt stor vekt på hvorvidt lovgiver har konkretisert de samfunnsbehovene som begrun-

ner avveiningen, samt foretatt den nærmere avveiningen. En har vært mer forsiktig med å overprøve statenes vurdering av rimeligheten og hensiktsmessigheten av det aktuelle tiltaket (gjerne omtalt som statenes skjønnsmargin).

Ved vurderingen av hvilken adgang det skal være til å benytte tvangsmidler for å avverge og forebygge kriminalitet, må det således først og fremst tas stilling til om de lovhjemlede inngrep ivaretar legitime formål og er forholdsmessige. Departementet understreker at det ikke er enhver kriminell handling som vil kunne gi grunnlag for ransaking og romavlytting i avvergende øyemed.

Adgangen etter straffeprosessloven § 222 d til å benytte tvangsmidler i avvergende øyemed er i dag uttrykkelig begrenset, både med hensyn til hvilket skjult tvangsmiddel som kan benyttes og alvorlighetsgraden av lovbruddet som søkes avverget. Politiet kan bruke tvangsmidler, for eksempel ransaking, kameraovervåking, teknisk sporing, beslag, kommunikasjonskontroll og romavlytting, for å avverge terrorhandlinger eller trussel om terrorhandlinger, drap som ledd i motarbeiding av rettsvesenet eller drap, grovt ran eller særlig grov narkotikaforbrytelse som ledd i virksomheten til en organisert kriminell gruppe. Det må være «rimelig grunn til å tro» at noen kommer til å begå slik handling. Hemmelig ransaking og romavlytting kan, i likhet med kommunikasjonskontroll og personnær teknisk sporing, bare benyttes når særlige grunner tilsier det, og dette innebærer et *skjerpet forholdsmessighetskrav*, jf. § 222 d tredje ledd annet punktum. Videre er PSTs adgang til romavlytting ytterligere begrenset ved særregelen i § 222 d tredje ledd tredje punktum, til de mest alvorlige lovbrudd innenfor PSTs ansvarsområde, nærmere bestemt terrorlovbrudd etter § 147 a, spredning av masseødeleggelsesvåpen, spionasje og ulovlig etterretning. Rettssikkerheten er dessuten ivaretatt gjennom *domstolsbehandling* og *etterfølgende kontroll* fra KK-utvalget (for politiet) og EOS-utvalget (for PST). Det bemerkes at dagens regelverk forutsetter at både politiet og domstolen tar stilling til om forholdsmessighetskravet er oppfylt.

Det er ikke, som i politiloven § 17 d om tvangsmiddelbruk i forebyggende øyemed, gjort unntak for ransaking av private hjem, jf. særmerknaden til straffeprosessloven § 222 d i Ot.prp. nr. 60 (2004–2005) side 149, der dette påpekes. Dette kan tyde på at Stortinget ikke fant den begrensede adgangen til å benytte slikt tvangsmiddel for å avverge alvorlig kriminalitet konstitusjonelt problematisk da adgangen ble gitt. Dette fremgår imidlertid ikke klart av proposisjonen, og unnlatelsen kan også skyldes at problemstillingen er oversett. Under enhver omstendighet er man i avvergingstilfellene nærmere den kriminelle handling enn i forebyggingstilfellene, og det er grunnlag for å åpne etterforskning i avvergingstilfellene. Departementet mener at det heller ikke i dag er grunn til å innskrenke adgangen til ransaking, da bruken kan anses nødvendig og proporsjonal for å avverge så alvorlige lovbrudd som kriminalitetskravet i straffeprosessloven § 222 d forutsetter, og det er dessuten av betydning at rettssikkerhetsgarantiene er gode.

Departementet understreker at graden av inngripen for det enkelte tvangsmiddel vil være av stor betydning for vurderingen av hvorvidt det skal være adgang til å benytte tvangsmiddelet i avvergende øyemed. Det kan i den anledning bemerkes at romavlytting er ansett å være et meget inngripende tvangsmiddel, noe som blant annet kommer til syne i det strenge kriminalitetskravet for bruk av romavlytting i alminnelig etterforskning, jf. straffeprosessloven § 216 m. Når man til slutt fant det berettiget å åpne for metoden, var dette særlig begrunnet i endringer i kriminalitets- og trusselsituasjonen, som hadde gitt et større behov for å verne seg mot terrorhandlinger og organiserte kriminelle grupper. Samtidig ble det understreket at det er begrenset hvor langt samfunnet kan gå i å tillate romavlytting og andre inngripende metoder, uten at mange vil oppfatte prisen – i form av inngrep i den personlige sfære – som for høy, jf. Ot.prp. nr. 60 (2004–2005) side 96 flg.

Det bemerkes at Sverige har kommet til at det ikke bør gis adgang til å benytte romavlytting i avvergende øyemed, jf. Prop. 2013/14:237 side 101, der det heter:

> «Regeringen delar (…) utredningens bedömning att behovet och den förventade nyttan av hemlig rumsavlyssning i preventivt syfte inte väger upp det förventade integritetsintrånget. Hemlig rumsavlyssning bör därför inte tillåtas utom ramen för en förundersökning».

Når lovgiver nå skal vurdere om adgangen til romavlytting i private hjem i avvergende øyemed skal opprettholdes, må det blant annet ses hen til om behovet for metoden er like sterkt i dag som det var den gang bestemmelsen ble gitt. Samfunnets behov for beskyttelse defineres av risikoen for kriminalitet, og denne risikoen er et produkt av sannsynligheten for at kriminelle handlinger vil finne sted og konsekvensene av at slike handlinger inntreffer. I den sammenheng kan det

bemerkes at kriminalitetsbildet er noe endret, jf. kapittel 4 ovenfor.

Departementet vil påpeke at behovet for romavlytting synes å ha økt i takt med den teknologiske utviklingen. Profesjonaliserte kriminelle miljøer vil ofte ha kunnskap om politiets arbeidsmetoder og tilpasse seg ved å benytte tilgjengelige teknologiske løsninger for å skjule informasjon som knytter seg til den kriminelle virksomheten. Etter departementets oppfatning viser Metodekontrollutvalgets utredning og høringen at tvangsmidler som kommunikasjonsavlytting og hemmelig ransaking har tapt effekt som følge av den teknologiske utviklingen, herunder fremveksten av ulike løsninger for informasjonsbeskyttelse, jf. punkt 14.8.2 nedenfor. Informasjon som mistenkte tidligere kommuniserte over ubeskyttede forbindelser, formidles i dag gjerne gjennom kryptert IP-telefoni, herunder samtaletjenester som Skype og Viber. Dette medfører at romavlytting ofte gjenstår som politiets eneste virkemiddel for å sikre seg taleinformasjon.

Dette vil likevel kunne avhjelpes noe dersom Stortinget beslutter å åpne for dataavlesing, jf. kapittel 14 nedenfor, som også vil kunne omfatte signalene (lydstrømmen) som sendes til datamaskinen fra en mikrofon eller fra datamaskinen til en høyttaler. Det er imidlertid en ytre grense for hva politiet skal ha anledning til å foreta seg med grunnlag i en tillatelse til dataavlesing. Det er mistenktes *bruk* av datasystemet, smarttelefonen mv. som skal kunne kontrolleres gjennom dataavlesing, og den vil ikke gi politiet adgang til å fange opp informasjon som ikke er et resultat av mistenktes bruk. Slik målrettet overvåking må eventuelt foretas ved romavlytting.

Det er dessuten en fare for at de kriminelle tilpasser seg også etter at dataavlesing innføres, fra å kommunisere elektronisk til å møtes fysisk hjemme hos hverandre, for eksempel dersom det er tale om små terrorceller. Tradisjonelle metoder som spaning vil kunne avdekke hvem som møtes hvor, men en vil ikke få innholdet i kommunikasjonen dem imellom. En vil i slike tilfeller ikke ha andre muligheter for å få avkreftet eller verifisert informasjon som for eksempel gir grunn til å tro at noen planlegger en alvorlig straffbar handling. En vil således kunne miste muligheten til å fange opp detaljer knyttet til gjennomføringen av handlingen (tid, sted osv.) som er nødvendig for å avverge den.

Når det gjelder terrorlovbrudd, legger departementet til grunn at terrortrusselen mot Norge økte våren 2015, i tråd med sikkerhetstjenestenes vurderinger. I trusselvurderingen februar 2015 slo PST fast at den negative utviklingen av trusselsituasjonen i Norge var forventet å fortsette i 2015, og at norsk militær deltagelse mot ISIL og al-Qaida ville bidra til å forsterke fiendebildet. Departementet bemerker at terrortrusselen synes å være noe mindre høsten 2015. Den 28. oktober 2015 uttalte PST at sannsynligheten for terrorangrep fra ISIL-sympatisører er noe redusert, som følge av at 18 personer fra de norske ekstremistmiljøene miljøene mest sannsynlig er drept i Syria, mens 9 er varetektsfengslet og siktet for terrorrelatert kriminalitet. Dette innebærer at miljøene totalt sett fremstår som noe svekket. Utviklingen fremover vil likevel være ustabil og usikker, ifølge PST, og oppfordringer, blant annet fra ISIL, kan fortsatt påvirke enkeltpersoner eller små grupper til å gjennomføre terrorangrep. Den økte tilstrømningen av flyktninger og asylsøkere til Norge kan dessuten få negative følger for trusselbildet knyttet til både det høyreekstreme og venstreekstreme miljøet i Norge. På lengre sikt er det dessuten mulig at enkelte asylsøkere vil kunne utgjøre en terrortrussel i Norge, som følge av en sårbarhet for radikalisering, jf. punkt 4.5 ovenfor. Departementet mener at behovet for bruk av avvergende tvangsmidler i dag er mer prekært enn da adgangen opprinnelig ble gitt, og at bruk av ransaking og romavlytting i private hjem i avvergende øyemed både er nødvendig og forholdsmessig, sett hen til de skader og tap av liv en terroraksjon kan medføre. Det kan i den sammenheng bemerkes at staten også har et ansvar for å verne om retten til liv og den personlige, herunder fysiske, integritet, jf. Grunnloven §§ 93 og 102 annet ledd.

Masseødeleggelsesvåpen utgjør en av de største potensielle truslene mot internasjonal stabilitet og sikkerhet. I den samordnede vurderingen fra E-tjenesten, NSM og PST for 2013 nevnes spredning av masseødeleggelsesvåpen som en reell trussel. I PSTs trusselvurdering fra 2014 og 2015 bekreftes det at iranske aktører står bak de fleste forsøk i Norge på å skaffe varer og teknologi som kan anvendes til fremstilling av masseødeleggelsesvåpen. Dette ses i sammenheng med de internasjonale sanksjonene, som har medført omfattende restriksjoner på handel med Iran. De fem faste medlemslandene i FNs sikkerhetsråd, samt Tyskland og EU, inngikk 14. juli 2015 en avtale med Iran som blant annet innebærer sanksjonslettelser, men det er for tidlig å si noe om konsekvensene for trusselsituasjonen i Norge. I lys av de skadevirkninger bruk av masseødeleggelsesvåpen kan medføre, mener departementet at det er nødvendig og forholdsmessig å opprett-

holde adgangen til avvergende tvangsmiddelbruk, herunder ransaking og romavlytting av private hjem, ved slikt lovbrudd.

Bruk av romavlytting kan også sies å være forholdsmessig i saker om spionasje og ulovlig etterretning, som gjerne omfatter utenlandske «profesjonelle spillere». I PSTs trusselvurdering februar 2015 heter det at de to statene som Norge ikke har et sikkerhetspolitisk samarbeid med, samtidig har den største etterretningskapasiteten. Den alvorligste etterretningsvirksomheten antas i 2015 å rettes mot Norges evne til å beskytte landet og politiske beslutningsprosesser. Departementet mener at det i disse utenrikspolitisk urolige tider, med blant annet konflikten i Ukraina og flyktningekrisen som bakteppe, er viktig å sikre de hemmelige tjenester tilstrekkelige verktøy til å kunne oppfylle de oppgaver tjenestene er tildelt, herunder å beskytte rikets sikkerhet.

Departementet finner etter dette gode grunner for å *opprettholde* politiets begrensede adgang til å benytte *ransaking* og *romavlytting* for å avverge alvorlig kriminalitet som nevnt i straffeprosessloven § 222 d første ledd, herunder terrorhandling, drap, grovt ran eller særlig grov narkotikaforbrytelse som ledd i virksomheten til en organisert kriminell gruppe, samt PSTs adgang til å benytte romavlytting ved avverging av terrorlovbrudd etter § 147 a, spredning av masseødeleggelsesvåpen, spionasje og ulovlig etterretning. Selv om ransaking og romavlytting i private hjem er svært inngripende metoder som kan ha konsekvenser for tredjeparter, så viser dagens trusselbilde at faren for liv, helse og sikkerhet ved ikke å få avverget de meget alvorlige lovbrudd som hjemler slik tvangsmiddelbruk, er så stor at dagens tvangsmiddeladgang må anses nødvendig, forholdsmessig og innenfor Grunnlovens skranker.

Departementet mener at det samme må gjelde ved innbrudd ved dataavlesing, dersom dette tvangsmiddelet innføres, og det foreslås derfor at adgangen *utvides* til også å omfatte *innbrudd ved dataavlesing*. Det bemerkes at 22. juli-kommisjonen i NOU 2012: 14 på side 15 ga uttrykk for at PST, med en bedre arbeidsmetodikk og et bredere fokus, kunne ha kommet på sporet av gjerningsmannen før 22. juli. Om kommisjonens syn på hvilken adgang PST bør ha for å ta i bruk inngripende metoder for å bekjempe terror, heter det i utredningen punkt 16.6 side 390:

> «Kommisjonen mener det er viktig at PST får tilgang til effektive metoder også innenfor IKT-basert informasjonsinnhenting, knyttet til de konkrete sakene hvor det foreligger et reelt behov for å undersøke om noen er i ferd med å planlegge et terrorangrep. Det vil være situasjoner der det er legitimt å ta i bruk inngripende tiltak for å beskytte det som terrorister ønsker å ramme – demokratiet som styreform og verdier som individets frihet og grunnleggende menneskerettigheter.»

Dataavlesing, herunder innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen, vil bare kunne benyttes når særlige grunner tilsier det, jf. forslag til endring av § 222 d tredje ledd annet punktum. Det foreligger således, som ved bruk av ransaking og romavlytting, et skjerpet forholdsmessighetskrav, og både politiet og domstolen må vurdere hvorvidt dette er oppfylt. Departementet legger til grunn at de rettssikkerhetsmessige garantiene her er gode.

Departementet foreslår dessuten at PSTs adgang til å benytte romavlytting *utvides* til å omfatte *trusler og attentat mot myndighetspersoner*, jf. nedenfor i punkt 13.4.4.2. Det kan i den sammenheng bemerkes at Politihøgskolens forskningsavdeling nå har foretatt en kartleggingsstudie av trusler og trusselhendelser mot norske rikspolitikere og regjeringsmedlemmer på oppdrag fra PST. Av 112 spurte stortingsrepresentanter og regjeringsmedlemmer, hadde 27 % opplevd at noen truet med å skade dem eller noen av deres nærmeste, mens 14,4 % hadde opplevd fysiske angrep eller forsøk på dette. Et levende demokrati forutsetter at folk ikke unnlater å delta i politikken på grunn av frykt for egen eller nærståendes sikkerhet. Trusler og angrep mot myndighetspersoner kan svekke grunnleggende demokratiske og konstitusjonelle funksjoner, og dette tilsier at utvidelsen er forholdsmessig og nødvendig.

Tillatelse til bruk av tvangsmidler etter § 222 d skal ikke kunne gis dersom det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep, jf. § 170 a. Det forutsettes at domstolene foretar en reell og grundig forholdsmessighetsvurdering i hver enkelt sak. Foruten de momentene som er særskilt fremhevet i § 222 d tredje ledd første punktum (indikasjons- og subsidiaritetskravene), vil blant annet lovbruddets alvorlighetsgrad og sannsynligheten for at en straffbar handling kommer til å bli begått, være sentrale momenter i vurderingen. Dette bidrar til å sikre at bruken av tvangsmidlene som er hjemlet i straffeprosessloven § 222 d ikke blir for eksessiv. Det skjerpede forholdsmessighetskravet i § 222 d tredje ledd annet punktum foreslås utvidet til å

omfatte dataavlesing og kameraovervåking på privat sted (ikke privat bolig). For øvrig vises det til punkt 13.4.5.4 om disse supplerende vilkårene for bruk av tvangsmidler i avvergende øyemed.

13.4.2 Mistankekravet

13.4.2.1 Gjeldende rett

Straffeprosessloven § 222 d krever at det er «rimelig grunn til å tro» at noen kommer til å begå enkelte nærmere bestemte alvorlige straffbare handlinger. Departementet foreslo opprinnelig å bruke formuleringen «grunn til å tro», og at mistanken dermed måte være forankret i objektive holdepunkter. Likevel skulle kravet være mindre restriktivt enn «god grunn til å tro», som flertallet i Politimetodeutvalget hadde foreslått, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.3.3 side 69–70. Justiskomiteen satte inn begrepet «rimelig» for å klargjøre kravene til saklighet, sannsynlighet og forholdsmessighet, jf. Innst. O nr. 113 (2004–2005) side 20:

> «Komiteen mener det er viktig med klare og tydelige vilkår i loven for å ivareta personvernhensyn og gjøre domstolskontrollen effektiv. Komiteen mener det er behov for en ytterligere klargjøring av mistankekravet i straffeprosesslovens § 222 d første ledd. Dette kan gjøres ved at lovteksten bruker begrepet «rimelig grunn». Dette innebærer en ytterligere klargjøring av krav til saklighet, sannsynlighet og forholdsmessighet.»

Det uttalte pedagogiske formålet med tilføyelsen tilsier at det ikke var meningen å skjerpe de krav til grunn som fremgikk av proposisjonen, jf. Bjerke/Keiserud/Sæther, Straffeprosessloven kommentarutgave Bind I (4. utgave, Oslo 2011) side 795. Det fremgår av Ot.prp. nr. 60 (2004–2005) punkt 13 side 148 at uttrykket «grunn til å tro» skal forstås på samme måte som i §§ 222 a og 222 c. Det stilles således ikke krav til sannsynlighetsovervekt, men en teoretisk mulighet er ikke nok. Konklusjonen må være forankret i objektive holdepunkter, typisk vitneforklaringer, dokumenter eller andre bevis som indikerer at noen har planer om å begå en slik handling.

13.4.2.2 Utvalgets forslag

Utvalget konkluderer med at den nåværende formuleringen «rimelig grunn til å tro» kan beholdes. Etter de presiseringer som ble foretatt i forarbeidene til lovendringen i 2005, stilles det krav om konkrete holdepunkter for at personen(e) kommer til å begå en slik alvorlig straffbar handling som søkes avverget. Utvalget mener at det samme vilkåret også kan benyttes i tilknytning til det foreslåtte vilkåret om at det som ledd i forberedelsen allerede er begått en straffbar handling. Dette vilkåret antas å oppfylle minstekravet til mistanke som følger av Grunnloven § 102. På denne måten vil det etter § 222 d stilles et noe svakere krav til mistanke om den begåtte, straffbare handling enn det som følger av de alminnelige hjemler for tvangsmiddelbruk, der kravet er «skjellig grunn til mistanke». Dette oppveies imidlertid av at det også må være rimelig grunn til å tro at en mer alvorlig straffbar handling kommer til å bli begått. I merknaden heter det:

> «Kriteriet «rimelig grunn til å tro» skal forstås i samsvar med de presiseringer som ble gjort i samband med lovendringene i 2005 (se punkt 22.1.1). Det nye er at dette vilkåret ikke bare stilles i relasjon til at noen kommer til å begå en alvorlig forbrytelse, men også i relasjon til at noen allerede, som ledd i forberedelsen av denne, har begått en straffbar handling som kan medføre fengselsstraff. Mens det i den førstnevnte relasjon kreves en prognose om hva som vil skje i fremtiden, må det i den sistnevnte relasjon foretas en sannsynlighetsbedømmelse av hva som allerede har skjedd. Det stilles imidlertid ikke et like høyt krav til sannsynligheten for en begått forbrytelse etter § 222d som ved ordinær tvangsmiddelbruk på etterforskingsstadiet, der kravet er «skjellig grunn» til mistanke. Dette kompenseres imidlertid av at § 222d både stiller krav til konkret mistanke om at noe straffbart har skjedd og at en alvorlig forbrytelse kan komme til å bli begått.»

13.4.2.3 Høringsinstansenes syn

Oslo politidistrikt er enig i at kriteriet «rimelig grunn til å tro» ikke bare må gjelde i relasjon til om noen kommer til å begå en alvorlig forbrytelse, men også i relasjon til at noen allerede, som ledd i forberedelsen til denne, har begått en straffbar handling som kan medføre fengselsstraff.

Advokatforeningen støtter generelt alle endringer om innsnevring og presisering av § 222 d.

Enkelte høringsinstanser ønsker en ytterligere skjerping av vilkårene.

KROM er uenig med utvalget i at lovforslaget går klar av Grunnloven § 102 ved å legge mistan-

kekravet i forhold til allerede begåtte handlinger til «rimelig grunn til å tro». KROM gir uttrykk for at når Grunnloven hjemler «Husinkvisisjoner» kun i kriminelle tilfeller, må det i det minste foreligge sannsynlighetsovervekt for at en kriminell handling er begått, med andre ord at det foreligger «skjellig grunn til mistanke». Uansett om lovforslaget går klar av Grunnloven § 102, mener KROM at det må foreligge skjellig grunn til mistanke. Dette begrunnes med at dersom listen for sannsynlighet for begåtte straffbare handlinger legges for lavt, vil dette innebære nær sagt en blankofullmakt for ransaking og romavlytting av privat bolig, noe som vil kunne åpne for misbruk. KROM mener imidlertid at det er tilstrekkelig at det stilles krav om «rimelig grunn til å tro» når det gjelder fremtidige handlinger som skal avverges.

Også *Forsvarergruppen av 1977* mener at mistankekravet bør heves til «skjellig grunn» for at det er begått en straffbar handling. Det gis uttrykk for at det i det minste bør være sannsynlighetsovervekt for at det foreligger «kriminelle Tilfælde», jf. Grunnloven § 102. Uten et slikt beviskrav, mener forsvarergruppen at inngangskriteriene i § 222 d blir for vide, og det vises til tvangsmiddelets svært inngripende karakter.

Ellers gir *Oslo statsadvokatembeter* uttrykk for at det er prinsipielt betenkelig at lovens system forutsetter en prognose om svært alvorlige handlinger. Embetet mener at det lett vil fremstå som lite attraktivt for norske dommere å avslå begjæringer om for eksempel telefonkontroll i avvergende øyemed for å forhindre et drap.

13.4.2.4 Departementets vurdering

Departementet mener, i likhet med Stortinget ved vedtakelsen av straffeprosessloven § 222 d, at kriteriet «rimelig grunn til tro» stiller et tilfredsstillende krav til saklighet, sannsynlighet og forholdsmessighet. Departementet finner dessuten at et slikt mistankekrav er innenfor den konstitusjonelle rammen, jf. punkt 5.1. Departementet foreslår derfor å beholde mistankekravet uendret.

13.4.3 Kriminalitetskravet

13.4.3.1 Gjeldende rett

Det oppstilles krav om at den straffbare handling som skal kunne avverges er av en viss alvorlighet (kriminalitetskravet). Politiet kan etter straffeprosessloven § 222 d bruke tvangsmidler for å avverge terrorhandlinger eller trussel om terrorhandlinger (straffeloven §§ 131 eller 134), drap som ledd i motarbeiding av rettsvesenet (straffeloven §§ 275 jf. 157 eller 275 jf. 159), eller drap, grovt ran eller særlig grov narkotikaforbrytelse som ledd i virksomheten til en organisert kriminell gruppe (jf. straffeloven §§ 232 annet ledd, 275 eller 328, jf. straffeloven § 79 bokstav c).

Det fremgår av Ot.prp. nr. 60 (2004–2005) punkt 6.2.4 side 65 at hovedformålet med lovarbeidet var å bedre politiets muligheter til å avverge *den aller groveste kriminaliteten*, og at behovet for å beskytte samfunnet mot grov kriminalitet måtte veies mot hensynet til personvern og rettssikkerhet for de berørte. Til tross for begrenset støtte under høringen, viderefører departementet forslaget i høringsbrevet om å utforme kriminalitetskravet i straffeprosessloven § 222 d slik at bare noen få utvalgte straffbare handlinger kunne gi grunnlag for bruk av tvangsmidler i avvergende øyemed, og departementet manet til måtehold ved valg av disse, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.2.4 side 66–67:

> «En slik løsning åpner for å målrette metodebruken mot de forbrytelseskategoriene som det er aller viktigst å avverge, og hvor risikoen for at metodebruken rammer personer som ikke har gjort seg fortjent til det, er relativt lav. For departementet har det vært viktig å utforme de nye hjemlene slik at bruken av integritetskrenkende tvangsmidler som kommunikasjonsavlytting, romavlytting og ransaking, først og fremst rammer de tunge og organiserte kriminelle miljøene. Personer som velger å være en del av eller å ha befatning med slike miljøer, må i større grad enn andre finne seg i at samfunnet holder dem under oppsikt.
>
> I spørsmålet om hvilke forbrytelseskategorier som skal kunne søkes avverget med hjemmel i den nye § 222 d, har departementet lagt vekt på at det er spørsmål om å åpne for anvendelse av svært inngripende etterforskingsmetoder som romavlytting og kommunikasjonsavlytting uten at det foreligger sannsynlighetsovervekt for at en straffbar handling er begått. Personvernhensyn tilsier derfor at lovgiverne utviser en stor grad av måtehold når det tas stilling til hvilke forbrytelser som skal kunne søkes avverget ved bruk av tvangsmidler.»

Departementet ga uttrykk for at det var særlig viktig å gjøre politiet bedre i stand til å avdekke planer om forbrytelser som vil kunne ha *uopprettelige skadevirkninger*, for derved å stå bedre rustet til å avverge forbrytelsene. Terroraksjoner ble trukket frem som et åpenbart eksempel på

handlinger hvor samfunnets interesse av avverging var så stor at bruk av slike inngripende tvangsmidler kunne forsvares. Ved de øvrige utvalgte straffbare handlinger som kunne gi grunnlag for bruk av tvangsmidler i avvergende øyemed, forsettlig eller overlagt drap, grovt ran og særlig grove narkotikaforbrytelser, ble det oppstilt tilleggsvilkår om at forbrytelsen vil utøves som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven 1902 § 60 a. Dette ble begrunnet slik:

> «[…] Begrensningen til organisert kriminalitet er etter departementets syn viktig for å oppnå en tilfredsstillende målretting av metodebruken. Følgende eksempel illustrerer betydningen av dette tilleggsvilkåret: Dersom det er grunn til å tro at en person som er en del av et organisert ransmiljø, planlegger nye grove ran som ledd i gruppens virksomhet, vil retten kunne gi politiet tillatelse til å iverksette for eksempel romavlytting for å bringe klarhet i om det er hold i mistanken. Dersom mistanken knytter seg til en tidligere ustraffet person, som heller ikke har forbindelseslinjer til noe organisert kriminelt miljø, kan det etter departementets forslag ikke gis slik tillatelse. Selv om samfunnets interesse av å beskytte seg mot grove ran er det samme enten ranet begås av en organisert gruppe eller ikke har denne forskjellsbehandlingen etter departementets syn gode grunner for seg. Synspunktet er at personer som har gjort kriminalitet til en levevei, eller som pleier nære bånd til organiserte kriminelle grupper, ikke har samme krav på beskyttelse mot overvåkning som andre. Personer uten tilknytning til en organisert kriminell gruppe bør på den annen side være forskånet fra å bli utsatt for integritetskrenkende inngrep som romavlytting og kommunikasjonsavlytting, med mindre det foreligger sannsynlighetsovervekt for at vedkommende har begått en alvorlig kriminell handling.»

Anvendelsesområdet for den såkalte «mafia-paragrafen» i straffeloven 1902 § 60 a (straffeloven § 79 bokstav c) er utvidet. I Justisdepartementets Meld. St. 7 (2010–2011) ble det uttalt at manglende bruk av bestemmelsen kunne tyde på at den hadde et for snevert anvendelsesområde og at det således var behov for justeringer. Dette sluttet Stortinget seg til. I Prop. 131 L (2012–2013) ble bestemmelsen foreslått utvidet for å være mer anvendelig på løsere grupperinger og nettverk. Siktemålet var å gjøre bestemmelsen til et mer effektivt redskap for å bekjempe organisert kriminalitet. Lovendringen ble vedtatt av Stortinget 20. juni 2013 og trådte i kraft dagen etter.

13.4.3.2 Utvalgets forslag

Utvalget påpeker at den sentrale begrunnelse for å tillate tvangsmiddelbruk i avvergende øyemed, er at det er fare for svært alvorlige straffbare handlinger som vil kunne påføre enkeltmennesker eller samfunnet ubotelig skade. I slike tilfeller mener utvalget det er rimelig at det gis anledning til å bruke skjulte tvangsmidler for lettere å kunne avverge at forbrytelsen blir realisert.

Politiets adgang til tvangsmiddelbruk i avvergende øyemed bør etter utvalgets mening fortsatt begrenses til avverging av et fåtall svært alvorlige forbrytelsestyper, jf. § 222 d første ledd. Utvalget slutter seg til utgangspunktet om at metodebruken så langt som mulig bør målrettes. Utvalget er enig i at terrorhandlinger (straffeloven 1902 § 147 a, straffeloven §§ 131–134) bør medregnes. For så vidt gjelder grove ran (straffeloven 1902 § 268 annet ledd, straffeloven § 328), er begrensningen til ran som begås som ledd i virksomheten til en organisert kriminell gruppe etter utvalgets syn berettiget, fordi det nettopp er i slike situasjoner at faren for at det går menneskeliv tapt er særlig stor. Utvalget er mer i tvil om grov narkotikaforbrytelse begått innenfor en organisert kriminell gruppe bør kunne gi grunnlag for avvergende tvangsmiddelbruk (straffeloven 1902 § 162 tredje ledd jf. § 60 a, straffeloven § 232 annet ledd jf. § 79 bokstav c). Utvalget påpeker at selv om narkotikaomsetning har svært skadelige følger, er disse noe mer indirekte og langsiktige enn følgene av de øvrige forbrytelsestyper som i dag medregnes i § 222 d annet ledd. Utvalget uttaler likevel at det ikke fremmes noe endringsforslag her.

Utvalget går deretter over til å drøfte begrensningen i § 222 d til drap som det er rimelig grunn til å tro at vil bli utført som ledd i virksomheten til en organisert kriminell gruppe (jf. straffeloven 1902 § 233 jf. § 60 a, straffeloven § 275 jf. § 79 bokstav c) eller som ledd i motarbeidelsen av rettsvesenet (jf. straffeloven 1902 § 132 a, straffeloven §§ 157–159). Utvalget har vanskelig for å se hvorfor det bør skilles etter hvilken sammenheng det planlagte drapet inngår i, og mener at drap uansett er en så alvorlig og uavvendelig krenkelse av menneskelivet at politiet bør ha anledning til å søke det avverget. Det vises til at skjulte tvangsmidler uansett bare vil kunne tas i bruk dersom det må antas at inngrepet vil gi opplysninger av vesentlig betydning for å kunne avverge handlingen og at avverging ellers i vesentlig grad vil bli

vanskeliggjort, jf. § 222 d tredje ledd første punktum. Utvalget foreslår derfor å ta bort tilleggskriteriene knyttet til drap.

13.4.3.3 Høringsinstansenes syn

Riksadvokaten og *Oslo politidistrikt* slutter seg til forslaget om å endre straffeprosessloven § 222 d slik at det åpnes for metodebruk for å avverge drap, uavhengig av om straffeloven 1902 § 60 a eller § 132 a (straffeloven § 79 bokstav c eller §§ 157–159) er anvendelig.

Også *Kripos* støtter utvalgets forslag om å innta straffeloven 1902 § 233 om drap (straffeloven § 275) i listen over straffebud som gir grunnlag for slik tvangsmiddelbruk uten å knytte dette til straffeloven 1902 § 60 a om organisert kriminalitet (straffeloven § 79 bokstav c), men uttaler seg ikke eksplisitt om tilknytningen til straffeloven 1902 § 132 a (straffeloven §§ 157–159).

Oslo statsadvokatembeter stiller spørsmål om hvorfor det ansees viktigere å beskytte menneskelivet i en sammenheng, men ikke en annen, og mener forskjellen kommer tydelig frem ved drap. Det bemerkes at det heller ikke er enkelt å forstå at for eksempel forbrytelser med livsvarig invaliditet er så mye mindre beskyttelsesverdig enn drap.

Oslo politidistrikt påpeker at utvalget gir uttrykk for tvil om overtredelse av straffeloven 1902 § 162 tredje ledd jf. § 60 a (straffeloven § 232 annet ledd jf. § 79 bokstav c) bør gi grunnlag for bruk av tvangsmidler i avvergende øyemed, men at henvisningen til nevnte bestemmelser er utelatt i lovforslaget, til tross for at utvalget konkluderer med at det ikke fremmes noe endringsforslag om dette. Oslo politidistrikt anfører at selv om tvangsmidler i avvergende øyemed er mindre praktisk i narkotikasaker, bør det, som fremholdt av utvalget, ikke foretas noen endring her.

Også *Kripos* er enig i at straffeloven 1902 § 162 tredje ledd jf. § 60 a (straffeloven § 232 annet ledd jf. § 79 bokstav c) fortsatt bør inngå i bestemmelsen, og legger til grunn at det formentlig beror på en utilsiktet feil at bestemmelsen har falt ut i lovendringsforslaget i utredningen.

13.4.3.4 Departementets vurdering

Departementet mener tiden er moden for en ny vurdering av om tilknytningen til organisert kriminalitet skal opprettholdes som vilkår for bruk av tvangsmidler i avvergende øyemed ved forsettlig og overlagt drap, jf. straffeloven § 275. Departementet legger vekt på at både utvalget og samtlige høringsinstanser som har uttalt seg om problemstillingen, herunder *Riksadvokaten*, *Oslo politidistrikt*, *Kripos* og *Oslo statsadvokatembeter*, gir uttrykk for at tilleggskriteriet om organisert kriminalitet bør fjernes ved slik kriminalitet. Flertallet av høringsinstansene mener dessuten at det bør åpnes for metodebruk i avvergende øyemed uavhengig av om straffeloven 1902 § 132 a (straffeloven §§ 157–159) er anvendelig, altså om det er grunn til å tro at noen kommer til å begå et drap som ledd i motarbeiding av rettsvesenet.

Departementet støtter utvalget i at drap, uavhengig av hvilken sammenheng det inngår i, er en så alvorlig krenkelse av menneskelivet at politiet bør ha anledning til å benytte tvangsmidler for å søke det avverget. En endring her vil dessuten kunne minske bruken av nødrett som hjemmel, og slik sørge for bedre kontroll med tvangsmiddelbruken.

Departementet bemerker for øvrig at forsettlig og overlagt drap er forbrytelser som vil ha uopprettelige skadevirkninger, i motsetning til grovt ran og særlig grove narkotikaforbrytelser, hvor faren for at det går menneskeliv tapt er mer avledet. Departementet mener at tilleggskriteriet om organisert kriminalitet, jf. straffeloven § 79 bokstav c, er berettiget og bør opprettholdes ved de sistnevnte forbrytelser.

I forlengelsen av dette foreslår departementet at det også foretas en endring i § 222 d annet ledd bokstav d, som gir PST utvidet myndighet til å benytte tvangsmidler for å avverge integritetskrenkelser, herunder drap, jf. nedenfor i punkt 13.4.4.2.1. Her stilles det krav om at handlingen retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater. *Oslo statsadvokatembeter* reiser spørsmål om hvorfor avverging av grove integritetsforbrytelser etter nevnte bestemmelse kun knyttes til en bestemt personkrets; innehavere av de høyeste stillinger i våre tre statsmakter. Dette antas å være en konsekvens av PSTs oppgaver, jf. politiloven § 17 b, der det vises til straffeloven kapittel 17 og § 184 og sikkerhetsloven (straffeloven 1902 kapittel 9 om «Forbrydelser mod Norges Statsforfatning og Statsoverhoved»). Departementet foreslår at straffeloven § 275 fjernes fra annet ledd bokstav d, da det ikke bør kreves slik tilknytning ved drap, og da PST vil ha tilstrekkelig hjemmel i § 222 d første ledd til å benytte tvangsmidler for å avverge drap generelt.

I likhet med *Oslo politidistrikt* og *Kripos* mener departementet at det fortsatt bør være adgang til å bruke tvangsmidler i avvergende

øyemed der det er rimelig grunn til å tro at noen kommer til å begå grove narkotikaforbrytelser som ledd i organisert kriminalitet, jf. straffeloven § 232 annet ledd jf. § 79 bokstav c. Selv om de skadelige følgene av slikt lovbrudd er noe mer indirekte og langsiktige, er de av svært alvorlig karakter, og departementet ønsker ikke å svekke politiets evne til å bekjempe slike narkotikalovbrudd. Det legges dessuten vekt på at begrensningen til organisert kriminalitet er tilstrekkelig for å oppnå en tilfredsstillende målretting av metodebruken, samt at deltagere i organiserte kriminelle grupper ikke bør ha samme krav på beskyttelse mot overvåking som andre. Det antas at også utvalget har konkludert slik og at det beror på en utilsiktet feil at bestemmelsen har falt ut i utredningens lovendringsforslag.

13.4.4 PSTs utvidede myndighet

13.4.4.1 Mistankekravet

Bestemmelsen i § 222 d annet ledd gir PST en utvidet hjemmel til å bruke skjulte metoder for å avverge alvorlige forbrytelser som hører inn under PSTs ansvarsområde. Grunnvilkåret er her «grunn til å tro», og i motsetning til i første ledd satte ikke Justiskomiteen inn ordet «rimelig» her.

Utvalget legger til grunn at det trolig skyldes en inkurie at straffeprosessloven § 222 d annet ledd om PSTs utvidede adgang til avvergende tvangsmiddelbruk kun krever «grunn til å tro», jf. utredningen punkt 22.1.1 side 227. Utvalget foreslår derfor å endre § 222 d på dette punktet, slik at det stilles samme krav til mistanke («rimelig grunn til å tro»), enten tillatelsen skal gis til PST eller politiet for øvrig.

Det er få *høringsuttalelser* som knytter seg konkret til mistankekravet i § 222 d annet ledd. *Oslo statsadvokatembeter* antar at forskjellen mellom første og annet ledd skyldes en «lapsus» fra Justiskomiteens side. Det gis uttrykk for at det naturligvis er mulig at komiteen har ment at det for PSTs del skulle kreves en lavere sannsynlighetsgrad for å kunne benytte tvangsmidler i avvergende øyemed enn etter straffeprosessloven § 222 d første ledd, men at det ikke er noen uttalelser som tyder på dette i komiteens innstilling. Statsadvokatembetet mente for øvrig at det ville være søkt om det skulle kreves en lavere sannsynlighetsgrad ved avverging av forberedelse til terror etter straffeloven 1902 § 147 a siste ledd (straffeloven § 131 tredje ledd), som var opplistet i § 222 d annet ledd, enn selve terrorhandlingen etter § 147 a første ledd (straffeloven § 131 første ledd jf. annet ledd) som var opplistet i første ledd.

Departementet legger til grunn at det trolig ikke har vært Justiskomiteens hensikt å kreve en lavere sannsynlighetsgrad for at PST skal kunne benytte tvangsmidler i avvergende øyemed etter straffeprosessloven § 222 d annet ledd enn etter bestemmelsens første ledd. Departementet foreslår derfor at tilsvarende ordlyd («rimelig grunn til å tro») inntas i bestemmelsens annet ledd og tredje ledd siste punktum. Det påpekes at dette ikke er ment å innebære noen realitetsendring. Også etter gjeldende rett må det foreligge objektive holdepunkter for at noen kommer til å begå en nærmere bestemt alvorlig straffbar handling.

13.4.4.2 Kriminalitetskravet

13.4.4.2.1 Gjeldende rett

Som nevnt gir § 222 d annet ledd PST en utvidet adgang til å bruke tvangsmidler for å avverge de mest alvorlige av de forbrytelsene tjenesten har til oppgave å forebygge og etterforske. Dette gjelder enkelte lovbrudd mot statens selvstendighet og grunnleggende nasjonale interesser (straffeloven §§ 111, 113, 115, 117, 119, 123, 126, 128 første punktum eller 129), terrorforbund (straffeloven § 133), terrorfinansiering (straffeloven § 135), deltakelse i terrororganisasjon (straffeloven § 136 a) eller ulovlig befatning med farlig materiale mv. (straffeloven § 142). Adgangen gjelder også handlinger som er straffbare etter eksportkontrolloven § 5, enkelte straffbare handlinger begått med sabotasjehensikt (straffeloven §§ 139, 140, 192, 194, 238, 239, 240, 241, 242, 355, 356, 357 eller 358) og enkelte forbrytelser som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller tilsvarende organer i andre stater (straffeloven §§ 251, 253, 254, 263, 273 eller 275).

For romavlytting som omhandlet i straffeprosessloven § 216 m er adgangen ytterligere begrenset, jf. straffeprosessloven § 222 d tredje ledd siste punktum. Slik avlytting kan etter bestemmelsen kun benyttes for å avverge en handling som rammes av straffeloven §§ 121, 123, 125, 126 (ulovlig etterretningsvirksomhet), §§ 131, 133, 134 (terrorhandlinger, terrorforbund og terrortrusler) eller § 142 (ulovlig befatning med farlig materiale mv.). Den særskilte begrensningen er begrunnet i at romavlytting anses som et enda mer inngripende tiltak enn de øvrige metoder PST kan benytte med hjemmel i straffeprosessloven § 222 d.

13.4.4.2.2 Utvalgets og PSTs forslag

Utvalget er enig i at PST bør ha en noe videre hjemmel for bruk av tvangsmidler i avvergende øyemed, slik det i dag følger av § 222 d annet ledd. Som følge av den foreslåtte innstrammingen av vilkårene i § 222 d, foreslår imidlertid utvalget å fjerne forbund om terrorisme (straffeloven 1902 § 147 a fjerde ledd) og forbund om visse allmenfarlige forbrytelser (straffeloven 1902 § 159) fra listen i tredje ledd. Begrunnelsen er at dette er forberedelseshandlinger som ikke i seg selv medfører alvorlige skader på individ eller samfunn. Utvalget mener at slik § 222 d foreslås utformet, vil mistanke om forberedelseshandlinger typisk oppfylle vilkåret om at det som ledd i forberedelsen allerede er begått en straffbar handling, mens listen over de forbrytelsestyper som kan søkes avverget bør begrenses til straffbare handlinger som i seg selv kan ha alvorlige skadefølger. Av samme grunn mener utvalget at også straffeloven 1902 § 147 b om terrorfinansiering og § 104 a om deltagelse i samfunnsskadelige organisasjoner bør holdes utenfor. Slike handlinger kan imidlertid utgjøre straffbare forberedelseshandlinger til andre forbrytelser som inngår på listen i forslaget til ny § 222 d.

Utvalget er av den oppfatning at det trolig beror på en inkurie at straffeloven 1902 § 151 a om kapring ikke er nevnt i § 222 d annet ledd bokstav c, i listen over straffbare handlinger som kan gi PST grunn til å bruke tvangsmidler i avvergende øyemed dersom de er begått med sabotasjehensikt. Utvalget mener dette synet støttes av at straffeloven 1902 § 159 om forbund om å begå blant annet kapring *er* inkludert, samt at straffeloven 1902 § 151 a også er inkludert i en oppregning av hvilke former for sabotasje departementet mente man burde kunne avverge ved hjelp av tvangsmidler, jf. Ot.prp. nr. 60 (2004–2005) punkt 9.4.2.2 side 131:

> «Departementet går derfor inn for at sabotasjehandlinger bør nevnes særskilt i lovteksten, men avgrenses til nærmere bestemte straffbare handlinger som begås med sabotasjehensikt, jf. for eksempel straffeloven §§ 148, 150, 151 a, 151 b, 152 annet ledd, 153 første til tredje ledd og 154.»

Utvalget foreslår derfor at § 151 a tas inn på listen over de forbrytelsestyper som kan gi PST grunnlag for avvergende tvangsmiddelbruk.

Når det gjelder hvilke tvangsmidler som kan benyttes, foreslår utvalget at PST bare skal gis tillatelse til å romavlytte, jf. § 216 m, for å avverge en handling som rammes av straffeloven 1902 §§ 90, 91, 91 a, 152 a eller 153 a.

PST ønsker på sin side å utvide adgangen til romavlytting til også å gjelde ved avverging av trusler eller angrep mot myndighetspersoner. Dette formidles i høringsnotat 12. juli 2012 om kriminalisering av forberedelse til terrorhandlinger, utvidet adgang til tvangsmiddelbruk og endringer i straffeloven 1902 § 60 a, se punkt 2.4. Tjenesten vurderer det slik at tilsvarende faglige grunner som i dag begrunner at romavlytting tillates for de positivt oppregnede straffebudene i straffeprosessloven § 222 d tredje ledd siste punktum, også gjør seg gjeldende når trusler og angrep mot myndighetspersoner skal avverges.

13.4.4.2.3 Høringsinstansenes syn

PST er uenig i at forberedelseshandlinger ikke alene skal kunne begrunne tvangsmiddelbruk i avvergende øyemed og at blant annet straffeloven 1902 §§ 147 a tredje (senere fjerde) ledd og 159 fjernes fra listen i straffeprosessloven § 222 d andre ledd. PST antar videre at det er en inkurie at straffeloven 1902 § 147 a ikke er opplistet over de straffebud som kvalifiserer for bruk av romavlytting, og kan ikke se at en slik endring er behandlet av utvalget. I sin uttalelse til høringsnotatet 12. juli 2012 foreslår PST at straffeloven 1902 § 147 c om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, legges inn i oppramsingen av bestemmelser i straffeprosessloven § 222 d annet ledd bokstav a og tredje ledd siste punktum.

Oslo statsadvokatembeter gir noen generelle betraktninger om de lovbrudd som er omfattet, uten å kommentere utvalgets forslag spesielt. Det påpekes blant annet at straffeloven 1902 § 94, som rammer flere konkrete forberedelseshandlinger, ikke er med i opplistingen, og at det derfor ikke kan iverksettes telefonkontroll for å avverge at noen innlater seg med en fremmed stat med formål å utføre spionasje. Statsadvokatembetet mener videre at det er oppsiktsvekkende at § 104 a annet ledd er omfattet, siden både Straffelovkommisjonen og Lund-utvalget foreslo bestemmelsen opphevet. Videre stilles det spørsmål om PST adgang til å benytte tvangsmidler for å avverge grove integritetsforbrytelser kun knyttes til en bestemt personkrets, nemlig innehavere av de høyeste stillinger i våre tre statsmakter.

Det nasjonale statsadvokatembetet, *Hordaland politidistrikt* og *Politijuristene (Norges juristforbund)* støtter uttrykkelig forslaget om å tillate romavlytting for å avverge trussel eller angrep mot

myndighetspersoner. Høringsinstansene fremholder blant annet at ytringer og trusler mot myndighetspersoner har økt i omfang de senere årene, samtidig med at innholdet generelt er blitt grovere og mer alvorlig. Trusselsituasjonen tilsier derfor at det foreligger et behov for å utvide adgangen til å benytte romavlytting i denne sakstypen.

Riksadvokaten mener at dersom metoden skal tillates, bør den begrenses til å gjelde voldelige angrep mot myndighetspersoner. Fra høringsuttalelsen hitsettes:

> «Romavlytting fremstår etter vårt syn som mindre egnet metode for å avverge *trusler* mot myndighetspersoner. Fremsatte trusler vil i så fall være grunnlaget for å iverksette/begjære slik metodebruk. Dersom departementet finner at det kan påvises et særlig behov for etterforskingsmetoden, bør den begrenses til å gjelde voldelige angrep mot myndighetspersoner.»

Høringsinstansen viser samtidig til straffeprosessloven § 222 d annet ledd bokstav d som mulig norm for ny regulering.

13.4.4.2.4 Departementets vurdering

Forbund

Departementet vil påpeke at det i Ot.prp. nr. 60 (2004–2005) punkt 9.4.2.2 side 129–130 ble foretatt en grundig vurdering av hvilke av de straffbare forholdene som er nevnt i politiloven § 17 b første ledd som burde kunne kvalifisere til avvergende bruk av tvangsmidler som ledd i etterforskning. Målsetningen var å finne frem til en god balanse mellom de kryssende hensynene som gjorde seg gjeldende og til en snever og presis oppregning:

> «Ettersom rettssikkerhetshensyn og hensynet til personvernet taler for å begrense avvergende bruk av tvangsmidler, bør slik bruk bare tillates for å avverge de mest alvorlige straffbare handlingene som omfattes av politiloven § 17 b første ledd. I utgangspunktet gir strafferammen et dekkende uttrykk for hvor alvorlig lovbruddet er. I enkelte tilfeller kan imidlertid ønsket om å forhindre at handlingen blir gjennomført veie så tungt at bruk av tvangsmidler bør tillates selv om den øvre strafferammen ikke er særskilt høy.»

Her ble også enkelte bestemmelser om forbund drøftet, og departementet konkluderte for eksempel med at deltagelse i samfunnsskadelige organisasjoner skulle kvalifisere til slik tvangsmiddelbruk, i motsetning til forbund om å begå forbrytelser mot rikets sikkerhet:

> […] Departementet har vurdert om også § 94 (forbud mot å inngå forbund om å begå forbrytelser mot rikets sikkerhet) bør kunne kvalifisere for slik bruk av tvangsmidler, men har kommet til at det vil rekke for langt å inkludere denne forbundsbestemmelsen. Paragraf 94 vil imidlertid ofte kunne danne grunnlag for å iverksette etterforskning, fordi det regelmessig vil være rimelig grunn til å undersøke om noen har inngått et straffbart forbund om ulovlig etterretningsvirksomhet.
>
> Departementet går inn for at også straffeloven § 104 a skal kunne kvalifisere for bruk av tvangsmidler i forebyggende øyemed, men bare de groveste overtredelsene som kan straffes med fengsel inntil 6 år, jf. § 104 a første ledd annet punktum og § 104 a annet ledd jf. første ledd annet punktum.»

Departementet mener fortsatt at det ikke kan være avgjørende for adgangen til bruk av tvangsmidler i avvergende øyemed om handlingen i seg selv direkte medfører alvorlig skade på individ eller samfunn. Også forberedelseshandlinger, som på sikt vil kunne lede til andre og mer alvorlige skadefølger, må kunne hjemle slik bruk.

Etter straffeloven § 133 første ledd (straffeloven 1902 § 147 a fjerde ledd) er det å inngå forbund om å begå en terrorhandling gjort straffbart. Dette er et eksempel på at noe som ellers ville vært straffri forberedelse, er gjort straffbart ved et eget straffebud. Straffbarhetsterskelen inntrer i tid *før* det alminnelige forsøksansvaret, jf. straffeloven § 16 (straffeloven 1902 § 49). Forbrytelsen er fullbyrdet idet forbundet inngås, og det er dermed ikke adgang til straffritt å tre tilbake dersom avtalen senere skrinlegges. Høyesterett har i Rt. 2013 side 789 tatt stilling til innholdet i § 147 a fjerde ledd om terrorforbund i den såkalte Davud-saken. Førstvoterende uttaler at det må foreligge en reell avtale om slikt forbund, men det stilles ikke krav om at det skal være avtalt nærmere detaljer omkring terrorhandlingen, jf. avsnitt 31.

Inngåelse av terrorforbund er en alvorlig forbrytelse, hvor strafferammen etter straffeloven 1902 § 147 a fjerde ledd var 12 år. Alvorlighetsgraden er også fremhevet i forarbeidene til bestemmelsen, jf. Ot.prp. nr. 61 (2001–2002) punkt 15 side 136:

> «[…] For å markere at det er ekstra straffverdig å inngå forbund om terrorhandlinger, skal slike forbundshandlinger straffes med fengsel inntil 12 år. De særskilte forbundsbestemmelsene har stort sett en øvre strafferamme på 10 år. Tredje ledd skal ikke anvendes i konkurrens med de særlige forbundsbestemmelsene som knytter seg til bestemmelsene det er vist til i første ledd.»

I straffeloven er 12 års strafferamme på generelt grunnlag ikke videreført, og strafferammen for terrorforbund er satt til fengsel inntil ti år, jf. § 133 første ledd. Dette innebærer ikke at lovbruddet anses mindre alvorlig enn tidligere. Departementet vil påpeke at lovbruddets alvorlighetsgrad fortsatt gjenspeiles i den høye strafferammen og legger vekt på at terrorforbund av lovgiver er vurdert som ekstra straffverdig. Dette tilsier at utvalgets forslag ikke tas til følge. Det er heller ikke i tidens ånd å fjerne forberedelseshandlinger til terror som grunnlag for å iverksette bruk av tvangsmidler i avvergende øyemed. Det nevnes i den sammenheng at virkeområdet til § 222 d etter utvalgets utredning er utvidet til å omfatte også kvalifisert deltagelse i terrororganisasjon (straffeloven 1902 § 147 d, straffeloven § 136 a). Slik handling ble kriminalisert ved lov 21. juni 2013 nr. 85, som trådte i kraft straks. Det vises til Prop. 131 L (2012–2013) Endringer i straffeloven 1902 og straffeloven 2005 mv. (forberedelse av terror m.m.) punkt 7.6 side 42, hvor det heter:

> «Straffeloven 1902 § 104 a annet ledd er angitt som en særskilt hjemmel for bruk av tvangsmidler som nevnt i straffeprosessloven §§ 200 a om skjult ransaking, 202 c om teknisk sporing og § 216 a om kommunikasjonskontroll. I forlengelsen av dette foreslås at også overtredelse av forbudet mot deltakelse i terrororganisasjoner, kan danne grunnlag for anvendelsen av disse tvangsmidlene. Disse endringene i straffeprosessloven har ikke vært på høring. Det anses ikke påkrevd siden forslaget til straffeloven 1902 § 147 d bare delvis er en utvidelse av virkeområdet til straffeloven 1902 § 104 a annet ledd. Også det forhold at lovforslaget rammer mer alvorlige forhold enn straffeloven 1902 § 104 a annet ledd, jf. skjerpede straffbarhetsvilkår og høyere strafferamme, taler for denne løsningen. Idet forbudet mot terrororganisasjoner rammer særskilte forberedelseshandlinger, blir det også viktigere at tvangsmidler kan benyttes for å stanse handlingene.
>
> Tvangsmidler kan også benyttes i avvergende øyemed ved brudd på straffeloven 1902 § 104 [a] annet ledd, jf. straffeprosessloven § 222 d. Med samme begrunnelse som ovenfor foreslås at tvangsmidler også kan benyttes i avvergende øyemed for å hindre overtredelse av forbudet mot deltakelse i en terrororganisasjon.»

Departementet går etter dette ikke inn for utvalgets forslag om å fjerne bestemmelsene om terrorforbund som grunnlag for å iverksette bruk av tvangsmidler i avvergende øyemed.

Departementet legger videre til grunn at det beror på en inkurie at straffeloven 1902 § 147 a (straffeloven §§ 131–134) om terrorhandlinger i utvalgets forslag ikke er opplistet blant de straffbare handlinger som kvalifiserer for bruk av romavlytting, jf. § 222 d tredje ledd, og kan ikke se at en slik endring er behandlet av utvalget. Det kan se ut som om bestemmelsen er tatt ut som følge av at bestemmelsen om forbund om terrorisme (straffeloven 1902 § 147 a fjerde ledd) er foreslått fjernet fra den særskilte bestemmelsen om PSTs utvidede myndighet i § 222 d annet ledd. Det er imidlertid på det rene at PST også har anledning til å benytte tvangsmidler for å avverge handlinger som nevnt i § 222 d første ledd, herunder terrorhandlinger. Slik departementet ser det, er det ingen grunn til å fjerne PSTs adgang til romavlytting for å avverge slike handlinger. Bestemmelsen bør forbli uendret.

Bør det kunne benyttes tvangsmidler for å avverge ytterligere terrorrelaterte handlinger?

PST foreslår i sin høringsuttalelse til høringsnotatet 12. juli 2012, at straffeloven 1902 § 147 c (straffeloven § 136) og de nye bestemmelsene om terrorforberedelse legges inn i oppramsingen av bestemmelser i straffeprosessloven § 222 d annet ledd bokstav a og tredje ledd siste punktum, samt i oppregningen i straffeprosessloven § 200 a første ledd, § 202 c første ledd og § 216 a første ledd litra b, jf. punkt 7.4.11 ovenfor.

PST peker på de lave strafferammene i bestemmelsene om terrorforberedelse og mener det er behov for å bøte på problemene rundt metodeadgang og muligheten til å anvende materialet fra metoder som bevis. Ifølge PST skyldes problemet de restriktive reglene i Norge for bruk av overskuddsinformasjon, hvor hovedregelen er at materiale innhentet ved bruk av en metode, eksempelvis kommunikasjonskontroll, ikke kan brukes som bevis for straffbare forhold som ikke i

seg selv gir adgang til metoden. Det uttales i den sammenheng:

> «Det er i dag et vanlig scenario at det foreligger grunn til å tro at noen kommer til å begå en terrorhandling eller inngå forbund om en slik handling. Det igangsettes så en avvergende etterforsking etter straffeprosessloven § 222 d (avvergende etterforskning), hvor en vil ha full metodeadgang, og hvor det f eks kan anvendes kommunikasjonskontroll (KK) og romavlytting. Slik reglene er i dag, er det kun hvis man tar ut tiltale for overtredelse av straffeloven § 147 a (terrorhandlinger) at alle opplysninger fra metodebruken i den avvergende etterforsking kan brukes. Videre kan f eks KK-informasjon brukes for straffeloven § 147 b (terrorfinansiering).
>
> […]
>
> Det er PSTs erfaring at den viktigste beviskilde i terrorsakene er avlytting av kommunikasjon. Dette gjelder der flere er involvert og i saker om rekruttering, finansiering og trening. Det vil også være viktig mot soloterrorister f eks ved avdekking av anskaffelse av gjenstander og bruk av internett. I saker om oppfordring til terror kan det være avgjørende med tanke på å skaffe informasjon rundt hvem som f.eks. har fremsatt oppfordringen på internett. Dersom PST ikke kan bruke informasjon fra avlytting av kommunikasjon i disse sakene, vil de i praksis ofte være virkningsløse.»

Departementet bemerker at straffeprosessloven § 216 i også gjelder ved bruk av tvangsmidler i avvergende øyemed, jf. § 222 d siste ledd siste punktum. Ved lov 21. juni 2013 nr. 86, som trådte i kraft 13. september s.å., ble det gitt utvidet adgang til å bruke opplysninger fra kommunikasjonskontroll og romavlytting om andre straffbare forhold enn dem etterforskningsskrittet var ment å avdekke – såkalt «overskuddsinformasjon» – som bevis. Dette ble begrunnet med at et forbud mot bruk av overskuddsinformasjon som bevis for straffbare forhold som ikke i seg selv kunne ha begrunnet den aktuelle metodebruken, harmonerer dårlig med politiets generelle plikt til å forebygge og oppklare straffbare handlinger. Etter lovendringen skal slik overskuddsinformasjon kunne brukes som bevis såfremt det «etter sakens art og forholdene ellers ikke vil være et uforholdsmessig inngrep» og «oppklaring av saken uten bruk av overskuddsinformasjonen i vesentlig grad vil bli vanskeliggjort», jf. Prop. 147 L (2012–2013) kapittel 5 side 72–84 og side 178–179. Endringen vil i noen grad kunne avhjelpe den situasjon PST beskriver.

Det kan likevel stilles spørsmål om straffeloven § 136 (straffeloven 1902 § 147 c) om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, bør inntas i listen over lovbrudd som gir adgang til avvergende bruk av tvangsmidler som ledd i etterforskning, jf. straffeprosessloven § 222 d annet ledd bokstav a. Det bemerkes i den sammenheng at både svensk og finsk rett åpner for bruk av tvangsmidler i avvergende øyemed i slike saker.

Det faktum at bestemmelsen om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger har samme strafferamme som kvalifisert deltagelse i terrororganisasjon etter straffeloven § 136 a (straffeloven 1902 § 147 d), som nå er inntatt, kan tilsi slik innlemmelse. Mot dette kan det innvendes at straffebudet har en noe annen karakter enn forbundsbestemmelsene som er opplistet i § 222 d annet ledd bokstav a og som begrunnet innlemmelsen av § 147 d om kvalifisert deltagelse i terrororganisasjon. På den annen side er det likhetstrekk mellom handlinger som rammes av straffeloven § 128 første punktum (straffeloven 1902 § 104 a), som allerede er omfattet i oppramsingen i straffeprosessloven § 222 d annet ledd, og straffeloven § 136 (straffeloven 1902 § 147 c). Forskjellen mellom § 128 første punktum og § 136, er at førstnevnte rammer rekruttering til terrorgruppe, men ikke rekruttering til terrorhandlinger som sådan, i motsetning til sistnevnte bestemmelse.

Terrorvirksomhet er svært alvorlig kriminalitet, som ofte har forgreninger på tvers av landegrenser og som i stor grad rammer det sivile samfunnet. Gjennom den frykt og utrygghet terrorhandlinger skaper, rammer terrorhandlinger dessuten bredere enn tap av menneskeliv og materielle skader. Utviklingen de senere årene viser at vi står overfor et mer skjerpet, fragmentert og uoversiktlig trusselbilde. Dette fremgår av Nasjonalt risikobilde 2013, utarbeidet av Direktoratet for samfunnssikkerhet og beredskap, side 146 og den samordnede trussel- og sårbarhetsvurderingen 2013 *(«Trusler og sårbarheter 2013. Samordnet vurdering fra E-tjenesten, NSM og PST»)* side 7. Ekstreme gruppers oppfordring, rekruttering og opplæring til terror fremheves som en kilde til økt risiko for vold og terrorhandlinger:

> «I Norge er det et multietnisk ekstremt islamistisk miljø som utgjør kjernen i terrortrusselen. Miljøet består hovedsakelig av unge menn oppvokst i Norge. Miljøet har flere handlings-

> orienterte ledere, og de formidler en ekstremistisk retorikk der blant annet Norge er sentral i fiendebildet. Det forventes at dette miljøet fortsatt vil være aktivt med på å radikalisere, rekruttere, spre voldelig propaganda samt samle inn penger.
>
> […]
>
> Reisevirksomheten kan være med på å øke trusselen. Dette fordi de som reiser kan få økt vilje og evne til å gjennomføre terrorhandlinger på norsk jord, eller mot norske interesser i utlandet. På slike utenlandsopphold får de ideologisk skolering, kamperfaring og utvider kontaktnettet til ekstreme islamister. Viktigst er at de ved å ta del i krigshandlinger kan få økt mental evne og vilje til å utføre vold og drap. Voldspotensialet i deler av miljøet forventes derfor å kunne øke.»

Oppfordring, rekruttering eller opplæring til terrorhandlinger vil senere kunne avføde nettopp slike. Departementet mener det er hensiktsmessig å kunne benytte tvangsmidler allerede for å avverge de opprinnelige, forberedende lovbruddene for å unngå at disse handlingene avføder kriminalitet. Dersom slike terrorrelaterte handlinger i større grad kan avverges, vil det kunne bidra til å redusere den generelle terrortrussel som kan tilskrives rekruttering og opplæring til terrorvirksomhet. Den siste tiden har vist at dette er en aktuell problemstilling også her i landet, hvor et økende antall mennesker rekrutteres til å reise til for eksempel Syria. Terrorrelaterte handlinger er i seg selv alvorlige lovbrudd og har dessuten et så omfattende avledet skadepotensiale at hensynet til kriminalitetsbekjempelse bør veie tyngre enn hensynet til personvernet.

Departementet mener imidlertid at det ikke er påvist et tilstrekkelig behov for å tillate bruk av det inngripende tvangsmiddelet romavlytting for å avverge rekruttering og opplæring til terrorhandlinger, jf. PSTs forslag om å innta bestemmelsen i § 222 d tredje ledd siste punktum. Nødvendighets- og forholdsmessighetskravet anses her ikke oppfylt.

Bør det kunne benyttes romavlytting for å avverge trussel eller angrep mot myndighetsperson?

Som det fremgår av høringsnotatet 12. juli 2012 etterspør PST en adgang til å kunne benytte romavlytting for å avverge trusler eller angrep mot myndighetspersoner. Slike trusler eller angrep utgjør meget alvorlige forbrytelser, som kan føre til vidtrekkende konsekvenser i form av forstyrrelse av sentrale samfunnsmessige funksjoner. Dette tilsier at PST gis tilstrekkelig effektive virkemidler til å avverge denne kriminalitetsformen.

Departementet understreker imidlertid at høy alvorlighetsgrad ikke i seg selv er tilstrekkelig som begrunnelse for inngripende tvangsmiddelbruk. For å tillate et så vidt inngripende tvangsmiddel som romavlytting, må det i tillegg kunne påvises et konkret behov for å ta i bruk metoden for å avverge den aktuelle sakstypen.

I PSTs åpne trusselvurdering for 2014 uttales under overskriften «Trusler mot myndighetspersoner» følgende:

> «Hvert år etterforsker vi et relativt stabilt antall saker relatert til fremsatte trusler mot myndighetspersoner. Fremsatte trusler er primært ment for å skremme, og representerer svært sjelden en faktisk vilje til å utføre handlingen det trues med. Antall straffesaker relatert til trusler mot myndighetspersoner i det kommende året, vil trolig være uendret. Straffbare trusler vil i hovedsak bli rettet mot sentrale medieeksponerte politikere, og i noen tilfeller medlemmer av kongehuset.»

Det fremgår samtidig at norske myndighetspersoner kun et fåtall ganger har blitt utsatt for fysiske angrep, men at en likevel må ta høyde for at personer i løpet av kort tid kan utvikle vilje til å skade en myndighetsperson på grunn av for eksempel personlige forhold eller politisk misnøye.

Temaet omhandles også i den samordnede trussel- og sårbarhetsvurderingen 2013 fra E-tjenesten, NSM og PST, hvor det fremgår:

> «Majoriteten av de som fremsetter trusler mot norske myndighetspersoner anses å være psykisk ustabile. Det er generelt lite samsvar mellom truslene som fremsettes og den faktiske viljen og evnen til å utføre handlingen det trues med. Erfaringer fra andre europeiske land tilsier at de som faktisk angriper en myndighetsperson, gjør dette uten at det er blitt fremsatt konkrete trusler i forkant. Ofte har personen på en eller annen måte tilkjennegitt sterk misnøye med eller hatt et bekymringsfullt fokus på myndighetspersonen forut for angrepet. I noen tilfeller har angrep vært spontane og uten forvarsel.»

Det fremgår av PSTs trusselvurdering 2015 at økt aktivitet og eksponering i forbindelse med høstens valg vil føre til at politikere blir mer utsatt for negativ oppmerksomhet i det kommende året. Sterkt personfokus i kombinasjon med saker som

oppfattes som kontroversielle, har tidligere forårsaket trusselrelaterte hendelser.

Politihøgskolens forskningsavdeling, ved doktorgradsstipendiat Heidi Fischer Bjelland og professor i politivitenskap Tore Bjørgo, har foretatt en kartleggingsstudie av trusler mot norske rikspolitikere og regjeringsmedlemmer på oppdrag fra PST. Funnene ble presentert i rapporten Trusler og trusselhendelser mot politikere (PHS Forskning 2014: 4). Her fremgår det at av 112 spurte stortingsrepresentanter og regjeringsmedlemmer, hadde 27 % opplevd at noen truet med å skade dem eller noen av deres nærmeste, mens 14,4 % hadde opplevd fysiske angrep eller forsøk på dette. Slike lovbrudd kan svekke grunnleggende demokratiske og konstitusjonelle funksjoner.

Til tross for at trusler mot myndighetspersoner ikke nødvendigvis manifesterer seg i faktiske angrep, viser funnene etter departementets syn at det er en reell fare for at sentrale myndighetspersoner kan bli utsatt for voldelige angrep, og at trusler mot myndighetspersoner ikke er et uvanlig forekommende fenomen i det norske samfunnet. Departementet vil i den forbindelse understreke at ikke bare faktiske angrep, men også rene trusler, kan forstyrre politikere eller andre i deres virke og få dem til å begrense sine uttalelser og handlinger. Trusler og angrep mot myndighetspersoner kan svekke grunnleggende demokratiske og konstitusjonelle funksjoner. Et levende demokrati forutsetter at folk ikke unnlater å delta i politikken på grunn av frykt for egen eller nærståendes sikkerhet. For å sikre demokratiet og den liberale samfunnsformen, er det viktig at trusler, så vel som faktiske angrep, kan bekjempes på en effektiv måte. Departementet er av den oppfatning at romavlytting etter omstendighetene kan være et nødvendig og forholdsmessig virkemiddel i så henseende, jf. også punkt 13.4.1.4 ovenfor, der det slås fast at en slik utvidelse er innenfor Grunnlovens skranker.

Etter departementets oppfatning kan også sammenhengen i lovverket tale for at det åpnes for avvergende bruk av romavlytting i den her omtalte sakstypen. Etter politiloven § 17 d første ledd bokstav c kan PST benytte ulike former for skjulte tvangsmidler – i utgangspunktet også romavlytting – for å forebygge handlinger som rammes av straffeloven §§ 251, 253, 254, 256, 263, 273, 274 eller 275 og som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater. De nevnte bestemmelsene rammer alvorlige voldshandlinger og trusler mot statsorganene og deres medlemmer. Etter departementets syn er det naturlig at lovbrudd som kan begrunne tvangsmiddelbruk i forebyggende øyemed, også skal kunne brukes for å avverge disse. Det vises til følgende uttalelse i Ot.prp. nr. 60 (2004–2005) punkt 9.4.2.2 side 129:

> «Sammenhengen i regelverket tilsier at de straffbare handlingene som skal kunne forebygges ved bruk av tvangsmidler utenfor etterforsking, dvs. terrorhandlinger, ulovlig etterretningsvirksomhet og de mest alvorlige formene for vold eller trusler mot representanter for våre øverste statsmyndigheter eller representanter for tilsvarende organer i andre land, også bør kunne avverges ved bruk av tvangsmidler som ledd i etterforsking.»

Når romavlytting i prinsippet er tillatt for å *forebygge* trusler og angrep mot myndighetspersoner, bør metoden også kunne brukes for å *avverge* slike handlinger. Det foreslås derfor at PST skal kunne benytte romavlytting for å avverge handlinger som rammes av straffeloven §§ 251, 253, 254, 256, 263, 273, 274 eller 275 og som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater.

Øvrige forhold

Ved lovendring 10. desember 2010 nr. 76 ble en inkurie rettet opp slik at også straffeloven 1902 § 151 a om kapring nå er nevnt i oppregningen i lovteksten, jf. Prop. 141 L (2009–2010) pkt. 11.4 side 138. Utvalgets oppfordring om å inkludere bestemmelsen blant de straffbare handlinger som PST kan bruke tvangsmidler for å avverge er således allerede fulgt. Dette er videreført også etter ikraftsettingen av straffeloven, ved at straffeloven § 142 er inntatt i straffeprosessloven § 222 d annet ledd bokstav a.

For øvrig ble straffeloven 1902 § 153 a opphevet ved lov 22. juni 2012 nr. 49 (i kraft 22. juni 2012), som følge av at innholdet ble inkorporert i § 152 a. I § 222 d annet ledd bokstav a og tredje ledd tredje punktum er henvisningen til § 153 a nå fjernet, som følge av opphevelsen, jf. Prop. 53 L (2012–2013) og lov 24. mai 2013 nr. 18.

13.4.5 Supplerende vilkår og saksbehandlingsregler

13.4.5.1 Gjeldende rett

Tredje ledd inneholder supplerende vilkår for avvergende metodebruk. Tillatelse til bruk av

tvangsmidler kan bare gis dersom det må antas at «inngrepet vil gi opplysninger av vesentlig betydning for å kunne avverge handlingen» (indikasjonskravet), og at «avverging ellers i vesentlig grad vil bli vanskeliggjort» (subsidiaritetskravet). Ordet «antas» medfører at det må foreligge mer enn en ren formodning om at tvangsmiddelbruken vil oppfylle de to vilkårene. Sannsynlighetsovervekt kreves likevel ikke. Kjernen i disse vurderingstemaene – som til en viss grad glir inn i hverandre – er at tvangsmidler bare skal kunne anvendes hvor det er en viss sannsynlighet for at tvangsmiddelbruken vil gi opplysninger som kan bidra til å avverge en handling som nevnt i annet ledd, og bare hvor det må antas at mindre inngripende etterforskningsmetoder vil komme til kort, jf. Ot.prp. nr. 60 (2004–2005) punkt 13.1 side 149. I denne vurderingen kan domstolen også ta hensyn til en fornuftig ressursanvendelse, slik at tvangsmidler i enkelte situasjoner vil kunne tillates brukt selv om tilsvarende opplysninger for eksempel kunne vært fremskaffet ved omfattende og ressurskrevende spaning. Videre skal retten ta hensyn til om politiet har begrenset tid til rådighet for å få avverget handlingen og om alternative fremgangsmåter vil kunne innebære at noens liv og helse settes i fare, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.4.3 side 71–72.

I tillegg gjelder forholdsmessighetskravet etter straffeprosessloven § 170 a. De samme momentene vil være relevante her som ved alminnelig tvangsmiddelbruk, men enkelte vil kunne være noe mer tungtveiende ved forholdsmessighetsvurderingen av tvangsmiddelbruk i avvergende øyemed. Ved innføringen av regelen understreket departementet at mistankens styrke er relevant også i denne forbindelse, og at det, dersom det er svært sannsynlig at en alvorlig straffbar handling vil bli begått, sjelden vil være uforholdsmessig å tillate tvangsmiddelbruk for å avverge handlingen, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.5.2 side 73. Videre uttalte departementet at § 222 d er utformet slik at tvangsmiddelbruken som regel vil rette seg mot personer som tilhører eller har nære bånd til et organisert kriminelt miljø. Dersom politiet likevel har grunnlag for å gripe inn overfor personer uten slik tilknytning, kan det være grunn til å praktisere et strengt forholdsmessighetsprinsipp.

For enkelte særlig integritetskrenkende tvangsmidler gjelder det et skjerpet forholdsmessighetskrav. Det er et tilleggsvilkår at det må foreligge «særlige grunner» for å kunne benytte hemmelig ransaking, teknisk sporing av person, kommunikasjonsavlytting og romavlytting, jf. § 222 d tredje ledd annet punktum. Kravet er ment å markere at det her skal mer til enn ellers for å tillate bruk av tvangsmidler i avvergende øyemed, men innebærer ikke at forholdsmessighetsvurderingen i disse tilfellene skal være vesensforskjellig fra den som må foretas i tilknytning til mindre inngripende tvangsmidler.

Videre gjelder de bestemmelsene som ordinært regulerer bruken av det aktuelle tvangsmiddelet som nå benyttes i avvergende øyemed «så langt de passer», jf. § 222 d femte ledd første punktum. Her siktes det særlig til saksbehandlingsreglene. Informasjon innhentet gjennom slik tvangsmiddelbruk er underlagt den særlige taushetsplikten etter § 216 i, og denne bestemmelsen regulerer også den videre bruken av den innhentede informasjonen.

Beslutning om bruk av etterforskningsmetoder i avvergende øyemed treffes av retten ved kjennelse. Ordre fra påtalemyndigheten kan tre i stedet for kjennelse av retten dersom det ved opphold er stor fare for at den aktuelle handlingen ikke vil kunne avverges, jf. § 222 d fjerde ledd første punktum. Unntaket er ment å fange opp behovet for umiddelbart å komme i gang med tvangsmiddelbruken hvor politiet har opplysninger om at en alvorlig straffbar handling er nært forestående. Beslutningen skal imidlertid forelegges retten for godkjennelse snarest mulig og senest 24 timer etter at tvangsmiddelet ble tatt i bruk. Straffeprosessloven § 216 d første ledd tredje til femte punktum om påtalemyndighetens hastekompetanse gjelder tilsvarende. For kompetansefordelingen innenfor påtalemyndigheten gjelder § 216 d annet ledd. Påtalemyndighetens beslutning skal så vidt mulig være skriftlig og opplyse om hva saken gjelder og om formålet med bruken av tvangsmidlet. Muntlig beslutning skal snarest mulig nedtegnes.

13.4.5.2 Utvalgets forslag

De øvrige vilkår for avvergende tvangsmiddelbruk, slik disse fremgår av straffeprosessloven § 222 d tredje ledd, utgjør etter utvalgets oppfatning en viktig begrensing, og skal sikre at tvangsmidler bare brukes i avvergende øyemed dersom det er strengt påkrevd. Utvalget foreslår ingen endringer her.

13.4.5.3 Høringsinstansenes syn

Oslo statsadvokatembeter uttaler at det ikke er helt enkelt å forstå på hvilken måte en domstol skal kunne ha en begrunnet oppfatning om indika-

sjonskravet. Også subsidiaritetskravet forutsetter en hypotetisk vurdering som, ifølge statsadvokatembetet, selvsagt må fremstå som ytterst problematisk for en domstol. Det settes også spørsmålstegn ved hva som egentlig skal ligge i det skjerpede krav til forholdsmessighet. Samlet sett anføres det at lovgiveren har gitt domstolene en oppgave som nesten er umulig dersom loven skal tas på ordet. Dette kan medføre at lovens krav fremstår som «fasadepynt» som ikke følges i praksis, med de åpenbare uheldige konsekvenser som dette kan innebære. Statsadvokatembetet understreker at det kan reises prinsipielle motforestillinger mot å involvere domstolene i beslutninger av denne karakter, til tross for at lovgiver, ved å legge beslutningsansvaret til domstolene, selvsagt har søkt å ivareta rettssikkerhetshensyn.

13.4.5.4 Departementets vurdering

Departementet vil innledningsvis slå fast at domstolskontrollen med avvergende tvangsmiddelbruk representerer en viktig rettssikkerhetsgaranti. Dette dannet også utgangspunktet for departementets vurdering i Ot.prp. nr. 60 (2004–2005) punkt 6.7.2 side 76:

> «Etter departementets syn bør kompetansen til å tillate bruk av tvangsmidler i avvergende øyemed legges til domstolene. 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 at folk skal ha tillit til at misbruk ikke skjer. Disse hensynene får særlig vekt ved metodebruk i avvergende øyemed, ettersom det ikke er noe vilkår for bruken av tvangsmidler at personen de retter seg mot, mest sannsynlig har begått en straffbar handling. […] På et område som dette må rettssikkerhetshensyn veie tungt. […]»

Departementet var den gang innforstått med at lovforslaget ville innebære at domstolene ville få en mer fremtredende rolle i etterforskningsfasen, og bemerket at daværende tingrettsdommer Tor Langbach i Lov og Rett 2000 (side 309–314) hadde pekt på mulige betenkeligheter ved en slik utvikling. Han viste blant annet til at dommerne i stadig større grad involveres i politiets taktiske vurderinger og beslutninger allerede på etterforskningsstadiet, og at domstolenes avgjørelser ofte må skje uten reell kontradiksjon – for eksempel når det fremmes begjæringer om kommunikasjonskontroll. Departementet var enig med Langbach i at det ikke var uten betenkeligheter å involvere domstolene i større utstrekning på etterforskningsstadiet, men var likevel av den oppfatning at fordelene ved å kreve at tillatelse må gis av retten på forhånd – først og fremst ved den økte rettssikkerheten som ligger i forhåndskontroll ved en nøytral instans – oppveide ulempene. Departementet opprettholder også i dag dette standpunktet.

Videre vil departementet understreke at de strenge indikasjons-, subsidiaritets- og forholdsmessighetskravene ikke bare angir den terskel som *domstolen* skal legge til grunn for sin vurdering av om det foreligger hjemmel for å benytte tvangsmidler i avvergende øyemed, men også gir klare anvisninger til *politiet* om når tillatelse kan gis.

Det bemerkes i den anledning at Kontrollutvalget for kommunikasjonskontroll (KK-utvalget) i årsrapporten for 2014 konkluderer med at politiets bruk av kommunikasjonskontroll gjennomgående er forsvarlig og godt begrunnet. Det gis uttrykk for at Norge generelt har en høy faglig og etisk standard i politiet, at regelverket, saksbehandlingen og gjennomføringen er lagt opp slik at avgjørelsene om å begjære bruk av kommunikasjonskontroll blir behandlet og kvalitetssikret på flere nivåer i politiet, samt at politiet ønsker å ha en godt underbygd sak når det ber om rettens tillatelse. Samlet sett innebærer dette et strengt tiltaks- og kontrollregime som bidrar til en høy grad av rettssikkerhet i denne type saker. KK-utvalget er av den oppfatning at kvaliteten på grunnlagsrapportene de siste årene er blitt enda bedre og nå gjennomgående er meget tilfredsstillende. Det fremmes stort sett bare begjæringer om avlytting i saker som politiets ledelse oppfatter som saker som forventes å føre til domfellelse og strenge straffer. KK-utvalget har ikke rettet alvorlig kritikk til politiet i noen enkeltsak i 2013.

Departementet mener at de strenge kravene som stilles for å kunne anvende tvangsmidler i avvergende øyemed, er med å sikre at politiet ikke uberettiget ber om tillatelse til slik tvangsmiddelbruk. Den høye kvaliteten på underlagsrapportene fra politiet bidrar til å gjøre domstolens kontrolloppgave enklere. For øvrig er påtalemyndighetens objektivitetsplikt, som gjelder hele dets virksomhet, også på etterforskningsstadiet, nå kodifisert i straffeprosessloven § 55 fjerde ledd, som trådte i kraft 13. september 2013.

13.5 Tvangsmiddelbruk i forebyggende øyemed

13.5.1 Generelt

Ved lov 17. juni 2005 nr. 87 ble PST gitt adgang til å bruke tvangsmidler for å kunne forebygge de mest alvorlige forbrytelsene innenfor tjenestens arbeidsområde, jf. politiloven § 17 d. Bestemmelsene trådte i kraft august samme år, jf. kgl. res. 5. august 2005 nr. 849. Som forebyggende virksomhet regnes den informasjonsinnhenting PST driver uten at vilkårene for å igangsette etterforskning er oppfylt, det vil si uten at det er rimelig grunn til å undersøke om det foreligger et straffbart forhold, jf. straffeprosessloven § 224 første ledd.

Bakgrunnen for at det ble åpnet for bruk av tvangsmidler også i forebyggende øyemed var at PSTs virksomhet i stor grad skal være forebyggende, og at målet ofte vil være å sørge for at det ikke blir grunnlag for å iverksette etterforskning, jf. Ot.prp. nr. 60 (2004–2005) punkt 9.1 side 112. Departementet påpekte at forebyggingsaspektet er særdeles viktig. Det sentrale er å oppdage mulige trusler mot samfunnssikkerheten tidligst mulig, helst lenge før hendelsesforløpet har kommet så langt at grensen for det straffbare er nådd. Departementet slo fast at det var et misforhold mellom de forventningene som stilles til PSTs forebyggende arbeid og de virkemidlene tjenesten har lovlig tilgang til som ledd i sin forebyggende virksomhet.

Justiskomiteen støttet departementet, jf. Innst. O. nr. 113 (2004–2005) punkt 9.2 side 33, hvor det heter:

> «Komiteen viser til at Politiets sikkerhetstjeneste (PST) har en særlig viktig rolle for å forebygge og etterforske handlinger som truer sikkerheten i samfunnet. Innbyggerne har forventninger til at PST skal oppdage og forhindre trusler mot samfunnssikkerheten før disse realiseres. Komiteen mener det er en viktig oppgave å sikre tjenesten arbeidsvilkår og metoder som gjør dette mulig, men samtidig må disse metodene ikke være egnet til å redusere tilliten til PST.»

Beslutningen om bruk av slike tvangsmidler vil kunne bli kontrollert i ettertid av EOS-utvalget.

Utvalget går inn for at adgangen til å bruke tvangsmidler i forebyggende øyemed i hovedsak beholdes som i dag.

Enkelte av *høringsinstansene* knytter generelle kommentarer til forholdet mellom bruk av skjulte tvangsmidler i avvergende og forebyggende øyemed.

Oslo statsadvokatembeter påpeker at hjemmelen for avvergende tvangsmidler er plassert i straffeprosessloven, med den konsekvens at bruken av disse behandles av politiet som påtalemyndighet med statsadvokatene og riksadvokaten som overordnede myndigheter. Forebyggende tvangsmidler er derimot tatt ut av den ordinære, straffeprosessuelle ramme og tillagt PST som forvaltningsorgan. Oslo statsadvokatembeter understreker at PST i denne sammenheng ikke opptrer som påtalemyndighet, men som et forvaltningsorgan undergitt Politidirektoratet og Justisdepartementet. Dette har som konsekvens at PST er et politisk styrt organ i den forstand at statsråden plikter å sørge for tilsyn og faglig kontroll med virksomheten. Det anføres at det legges stor vekt på EOS-utvalgets tilsynsfunksjoner i Ot.prp. nr. 60 (2004–2005). Imidlertid nevnes det ikke at departementets virksomhet ikke er underlagt EOS-utvalget, jf. lov 3. februar 1995 nr. 7 § 6. Statsadvokatembetet mener at det dermed kan oppstå nokså underlige konstellasjoner. Dersom EOS-utvalget finner at det var kritikkverdig av PST å anvende tvangsmidler og departementet har hatt eller kan ha hatt kunnskap om dette, blir dette uheldig dersom statsråden reelt sett har ansvaret.

Statsadvokatembetet gir videre uttrykk for at begrepet forebygging er svært upresist. Det anføres at Ot.prp. nr. 60 (2004–2005) er noe uklar når det gjelder valg av spor – etterforskning eller forebygging – blant annet ved spionasje. Det uttrykkes bekymring over at PST kan binde opp påtalemyndigheten dersom det forbyggende tvangsmiddel for eksempel skulle avdekke omfattende spionasje som allerede har funnet sted, på grunn av den svært begrensede adgang som politiloven § 17 f gir til å anvende slikt materiale. Embetet mener at en lojal forståelse tilsier at dersom det foreligger rimelig grunn til å etterforske, må dette alternativ velges.

Forsvarergruppen av 1977 gir uttrykk for at snevre hjemler alltid har en tendens til å bli utvidet i praksis, og er bekymret over den manglende rett til dokumentinnsyn for den som utsettes for PSTs bruk av tvangsmidler i forebyggende øyemed. Det vises til Høyesteretts avgjørelser i Rt. 2008 side 1575 og Rt. 2009 side 1075, hvor slikt innsyn ble nektet. Dette ble blant annet begrunnet med at det dreier seg om «utøvelse av forvaltningsrettslige oppgaver uavhengig av etterforskningen», og at PST er «organisert med et klart og notorisk skille mellom virksomhetsdelene». Forsvarergruppen mener at det likevel er et betydelig

rettssikkerhetsmessig problem at manglende dokumentinnsyn hindrer kontroll med om innhentede opplysninger likevel blir brukt i etterforskningen. Det anføres at når PST opptrer både som forvaltningsorgan og etterforskende myndighet, og selv definerer tidspunktet for når man går over fra forebygging til etterforskning, er det en nærliggende fare for at opplysninger innhentet gjennom bruk av skjulte tvangsmidler i forebyggende øyemed også kan få betydning for etterforskningen. Det er dessuten en nærliggende mulighet for at den som blir etterforsket selv vil kunne gjøre nytte av de innhentede opplysninger til sitt forsvar. Forsvarergruppen ønsker derfor en lovendring som sikrer at den som blir etterforsket av PST gis innsyn også i opplysninger innhentet ved bruk av tvangsmidler i forebyggende øyemed.

Departementet bemerker at spørsmålet om innsynsrett i materiale fra skjult tvangsmiddelbruk ble behandlet i Prop. 147 L (2012–2013) punkt 4.11.4 side 59–60, hvor det heter:

> «Utvalget drøfter unntak fra innsyn i materiale fra skjult tvangsmiddelbruk på grunnlag av et utvidet saksdokumentbegrep. Etter utvalgets forslag vil slikt materiale automatisk inngå i saksdokumentene og derfor i utgangspunktet omfattes av innsynsretten. I motsetning til utvalget går departementet inn for å videreføre gjeldende saksdokumentbegrep, jf. punkt 4.4.4. Departementet er enig med riksadvokaten i at det blir en kunstig betraktningsmåte å anse materiale fra skjult tvangsmiddelbruk som del av sakens dokumenter som det må besluttes unntak for innsyn fra. Departementets forslag innebærer at gjeldende rett om materiale fra skjult tvangsmiddelbruk opprettholdes; materialet inngår ikke i saksdokumentene med mindre det er tatt i bruk under etterforskningen.»

Departementet opprettholder disse synspunktene og legger til grunn at PST lojalt skiller mellom sine forvaltningsrettslige og påtalemessige oppgaver. Det vises for øvrig til Høyesteretts avgjørelser i Rt. 2008 side 1575 og Rt. 2009 side 1075. Høyesterett anså ikke at dokumenter utarbeidet av PST i egenskap av å være forvaltningsorgan – henholdsvis innenfor sikkerhetsrådgivning og i dets «forebyggende virksomhet», jf. politiloven § 17 b første ledd – kunne regnes som en del av «sakens dokumenter». Dersom materialet er tatt i bruk under etterforskning, vil det imidlertid inngå i sakens dokumenter, som det eventuelt må besluttes unntak fra innsyn for.

Departementet legger til grunn at en lojal forståelse av dagens lovverk tilsier at dersom det foreligger grunnlag for å åpne etterforskning, bør dette alternativ i utgangspunktet velges, fremfor å benytte tvangsmidler i forebyggende øyemed. Under Justiskomiteens behandling av forslaget, ble det understreket at bruk av tvangsmidler i forebyggende øyemed skulle være en sikkerhetsventil, som bare kunne bli brukt når reglene om avverging som ledd i etterforskning ikke var anvendbare. Det vises til Innst. O. nr. 113 (2004–2005) punkt 9.2. Likevel vil departementet understreke at PST må ha en viss skjønnsmessig kompetanse til å vurdere når en sak bør gå over fra forebyggingsstadiet til etterforskningsstadiet. I den forbindelse kan det bemerkes at PST kan motta troverdige, men ikke-verifiserte opplysninger som gir grunn til å avvente den videre utvikling før eventuell etterforskning iverksettes. En del av informasjonen som PST mottar, må dessuten antas å komme fra samarbeidende utenlandske tjenester o.l. og være konfidensiell. Forholdet til kilden kan her gjøre det vanskelig å starte en etterforskning og innta informasjonen i en straffesak, både fordi PST i utgangspunktet ønsker å være lojale mot sine kilder og fordi en slik eksponering kan føre til at PST mister kilder, med uhensiktsmessig informasjonstørke som resultat. Det bemerkes for øvrig at påtalemyndighetens objektivitetsplikt nå er lovfestet i straffeprosessloven § 55 fjerde ledd, som trådte i kraft 13. september 2013.

13.5.2 Mistankekravet

Etter *gjeldende rett* kan tvangsmidler bare brukes i forebyggende øyemed der det er «grunn til å undersøke om noen forbereder en [nærmere angitt] handling». Uttrykket ble inntatt i bestemmelsen under stortingsbehandlingen av lovforslaget, og erstattet passusen «for å undersøke om noen forbereder en handling». Endringen understreker at PST, for å få tillatelse til å ta i bruk lovregulerte metoder, må godtgjøre overfor domstolen at opplysninger i det konkrete saksforholdet gir grunn til å gjennomføre nærmere undersøkelser, jf. Innst. O. nr. 113 (2004–2005) punkt 9.2 side 34. Justiskomiteens flertall uttalte at grunnen til å undersøke må være forankret i objektive holdepunkter, for eksempel saksopplysninger i form av spanings- eller infiltrasjonsopplysninger, tips, dokumentfunn eller andre bevis som indikerer at noen kan være i ferd med å forberede for eksempel en terrorhandling. Flertallet viste til at vilkåret har klare likhetstrekk med vilkåret i straffeprosessloven § 224 første ledd om når etterforskning

skal settes i verk. Grovt sett ligger det tre krav innbakt i uttrykket: Et saklighetskrav, et krav om en viss sannsynlighet for at noe er under oppseiling, og et krav til forholdsmessighet mellom det som skal undersøkes, og de virkemidler som tas i bruk, jf. innstillingen side 35.

Utvalget foreslår ingen endringer.

Av *høringsinstansene* er det kun *Oslo statsadvokatembeter* som har betraktninger om mistankekravet:

> «Det er åpenbart at det må legges inn en vurdering som knytter seg til en mulighet for en forberedelse av den straffbare handling. Det vil med andre ord si at man må legge inn en sannsynlighetsvurdering for at noen befinner seg i en forberedelsesfase til det straffbare. Hvor stor muligheten skal fremstå som, er ikke enkelt å besvare.»

Statsadvokatembetet uttaler at det er åpenbart at generelle risikobetraktninger ikke kan være relevante, og viser til Justiskomiteens uttalelse om at grunnen til å undersøke må være forankret i objektive holdepunkter. Etter statsadvokatembetets oppfatning reiser imidlertid dette nye spørsmål, for eksempel om spanings- eller infiltrasjonsopplysningene som stammer fra en pågående etterforskning kan brukes som grunnlagsmateriale for å begjære forebyggende tvangsmidler. Det gis uttrykk for at et bekreftende svar kan åpne for omgåelse av sentrale rettsikkerhetsgarantier og tunge personvernhensyn. Det anføres at dersom en spionsak henlegges av mangel på bevis, vil det være underlig om nye tvangsmidler skal kunne anvendes med utgangspunkt i det samme materialet.

Når det gjelder kvaliteten på opplysningene, anfører statsadvokatembetet at det vil være vanskelig for dommeren å etterprøve om politiets tolkning av det foreliggende materiale er korrekt. Dommeren vil lett komme i en nesten umulig tvangssituasjon. Som eksempel nevnes at politiet vurderer det som en mulighet at det foreliggende materialet kan gi grunnlag for å forhindre en terroraksjon. Dersom begjæringen avslås og handlingen inntreffer, vil dommeren lett bli tillagt ansvar.

D e p a r t e m e n t e t viser til drøftelsen i punkt 13.4.5.4 ovenfor. Domstolskontrollen representerer en viktig rettssikkerhetsgaranti, og det legges til grunn at politiet nøye og objektivt vurderer hvorvidt de strenge inngangsvilkårene for bruk av tvangsmidler i forebyggende øyemed er oppfylt, før det bes om rettens tillatelse til slik tvangsmiddelbruk. Godt grunnlagsmateriale vil gjøre det lettere for dommeren å etterprøve politiets vurdering. Det bemerkes for øvrig at påtalemyndighetens objektivitetsplikt nå er lovfestet i straffeprosessloven § 55 fjerde ledd, som trådte i kraft 13. september 2013.

13.5.3 Kriminalitetskravet

13.5.3.1 Gjeldende rett

PST kan bare bruke tvangsmidler i forebyggende øyemed for å forebygge terrorhandlinger etter straffeloven §§ 131, 133 og 134 (straffeloven 1902 § 147 a), ulovlig etterretningsvirksomhet etter straffeloven §§ 121 til 126 (straffeloven 1902 §§ 90, 91 og 91 a) og vold eller trusler mot representanter for Norges øverste statsmyndigheter eller tilsvarende organer i andre stater etter straffeloven §§ 251, 253, 254, 256, 263, 273, 274 eller 275 (straffeloven 1902 §§ 222, 223, 227, 229, 231 eller 233).

Spørsmålet om hvilke tvangsmidler PST bør gis adgang til for at tjenesten skal kunne utføre sine lovpålagte oppgaver på en best mulig måte, er blitt berørt i en rekke forskjellige sammenhenger de siste årene. Det er blant annet drøftet av Fostervoll-utvalget (vedlegg 2 til St.meld. nr. 39 (1992–93)), Sikkerhetsutvalget (NOU 1993: 3 *Strafferettslige regler i terroristbekjempelsen*), Lund-kommisjonen (Dok. nr. 15 (1995–96)), Metodeutvalget (NOU 1997: 15 *Etterforskingsmetoder for å bekjempe kriminalitet – delinnstilling II*), Danielsen-utvalget (NOU 1998: 4 *Politiets overvåkningstjeneste*), Lund-utvalget (NOU 2003: 18 *Rikets sikkerhet*) og av Politimetodeutvalget (NOU 2004: 6 *Mellom effektivitet og personvern: politimetoder i forbyggende øyemed*). For en nærmere oversikt vises det til Ot.prp. nr. 60 (2004–2005) punkt 9.3.2–9.3.4 side 115 flg.

Lund-utvalget tar i NOU 2003: 18 *Rikets sikkerhet* utgangspunkt i at inngripende tvangsmidler bare skal kunne brukes dersom det er nødvendig etter en avveining av hensynet til samfunnsvern mot hensynet til rettssikkerhet, jf. utredningen side 17–18:

> «Det må være samsvar mellom de skadevirkninger den aktuelle kriminalitet kan medføre og de metoder som tas i bruk for å bekjempe den. Kravet til forholdsmessighet tilsier som en nødvendig – men ikke tilstrekkelig – forutsetning at det er dokumentert et behov for metoden: Dette innebærer en vurdering av kriminalitetens sannsynlige skadevirkninger og av metodens økte nytteverdi for oppklaring

> og bekjempelse av kriminaliteten. Jo mer alvorlig kriminalitet og jo større skadevirkninger det er fare for, jo lavere er det naturlig å sette kravet til sannsynlighet. Det er forskjell på en terrorhandling som kan medføre tap av mange menneskeliv og et forsøk på å skaffe seg opplysninger som nok bør holdes hemmelig av hensyn til rikets sikkerhet, men hvor skadevirkningene ved kompromittering er relativt begrenset […].»

Lund-utvalget ga uttrykk for at ved inngrep som har et mer generelt forebyggende formål, for eksempel å skaffe oversikt over en organisasjon eller en personkrets som man antar kan komme til å begå straffbare handlinger rettet mot grunnleggende nasjonale interesser, måtte hensynet til rettssikkerhet og beskyttelse av personvernet veie tyngre enn hensynet til et mulig samfunnsvern. Utvalget gikk derfor ikke inn for å lovhjemle bruk av straffeprosessuelle tvangsmidler i forebyggende øyemed.

I Ot.prp. nr. 60 (2004–2005) punkt 9.3.6.1 side 122 sa departementet seg enig i Lund-utvalgets prinsipielle utgangspunkt om at det bare bør åpnes for økt bruk av tvangsmidler i den grad det er dokumentert et tilstrekkelig behov for en slik utvidelse. Departementet mente imidlertid at dette særlig ville avhenge av om trusselbildet utfordrer samfunnssikkerheten på en måte som gjør bruk av tvangsmidler nødvendig, og om adgangen til å bruke tvangsmidler etter gjeldende rett er utilstrekkelig. Etter departementets syn måtte begge spørsmålene besvares bekreftende. Departementet foreslo derfor å åpne for bruk av tvangsmidler i forebyggende øyemed, og uttalte i den sammenheng:

> «PSTs virksomhet er i langt større grad rent forebyggende enn for andre straffbare handlinger, der tvangsmidler brukes avvergende som ledd i en etterforsking som primært har til formål å strafforfølge de antatte gjerningspersonene. Når det er aktuelt for PST å anvende tvangsmidler med sikte på å forhindre for eksempel ulovlig etterretningsvirksomhet, vil det derfor ofte ikke være naturlig å karakterisere virksomheten som etterforsking. På disse områdene har PST et særskilt behov for å kunne gripe inn for å forhindre straffbare handlinger, uten at det stilles krav om at etterforsking må være iverksatt. Departementet foreslår derfor at det åpnes for at PST til en viss grad skal kunne anvende tvangsmidler også utenfor etterforsking, men bare når formålet er å forebygge terrorhandlinger, ulovlig etterretningsvirksomhet og attentatforsøk mot representanter for våre øverste statsmyndigheter. Det siste alternativet bør også omfatte de mest alvorlige formene for trusler eller vold mot representanter for tilsvarende organer i andre stater, for eksempel ved statsbesøk eller for å avverge angrep på andre staters ambassadører i Norge.»

At adgangen til å benytte tvangsmidler i forebyggende øyemed skulle være snever, understrekes også i proposisjonen punkt 9.4.2.1 side 128:

> «Fordi det reiser særlige rettssikkerhetsmessige og personvernmessige betenkeligheter å tillate bruk av tvangsmidler i slike situasjoner, går departementet inn for at hjemmelen kun skal gjelde for tre typer saker der behovet for slike virkemidler er størst: Terrorhandlinger, ulovlig etterretningsvirksomhet og de mest alvorlige formene for vold eller trusler mot representanter for våre øverste statsmyndigheter eller representanter for tilsvarende organer i andre land.»

13.5.3.2 Utvalgets og PSTs forslag

Metodekontrollutvalget gir uttrykk for at mye tyder på at en større andel av PSTs tvangsmiddelbruk skjer som ledd i forebyggende virksomhet enn i avvergende øyemed, noe som ikke er i tråd med det som ble uttrykt både av departementet og Stortinget ved innføringen av reglene. Det er imidlertid, slik utvalget ser det, ingenting som tyder på at PST bruker tvangsmidler ut over det som straffeprosessloven og politiloven tillater, jf. utredningen punkt 22.2 side 230–231. Utvalget går inn for at adgangen til å bruke tvangsmidler i forebyggende øyemed i hovedsak skal beholdes uendret, jf. utredningen punkt 22.4 side 233.

PST avga følgende høringsuttalelse under høringen av Metodekontrollutvalgets utredning:

> «PST registrerer at utvalget ikke fremmer forslag som har konsekvenser for hvilke straffebud som skal kunne utløse tvangsmiddelbruk i forebyggende øyemed. Dette innebærer at det ikke er fremmet forslag om en utviding av tvangsmiddelbruken for PST utover de straffebud som i dag allerede er omtalt i politiloven § 17d. Det er PSTs vurdering at utvalget i større grad burde vurdert og evaluert om ikke også andre straffebud enn de som i dag er oppregnet i politiloven § 17d burde kunne kvalifisere for tvangsmiddelbruk i forebyggende øyemed.

PST er av den oppfatning at de straffebud som kvalifiserer til tvangsmiddelbruk i avvergende øyemed etter straffeprosessloven § 222 d andre ledd også burde kvalifisert til tvangsmiddelbruk i forebyggende øyemed. På denne måten ville for eksempel forbudet mot spredning av plutonium (straffeloven § 152a) og forbudet mot å skaffe eller inneha bakteriologiske eller andre biologiske substanser (straffeloven 153a) kunne forebygges gjennom bruk av tvangsmidler og ikke bare avverges etter at det straffbare forhold har materialisert seg. Tilsvarende ville brudd på eksportkontrolloven kunne forebygges gjennom bruk av tvangsmidler.»

PSTs forslag om utvidelse av adgangen til å beslutte bruk av tvangsmidler i forebyggende øyemed ble sendt på høring 12. juli 2012. I høringsnotatet tas det utgangspunkt i at en rekke av de straffebud som faller innenfor PSTs mandat, ikke gir anledning til tvangsmiddelbruk i forebyggende øyemed. Det ble vist til blant annet straffeloven 1902 kapittel 8 (forbrytelser mot statens selvstendighet og sikkerhet), kapittel 9 (forbrytelser mot Norges statsforfatning og statsoverhode), § 147 b (terrorfinansiering), § 147 c (oppfordring, rekruttering og opplæring i terrorhandling), § 152 a (omgang med plutonium), § 153 a (omgang med bakteriologiske midler), samt brudd på eksportkontrolloven. Etter PSTs vurdering er dette straffebud som etter sitt innhold er ment å beskytte grunnleggende nasjonale interesser, og forebygging av slike lovbrudd krever bruk av tvangsmidler i forebyggende øyemed. Det anføres at slik endring vil innebære en større grad av parallellitet mellom tvangsmiddelbruk for å forebygge alvorlig kriminalitet og som ledd i å avverge kriminalitet etter straffeprosessloven § 222 d annet ledd.

13.5.3.3 Høringsinstansenes syn

Høringsinstansene er delt i synet på om adgangen til å beslutte bruk av tvangsmidler i forebyggende øyemed bør utvides. Under høringen av høringsnotat 12. juli 2012 var de fleste aktørene fra politiet og påtalemyndigheten positive til en utvidelse av de straffebud som kan utløse tvangsmiddelbruk i forebyggende øyemed.

Politiets Fellesforbund gir generelt full støtte til lovendringene som fremgår av høringsnotatet del I og del II. Forbundet mener disse balanserer forholdet mellom frihet og sikkerhet opp mot de forventninger samfunnet har til politiet om å skape et tryggere samfunn.

Etterretningstjenesten anser det som en svakhet ved høringsnotatet at det ikke er skissert konkrete lovforslag, da dette gjør det vanskeligere å vurdere den eksakte rekkevidden av de ulike forslag. Etterretningstjenesten støtter likevel PSTs forslag om å utvide adgangen til å bruke tvangsmidler i forebyggende øyemed.

Oslo statsadvokatembeter har ikke ytterligere bemerkninger til de enkelte forslag til regler om tvangsmidler i høringsnotatet, utover at de fremstår som vel funderte. Departementet vil påpeke at dette likevel til en viss grad er i strid med statsadvokatembetets høringsuttalelse om Metodekontrollutvalgets utredning, der en innskrenkning av hjemlene drøftes. Det gis blant annet uttrykk for at det er underlig at bestemmelsene om ordinær spionasje og flyktningespionasje (straffeloven 1902 §§ 90, 91 og § 91 a) er tatt med i oppramsingen over lovbrudd som gir adgang til bruk av tvangsmidler i forebyggende øyemed. Det uttales i den sammenheng at det er åpenbart at faren for terrorangrep mot Norge er større, mens det for spionasje er vanskelig å hevde at situasjonen skulle være spesielt alarmerende. Det pekes også på at strafferammen i § 91 a er lav, og at bestemmelsen derfor neppe kan være tatt med på grunn av forbrytelsens alvorlighetsgrad.

Det nasjonale statsadvokatembetet mener at når det gjelder bruk av metoder i forebyggende øyemed, så er det viktig at lovverket åpner opp for dette på bred front i terrorsaker, samt at det gis hjemmel for bruk i saker som omfatter lovbud som skal sikre grunnleggende nasjonale interesser eller beskytte myndighetspersoner. Dette taler for at en del av straffeprosesslovens bestemmelser om bruk av metoder bør utvides til å gjelde flere lovbud enn de som omfattes av lovverket i dag. Forslag fra PST om endringer i straffeprosessloven, og som omhandles i høringsnotatet, synes godt begrunnet og de bør etter Det nasjonale statsadvokatembetets mening gjennomføres i sin helhet, med mulig unntak for utvidelse av hastekompetansen til sjefen for PST.

Hordaland politidistrikt støtter PSTs forslag om å utvide adgangen til å bruke tvangsmidler til andre straffebestemmelser som også skal verne grunnleggende nasjonale interesser. Det påpekes at trusselbildet har endret seg siden 2005, og det er heller ikke opplysninger om misbruk eller uheldig praktisering av dagens ordning. Det legges videre vekt på at en utvidelse til andre straffebestemmelser vil omfattes av den samme rettsikkerhetskontroll utøvd av domstolen i forkant og av EOS-utvalget og andre kontrollinstanser i etterkant av tvangsmiddelbruken.

Nordre Buskerud politidistrikt uttaler at politidistriktet har begrenset erfaring i bruk av de tvangsmidlene PST ønsker endringer i, men at det generelt er viktig at PST får de hjelpemidler tjenesten mener det er et saklig behov for, slik at den står best mulig rustet til å utføre sine oppgaver. Det anføres at de erfaringene PST har gjort seg de senere år i forbindelse med konkrete saker, bør veie tungt i vurderingene av om endringene skal gjennomføres.

Andre høringsinstanser stiller seg avventende eller avvisende til forslaget om å utvide adgangen til å bruke tvangsmidler i forebyggende øyemed.

Riksadvokaten slår fast at politiets oppgaver etter politiloven § 17 d faller utenfor Riksadvokatens ansvarsområde og er underlagt Justisdepartementet. Det påpekes at en eventuell utvidelse av handlinger som omfattes av bestemmelsen, vil utvide departementets overordnede ansvar tilsvarende. Det vises for øvrig til Riksadvokatens høringssvar til Metodekontrollutvalget av 7. juli 2010 punkt 11.

Nasjonal institusjon for menneskerettigheter (UiO) anfører at departementet tilsynelatende ikke har foretatt noen vurderinger av hvordan forslagene forholder seg til Norges internasjonale menneskerettighetsforpliktelser, og at dette er i strid med hva Utredningsinstruksen foreskriver. Det påpekes at høringsnotatet inneholder forslag til lovendringer som – til dels – er av svært inngripende karakter overfor enkeltindividet. Generelt anses PSTs ønske om lovendringer som legitimt, men institusjonen gjør oppmerksom på at Norges internasjonale forpliktelser setter skranker.

Amnesty International påpeker at enhver bruk av tvangsmidler innebærer et inngrep i menneskerettigheter og vil dermed bare være akseptabelt i de tilfellene internasjonal menneskerettighetslov åpner for det. Amnesty er ikke prinsipielt kritisk til en utvidelse av mulige tvangsmidler for å avverge terrorhandlinger, dersom det bedømmes som nødvendig for at staten kan oppfylle sin forpliktelse om å ivareta sikkerheten i samfunnet. Forutsetningen er imidlertid at enhver tvangsmiddelbruk må autoriseres, på grunnlag av gjeldende lover, av en kompetent uavhengig rettsinstans som blant annet skal bedømme om inngrepet innfrir kravene om nødvendighet og er så lite omfattende som mulig.

ICJ-Norge – Den internasjonale juristkommisjon mener forslagene i høringsnotatet er av svært inngripende karakter. Det anføres at kombinasjonen av utvidet kriminalisering og utvidede hjemler for skjulte tvangsmidler i så vel etterforskningssammenheng som i forebyggende etterretning potensielt vil ramme store deler av befolkningen, uten at den enkelte har noen mulighet til å forutberegne når og under hvilke omstendigheter han eller hun kan bli gjenstand for slik skjult overvåking. Dette reiser alvorlige spørsmål i et demokratisk samfunn, blant annet om borgernes rettigheter etter Grunnloven og EMK, særlig med hensyn til personvern, ytringsfrihet, forsamlings- og organisasjonsfrihet og rettssikkerhet generelt.

Utenriksdepartementet finner ikke grunnlag for å gi nærmere kommentarer til forslagene fra PST om endringer i reglene om tvangsmiddelbruk, annet enn å vise til betydningen av også å ta hensyn til den rettsutvikling som har funnet sted i de øvrige nordiske og andre europeiske land, som alle er bundet av Den europeiske menneskerettighetskonvensjon.

Dommerforeningens menneskerettighetsutvalg mener at før det vurderes om det skal kunne tas i bruk tvangsmidler i forebyggende øyemed også for andre straffbare forhold enn de som er nevnt i politiloven§ 17 d, bør det dokumenteres et behov for bruk av tvangsmidler på et tidlig stadium også i slike saker. For øvrig påpekes det at det er en grunnleggende rettsikkerhetsgaranti at begjæring om tvangsmiddelbruk prøves av en dommer.

Datatilsynet slår fast at det påhviler staten å dokumentere at tiltak som griper inn i menneskerettighetene fyller vilkårene i menneskerettighetskonvensjonen. Tilsynet kan ikke se at departementet tilfredsstillende har utredet og dokumentert behovet for de øvrige lovforslagene.

Også *Politidirektoratet* er av den oppfatning at sentrale spørsmål i høringsnotatet fremstår som mindre gjennomarbeidet, både når det gjelder faktiske og rettslige sider. Politidirektoratet savner en nærmere analyse av behovet for endringsforslagene i politiets kontraterrorarbeid.

Den norske advokatforening mener at når det gjelder tvangsmiddelbruk, er det vanskelig å se at det foreligger noe som skulle medføre at man bør gå bort fra de vurderinger som ble foretatt av Metodekontrollutvalget.

KROM uttaler at det er forståelig at det etter en så omfattende tragedie som bomben mot regjeringsbygget og massakren på Utøya, kommer et press om at lovverket og sikkerhetstjenestens beføyelser skal kunne ta høyde for slike grusomheter. KROM mener imidlertid at hastelover bryter med de prinsipper det norske samfunn og rettsstaten er bygd på, og uttaler at det er som om Lund-kommisjonens konklusjoner for lengst er glemt, eller avgrenset til fortidens kalde krig.

13.5.3.4 Departementets vurdering

Det kan stilles spørsmål om adgangen til å bruke tvangsmidler i forebyggende øyemed er for snever etter gjeldende rett og om den bør utvides til å omfatte også andre lovbrudd. Departementet mener at tilgangen til skjulte tvangsmidler bør fastlegges ut fra PSTs behov, sett opp mot hvilke betenkeligheter som kan knyttes til tvangsmiddelbruken.

Departementet er av den oppfatning at det ikke kan være aktuelt at samtlige straffebud som kvalifiserer til tvangsmiddelbruk i avvergende øyemed etter straffeprosessloven § 222 d annet ledd, også skal gi adgang til tvangsmiddelbruk i forebyggende øyemed. Det er på det rene at lovgiver ønsket en snevrere adgang til å benytte sistnevnte inngrep. Under Justiskomiteens behandling av forslaget, ble det som nevnt understreket at bruk av tvangsmidler i forebyggende øyemed skulle være en sikkerhetsventil, som bare kunne bli brukt når reglene om avverging som ledd i etterforskning ikke var anvendbare, jf. Innst. O. nr. 113 (2004–2005) punkt 9.2. Flertallet slo fast at PSTs mulighet til å benytte tvangsmidler i forebyggende virksomhet skulle være et begrenset supplement til den anledningen PST har til å bruke tvangsmidler for å avverge som ledd i etterforskning. Risikoen for at uskyldige rammes av tvangsmidler ble vurdert som større i slike saker, og det ble derfor presisert at dette skulle være et siste virkemiddel i forebyggingen av svært alvorlige forbrytelser som begås av lukkede og profesjonelle miljøer.

Departementet mener at det reiser særlige personvernmessige og rettssikkerhetsmessige betenkeligheter å tillate bruk av tvangsmidler i forebyggende øyemed, det vil si uten at det er grunnlag for å iverksette etterforskning, og dette tilsier at adgangen bør være snevrere i slike tilfelle. Det er således ikke et mål i seg selv å oppnå en parallellitet mellom tvangsmiddelbruk for å forebygge alvorlig kriminalitet etter politiloven § 17 d og for å avverge kriminalitet etter straffeprosessloven § 222 d annet ledd. En avveining mellom hensynet til samfunnssikkerheten på den ene siden og rettssikkerhets- og personvernhensyn på den andre siden, tilsier at tvangsmidler bare bør kunne nyttes for å forebygge de mest alvorlige straffbare handlingene som hører under PSTs ansvarsområde. For øvrig antas det at den økte kriminaliseringen av forberedelseshandlinger gjør det enklere, som ledd i etterforskning, å benytte tvangsmidler for å avverge lovbrudd, slik at behovet for å benytte tvangsmidler i forebyggende øyemed blir mindre.

Departementet tar til etterretning at det er stilt spørsmål om det i tilstrekkelig grad er utredet og dokumentert et behov for bruk av tvangsmidler på det forebyggende stadiet ved andre typer lovbrudd enn terrorhandlinger, ulovlig etterretningsvirksomhet og vold eller trusler mot de øverste statsmyndigheter, jf. synspunkter fremmet i høringsuttalelser fra Dommerforeningens menneskerettighetsutvalg, Datatilsynet og Politidirektoratet. Enkelte av de lovbrudd som PST nevner, vil imidlertid kunne innebære store og uopprettelige skader. Det må være samsvar mellom de skadevirkninger det aktuelle lovbrudd kan medføre og de metoder som tas i bruk for å bekjempe lovbruddet.

Departementet er av den oppfatning at skadepotensialet er vesentlig ved ulovlig befatning med radioaktivt materiale, biologiske eller kjemiske våpen eller en kjernefysisk eller radioaktiv anordning, jf. straffeloven § 142 (straffeloven 1902 § 152 a), og at det her bør åpnes for å benytte tvangsmidler i forebyggende øyemed. Departementet bemerker at det i Prop. 96 L (2011–2012) ble foreslått lovendringer i straffebud rettet mot slike handlinger, som ledd i det internasjonale arbeidet mot terror. For at Norge skulle kunne ratifisere konvensjonen mot kjernefysisk terrorisme før straffeloven trådte i kraft, ble det foreslått å endre straffeloven 1902 § 152 a om atomlovbrudd i samsvar med straffeloven § 142. Bestemmelsen ble endret ved lov 22. juni 2012 nr. 49, som trådte i kraft straks. Den inkorporerte også innholdet i den tidligere § 153 a om befatning med bakteriologiske våpen, som samtidig ble opphevet.

Departementet bemerker at strafferammen er høy ved slike straffbare handlinger, nærmere bestemt 21 år ved ulovlig bruk, 15 år ved ulovlig befatning og 10 år ved transport eller når man på ulovlig måte søker å sette seg i besittelse av slike materialer, anordninger eller våpen, noe som illustrerer forholdets alvorlige karakter. Lovbruddet er dessuten likestilt med andre alvorlige lovbrudd, nærmere bestemt ulovlig etterretningsvirksomhet og terrorhandling, når det gjelder adgangen til romavlytting i avvergende øyemed, jf. § 222 d tredje ledd siste punktum. Slik tvangsmiddelbruk er ansett å være særlig inngripende, og dette kan tale for at de aktuelle lovbruddene er så alvorlige at tvangsmiddelbruk også bør tillates for å forebygge slik kriminalitet.

Selv om Norge ikke har masseødeleggelsesvåpen eller noen umiddelbar trussel fra slike våpen mot oss, så har vi meget avansert teknologi som kan inngå som viktige deler i utviklingen av masseødeleggelsesvåpen, se punkt 4.7. I den sam-

ordnede vurderingen fra E-tjenesten, NSM og PST for 2013 side 10 nevnes spredning av masseødeleggelsesvåpen som en trussel. Her fremgår det at spredning av materiale, teknologi og utstyr til bruk i produksjon av masseødeleggelsesvåpen blir stadig mer krevende å avdekke og kontrollere for nasjonale og internasjonale eksportkontrolletater. Dette gjentas i PSTs trusselvurdering for 2015, hvor det heter:

> «Norge er et attraktivt land for aktører som søker teknologi og kunnskap som kan brukes for å utvikle og fremstille masseødeleggelsesvåpen og leveringsmidler til disse. Slik anskaffelsesvirksomhet foregår hovedsakelig på en fordekt måte.
>
> […]Det forventes at flere aktører kan inngå ulike former for samarbeid for å omgå norsk eksportkontroll. Slikt samarbeid vil kunne etableres på tvers av nasjonalitet og over landegrenser. Denne typen anskaffelsesforsøk kan rettes mot alle typer varer, tjenester og teknologi som kan benyttes til produksjon eller utvikling av masseødeleggelsesvåpen.»

Det fremgår av PSTs trusselvurdering for 2016 at ulovlige leveranser av varer og teknologi til bekymringsland kan få store negative konsekvenser, og både norske bedrifter og norske myndigheters omdømme kan bli skadelidende. Departementet mener at dette tilsier at det er behov for forebyggende tvangsmidler ved lovbrudd som nevnt i straffeloven § 142 (straffeloven 1902 § 152 a).

13.5.4 PSTs hastekompetanse

13.5.4.1 Gjeldende rett

Sjefen eller den assisterende sjefen for PST kan selv beslutte igangsetting av teknisk sporing av kjøretøy, jf. straffeprosessloven § 202 b, og samtykkebasert avlytting av samtaler, jf. § 216 l, jf. politiloven § 17 d fjerde ledd. Annen tvangsmiddelbruk i forebyggende øyemed krever rettens tillatelse. Dersom det er stor fare for at muligheten til å forebygge et attentat mot representanter for Norges øverste statsmyndigheter eller tilsvarende organer i andre stater vil gå tapt, er PSTs sjef og assisterende sjef gitt hastekompetanse til å igangsette bruk av alle tillatte tvangsmidler, bortsett fra romavlytting, som uten unntak krever tillatelse fra retten, jf. politiloven § 17 d tredje ledd.

Vilkårene for bruk av hastekompetanse er vesentlig strengere enn de tilsvarende reglene i straffeprosessloven, og bestemmelsen er ment å være en «meget snever unntaksregel», jf. Ot.prp. nr. 60 (2004–2005) punkt 9.4.3.2 side 134. Departementet uttalte i den sammenheng:

> «Forslaget bygger på prinsippet som har nedfelt seg i en rekke av reglene om bruk av tvangsmidler som ledd i etterforsking, se for eksempel straffeprosessloven § 200 a sjette ledd og § 216 d første ledd, men vilkårene er gjort vesentlig strengere og bestemmelsen er ment som en meget snever unntaksregel.»

Departementet foreslo opprinnelig at sjef PST skulle gis hastekompetanse i alle sakstyper som er nevnt i politiloven § 17 d første ledd. Begrensningen til sakstyper som nevnt i § 17 d første ledd bokstav c ble tatt inn under komitébehandlingen i Stortinget, med følgende begrunnelse (Innst. O. nr. 113 (2004–2005) side 35):

> «Flertallet mener metodebruk i det forebyggende sporet uten rettslig kjennelse bør begrenses til et minimum. Flertallet viser til brev fra justisministeren 30. mai 2005 hvor han redegjør for at hastekompetansen til PST er viktigst i attentatsaker.»

13.5.4.2 Utvalgets og PSTs forslag

Politiets hastekompetanse til å beslutte bruk av skjulte tvangsmidler er omtalt i Metodekontrollutvalgets utredning punkt 15.3. Omtalen dekker både politiets hastekompetanse til å beslutte bruk av skjulte tvangsmidler på etterforskningsstadiet og sjef PSTs særskilte kompetanse etter politiloven § 17 d tredje ledd. Utvalget uttalte følgende om påtalemyndighetens faktiske bruk av hastekompetansen, jf. utredningen punkt 15.3 side 167:

> «Tallmateriale utvalget har fått tilgang til viser at hastekompetansen brukes ved drøyt en tredjedel av beslutningene om kommunikasjonskontroll. Utvalget har vurdert om det foreligger omstendigheter som tilsier at hastekompetansen brukes oftere enn det er grunnlag for, eventuelt om dette foranlediger lovendringer.
>
> Utvalget har imidlertid ikke fått tilbakemeldinger om at påtalemyndighetens bruk av hastekompetanse til å iverksette skjulte tvangsmidler generelt oppfattes som problematisk. Den sterkeste indikasjonen på at hastekompetansen ikke brukes ugrunnet, er tallene som viser at svært få hurtigkoblinger ikke godkjennes ved domstolens etterkontroll, i snitt dreier det seg om ca. en prosent i året.»

Utvalget gikk inn for å opprettholde påtalemyndighetens hastekompetanse, under henvisning til «de alvorlige straffbare forholdene som gjennomgående ligger til grunn for bruken av skjulte tvangsmidler». Utvalget fant likevel ikke grunn til å foreslå utvidelser av sjef PSTs hastekompetanse til å beslutte tvangsmiddelbruk i forebyggende øyemed, jf. utredningen side 167:

> «Det er overfor utvalget gitt uttrykk for at PST også kan ha behov for hastekompetanse i andre saker enn attentat mot representanter for Norges øverste statsmyndigheter og tilsvarende organer i andre stater. Utvalget har imidlertid ikke mottatt dokumentasjon på konkrete tilfeller som kunne gitt grunnlag for å overprøve Justiskomiteens vurdering. Utvalget deler for øvrig synspunktet om at tvangsmiddelbruken i forebyggende øyemed uten rettslig kjennelse bør holdes på et minimum.»

PST ga følgende uttalelse under høringen av Metodekontrollutvalgets utredning:

> «PST er av en annen oppfatning enn utvalget i dette spørsmålet og mener at behovet for bruk av hastekompetanse gjør seg gjeldende ved tvangsmiddelbruk i forebyggende øyemed. I dag er bruk av hastekompetanse i forebyggende øyemed begrenset til forebygging av trusler mot myndighetspersoner. Det er PSTs vurdering at de samme gode grunner som at hastekompetanse skal kunne benyttes ved forebygging av trusler mot myndighetspersoner gjør seg tilsvarende gjeldende ved forebygging av terrorhandlinger.»

PST ønsker en ytterligere utvidelse av PSTs hastekompetanse til å beslutte bruk av tvangsmidler i forebyggende øyemed. PST anfører i brev 1. november 2011, som høringsnotat 12. juli 2012 viser til, at sjef PST i dag bare kan beslutte bruk av tvangsmidler i forebyggende øyemed ved fare for opphold «når det er grunn til å undersøke om noe[n] forbereder en handling som rammes av straffeloven 1902 §§ 147 a, 90, 91, 91 a og § 222, 223, 227, 229, 231 og 233 og som retter seg mot nærmere bestemte myndighetspersoner.» Etter PSTs oppfatning bør det vurderes om sjefen for PSTs hastekompetanse bør utvides til å gjelde «alle de straffebud som kan kvalifisere for bruk av tvangsmidler i forebyggende øyemed.» PST anfører i den sammenheng at erfaring har vist at det ved flere anledninger har hastet med å iverksette tvangsmiddelbruk i forebyggende øyemed, men at man har vært nødt til å avvente rettens kjennelse før inngrepet kunne iverksettes. PST gir uttrykk for at det «er uheldig hvis hasteperspektivet tvinger frem løsninger som går på akkord med det tosporede system.»

13.5.4.3 Høringsinstansenes syn

Få av høringsinstansene er positive til en utvidelse av sjef PSTs hastekompetanse.

Hordaland politidistrikt uttaler at det, ut fra PSTs opplyste behov om å styrke arbeidet for å forhindre andre alvorlige angrep, synes mindre problematisk at hastekompetansen utvides til å omfatte alle de straffebud som kvalifiserer for bruk av tvangsmidler. Den etterfølgende domstolskontroll vil gjøre utvidelsen mindre betenkelig ut fra personvernhensynet.

En rekke av høringsinstansene avviser imidlertid en utvidelse av PSTs hastekompetanse.

Det nasjonale statsadvokatembetet legger til grunn at det dreier seg om en meget betydelig utvidelse og mener at dette klart har sine betenkeligheter ut fra både rettssikkerhets- og personvernhensyn. Det påpekes at det er viktig med domstolskontroll med beslutninger som griper dypt inn i den enkelte borgers privatliv, og at slik kontroll utvilsomt motvirker påstander om misbruk av kompetansen. Dette tilsier at sjef PSTs hastekompetanse ikke bør strekkes lenger enn til det helt nødvendige. Det stilles spørsmål om det er grunn til å foreta en så drastisk endring av hastekompetansen som foreslått av PST. Slik Det nasjonale statsadvokatembetet ser det, bør PST bes om en nærmere redegjørelse for hvorfor det er behov for hastekompetanse knyttet til de enkelte straffebud, da det kan være vanskelig å se at det er nødvendig med hastekompetanse tilknyttet alle de bestemmelser som er foreslått av PST.

Datatilsynet vil særlig peke på det uheldige i at forslaget om å utvide PSTs hastekompetanse er lite problematisert. Det gis uttrykk for at forslaget isolert sett reiser prinsipielle spørsmål som krever en grundig behandling. Datatilsynet forutsetter at forslagene utredes ytterligere, og at de sendes på en ny, alminnelig høring før de eventuelt fremmes overfor Stortinget.

Norsk forening for kriminalreform (KROM) mener at forslagene i sum betyr at PST ønsker friere hender i alle sider av sin forebyggende virksomhet, og minner om Lund-kommisjonens avdekning av irregulær politisk overvåkning gjennom etterkrigstiden. Det anføres at det er grunn til å frykte at krigen mot terror betyr at etterret-

ningstjenesten igjen blir en statsmakt utenfor kontroll, som selv bestemmer lov og rett. Det anføres videre at det hele veien i høringsnotatet kan avleses en utvikling mot et stadig mer autonomt PST, befridd for den rettslige kontroll som tidligere er funnet nødvendig. Det påpekes at de ønsker og operasjonelle drømmer PST nå fremmer, går langt ut over hva Metodekontrollutvalgets utredning åpnet for, og at dette gir grunn til bekymring.

Riksadvokaten slår fast at spørsmålet faller utenfor riksadvokatens ansvarsområde, men nevner likevel at Metodekontrollutvalget viser til at det ikke har mottatt dokumentasjon på konkrete tilfeller som har gitt grunnlag for å overprøve Justiskomiteens vurdering i Innst. O. nr. 113 (2004–2005) side 35, hvor hastekompetansen ble begrenset til attentatsaker, jf. NOU 2009: 15 punkt 15.3 side 166–167.

Dommerforeningens menneskerettighetsutvalg viser til at utvalget mener at det bør dokumenteres et behov for utvidet hastekompetanse for sjef PST til å beslutte tvangsmiddelbruk. For øvrig påpekes det at det er en grunnleggende rettsikkerhetsgaranti at begjæring om tvangsmiddelbruk prøves av en dommer.

Politijuristene mener det er viktig at lovgiver har en vurdering av hvilke metoder som skal tillates ved etterforskning av hvilke straffebud. Men det anføres at rettsstatsgarantier og rettssikkerhet ivaretas vel så godt igjennom rettsstatens kontrollfunksjoner, de uavhengige kontrollørene som påtalemyndighet, domstol, forsvarer og § 100 a-advokat skal utgjøre. Sett i den sammenheng er det vanskelig å forsvare straffeprosesslovens åpning for å gi påtalemyndighet til personer som ikke besitter juridisk kompetanse og som ikke innehar juridisk embetseksamen eller mastergrad i rettsvitenskap, jf. straffeprosessloven § 55 annet ledd.

13.5.4.4 Departementets vurdering

Departementet bemerker at PSTs beskrivelse av gjeldende rett i brev 1. november 2011 er uriktig, da hastekompetansen i dag er begrenset til attentatsaker, jf. § 17 d første ledd bokstav c. Departementet legger til grunn at PST mener at hastekompetansen for det første bør utvides til å gjelde også forebygging av handling som rammes av straffebud som nevnt i § 17 d første ledd bokstav a (terrorhandlinger, terrorforbund og terrortrusler, jf. straffeloven §§ 131, 133 og 134, straffeloven 1902 § 147 a) og bokstav b (ulovlig etterretningsvirksomhet, jf. straffeloven §§ 121 til 126, straffeloven 1902 §§ 90, 91 og 91 a). Videre forstår departementet det slik at PST foreslår at hastekompetansen også utvides til å gjelde de øvrige straffebud som PST mener bør kvalifisere til tvangsmiddelbruk i forebyggende øyemed, jf. punkt 13.5.3.2 ovenfor. PSTs forslag om utvidelse av hastekompetansen må således vurderes i sammenheng med forslaget om utvidelse av adgangen til å bruke tvangsmidler i forebyggende øyemed.

Den eksisterende adgangen for sjef PST til å beslutte tvangsmiddelbruk etter politiloven § 17 d tredje ledd er ment å være en snever unntaksregel, og er reservert for saker om de mest alvorlige formene for vold eller trusler mot Norges øverste statsmyndigheter eller tilsvarende organer i andre stater. Rettssikkerhets- og personvernhensyn kan tale mot en utvidelse av hastekompetansen. Det legges vekt på at det er en grunnleggende rettssikkerhetsgaranti at bruk av tvangsmidler som hovedregel må tillates av domstolene ved kjennelse. Dette påpekes av Det nasjonale statsadvokatembetet, Politijuristene og Dommerforeningens menneskerettighetsutvalg. Det er viktig med domstolskontroll med beslutninger som griper dypt inn i den enkelte borgers privatliv.

Det er dessuten viktig å bevare allmennhetens tillit til at kompetansen ikke misbrukes. Der tvangsmidler benyttes etter beslutning truffet av sjef PST, vil den etterfølgende domstolskontrollen ikke kunne forhindre inngrep som det ikke er lovlig grunnlag for.

På den annen side er det viktig at PST sikres tilstrekkelige virkemidler for å forebygge alvorlig kriminalitet, slik politiloven § 17 b forutsetter. I følge PST har det ved flere anledninger hastet med å iverksette tvangsmiddelbruk i forebyggende øyemed i saker om annen kriminalitet enn attentat mot de øverste statsmyndigheter. Metodekontrollutvalgets bemerkninger i utredningen punkt 15.3 tyder dessuten på at den eksisterende hastekompetansen i liten grad benyttes uten at det er grunnlag for det. I utgangspunktet synes det derfor å være liten grunn til å frykte at hastekompetansen vil bli misbrukt, selv om adgangen til å beslutte tvangsmiddelbruk utvides til å gjelde forebygging av handlinger som rammes av andre straffebud enn de som er nevnt i politiloven § 17 d første ledd bokstav c, forutsatt at de øvrige vilkårene for slik hastebeslutning videreføres.

Departementet setter imidlertid spørsmålstegn ved om uttalelsene fra PST gir grunn til å overprøve vurderingene fra et bredt flertall i Justiskomiteen om at adgangen til å fatte hastebeslutninger om bruk av tvangsmidler i det forebyggende sporet bør holdes på et minimum og reserveres attentatsakene. I brevet 1. november 2011 bes det om at sjef PSTs hastekompetanse

utvides til å gjelde «alle de straffebud som kan kvalifisere for bruk av tvangsmidler i forebyggende øyemed», og her synes ønsket om utvidelse lite målrettet. Til tross for at departementet finner liten grunn til å betvile PSTs utsagn om behovet, savner departementet en presisering fra PSTs side om i hvilke saker det hittil har hastet med å iverksette tvangsmidler i forebyggende øyemed.

Departementet mener likevel at det kan være gode grunner for at sjef PST gis hastekompetanse i terrorsaker. 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 (1902 § 147 a) er meget alvorlige, og i dag kan det synes inkonsekvent å la PST ha hastekompetanse i forebygging av attentatsaker, men ikke i terrorsaker. Faren for misbruk må dessuten sies å være begrenset, ettersom PSTs hastebeslutning vil overprøves av retten i etterkant og dessuten vil inngå i EOS-utvalgets kontrollarbeid. Departementet konkluderer etter dette med at det er hensiktsmessig å utvide sjef PSTs hastekompetanse til å omfatte forebygging av handling som rammes av straffebud som nevnt i § 17 d første ledd bokstav a, nærmere bestemt straffeloven §§ 131–134 (straffeloven 1902 § 147 a).

13.5.5 Tvangsmidler

13.5.5.1 Gjeldende rett

For å forebygge lovbrudd som nevnt i punkt 13.5.3.1, kan PST anvende skjult fjernsynsovervåking av offentlig sted (straffeprosessloven § 202 a), teknisk sporing (§§ 202 b og 202 c), postbeslag (§§ 211 og 212), kommunikasjonskontroll (§§ 216 a og 216 b), samtaleavlytting med samtykke (§ 216 l) og romavlytting (§ 216 m), i tillegg til beslag og utleveringspålegg i kombinasjon med utsatt eller unnlatt underretning (§§ 208 a og 210 a). PST kan også foreta hemmelig ransaking (§ 200 a), men ikke i noens «private hjem», jf. politiloven § 17 d annet ledd siste punktum. Etter at Metodekontrollutvalgets flertall, på bakgrunn av de to betenkningene fra Husabø og Høgberg/Stub, konkluderte med at romavlytting i private hjem var i strid med Grunnloven, ga Justisdepartementet 6. juli 2009 instruks til PST om straks å suspendere eventuelle pågående forebyggende romavlyttingssaker og inntil videre ikke fremme nye begjæringer om bruk av slik metode i private hjem.

13.5.5.2 Utvalgets forslag

Både Husabø og Høgberg/Stub legger som nevnt til grunn at unntaket for «kriminelle Tilfælde» i Grunnloven § 102, slik den da lød, bare kommer til anvendelse der det allerede er begått en straffbar handling. Videre konkluderer både Husabø og Høgberg/Stub med at forbudet mot «Hus-inkvisisjoner» ikke bare omfatter ransaking, men også romavlytting og visse former for dataavlesing.

Utvalget har et delt syn på bruk av tvangsmidler i forebyggende øyemed i privat bolig, på grunn av ulike syn på tolkningen av Grunnloven § 102, jf. utredningen punkt 22.4 side 233. Et samlet utvalg er kommet til at hemmelig ransaking og kommunikasjonsavlytting også i det forebyggende sporet bør kunne gjennomføres ved hjelp av innbrudd i et datasystem (dataavlesing). På bakgrunn av utvalgets flertalls vurdering av forholdet til Grunnloven § 102 må det likevel gjøres en begrensning i adgangen til fysisk å gå inn i noens private bolig for å montere utstyr som er nødvendig for å kunne gjennomføre slikt innbrudd i datasystemet, jf. utredningen punkt 23.3.4 side 247 og punkt 13.3 side 153.

Utvalgets flertall, medlemmene Dalseide, Elden, Husabø, Nylund, Schartum og Schou, foreslår å utvide dagens forbud mot ransaking av private hjem i forebyggende øyemed etter § 17 d annet ledd tredje punktum til også å gjelde romavlytting. Sett i lys av utvalgets forslag om å tillate visse former for dataavlesing i forebyggende øyemed, foreslås det at unntaket også skal gjelde innbrudd i privat bolig i forbindelse med gjennomføring av dataavlesing.

Utvalgets mindretall, medlemmene Pedersen, Schea og Sælør, går inn for å oppheve hele tredje punktum, slik at både ransaking og romavlytting i privat bolig blir tillatt i forebyggende øyemed. Det samme gjelder innbrudd i forbindelse med dataavlesing.

Utvalget foreslår dessuten at begrepet «private hjem» erstattes med «privat bolig». Dette begrunnes med at begrepet bolig er mer innarbeidet i lovgivningen for øvrig og ligger også nærmere begrepet «Hus» i Grunnloven. Det vil omfatte enhver bolig som tjener som ramme for en eller flere personers privatliv over et lengre tidsrom. I tillegg til vanlige helårsboliger, vil dette kunne gjelde fritidsboliger og mer atypiske boligformer som en husbåt.

Utvalget foreslår videre at det åpnes for bruk av utleveringspålegg fremover i tid, jf. straffeprosessloven § 210 b, med hjemmel i politiloven § 17 d, som resultat av forslaget om å iverksette opphe-

velsen av lov om postkontroll i saker om rikets sikkerhet. Henvisningene til straffeprosessloven § 211 og § 212 om postkontroll foreslås tatt ut, da disse bestemmelsene foreslås opphevet.

Utvalget foreslår dessuten at PST bør ha adgang til å gjennomføre skjult kameraovervåking av privat sted, unntatt privat bolig, som ledd i sin forebyggende virksomhet etter politiloven § 17 d. Bestemmelsen om dette er plassert i straffeprosessloven § 202 a, og omfattes dermed allerede av opplistingen i politiloven § 17 d over hvilke skjulte tvangsmidler som kan anvendes ved PSTs forebyggende virksomhet. Utvalget mener imidlertid at slik tillatelse bare bør gis når særlige grunner tilsier det, jf. annet ledd annet punktum, og det foreslås derfor at en henvisning til bestemmelsen tilføyes også her.

13.5.5.3 Høringsinstansenes syn

13.5.5.3.1 Konstitusjonelle skranker

Advokatforeningen er enig med utvalgets flertall i at forbudet mot ransaking av private hjem i politiloven § 17 d bør utvides til også å gjelde romavlytting og innbrudd i privat bolig i forbindelse med dataavlesing. Advokatforeningen finner det ikke tvilsomt at adgangen til romavlytting i privat bolig i forebyggende øyemed strider mot Grunnloven § 102.

Også *KROM* er enig med flertallets vurdering når det gjelder ransaking og romavlytting i privat bolig og forholdet til Grunnloven § 102.

Datatilsynet støtter utvalgets vurdering om at det må legges til grunn at Grunnloven § 102 er til hinder for ransaking og romavlytting i private hjem, i avvergende og forbyggende øyemed.

Oslo statsadvokatembeter sier seg enig i flertallets vurderinger, men gir samtidig uttrykk for at utvalget i for liten grad har vektlagt de legislative hensyn som bør være sentrale i dag. Statsadvokatembetet uttaler i den sammenheng blant annet følgende:

> «Den reelle begrunnelse må være at individene skal ha et materielt vern for sitt privatliv og at dette må være utgangspunktet ved fortolkningen. Dette prinsipp er også uttrykt i E.M.K. art 8, som fastslår at alle har krav på respekt for sitt privatliv, familieliv og korrespondanse. Et tilvarende utgangspunkt har man lagt til grunn for forståelsen av 4. grunnlovstillegg i den amerikanske forfatning. Dette innebærer rimeligvis ikke at dette vernet kan være absolutt. En slik løsning vil gjøre håndhevning av lovgivningen ganske umulig.
>
> Ordlyden i Grunnloven § 102 forbyr ransakning av hus bortsett fra slike som skjer i forbindelse med straffesaker. Det sier seg selv at en nesten 200 år gammel og meget knapt formulert grunnlovstekst ikke kan fortolkes strengt etter ordlyden. Dette gjelder særlig fordi det knapt finnes forarbeider, og om slike skulle finnes må de ha nokså begrenset vekt når de skal anvendes i forhold til dagens virkelighet. Som ellers ved fortolkning av grunnlovens bestemmelser må tolkningen baseres på en avveining av ulike og delvis motstridende hensyn. Ved forståelsen av Grunnloven § 102 blir det forholdet mellom hensynet til privatlivets fred og samfunnets behov, for å sikre en rimelig effektiv etterlevelse av lovgivingen, som bør være det sentrale element i tolkningen.»

Østfold politidistrikt er enig med utvalgets mindretall i at skjulte tvangsmidler i avvergende eller forebyggende øyemed ikke er i strid med Grunnloven § 102, som forbyr husinkvisisjon i andre enn «kriminelle Tilfælde», da slik bruk faller innenfor dette begrepet.

Politidirektoratet slår fast at tvangsmiddelbruk i forebyggende øyemed, jf. politilovens bestemmelser, er forbeholdt PST. Den grunnlovsmessige vurdering som er foretatt, og som innebærer at romavlytting i privat bolig i forebyggende øyemed anses grunnlovsstridig, berører derfor i utgangspunktet ikke det alminnelige politi, og direktoratet finner ikke grunn til å kommentere spørsmålet nærmere.

Riksadvokaten nøyer seg med å vise til de generelle bemerkningene om Grunnloven § 102, jf. ovenfor i punkt 14.4.1.3.

13.5.5.3.2 Øvrige forhold

Politiets sikkerhetstjeneste støtter utvalgets forslag om at PST i forebyggende øyemed skal kunne anvende utleveringspålegg fremover i tid, og uttaler:

> «En konsekvens av forslagene om opphevelse av straffeprosessloven §§ 211 og 212 samt loven om postbeslag, er at PSTs adgang til å bruke tvangsmidler innsnevres noe. Av den grunn foreslår utvalget at det i straffeprosessloven § 210 b åpnes for at PST i forebyggende øyemed kan anvende utleveringspålegg fremover i tid.
>
> PST støtter utvalgets forslag. Særlig ser vi forslaget om at det i straffeprosessloven § 210 b åpnes for at PST i forebyggende øyemed kan anvende utleveringspålegg fremover i tid, som positivt […]»

Riksadvokaten har ingen avgjørende innvendinger mot at straffeprosessloven § 210 b om fremtidig utleveringspålegg inntas i oppregningen i politiloven § 17 d.

Oslo statsadvokatembeter reiser spørsmål om politiloven § 17 d gir hjemmel for skjult ransaking hos tredjemann. Det påpekes at loven åpner for hemmelig ransaking etter straffeprosessloven § 202 a. Denne bestemmelsen henviser ikke direkte til straffeprosessloven § 192, som er hovedbestemmelsen om ransaking, men gir nærmere regler om såkalt utsatt underretning. Bestemmelsen i § 192 åpner for to hovedtyper av ransaking: hos siktede selv, jf. § 192 første ledd, og tredjemannsransaking, jf. annet ledd. Begrunnelsen for denne er primært bevissikringshensyn i forbindelse med straffesaken. Spørsmålet er ikke drøftet i forarbeidene.

13.5.5.4 Departementets vurdering

13.5.5.4.1 Konstitusjonelle skranker – tvangsmidler i private hjem

Departementet vil innledningsvis bemerke at dagens adgang etter politiloven § 17 d til å benytte tvangsmidler i forebyggende øyemed er snever. Adgangen er uttrykkelig begrenset, både med hensyn til hvilke skjulte tvangsmidler som kan benyttes og alvorlighetsgraden av lovbruddene som søkes forebygget. Den omfatter kun de mest alvorlige lovbruddene innenfor PSTs ansvarsområde, nærmere bestemt terrorhandlinger, attentat mot myndighetspersoner, spionasje og ulovlig etterretning. Samtlige lovbrudd vil, direkte eller indirekte, kunne medføre en fare for tap av liv, noe som tilsier at PST har behov for virkemidler for effektivt å kunne sikre borgerne, slik det er forventet av sikkerhetstjenesten. Det bemerkes at Grunnloven §§ 93 og § 102 annet ledd nå gir statens myndigheter en plikt til å beskytte retten til liv og til å verne om den personlige integritet, herunder den enkeltes fysiske integritet.

Det fremgår dessuten av § 17 d at det er strenge tilleggskrav for at tvangsmidler i forebyggende øyemed skal kunne tas i bruk, både i form av indikasjons-, subsidiaritets- og forholdsmessighetskrav, jf. bestemmelsens annet ledd. Tillatelse kan bare gis dersom det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen, at forebygging ellers i vesentlig grad vil bli vanskeliggjort og inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig. Adgangen er ytterligere begrenset ved at det stilles krav om særlige grunner for at blant annet hemmelig ransaking og romavlytting skal kunne iverksettes. Dette innebærer et skjerpet forholdsmessighetskrav, som både politiet og domstolen må forholde seg til. Rettssikkerheten er ivaretatt gjennom både domstolsbehandling og etterfølgende kontroll fra EOS-utvalget.

Lovgiver må nå ta stilling til om adgangen til å benytte tvangsmidler i forebyggende øyemed *i private hjem* skal *innskrenkes*, i tråd med utvalgsflertallets syn, eller *utvides*, slik mindretallet går inn for. Det er ikke ønskelig å opprettholde status quo, da forbudet mot hemmelig ransaking av private hjem følger av loven, mens begrensningen for romavlytting er gitt i instruks. Her kan det tenkes ulike alternative lovreguleringer med ulik grad av inngripen i den private sfære, som forenklet kan oppsummeres slik:

- Lovgiver kan forby ransaking, romavlytting og innbrudd i forbindelse med dataavlesing i private hjem i forebyggingsøyemed.
- Lovgiver kan åpne for slik tvangsmiddelbruk.
- Lovgiver kan velge en mellomløsning, der det differensieres mellom de tre metodene og eventuelt også ulike lovbrudd.

Som nevnt ovenfor legger departementet til grunn at det av formuleringen «kriminelle tilfeller» i Grunnloven § 102 første ledd annet punktum ikke kan utledes et krav om at det allerede må være begått en straffbar handling, jf. punkt 5.1.3 og 13.4.1.4.3 ovenfor. Det bør prinsipielt sett ikke være avgjørende for grunnlovsmessigheten om en i lovgivningen taler om avverging eller forebygging, når det gjelder adgangen til å foreta inngrep i hjemmet for å forhindre *fremtidig kriminalitet*. Argumentasjonen i punkt 13.4.1.4 for å tillate tvangsmidler i avvergende øyemed, kan i stor grad også benyttes i forebyggingssakene. Dette betyr imidlertid ikke at nærheten til den straffbare handling er uten betydning for tvangsmiddeladgangen.

Det fremgår av særmerknaden til straffeprosessloven § 222 d i Ot.prp. nr. 60 (2004–2005) at uttrykket «avverging» er brukt for å markere at tvangsmiddelbruken må skje som ledd i etterforskning og at handlingen som fryktes begått, ikke må ligge for langt frem i tid. Hvor det er spørsmål om å anvende tvangsmidler utenfor etterforskning, og for å forhindre straffbare handlinger som ligger lenger frem i tid, bruker departementet uttrykket «forebygging». Forskjellen i begrepsbruk markerer altså at en – når metodebruken skjer som ledd i etterforskning – i tid gjerne befinner seg nærmere handlingen som

søkes forhindret enn ved forebygging, jf. Ot.prp. nr. 60 (2004–2005) punkt 6.1 side 60. Det er derfor gode grunner til å være mer restriktiv til bruk av tvangsmidler i forebyggende enn i avvergende øyemed.

At Grunnloven ikke kan sies å sette en absolutt skranke for bruk av ransaking, romavlytting eller innbrudd i private hjem i forebyggende øyemed, betyr ikke at en utvidelse av tvangsmiddeladgangen er tilrådelig. Til tross for at Grunnloven ikke oppstiller et særskilt nærhets- eller aktualitetskrav til lovbruddet, mener departementet at det likevel er grunn til å skille mellom tvangsmiddelsbruk i avvergende og forebyggende øyemed, og at adgangen bør være snevrere i de sistnevnte tilfellene. Sannsynligheten for at en straffbar handling kommer til å bli begått og hvor prekært det fremstår at tvangsmidler er påkrevet for å hindre handlingen, vil være sentrale momenter i vurderingen av om et inngrep kan anses forholdsmessig.

På den annen side fremgår det av PSTs siste trusselvurderinger at forberedelsestiden på for eksempel terroraksjoner er blitt kortere. Dette skyldes at ekstrem islamistisk terror i Europa de siste årene har vært preget av lite komplekse angrep, utført med våpen og virkemidler som er enkle å anskaffe og bruke, noe som medfører at angrep kan være vanskelige å forhåndsvarsle. Departementet legger til grunn at dette også medfører at grensen for når en forebyggingssak bør gå over i etterforskningssporet ikke alltid er like enkel å trekke. Nærheten til den straffbare handling bør etter departementets oppfatning ikke alene være avgjørende for metodeadgangen, jf. også Riksadvokatens høringsuttalelse:

> «Riksadvokaten kan ikke se at det er grunnlag for å innfortolke et særskilt nærhets- eller aktualitetskrav i unntaket for «kriminelle Tilfælde» i Grunnloven § 102. Selvsagt kan det ved spørsmål om å gjøre bruk av inngripende metoder i forebyggende og avvergende øyemed være god grunn til å se hen til om de aktuelle straffbare handlingene antas å være nær forestående. Men det følger ikke av dette at Grunnloven stiller et slikt krav til nærhet».

Som nevnt ovenfor i punkt 5.1.3, la Kontroll- og konstitusjonskomiteens saksordfører under stortingsdebatten til grunn at uttrykket «kriminelle tilfeller» verken må avgrenses mot politiets arbeid for å avverge eller forebygge kriminalitet, men at den nærmere grenseoppgangen bør gjøres i lovs form. I den forbindelse må hensynet til privatlivet på den ene siden veies mot hensynet til kriminalitetsbekjempelse og samfunnssikkerhet på den annen side, og det må konkret vurderes hvorvidt inngrepet er forholdsmessig.

I det videre vil departementet skissere alternativer for regulering av tvangsmiddelbruk i forebyggende øyemed. En mulighet er altså å følge forslaget til Metodekontrollutvalgets flertall om å *utvide dagens forbud* mot ransaking av private hjem i forebyggende øyemed til også å omfatte romavlytting og innbrudd ved dataavlesing. En mulig ordlyd er:

> «Det kan ikke gis tillatelse til å ransake, *romavlytte eller ved dataavlesing å gjøre innbrudd i* noens private hjem etter bestemmelsen her.»

I den andre enden av skalaen kan lovgiver velge å støtte utvalgets mindretall i at hele bestemmelsen om forbud mot inngrep i private hjem bør *oppheves*, slik at både ransaking og romavlytting av bolig, i tillegg til innbrudd i forbindelse med dataavlesing eller romavlytting, kan tillates i forebyggende øyemed.

Mellom disse to ytterpunktene finnes det en rekke alternative reguleringsmåter med varierende grad av inngripen i den private sfære. Det kan differensieres både mellom de ulike tvangsmidler som skal kunne benyttes og mellom ulike lovbrudd som gir grunnlag for bruk av tvangsmidlene.

Et alternativ er å forby romavlytting i forebyggende øyemed, men åpne for ransaking og innbrudd ved dataavlesing. En mulig ordlyd er:

> «Det kan ikke gis tillatelse til å *romavlytte* noens private hjem etter bestemmelsen her.»

Lovgiver kan også velge å åpne for alle de nevnte tvangsmidler, men kun ved forebygging av spesifikke lovbrudd, for eksempel terrorhandlinger, der behovet er særlig prekært. En mulig ordlyd er:

> «Det kan *bare* gis tillatelse til å ransake*, romavlytte eller ved dataavlesing å gjøre innbrudd i* noens private hjem etter bestemmelsen her *når det er rimelig grunn til å undersøke om noen forbereder en handling som nevnt i første ledd bokstav a.*»

Det kan også tenkes en kombinasjonsløsning, der det gis adgang til ransaking og innbrudd ved dataavlesing for alle lovbrudd som er nevnt i § 17 d, altså både i terrorsaker, spionasjesaker og attentatsaker (samt i saker om masseødeleggel-

sesvåpen, da departementet vil foreslå at bestemmelsen utvides til å omfatte også dette), mens adgangen til bruk av romavlytting begrenses til forebygging av terrorhandlinger. En mulig ordlyd er:

> «Det kan *bare* gis tillatelse til å *romavlytte* noens private hjem etter bestemmelsen her *når det er rimelig grunn til å undersøke om noen forbereder en handling som nevnt i første ledd bokstav a.»*

Et annet alternativ er å åpne for ransaking og innbrudd ved dataavlesing ved forebygging av terrorhandlinger, men samtidig forby enhver romavlytting i private hjem. En mulig ordlyd er:

> «*Det kan ikke gis tillatelse til å romavlytte noens private hjem etter bestemmelsen her.* Det kan *bare* gis tillatelse til å ransake *eller ved dataavlesing å gjøre innbrudd i* noens private hjem etter bestemmelsen her *når det er grunn til å undersøke om noen forbereder en handling som nevnt i første ledd bokstav a.»*

Departementet vil foreslå at Stortinget velger en mellomløsning, da det verken anses hensiktsmessig med et generelt forbud mot, eller en ubetinget adgang til, tvangsmiddelbruk i private hjem i forebyggingsøyemed. Etter departementets oppfatning bør lovgiver differensiere mellom de tre metodene – romavlytting, ransaking og innbrudd ved dataavlesing – og også mellom de ulike lovbrudd – terrorhandlinger, spionasje og ulovlig etterretningsvirksomhet, attentat mot myndighetspersoner og ulovlig befatning med masseødeleggelsesvåpen. Slik vil det foretas en forholdsmessighetsvurdering allerede på lovgivningstidspunktet, i tillegg til den forholdsmessighetsvurdering som foretas av påtalemyndigheten og domstolen av metodebruken innenfor lovens ramme i den enkelte sak.

En vurdering av et inngreps forholdsmessighet vil måtte ta i betraktning alvorligheten av det lovbruddet som søkes avverget og hvor sikre holdepunkter en har for at en slik alvorlig straffbar handling vil bli begått. Departementet understreker videre at graden av inngripen for det enkelte tvangsmiddel vil være av stor betydning for vurderingen av hvorvidt det skal være adgang til å benytte det i forebyggende øyemed.

Departementet vil først sondre *mellom de ulike politimetodene*. Det kan i den sammenheng stilles spørsmål om det er forskjell i graden av inngripen for tvangsmidlene romavlytting, ransaking og innbrudd i forbindelse med dataavlesing, samt om behovet er det samme for de ulike metodene.

Det bemerkes at kriminalitetskravet for bruk av romavlytting etter straffeprosessloven § 216 m er strengere enn for hemmelig ransaking etter § 200 a. Kriminalitetskravet reflekterer i en viss grad lovgivers vurdering av det enkelte tvangsmiddelets inngrep i privatlivet, slik at det er satt høye kriminalitetskrav for bruk av tvangsmidler som er ansett å være særlig inngripende. Det er følgelig grunn til å utvise stor tilbakeholdenhet med – og kreve gode begrunnelser for – en eventuell utvidelse av anvendelsesområdet for romavlytting.

Som nevnt i punkt 13.4.1.4 ovenfor, har hyppig brukte metoder som kommunikasjonsavlytting og skjult ransaking tapt mye eller en del av sin effekt som følge av den teknologiske utviklingen, herunder fremveksten av ulike løsninger for informasjonsbeskyttelse, og de kriminelles tilpasning til denne. Informasjon som mistenkte tidligere kommuniserte over ubeskyttede forbindelser, formidles i dag gjerne gjennom kryptert IP-telefoni, noe som medfører at romavlytting kan gjenstå som politiets eneste virkemiddel for å sikre seg taleinformasjon.

Dette vil likevel kunne stille seg annerledes dersom Stortinget beslutter å åpne for dataavlesing, jf. kapittel 14 nedenfor, som også vil kunne omfatte lydstrømmen som sendes fra en tilknyttet mikrofon eller til en tilknyttet høytaler via operativsystemets driver. Det er imidlertid en ytre grense for hva politiet skal ha anledning til å foreta seg med grunnlag i en tillatelse til dataavlesing. Det er mistenktes *bruk* av datasystemet, smarttelefonen mv. som skal kunne kontrolleres gjennom dataavlesing, og den vil ikke gi politiet adgang til å fange opp informasjon som ikke er et resultat av mistenktes bruk, for eksempel ved selv å slå på mikrofoner tilknyttet datasystemet for å fange opp lydsignaler. Slik målrettet overvåking må eventuelt foretas ved romavlytting. Selv om en eventuell adgang til bruk av dataavlesing kan avhjelpe situasjonen, vil det altså fortsatt være et restbehov for mer målrettet romavlytting.

Romavlytting er kostbart og vil neppe brukes ofte i praksis, men være forbeholdt svært få og meget alvorlige tilfeller, noe som kan tilsi at færre rammes av overvåkingen. Et annet argument for å tillate romavlytting i private hjem i forebyggende øyemed er at dette vil kunne effektivisere perioden saken befinner seg i det forebyggende sporet betraktelig. Dersom det raskt verifiseres at det ikke foreligger en reell trussel, vil saken kunne avsluttes. I motsatt tilfelle vil det kunne åpnes etterforskning.

Departementet vil imidlertid understreke 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 overvåking. Den omfatter dessuten en kontinuerlig overvåking over tid, i motsetning til ransaking og innbrudd, der tvangsmiddelbruken vil være forholdsvis raskt overstått. Under noe tvil har departementet derfor konkludert med at det ikke vil foreslås at det skal være adgang til å benytte romavlytting i private hjem i forebyggende øyemed. Restbehovet for å få tilgang til taleinformasjon, utover den lydstrømmen som kan fanges opp ved bruk av dataavlesing, kan etter departementets oppfatning ikke rettferdiggjøre en så vidt inngripende skjult metode som romavlytting av private hjem.

Skjult ransaking av private hjem er tradisjonelt ansett å være et inngripende tvangsmiddel, noe som også er bakgrunnen for at forbudet mot ransaking av private hjem i forebyggende øyemed opprinnelig ble nedsatt, «for ikke å trå Grunnloven for nær», jf. Ot.prp. nr. 60 (2004–2005) punkt 9.4.2.4 side 132. Departementet legger imidlertid til grunn at skjult ransaking er mindre inngripende enn romavlytting av et privat hjem over tid. Som nevnt ovenfor reflekteres dette i kriminalitetskravet i tvangsmiddelbestemmelsene. En kontinuerlig overvåking av samtaler mv. i hjemmet vil høyst sannsynlig ramme uskyldige familiemedlemmer, og inngrepet i den private sfære er således betydelig. Det vises for øvrig til betenkningen fra Høgberg/Stub punkt 3.5.3 på side 437 i utredningen, der det heter:

> «I mange tilfeller vil romavlytting være klart mer inngripende enn ransaking. Dette skyldes først og fremst at romavlytting ofte blottlegger den avlyttedes privatliv på en mer intensiv måte enn annen metodebruk.»

Samtidig vil politiet ved en ransaking av boligen kunne avsløre om det oppbevares for eksempel våpen, sprengstoff, kontaktlister, kart eller planer der som kan settes i forbindelse med fremtidige alvorlige lovbrudd, noe som tilsier at et slikt tvangsmiddel vil kunne være svært nyttig for politiet og ha stor effekt. Det vil også kunne være nødvendig for å forebygge mot terrorhandlinger i den enkelte sak.

Departementet anser i utgangspunktet skjult ransaking for å være mer inngripende enn et innbrudd for å montere dataavlesingsutstyr. Dette kan selvfølgelig være avhengig av hvor omfattende undersøkelser politiet må foreta for å oppfylle formålet med ransakingen og hvor mye politiet må lete for å finne det datautstyret som skal avleses. Det siste vurderes likevel som et mer målrettet og mindre inngrep i den private sfære.

Departementet trekker i retning av å avgrense tvangsmiddeladgangen mot romavlytting av private hjem i forebyggingssakene, men å åpne for skjult ransaking og innbrudd ved dataavlesing. Departementet konkluderer med at selv om ransaking og innbrudd ved dataavlesing i private hjem er inngripende metoder som kan ha konsekvenser for tredjeparter, så er faren for liv, helse og sikkerhet ved at man ikke får forebygget de meget alvorlige lovbrudd som hjemler slik tvangsmiddelbruk så stor at en viss inngripen i det private hjem kan anses nødvendig, forholdsmessig og innenfor Grunnlovens skranker.

Videre er det hensiktsmessig å differensiere *mellom de ulike lovbrudd* hvor politiloven § 17 d åpner for metodebruk i forebyggende øyemed. Et inngrep i den enkelte borgers hjem bør forbeholdes de kvalifisert alvorligste lovbrudd.

PST har gitt signaler om at det er ønskelig å benytte alle metodene (også romavlytting), ved samtlige lovbrudd som nevnes i første ledd. Det anføres i den anledning at et slikt tvangsmiddel ville vært viktig i saker om spionasje og ulovlig etterretning, der det kan sies å være «profesjonelle spillere» som aksepterer yrkesrisikoen og som ikke bør tilgodeses samme personvern som øvrige borgere. Videre anfører PST at det i disse utenrikspolitisk urolige tider, med blant annet konflikten i Ukraina som bakteppe, er viktig å sikre de hemmelige tjenester tilstrekkelige verktøy til å kunne oppfylle de oppgaver tjenestene er tildelt.

Departementet mener at det er grunn til å utvise stor tilbakeholdenhet med å utvide adgangen til tvangsmiddelbruk i forebyggende øyemed. Behovet synes imidlertid å være størst når det gjelder å forebygge terrorhandlinger, jf. § 17 d første ledd bokstav a, der faren for tap av mange menneskeliv er betydelig.

PST og Etterretningstjenesten har tidligere varslet om en negativ utvikling i trusselbildet når det gjelder terror, jf. punkt 4.5 ovenfor. I oktober 2015 uttalte PST at sannsynligheten for terrorangrep fra ISIL-sympatisører er noe redusert. Dette skyldes primært at de norske ekstremistmiljøene er svekket, da 18 personer fra miljøene mest sannsynlig er drept i Syria, mens 9 er varetektsfengslet og siktet for terrorrelatert kriminalitet. Også i *Åpen trusselvurdering 2016* fremgår det at terror-

trusselen er forsiktig nedjustert. Utviklingen fremover vil likevel være ustabil og usikker. Den økte tilstrømningen av flyktninger og asylsøkere til Norge kan få negative følger for trusselbildet knyttet til både det høyre- og venstreekstreme miljøet i Norge. På lengre sikt er det dessuten mulig at enkelte asylsøkere vil kunne utgjøre en terrortrussel i Norge, fordi de kan være en sårbar gruppe for radikalisering.

Departementet mener at spørsmålet også må ses i lys av den senere tids terroraksjoner, herunder i Paris fredag 13. november 2015. Selv om politiets adgang til metodebruk ikke skal bestemmes av enkelthendelser, mener departementet at det, i lys av de senere års terroraksjoner, tegner seg et bilde av et Europa som vil oppleve slike angrep fra ISIL og andre ekstremistgrupper med ujevne mellomrom. Dette kan således synes å være et mønster eller et generelt utviklingstrekk snarere enn en tragisk enkelthendelse. Departementet mener at det er viktig at sikkerhetstjenesten kan benytte tvangsmidler for å forebygge slike alvorlige lovbrudd, all den tid tvangsmiddelbruken har tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig.

Departementet konkluderer med at lovgiver bør differensiere både mellom de ulike metodene og de ulike lovbruddene ved fastsettelsen av tvangsmiddeladgangen i forebyggingssakene. Nærmere bestemt foreslår departementet at det under visse vilkår åpnes for skjult ransaking og innbrudd ved dataavlesing for å forebygge terrorhandlinger, i motsetning til øvrige lovbrudd angitt i § 17 d, samt at enhver romavlytting i private hjem i forebyggende øyemed forbys. Det understrekes at påtalemyndigheten og domstolen i tillegg må foreta en forholdsmessighetsvurdering i den enkelte sak, og blant annet se hen til hvor sikre holdepunkter en har for at en terrorhandling vil kunne bli begått. Departementet foreslår etter dette følgende ordlyd:

> «*Det kan ikke gis tillatelse til å romavlytte noens private hjem etter bestemmelsen her.* Det kan *bare* gis tillatelse til *å ransake eller ved dataavlesing å gjøre innbrudd i* noens private hjem etter bestemmelsen her *når det er grunn til å undersøke om noen forbereder en handling som nevnt i første ledd bokstav a.*»

For øvrig støtter ikke departementet utvalget i at begrepet «private hjem» bør erstattes med «privat bolig». Det bemerkes i den anledning at Stortinget har valgt å benytte begrepet «hjem» i Grunnloven § 102 første ledd første punktum.

13.5.5.4.2 Fremtidig utleveringspålegg

Et annet spørsmål er om det skal åpnes for utleveringspålegg fremover i tid i forebyggende øyemed med hjemmel i politiloven § 17 d. Etter straffeprosessloven § 210 b kan retten ved kjennelse pålegge den som i fremtiden vil få besittelsen av en ting som antas å ha betydning som bevis, å utlevere tingen til politiet straks den mottas. Forskjellen fra vanlig utleveringspålegg etter § 210 er at det dreier seg om ting som den pålegget retter seg mot, vil få besittelsen av *i fremtiden*, og det gjelder et skjerpet kriminalitetskrav, jf. punkt 10.3 om fremtidig utleveringspålegg.

Hvilke tvangsmidler som skal kunne benyttes i PSTs forebyggende virksomhet ble drøftet i Ot.prp. nr. 60 (2004–2005) punkt 9.4.2.3 side 131. Departementet slo uttrykkelig fast at pågripelse og varetektsfengsling (jf. straffeprosessloven kapittel 14), båndlegging av formuesgoder (kapittel 15 b), heftelse (kapittel 17) og besøksforbud (kapittel 17 a) ikke skulle kunne anvendes utenfor etterforskning. Departementet vurderte deretter særskilt om det vil rekke for langt å åpne for bruk av romavlytting i forebyggende øyemed, men gikk inn for å tillate dette på særlig strenge vilkår. Videre heter det:

> «Departementet går inn for at de øvrige tvangsmidlene som nevnt i straffeprosesslovens fjerde del skal kunne anvendes i hemmelighet av PST i forebyggende øyemed. Departementet antar at alminnelig (åpen) bruk av tvangsmidler, som for eksempel ransaking og beslag (ransaking unntatt § 200 a og beslag unntatt § 208 a), svært sjelden vil være aktuelt i praksis, og ser ikke behov for også å foreslå at det skal være adgang til åpen bruk av disse tvangsmidlene. Departementet har lagt stor vekt på at tjenesten selv ikke ser noe praktisk behov for slike regler.»

Det kan stilles spørsmål om utelatelsen av fremtidig utleveringspålegg i oppregningen over tillatte tvangsmidler i politiloven § 17 d første ledd, var tilsiktet. Det er intet i bestemmelsens forarbeider som tyder på dette. Departementet støtter utvalget og foreslår at fremtidig utleveringspålegg inntas i oppregningen over tillatte tvangsmidler i politiloven § 17 d. Departementet mener at en slik utvidelse er hensiktsmessig uavhengig av om reglene om postbeslag og postkontroll oppheves,

jf. punkt 10.6 og 10.7, og den vil gi PST en ytterligere valgmulighet når det gjelder bruk av tvangsmiddel.

Departementet vil imidlertid bemerke at det riktige synes å være å innta en henvisning til straffeprosessloven § 210 c, som omhandler utsatt underretning ved fremtidig utleveringspålegg etter § 210 b. Som nevnt ovenfor ga departementet i Ot.prp. nr. 60 (2004–2005) punkt 9.4.2.3 side 131 uttrykk for at det kun var behov for å benytte slike tvangsmidler «i hemmelighet», og det avgrenses således mot alminnelig, åpen bruk av tvangsmidler. Det følger av ordlyden i politiloven § 17 d at bestemmelsen åpner for beslag og utleveringspålegg i kombinasjon med utsatt eller unnlatt underretning, jf. henvisningen til §§ 208 a og 210 a. Det foreslås etter dette at straffeprosessloven § 210 c om utsatt underretning ved fremtidig utleveringspålegg inntas i oppregningen i politiloven § 17 d.

13.5.5.4.3 Skjult ransaking

Når det gjelder spørsmålet om politiloven § 17 d gir hjemmel for skjult ransaking også hos tredjemann, kan dette besvares bekreftende. Det faktum at det vises til straffeprosessloven § 200 a om utsatt underretning, ikke direkte til straffeprosessloven § 192, som er hovedbestemmelsen om ransaking, er uten betydning. Som det fremgår ovenfor, er dette lovens system for å markere at det gjelder skjult, og avgrenses mot åpen, bruk av tvangsmidler. Det følger for øvrig også av § 200 a første ledd at bestemmelsen gjelder «ransaking […] uten underretning til den mistenkte eller andre».

13.5.5.4.4 Skjult kameraovervåking

Departementet kan i det vesentlige slutte seg til utvalgets vurderinger når det gjelder skjult kameraovervåking i avvergende og forebyggende øyemed. En mener således at det bør være adgang til overvåking både på eller fra offentlig sted og på privat sted som ikke er privat hjem, også for å forebygge eller avverge alvorlige straffbare handlinger, jf. kapittel 12 om kameraovervåking. Bestemmelsen om skjult kameraovervåking er plassert i straffeprosessloven § 202 a, og omfattes dermed allerede av opplistingen i politiloven § 17 d over hvilke skjulte tvangsmidler som kan anvendes ved PSTs forebyggende virksomhet. Departementet foreslår at det skjerpede forholdsmessighetskravet (særlige grunner) også skal gjelde for adgang til kameraovervåking på privat sted og for dataavlesing, jf. punkt 13.5.6.4 nedenfor.

13.5.6 Supplerende vilkår

13.5.6.1 Gjeldende rett

Ytterligere vilkår oppstilles i § 17 d annet ledd, som krever at det må være «grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen» (indikasjonskravet), at forebygging «ellers i vesentlig grad vil bli vanskeliggjort» (subsidiaritetskravet) og at «inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig». Uttrykket «det er grunn til å tro» kom inn under stortingsbehandlingen som en erstatning for det av departementet foreslåtte uttrykk «det må antas». Komiteens flertall understreket at det må foreligge objektive holdepunkter for at inngrepet vil gi opplysninger av vesentlig betydning, jf. Innst. O. nr. 113 (2004–2005) punkt 9.2 side 35. Den eksplisitte forholdsmessighetsbegrensningen er inkludert fordi politiloven ikke inneholder noen generell regel tilsvarende straffeprosessloven § 170 a. For at hemmelig ransaking, teknisk sporing av person, kommunikasjonsavlytting eller romavlytting skal kunne brukes er det oppstilt et skjerpet forholdsmessighetskrav, ved at det i tillegg kreves at «særlige grunner» tilsier det.

13.5.6.2 Utvalgets forslag

Utvalget foreslår å utvide det skjerpede forholdsmessighetskravet i politiloven § 17 d annet ledd annet punktum til også å gjelde kameraovervåkning etter straffeprosessloven § 202 a annet ledd. Utover dette foreslår ikke utvalget noen endringer i indikasjons-, subsidiaritets- og forholdsmessighetskravene, eller i domstolens kontroll med om disse er oppfylt.

13.5.6.3 Høringsinstansenes syn

Ingen av høringsinstansene uttaler seg om utvalgets forslag.

Oslo statsadvokatembeter kommer imidlertid med noen generelle betraktninger om indikasjons-, subsidiaritets- og forholdsmessighetskravet. Om indikasjonskravet uttales det at loven oppstiller et vesentlighetskrav som må være nesten umulig å oppfylle. Det gis uttrykk for at det er vanskelig å forstå at en på forhånd kan ha noen begrunnet oppfatning om for eksempel den aktuelle personen skal komme med informasjon av vesentlig betyd-

ning for å kunne forebygge en handling. Om subsidiaritetskravet hevdes det at dersom man besitter et godt grunnlagsmateriale, vil dette kunne medføre at domstolen vil avslå bruk av tvangsmidler hvis man på annen måte kan skaffe seg informasjon. Oslo statsadvokatembeter mener videre at dersom inngangsmaterialet er usikkert, vil det være ytterst vanskelig å ha noen oppfatning av hvorvidt indikasjonskravet og subsidiaritetskravet er oppfylt, og at disse to vurderingstemaene forutsetter at dommeren har kunnskaper om politimetoder som de færreste dommere vil inneha. Det gis uttrykk for at domstolen stilles overfor en ganske håpløs situasjon ved å oppstille slike strenge og delvis motstridende krav i loven. Dersom lovens skjønnstema skal følges, vil dette innebære at en begjæring vil være vanskelig å etterkomme. På den annen side vil et avslag og en etterfølgende terrorhandling medføre at domstolen tillegges et «ansvar» som den egentlig ikke skal ha. Oslo statsadvokatembeter mener at loven reelt sett gir uttrykk for en dobbeltkommunikasjon. Det uttales videre at det ikke er helt enkelt å forstå at forholdsmessighetsvurderingen kan få særlig selvstendig betydning. Oslo statsadvokatembeter mener det er vanskelig å forestille seg at en begjæring skal avslås som et uforholdsmessig inngrep dersom det som skal forhindres er en terrorhandling eller voldsforbrytelse mot medlemmer av regjeringen eller Stortinget.

13.5.6.4 Departementets vurdering

Et spørsmål er om skjult kameraovervåking på privat sted etter § 202 a nytt annet ledd bør likestilles med hemmelig ransaking, teknisk sporing av person, kommunikasjonsavlytting og romavlytting, slik at det oppstilles et skjerpet forholdsmessighetskrav. Utvalget mener at skjult kameraovervåking på privat sted må anses som et svært inngripende tiltak, som bare bør kunne skje på strenge vilkår. Etter utvalgets forslag skal slik overvåking kunne iverksettes i samme typer saker som kan gi grunnlag for kommunikasjonsavlytting etter straffeprosessloven § 216 a. Som nevnt i kapittel 12 anser departementet dette for å være et riktig utgangspunkt, som sikrer at en så vidt inngripende etterforskningsmetode bare kan benyttes i saker som gjelder alvorlig kriminalitet, samt ved lovbrudd som reiser særlige etterforskningsmessige utfordringer. Dette trekker i retning av at også de supplerende vilkårene bør tilsvare vilkår for bruk av slike inngripende tvangsmidler.

Departementet ser for øvrig at det er et tankekors at domstolen, til tross for de strenge inngangsvilkår som ligger til grunn for å tillate bruk av tvangsmidler i forebyggende øyemed, likevel kan hevdes å ha begrenset reell mulighet til å overprøve de vurderinger som er foretatt av PST. Dette ble også påpekt av departementet da regelen ble foreslått, jf. Ot.prp. nr. 60 (2004–2005) punkt 9.4.3.2 side 133:

> «[…] Det er et dilemma at domstolene, især når PST ber om tillatelse til hemmelig bruk av tvangsmidler, i relasjon til enkelte av vilkårene reelt sett vil ha begrensede muligheter til å etterprøve det faktiske grunnlaget som PST baserer sin begjæring på. Dette vil særlig gjelde vilkårene om at opplysningene må være av vesentlig betydning for å kunne forebygge den aktuelle straffbare handlingen, og om avverging ellers i vesentlig grad vil bli vanskeliggjort.[…] Enkelte vilkår for bruk av tvangsmidler i forebyggende øyemed kan imidlertid lettere prøves selvstendig av domstolene, som for eksempel kravet til forholdsmessighet og vilkåret om særlige grunner.»

Departementet mener at kravet om forhåndstillatelse fra domstolene virker disiplinerende på PST, og gir bedre rettssikkerhet og personvern enn om det ikke skulle kreves slik tillatelse fra retten. Ordningen vil i størst grad sikre kravet til uavhengighet, objektivitet og saklighet og dermed ivareta rettssikkerheten på best mulig måte. Dagens kontrollsystem bør etter dette opprettholdes. For øvrig vises det til punkt 6.3.4.

13.5.7 Bevis

13.5.7.1 Gjeldende rett

I politiloven § 17 f finnes regler om taushetsplikt ved bruk av tvangsmidler i forebyggende øyemed. Bestemmelsen er basert på straffeprosessloven § 216 i første ledd første og annet punktum, og skal forstås på samme måte, jf. Ot.prp. nr. 60 (2004–2005) side 153. Når det er snakk om å gjøre bruk av opplysningene som bevis under rettergang, snevres adgangen ytterligere inn sammenlignet med bruk i forebyggende øyemed og under etterforskning, jf. § 17 f annet ledd bokstav a og b. Det er kun adgang til å bruke opplysningene som bevis for en terrorhandling, jf. straffeloven §§ 131, 133 og 134 (straffeloven 1902 § 147 a), jf. § 17 f annet ledd bokstav c. Dersom det er nødvendig å nytte tvangsmidler for å skaffe til veie bevis i

andre saker som PST har ansvaret for å etterforske, må det skje ved bruk av hjemlene i straffeprosessloven. En sak om for eksempel terrorfinansiering kan derfor ikke baseres på bevis innhentet etter bestemmelsene i §§ 17 d flg.

13.5.7.2 Utvalgets forslag

Utvalgets mindretall foreslår å oppheve adgangen til å kunne bruke opplysninger som er innhentet ved bruk av forebyggende tvangsmidler som bevis for en terrorhandling, jf. politiloven § 17 f andre ledd bokstav c. Dette begrunnes med et ønske om å holde de to sporene for informasjonsinnhenting atskilt. Utvalgets flertall er derimot enig i den vurderingen som lå til grunn for å tillate slik bevisførsel i terrorsaker. Utvalget refererer departementets begrunnelse slik:

> «[E]n begrensning i bevisføringsmuligheten etter en terrorhandling der en rekke menneskeliv var gått tapt, ville kunne virke støtende på den alminnelige rettsbevissthet».

Etter flertallets oppfatning gjør imidlertid ikke departementets begrunnelse seg gjeldende ved forbund om terror etter straffeloven 1902 § 147 a fjerde ledd (straffeloven § 133 første ledd). Utvalgets flertall foreslår å begrense adgangen til å bruke opplysninger innhentet ved skjult tvangsmiddelbruk som ledd i PSTs forebyggende virksomhet som bevis for handlinger som omfattes av straffeloven 1902 § 147 a første og tredje ledd om terrorhandling og trussel om terrorhandling (straffeloven §§ 131 første jf. annet ledd og 134).

Utvalget foreslår også en presisering av at brudd på taushetsplikten etter bestemmelsen kan straffes etter straffeloven 1902 § 121 (straffeloven § 209), og at dette også gjelder personer som ikke er i tjeneste eller arbeid for statlig eller kommunalt organ. Også personer utenfor politiet eller påtalemyndigheten som får kjennskap til tvangsmiddelbruken, for eksempel ansatte hos teletilbyderne, vil dermed kunne straffes for brudd på taushetsplikten. Utenforstående bør imidlertid gjøres oppmerksom på denne muligheten, jf. også straffeprosessloven § 61 c siste ledd siste punktum.

13.5.7.3 Høringsinstansenes syn

Departementet har ikke mottatt noen høringsuttalelser om dette.

13.5.7.4 Departementets vurdering

Det er lagt strenge bånd på adgangen til å ta i bruk opplysninger innhentet ved bruk av forebyggende tvangsmidler som bevis i en straffesak. Dette har bakgrunn i et ønske om å unngå at rettssikkerhetsgarantier i strafforfølgningen blir undergravet ved at det oppstår et press i retning av å benytte forebyggende tvangsmidler i stedet for bruk av tvangsmidler som ledd i etterforskning, jf. Ot.prp. nr. 60 (2004–2005) punkt 9.4.4.1 side 135.

Fra utgangspunktet om at opplysninger som er innhentet ved bruk av tvangsmidler ikke skal kunne brukes som bevis under hovedforhandlingen i en straffesak, foreslo departementet likevel at det skulle gjøres unntak for terrorhandlinger, jf. straffeloven 1902 § 147 a (straffeloven §§ 131–134). Departementet uttalte i den forbindelse:

> «Dersom det ikke skulle lykkes å forebygge en terrorhandling som i verste fall kan lede til at en rekke mennesker mister livet, kan det støte an mot den alminnelige rettsbevissthet om det ikke skulle være mulig å føre opplysningene som bevis i en etterfølgende straffesak.»

Departementet bemerker at det er en nyanseforskjell mellom utvalgets gjengivelse av begrunnelsen (*at menneskeliv var gått tapt*) og departementets faktiske begrunnelse (*at handlingen i verste fall kan lede til at mennesker mister livet*). Den siste formuleringen synes i større grad å rettferdiggjøre et unntak der bevis også tillates ført i saker vedrørende forbund om terror. Det vil også kunne støte an mot den alminnelige rettsbevissthet dersom politiet avdekker at det er inngått forbund om terrorhandlinger og slik avverger handlinger som kunne føre til at menneskeliv går tapt, uten å kunne bruke opplysningene som bevis i en straffesak. Departementet ønsker ikke på nåværende tidspunkt, uten støtte i høringsuttalelser, å innsnevre adgangen til å føre opplysninger innhentet ved bruk av forebyggende tvangsmidler som bevis i straffesak.

Departementet bemerker ellers at § 17 f ble tilføyd et nytt fjerde ledd ved lovendring 15. april 2011 nr. 11, som gjør overtredelse av bestemmelsen om taushetsplikt straffbar etter straffeloven 1902 § 121 også for personer som ikke er i tjeneste eller arbeid for statlig eller kommunalt organ. Lovendringen er en del av gjennomføringen av EUs datalagringsdirektiv og er ennå ikke trådt i kraft. Det er således presisert at overtredelse av taushetsplikten etter denne bestemmel-

sen kan straffes etter straffeloven, og at dette også gjelder for personer som ikke er i tjeneste eller arbeid for statlig eller kommunalt organ, dersom vedkommende er gjort oppmerksom på at overtredelsen kan straffes.

13.5.8 Underretning

Ved bruk av skjulte tvangsmidler i forebyggende øyemed etter politiloven er det etter *gjeldende rett* ikke krav til underretning. Dette følger av politiloven § 17 e annet ledd tredje punktum. Om dette heter det i Ot.prp. nr. 60 (2004–2005) Punkt 9.4.3.2 side 134:

> «Når det gjelder spørsmålet om underretning, er departementet imidlertid enig med flertallet i utvalget og Politidirektoratet i at særtrekkene ved den forebyggende virksomheten gjør at underretning ikke bør gis. Forslaget til § 17 e annet ledd er utformet i samsvar med dette.»

Utvalget foreslår å endre politiloven § 17 e annet ledd slik at den inngrepet etter § 17 d retter seg mot, har krav på underretning etter at bruken av tvangsmiddelet har opphørt. Utvalget mener at en underretningsplikt er best i samsvar med Norges menneskerettslige forpliktelser.

De to *høringsinstansene* som har uttalt seg, har innvendinger mot forslaget. *PST* bemerker følgende:

> «Utvalgets forslag vil få store konsekvenser for PST. Forslaget rokker ved en helt avgjørende premiss for en sikkerhetstjeneste – muligheten til å bevare taushet om hvem virksomheten rettes mot. Det er PSTs vurdering at underretning alltid vil kunne være til vesentlig skade for PST, og det er derfor avgjørende at tvangsmiddelbruk i regi av PST også i fremtiden skal kunne forbli skjult.
>
> Det synes videre noe usikkert hvilke generelle rettsetninger som kan utledes fra de konkrete og situasjonsbetingende avgjørelser som utvalget har redegjort for fra den europeiske menneskerettighetsdomstol. En ren språklig forståelse av de sitater som er hentet fra EMD-avgjørelsene, synes ikke å gå lenger enn til å si at den som er utsatt for tvangsmiddelbruk i ettertid *burde* bli gjort kjent med tvangsmiddelbruken.
>
> På denne bakgrunn vil PST fremheve viktigheten av en ordning med unnlatt underretning må kunne videreføres såfremt dette, slik som i dag, balanseres av virkemidler som sikrer rettsikkerheten for den som er utsatt for tvangsmiddelbruken. Ikke bare er den som utsettes for tvangsmiddelbruk i dag representert gjennom en egen advokat i forhold til om vilkårene for tvangsmiddelbruken er tilstede. I tillegg etterkontrollerer EOS-utvalget at vilkårene for tvangsmiddelbruken rent faktisk etterfølges og at opplysninger fra tvangsmiddelbruken brukes etter forutsetningene.»

Videre fremhever Politiets sikkerhetstjeneste at det er viktig at spørsmålene om underretning utredes videre i forhold til deres særskilte behov.

Oslo statsadvokatembeter uttaler følgende:

> «Hva gjelder PST's saksområde er man enig med utvalget at det her gjør seg særlige hensyn gjeldende. Disse er imidlertid knyttet til utenlandske institusjoner i Norge. Her oppstår det spesielle problemstillinger hva gjelder bruk av tvangsmidler. En vil her likevel peke på at det kunne gis en særskilt lovhjemmel som gjelder bruk av kommunikasjonskontroll i forhold til disse. Dette er en løsning som er valgt i enkelte land. Hva gjelder norske statsborgere og personer med fast bopel i Norge, bør disse falle inn under de generelle regler som foreslås av utvalget.»

Departementet mener fortsatt at særtrekkene ved den forebyggende virksomheten som regel vil gjøre det nødvendig å holde opplysninger om bruken av tvangsmidlet og opplysningene som bruken resulterte i, hemmelig for den som ble utsatt for inngrepet. Det foreslås å videreføre PSTs adgang til å unnlate underretning om bruk av skjulte tvangsmidler i forebyggende øyemed, jf. punkt 6.10.6.2 ovenfor.

Departementet vil fremheve at PST skal etterforske og forebygge straffbare handlinger som truer sikkerheten i samfunnet eller grunnleggende samfunnsinstitusjoner, jf. politiloven § 17 b. Ofte begås slike handlinger av lukkede og profesjonelle miljøer. For personer med planer om å begå så alvorlige straffbare handlinger, antas straffens allmennpreventive effekt å spille en begrenset rolle. Dette gjør forebyggingsarbeidet særdeles viktig. Kjernen i sikkerhetstjenestens virksomhet er å oppdage mulige trusler mot samfunnssikkerheten tidligst mulig, og helst lenge før hendelsesforløpet har kommet så langt at grensen for det straffbare er nådd. I Ot.prp. nr. 60 (2004–2005) punkt 9.4.3.2 side 134 og 153 la departementet til grunn at særtrekkene ved denne forebyggende virksomheten som regel gjør det nødven-

dig å bevare metodebruken hemmelig for den som er utsatt for inngrepet.

Departementet er fremdeles av den oppfatning at det er grunn til å særbehandle PSTs forebyggende arbeid, slik at det fortsatt bør være adgang til å unnlate underretning her. Departementet kan ikke se at dette er i strid med EMK artikkel 8. Bruken av skjulte metoder i forebyggende øyemed kontrolleres av domstolene og den offentlig oppnevnte advokaten i forkant, og i etterkant av Justisdepartementet som overordnet myndighet for Politiets sikkerhetstjeneste og av EOS-utvalget. Det må også tas i betraktning at tillatelse gis på strenge vilkår og at adgangen til skjult tvangsmiddelbruk i forebyggende øyemed gjelder for et meget begrenset saksområde; terrorhandlinger, ulovlig etterretningsvirksomhet og de mest alvorlige formene for vold eller trusler mot representanter for våre øverste statsmyndigheter eller representanter for tilsvarende organer i andre land. Slike oppgaver tør være i kjernen for den nasjonale handlefrihet, se punkt 6.10.6.1 som refererer dommen *Klass mot Tyskland*, avsnitt 58. Ut fra det foreliggende fra EMD, mener departementet at det – særlig på dette området – er grunn til å være varsom med å innfortolke absolutte skranker i EMK artikkel 8.

Departementet går etter dette inn for å videreføre regelen i politiloven § 17 e om at den tvangsmidlet retter seg mot, ikke har krav på underretning etter at tvangsmiddelbruken har opphørt.

14 Dataavlesing

14.1 Hva er «dataavlesing»?

«Dataavlesing» er ikke et entydig juridisk begrep, og betegner heller ikke noen klart avgrenset teknologisk fremgangsmåte. Gjeldende rett inneholder ingen bestemmelser som hjemler dataavlesing som selvstendig tvangsmiddel eller gjennomføringsmåte for andre tvangsmidler. I mandatet til Metodekontrollutvalget er metoden definert som «avlesing av opplysninger i et ikke offentlig tilgjengelig informasjonssystem ved hjelp av programmer eller annet utstyr». Begrepet dataavlesing kan være dekkende for en rekke ulike fremgangsmåter for å skaffe tilgang til informasjon som produseres, lagres eller kommuniseres i eller mellom elektroniske informasjonssystemer.

I forbindelse med etterforskning, forebygging og avverging av kriminalitet kan dataavlesing særlig være interessant som fremgangsmåte for *skjult innhenting av informasjon* fra informasjonssystemer som benyttes av mistenkte. *Informasjonssystem* kan som begrep sies å favne videre enn *kommunikasjonsanlegg*, som er omtalt i punkt 7.1.2 ovenfor. Et eksempel vil være en kopimaskin, som det er naturlig å betegne som et informasjonssystem, men ikke nødvendigvis som et kommunikasjonsanlegg. Kopimaskinen kan manipuleres til å lagre informasjon som normalt ikke lagres – for eksempel bilder av alle dokumenter som kopieres på den. Denne informasjonen kan så hentes ut på ulike måter, jf. nedenfor. Betegnelsen informasjonssystem dekker også det som ellers kan betegnes som kommunikasjonsanlegg – for eksempel datamaskiner og mobiltelefoner. I det følgende bruker departementet også betegnelsen *«datasystem»* synonymt med informasjonssystem.

Det kan tilrettelegges for innhenting av informasjon gjennom dataavlesing ved at det installeres *maskinvare* («hardware») eller *programvare* («software») på eller i et elektronisk informasjonssystem. Plasseringen av programvare kan blant annet gjennomføres ved å modifisere filer som lastes ned av informasjonssystemets bruker, eller ved å sende programvaren som vedlegg til e-post (eller skjult i vedlegget), og få brukeren til å åpne vedlegget. Videre kan programvaren installeres i informasjonssystemet ved både fysisk og elektronisk innbrudd. Plassering av maskinvare forutsetter derimot fysisk tilgang til informasjonssystemet.

Med hensyn til hvilken type informasjon som kan avleses, følger begrensningene teknisk sett bare av hva slags informasjonssystem det dreier seg om og funksjonaliteten til program- eller maskinvaren som benyttes. Dataavlesing kan i prinsippet innebære avlesing av blant annet

- lydstrømmen som sendes fra en tilknyttet mikrofon til operativsystemets drivere
- lydstrømmen som sendes ut til en tilknyttet høyttaler fra operativsystemets drivere
- videostrømmen som sendes fra et tilknyttet kamera (webkamera) til operativsystemets drivere
- tastetrykkene som sendes fra et tastatur til operativsystemets drivere
- innholdet på en harddisk, minnepenn eller annet tilkoblet lagringsmedium
- data som hentes inn fra eller sendes ut på internett eller andre nettverk
- data i fysiske og virtuelle minneområder
- gjeldende ip-adresser for nettverksenhetene
- geografisk koordinatinformasjon fra en tilknyttet GPS-enhet
- signalstrømmen mellom tilkoblet skjerm og datautstyret

For å få tilgang til informasjonen som avleses, må programvaren enten lagre den, eller sende den via internett eller annet tilknyttet nettverks- eller radioutstyr. Den avleste informasjonen kan blant annet hentes ut ved fysisk tilstedeværelse (for eksempel ved innbrudd), ved å hente den ut fra internett ved å utnytte såkalte «bakdører» i programvaren eller ved å fange informasjonen opp gjennom kommunikasjonsavlytting.

14.2 Gjeldende rett

14.2.1 Innledning

Som nevnt ovenfor finnes det ingen bestemmelser som hjemler dataavlesing som selvstendig, skjult

tvangsmiddel i norsk rett. Blant de metodene som tillates etter gjeldende rett, fremstår særlig kommunikasjonsavlytting og hemmelig ransaking (omtales også som skjult ransaking) som relevante med hensyn til skjult innhenting av informasjon fra informasjonssystemer som benyttes av mistenkte. Nedenfor følger det derfor en kort redegjørelse for disse tvangsmidlene.

14.2.2 Kommunikasjonsavlytting

Det følger av straffeprosessloven § 216 a tredje ledd at kommunikasjonsavlytting kan bestå i «å avlytte samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon som den mistenkte besitter eller kan antas å ville bruke». Med hensyn til inngangsvilkårene vises det til den generelle redegjørelsen under punkt 7.1.2 ovenfor.

Formuleringen «samtaler eller annen kommunikasjon» er ment å omfatte all informasjonsutveksling mellom kommunikasjonsanlegg, uavhengig av hvilken form eller hvilket innhold informasjonen måtte ha, jf. Ot.prp. nr. 64 (1998–99) punkt 23 IV side 156. Bestemmelsen gir derfor adgang til å avlytte alle former for data som kommuniseres mellom bestemte «kommunikasjonsanlegg». Adgangen er uavhengig av hvilket overføringsmedium som benyttes, og adgangen skal ikke være begrenset til offentlige nett, men også omfatte private og lukkede nett, jf. Ot.prp. nr. 64 (1998–99) punkt 23 IV side 157. Det er imidlertid trukket en grense mot de minste private nettverkene. Avlytting av interne hustelefoner, eller flere datamaskiner i samme bygning koblet til et lukket nettverk, betraktes som romavlytting.

Straffeprosessloven § 216 a er nøytral med hensyn til hvilke teknologiske midler som kan benyttes for å gjennomføre kommunikasjonsavlytting. I utgangspunktet gir bestemmelsen derfor rom for å benytte for eksempel datatekniske løsninger, forutsatt at fremgangsmåten er forenlig med bestemmelsens øvrige skranker. I særmerknadene til straffeprosessloven § 216 a (Ot.prp. nr. 64 (1998–99) punkt 23 IV side 156) er det gitt uttrykk for at også avlytting av den *elektromagnetiske strålingen* fra et kommunikasjonsanlegg kan være aktuelt:

> «ØKOKRIM har under høringen uttrykt ønske om at avlyttingsreglene skal omfatte såkalt TEMPEST-avlytting, dvs avlytting av den elektromagnetiske strålingen fra blant annet datautstyr. Denne avlyttingsmetoden går ut på å fange opp den elektromagnetiske strålingen fra skjermer, kabler eller annet utstyr og omforme dette til meningsgivende data. Ved avlytting av utstyr som avgir sterk stråling, kan denne metoden brukes på lang avstand. Det er i dag mulig å gjenskape en datamaskins skjermbilde på flere hundre meters avstand.
>
> Tempoet i den teknologiske utviklingen gjør det sannsynlig at denne metoden raskt vil utvikles ytterligere. I tillegg vil det antagelig også dukke opp nye, hittil ukjente metoder for avlytting. Avlyttingsadgangen er derfor gjort uavhengig av hvilken teknologi som benyttes. Det avgjørende er om avlyttingen retter seg mot *kommunikasjon*. I forhold til TEMPEST-avlytting innebærer dette at metoden kan benyttes til å fange opp signaler mellom to kommunikasjonsanlegg idet signalene overføres. Metoden kan derimot ikke benyttes til å avlytte informasjon som ikke kommuniseres. Dette innebærer blant annet at en datamaskins skjermbilde ikke vil kunne avleses.»

Avlyttingsadgangen er som nevnt begrenset til «kommunikasjon». I særmerknadene til bestemmelsen (Ot.prp. nr. 64 (1998–99) punkt 23 IV side 156) er det fremhevet at dette innebærer at:

> «[…] det bare er signalstrømmen mellom to kommunikasjonsanlegg som kan avlyttes. Denne begrensningen er aktuell i tilfeller der informasjonen som kommuniseres og/eller annen informasjon finnes lagret på ett eller flere av de anlegg som benyttes i kommunikasjonen. For å få tilgang til slik lagret informasjon, må politiet benytte reglene om beslag eller utlevering. Dette er blant annet praktisk i forhold til e-post. En melding som er lagret hos avsender, mottager eller en internettilbyder (typisk på sistnevntes «mail-server»), kan politiet bare få tilgang til gjennom beslag eller utleveringspålegg.
>
> […]
>
> Med *kommunikasjon* menes i denne forbindelse overføring av informasjon fra en avsender til en mottager. Det er således ikke kommunikasjon når det tas utskrift av et datalagret dokument, selv om dokumentet da overføres fra datamaskinen til skriveren. Tilsvarende gjelder ved annen overføring mellom en datamaskin og periferienheter, for eksempel ved sikkerhetskopiering til et eksternt lagringsmedium.»

Kommunikasjonsavlytting etter straffeprosessloven § 216 a, må som følge av denne avgrensningen foregå i «transportfasen» – når informasjonen er under overføring fra avsenderanlegget til mottakeranlegget. Avlyttingen gjennomføres ofte med bistand av tele- eller internettilbyder, ved at det sendes kopi av datapakkene til politiet når disse passerer tilbyderens servere. I dag sendes de ulike datapakkene ofte *kryptert*. Brukeren kan bevisst ha valgt å bruke en krypteringsløsning, men stadig flere tjenester tilknyttet internett benytter krypteringsløsninger som standard, for å beskytte informasjonen i datapakkene i forsendelsen fra avsender til mottaker. Politiet er etter gjeldende rett henvist til å «knekke» krypteringen, eller å skaffe seg tilgang til krypteringsnøkkelen, for å kunne tilegne seg meningsinnholdet i krypterte datapakker som fanges opp i transportfasen mellom avsender og mottaker.

I merknadene til straffeprosessloven § 216 a ble det pekt på at politiet ikke har mulighet til å tilegne seg informasjon som verken lagres eller kommuniseres, siden verken utleveringspålegg, beslag eller kommunikasjonsavlytting kan benyttes i disse tilfellene. I denne forbindelse omtales bruk av dataavlesing, i form av programvare kalt «trojanske hester» slik (Ot.prp. nr. 64 (1998–99) punkt 23 IV side 156–157:

> «Det har i denne forbindelse vært reist spørsmål om bruken av såkalte trojanske hester. Dette er dataprogrammer som skjuler seg inne i andre, tilsynelatende nyttige programmer eller dokumenter. Det finnes slike programmer som er laget nettopp med tanke på etterforskning. Disse installeres på den mistenktes maskin når mistenkte åpner en e-post melding han får tilsendt. Mistenkte vil ikke kunne merke at programmet blir installert. Når programmet er installert, vil det registrere all aktivitet på maskinen i en logg, som med jevne mellomrom overføres til politiet via e-post. Heller ikke dette vil den mistenkte kunne oppdage. Slik metoden er beskrevet ovenfor, vil den ikke ha hjemmel i utkastet til §216a. Overvåkningen retter seg her mot all aktivitet på en datamaskin, ikke mot kommunikasjonen mellom maskiner. Departementet tar med dette ikke generelt stilling til bruken av trojanske hester som etterforskningsmetode, herunder de betenkeligheter som er knyttet til måten programmene installeres på.»

Uttalelsen gjelder bruk av dataprogrammer for å registrere «all aktivitet» på mistenktes datamaskin. Det ble ikke konkret tatt stilling til hvorvidt slike programmer likevel kunne brukes utelukkende til målrettet avlytting av informasjon som *kommuniseres*. Gjennomføringsmåten, som involverer skjulte inngrep på mistenktes datamaskin, synes imidlertid å ligge klart utenfor rammene for det straffeprosessloven § 216 a gir adgang til.

14.2.3 Hemmelig ransaking og beslag

Etter straffeprosessloven § 200 a første ledd kan retten ved kjennelse beslutte at ransaking kan settes i verk uten underretning til den mistenkte eller andre (hemmelig ransaking), dersom noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i ti år eller mer, eller som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136 a, 231, 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231 (straffeloven 1902 §§ 90, 91, 91 a, 94 jf. 90, 104 a første ledd annet punktum, eller 104 a annet ledd jf. første ledd annet punktum, 147 d, eller av §§ 162 eller 317, jf. 162).

Tillatelse til hemmelig ransaking kan bare gis dersom det må antas å være av vesentlig betydning for å oppklare saken, og oppklaring ellers i vesentlig grad vil bli vanskeliggjort, jf. straffeprosessloven § 200 a annet ledd, og bare dersom det ikke er et uforholdsmessig inngrep, sakens art og forholdene ellers tatt i betraktning, jf. straffeprosessloven § 170 a. Dersom det ved opphold er stor fare for at etterforskningen vil lide, kan ordre fra påtalemyndigheten tre istedenfor rettens kjennelse, jf. straffeprosessloven §§ 200 a sjette ledd, jf. 216 d. I så fall skal påtalemyndighetens beslutning snarest mulig, og senest innen 24 timer at ble påbegynt, forelegges retten for godkjennelse.

Hemmelig ransaking etter straffeprosessloven § 200 a kan foretas for å søke etter bevis eller annet som det kan tas beslag i etter reglene i straffeprosessloven kapittel 16. Om nødvendig «kan det åpnes adgang med makt», jf. straffeprosessloven § 200 annet ledd tredje punktum.

Ransakingsadgangen gjelder også for informasjon som er lagret *elektronisk* i et informasjonssystem, for eksempel på harddisken i en datamaskin. Et annet eksempel er ransaking av virtuelle brukerkontoer – for eksempel en e-postkonto eller annen lagringstjeneste hvor innholdet lagres på en ekstern server hos tilbyderen. I slike tilfeller gjennomføres politiets ransaking nødvendigvis uten fysisk tilstedeværelse.

Politiet kan etter straffeprosessloven § 199 a pålegge enhver som har befatning med datasys-

temet å gi opplysninger som er nødvendige for å gi tilgang til datasystemet.

Selv om hemmelig ransaking gjennomføres uten varsel, skal den mistenkte i utgangspunktet underrettes om kjennelsen og ransakingen i ettertid. Etter straffeprosessloven § 200 a tredje ledd kan retten ved kjennelse beslutte at underretning om ransakingen og resultatet av den, også i ettertid skal utsettes dersom det er strengt nødvendig for etterforskningen i saken at underretning ikke gis. Utsettelse kan besluttes for inntil åtte uker om gangen. I saker om overtredelse av straffeloven kapittel 17 kan retten beslutte at underretning kan utsettes for inntil seks måneder av gangen eller unnlates helt.

Straffeprosessloven § 208 a åpner for hemmelig beslag, hvilket vil være særlig aktuelt for bevis som oppdages i forbindelse med hemmelig ransaking, men utsatt underretning om beslaget kan også besluttes i andre tilfeller. Vilkåret for å utsette underretning om beslaget er at noen med skjellig grunn mistenkes for en handling eller forsøk på handling som etter loven kan medføre høyere straff enn fengsel i seks måneder, og at det er strengt nødvendig for etterforskningen i saken at underretning ikke gis. Beslutningen treffes av retten i kjennelse, men politiet er gitt tilsvarende hastekompetanse som for hemmelig ransaking, jf. straffeprosessloven § 208 a femte ledd.

14.2.4 Bruk av kommunikasjonsavlytting og hemmelig ransaking i avvergende og forebyggende øyemed

Både kommunikasjonsavlytting og hemmelig ransaking kan benyttes i avvergende øyemed etter straffeprosessloven § 222 d og som ledd i forebygging etter politiloven § 17 d. Det vises til fremstillingen av gjeldende rett under kapittel 13.

14.3 Andre lands rett

14.3.1 Dansk rett

Etter retsplejeloven § 780, stk. 1, nr. 1 kan politiet, på vilkårene som fremgår av lovens kapittel 71, avlytte «telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning)». Denne adgangen til *kommunikasjonsavlytting* er betinget av at det «er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt», og at inngrepet «må antages at være af afgørende betydning for efterforskningen», jf. henholdsvis retsplejeloven § 781, stk. 1, nr. 1 og nr. 2. Etterforskningen må angå en lovovertredelse som etter loven kan straffes med fengsel i seks år eller mer, eller enkelte andre, spesifikt angitte straffebud, jf. § 781, stk. 1, nr. 3. Tillatelse til kommunikasjonsavlytting gis av retten i kjennelse, jf. § 783, stk. 1. Politiet er gitt hastekompetanse, tilsvarende den norske straffeprosessloven § 216 d, i retsplejeloven § 783, stk. 4.

Adgangen til kommunikasjonsavlytting dekker ikke bare telefonsamtaler, men også «anden tilsvarende telekommunikation», som e-post og sms. Kommunikasjonsavlyttingen kan bare rettes mot budskap som er under transport mellom avsender og mottaker, slik regelen også er etter den norske straffeprosesseloven § 216 a. En e-post som er mottatt, men ikke åpnet hos mottakeren, må politiet således tilegne seg med hjemmel i reglene om ransaking og beslag.

I utgangspunktet skal kommunikasjonsanlegg som tillates avlyttet identifiseres i kjennelsen, jf. retsplejeloven § 783, stk. 1. I en viss utstrekning kan retten imidlertid også knytte tillatelsen til den mistenkte personen, uten angivelse av hvilke telefonnummer som kan avlyttes, jf. § 783, stk. 2. Det sistnevnte forutsetter at etterforskningen angår en overtredelse av ett eller flere av straffebudene som er listet opp i stk. 2, som gjelder alvorlig kriminalitet. Dersom det gis tillatelse til kommunikasjonsavlytting knyttet til person, skal politiet snarest mulig etter utløpet av tillatelsen gi retten underretning om hvilke nummer som har blitt kontrollert. Underretningen skal inneholde en angivelse af de «bestemte grunde, der er til at antage, at der fra de pågældende telefonnumre gives meddelelser til eller fra den mistænkte», jf. retsplejeloven § 783, stk. 2.

Inngrepet skal ikke tillates dersom det ville være uforholdsmessig de konkrete omstendighetene tatt i betraktning, jf. retsplejeloven § 782, stk. 1 – det samme prinsippet som i norsk rett.

Hemmelig ransaking, det vil si ransaking med utsatt eller unnlatt underretning, er i dansk rett hjemlet i retsplejeloven § 799. Hemmelig ransaking kan besluttes av retten ved kjennelse hvis etterforskningen angår en «forsætlig overtredelse» av den danske straffeloven kapittel 12 (forbrytelser mot statens selvstendighet og sikkerhet) eller 13 (forbrytelser mot statsforfatningen og de øverste statsmyndigheter, terrorisme mv.), eller andre straffebud som er listet opp i retsplejeloven § 799, stk. 1. Opplistingen omfatter straffebud som rammer menneskesmugling, forsettlig brannstiftelse eller forvoldelse av transportulykker eller sprengning med fare for menneskeliv eller omfattende ødeleggelser mv., kapring, ødeleggelse av drikke-

vannskilder og drikkevannsledninger mv. med fare for menneskeliv eller sunnhet, forgiftning av forbruksvarer, grove narkotikalovbrudd, utbredning av smittsom sykdom, grove våpenovertredelser, alvorlige former for befatning med radioaktive stoffer, drap, menneskehandel, særlig grovt tyveri, ran og særlig grove overtredelser av skatte-, toll- eller avgiftslovgivningen.

Sammenlignet med «åpen» ransaking gjelder det et skjerpet indikasjonskrav for å tillate hemmelig ransaking, da det må være «af afgørende betydning for efterforskningen» at ransakingen foretas uten underretning til den mistenkte eller andre. Mistankekravet er imidlertid det samme som for ordinær ransaking, hvilket innebærer at ransaking av husvære, andre lokaliteter eller gjenstander som en mistenkt har rådighet over, kan finne sted hvis vedkommende «med rimelig grund er mistænkt» for overtredelse av et av straffebudene som er opplistet i retsplejeloven § 799, stk. 1, jf. § 794, stk. 1. Ved ransaking av husvære, andre lokaliteter eller gjenstander som andre enn mistenkte har rådighet over, kreves det i tillegg at det er «bestemte grunde til at antage» at bevis i saken eller gjenstander som kan beslaglegges, kan finnes ved ransakingen, jf. retsplejeloven § 795, stk. 1, nr. 2.

I kjennelsen skal retten fastsette det tidsrommet ransakingen kan foretas innenfor. Dette skal være så kort som mulig, og ikke overstige fire uker, men kan forlenges, jf. retsplejeloven §§ 799, stk. 2, jf. 783, stk. 3. Ved hemmelig ransaking kan retten også bestemme at det kan foretas et bestemt antall *gjentatte ransakinger* innenfor det fastsatte tidsrommet. Hvis «særlige grunde taler derfor», kan retten gi tillatelse til et ubestemt antall ransakinger innenfor det fastsatte tidsrommet, jf. retsplejeloven § 799, stk. 3.

Adgangen til å tillate gjentatte ransakinger under én og samme beslutning ble innført i 2002 som et element i den såkalte «anti-terrorpakke I». Den ble begrunnet med at det kan være en rekke tilfeller hvor det er behov for å ransake et objekt flere ganger, for eksempel dersom våpen eller narkotika ikke finnes ved første ransaking, men det er mistanke om at levering av slikt vil finne sted innen kort tid.

Som etter norsk rett kan ransakingen også rette seg mot elektronisk lagret informasjon, for eksempel i form av ransaking av en datamaskin, en e-postkonto eller en brukerprofil på sosiale medier. Det følger blant annet av dansk Højesterets kjennelse 10. mai 2012 i sak 129/2011 at elektronisk ransaking ikke fordrer fysisk tilstedeværelse. I denne saken hadde politiet gjennom telefonavlytting gjort seg kjent med brukernavn og passord til mistenktes facebook- og messengerprofiler, og brukt disse opplysningene til å logge seg på profilene fra sine egne maskiner for å lete etter lagrede meldinger og andre opplysninger lagret på profilene – det vil si i tjenestetilbydernes servere. Højesteret fant at dette hadde karakter av gjentatte hemmelige ransakinger, som kunne foretas med hjemmel i retsplejeloven § 793, stk. 1, nr. 1, jf. § 799.

Politiet er gitt hastekompetanse til å beslutte hemmelig ransaking etter samme modell som for kommunikasjonsavlytting, jf. retsplejeloven § 796, stk. 3.

I Danmark er *«dataaflæsning»* dessuten innført som selvstendig metode i retsplejeloven § 791 b. Bestemmelsen ble innført ved lov nr. 378 av 6. juni 2002, som et ledd i gjennomføringen av blant annet FNs konvensjon om bekjempelse av finansiering av terrorisme, samt FNs sikkerhetsråds resolusjon nr. 1373 (2001) om tiltak for bekjempelse av terror.

I merknadene til lovforslaget ble det vist til at politiet allerede hadde adgang til å benytte kommunikasjonsavlytting og hemmelig ransaking for å tilegne seg innholdet i elektronisk kommunikasjon og elektronisk lagret informasjon, men at det i noen tilfeller hadde vist seg *praktisk umulig* å skaffe tilgang til informasjon som politiet rettslig sett hadde adgang til å gjøre seg kjent med gjennom slik tvangsmiddelbruk.

I merknadene pekes det særlig på en kjennelse fra dansk Højesteret inntatt i UfR 2001 side 1276. Avgjørelsen gjaldt en sak om etterforskning av narkotikahandel, hvor vilkårene var oppfylt for å avlytte e-postkommunikasjon fra en datamaskin i en leilighet i en boligblokk, samt for å pålegge danske teleselskaper å opplyse hvilke kommunikasjonsanlegg som hadde blitt satt i forbindelse med denne datamaskinen. Politiet hadde imidlertid ikke teknisk mulighet til å gjennomføre avlyttingen, siden installasjon av avlyttingsutstyret ville medføre for stor risiko for avsløring. Dessuten var det ikke mulig for politiet å skille e-post sendt fra mistenktes datamaskin fra e-post sendt av brukere av andre datamaskiner i den samme boligblokken. Politiet ba derfor retten om tillatelse til å installere et såkalt «sniffer-program» i mistenktes datamaskin. Med et slikt program ville politiet – uten mistenktes viten – få tilsendt kopi av alle elektroniske meddelelser som ble sendt fra datamaskinen. Programmet ville også gi mulighet til å registrere samtlige inntastinger foretatt av brukeren, og det kunne registrere og videresende opplysninger til politiet om at datamaskinen ble åpnet,

besøk av internettadresser, opprettelse og redigering av dokumenter, regnskaper mv.

Højesteret kom til at det var nærliggende å sidestille bruken av et slikt program med gjentatt, hemmelig ransaking, som retsplejeloven § 799 den gang ikke ga adgang til. I merknadene til lovforslaget vedrørende dataavlesing ble det under henvisning til kjennelsen lagt til grunn at bestemmelsen om hemmelig ransaking ikke hjemler undersøkelse av materiale i en datamaskin ved «løbende aflæsning, der foretages af politiet fra et andet sted».

Justitsministeriet pekte på at tekniske forhold og risikoen for avsløring innebar at politiet ikke i alle tilfeller hadde mulighet til å utnytte den eksisterende adgangen til å gjøre seg kjent med elektroniske meddelelser og elektronisk lagret materiale. Det uttalte at politiet, blant annet i lys av terrorangrepene mot USA 11. september 2001, kunne ha behov for å løpende kunne registrere innholdet og anvendelsen av «bestemte computere mv.» i forbindelse med etterforskningen av alvorlig kriminalitet, for eksempel gjennom installering av spesiell programvare, som «sniffer-programmer». Dette gjaldt ifølge Justitsministeriet særlig i forbindelse med etterforskningen i saker om overtredelse av den danske straffeloven kapittel 12 (forbrytelser mot statens selvstendighet og sikkerhet) og kapittel 13 (forbrytelser mot statsforfatningen og de øverste statsmyndigheter mv.), overtredelse av straffeloven § 180 om kvalifisert brannstiftelse, § 183, stk. 1 og 2 om forvoldelse av sprengning og spredning av skadevoldende luftarter, jernbaneulykke m.m., § 183 a om flykapring, § 186, stk. 1 om forvoldelse av fare for menneskers liv eller helbred ved å tilsette vannbeholdninger sunnhetsfarlige stoffer, § 187, stk. 1 om å tilsette gift eller andre lignende stoffer i ting som er bestemt til forhandling eller utbredt benyttelse, § 191 om grove narkotikalovbrudd, § 192 a om særlig grove våpenlovovertredelser, samt § 237 om drap. Justitsministeriet bemerket at en rekke av disse overtredelsene etter sin karakter kunne «tænkes at finde sted som led i eller i forbindelse med egentlige terrorhandlinger».

På ovennevnte bakgrunn ble bestemmelsen om dataavlesing foreslått for å gi politiet mulighet til å bruke «sniffer-programmer» eller annet utstyr for løpende å kunne motta kopi av ikke offentlig tilgjengelige opplysninger i et datasystem, inkludert e-post som mottas eller sendes, inntastinger som blir gjort i datasystemet, og informasjon som lagres i systemets minne, i etterforskning av overtredelser av de ovennevnte straffebudene. Samtidig ble det bemerket at en slik adgang også i noen tilfeller vil gi politiet mulighet til å lese elektroniske meddelelser som sendes til eller fra en mistenkt via en datamaskin eller lignende, selv om kommunikasjonen er kryptert, og derfor ikke er tilgjengelig i klartekst ved ordinær kommunikasjonsavlytting.

Justitsministeriet vurderte om bruken av «sniffer-program» og lignende burde hjemles i bestemmelsene om hemmelig ransaking, men kom til at ransaking etter den tradisjonelle oppfatningen innebærer fysisk tilstedeværelse ved det som skal ransakes, og at den nye metoden dessuten hadde visse likhetstrekk med romavlytting og observasjon av personer i bolig eller andre husvære, fordi opplysningene fremskaffes ved hjelp av teknisk utstyr, uten fysisk tilstedeværelse. Bestemmelsen om dataavlesing ble derfor plassert i retsplejeloven kapittel 71, som gjaldt «indgreb i meddelelseshemmeligheden og om observation».

Kriminalitetskravet for anvendelse av dataavlesing er senere endret. Retsplejeloven § 791 b gir i dag hjemmel for å benytte dataavlesing i etterforskning av overtredelser som etter loven kan straffes med fengsel i seks år eller mer, samt av forsettlige overtredelser av den danske straffeloven kapittel 12 eller 13 (kriminalitetskravet). Bestemmelsen lyder i sin helhet slik:

> «791 b. Aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (dataaflæsning) kan foretages, såfremt
>
> 1) der er bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3,
>
> 2) indgrebet må antages at være af afgørende betydning for efterforskningen, og
>
> 3) efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13.
>
> *Stk. 2.* Indgreb som nævnt i stk. 1 må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.
>
> *Stk. 3.* Afgørelse om dataaflæsning træffes af retten ved kendelse. I kendelsen angives det informationssystem, som indgrebet angår. I øvrigt finder reglerne i § 783, stk. 1, 3. og 4. pkt., samt stk. 3 og 4, tilsvarende anvendelse.
>
> *Stk. 4.* Efterfølgende underretning om et foretaget indgreb sker efter reglerne i § 788,

stk. 1, 3 og 4. Underretningen gives til den, der har rådigheden over det informationssystem, der har været aflæst efter stk. 1. I øvrigt finder reglerne i § 782, stk. 2, §§ 784, 785, 789 samt 791 tilsvarende anvendelse.»

Etter § 791 b, stk. 1 er det «oplysninger i et informationssystem» som kan avleses. Med dette forstås datamaskiner eller andre databehandlingsanlegg, inkludert annet elektronisk utstyr med tilsvarende funksjoner, for eksempel visse mobiltelefoner og elektroniske kalendere, jf Gomard m.fl., Kommenteret Retsplejelov Bind III, (9. udgave, København 2013), note 2 til § 791 b side 269. Både programvare, som «sniffer-program» og trojanere, samt maskinvare kan benyttes for å gjennomføre avlesingen.

Mistankekravet er angitt i stk. 1, nr. 1, hvor det fremgår at det må være «bestemte grunde til at antage» at informasjonssystemet anvendes av en mistenkt i forbindelse med en planlagt eller begått handling som nevnt i stk. 1, nr. 3. Videre innebærer stk. 1, nr. 2 et *indikasjonskrav*, idet dataavlesingen «må antages at være af afgørende betydning for efterforskningen» for å kunne tillates. Det alminnelige forholdsmessighetskravet fremgår av § 791 b, stk. 2.

Avgjørelse om å tillate dataavlesing treffes av retten ved kjennelse, jf. § 791 b, stk. 3. I kjennelsen skal retten angi det informasjonssystemet som tillates avlest. Identifiseringen kan skje ved at utstyrets fabrikat, nummer eller tilsvarende opplyses, eller ved angivelse av det geografiske sted hvor utstyret befinner seg, eller angivelse av hvem som har rådighet over det, jf. Gomard m.fl., Kommenteret Retsplejelov Bind III (9. udgave, København 2013), note 9 til § 791 b side 270. I kjennelsen skal det også fastsettes et tidsrom dataavlesingen kan foretas innenfor. Dette skal være så kort som mulig, og kan ikke overstige fire uker. Tillatelsen kan forlenges ved ny kjennelse med inntil fire uker om gangen, jf. retsplejeloven § 791 b, stk. 3, jf. § 783, stk. 3. Politiet er gitt hastekompetanse til å beslutte dataavlesing på samme vilkår som ved hemmelig ransaking og kommunikasjonsavlytting, jf. retsplejeloven § 791 b, stk. 3, jf. § 783, stk. 4.

I utgangspunktet skal byretten gi underretning om inngrepet etter at dataavlesingen er avsluttet, til den som har rådighet over det informasjonssystemet som har blitt avlest, jf. retsplejeloven § 791 b, stk. 4, jf. § 788, stk. 1. Retten kan etter begjæring fra politiet beslutte at underretning skal utsettes eller unnlates dersom det ville være til skade for etterforskningen eller er nødvendig for å beskytte fortrolige opplysninger om politiets etterforskningsmetoder mv., jf. retsplejeloven § 791 b, stk. 4, jf. § 788, stk. 4.

Når retten treffer avgjørelse om dataavlesing etter retsplejeloven § 791 b, skal det oppnevnes en advokat for den inngrepet angår, som skal ivareta vedkommendes interesser i forbindelse med behandlingen av begjæringen og eventuelt inngrepet, jf. retsplejeloven § 784, jf § 785. Ordningen har likhetstrekk med den norske bestemmelsen om oppnevning av offentlig advokat i forbindelse med skjult tvangsmiddelbruk etter straffeprosessloven § 100 a.

Justitsministeriet har redegjort for erfaringene med blant annet retsplejeloven § 791 b i «Redegørelse om erfaringerne med lovgivning indført i forbindelse med anti-terrorpakke I fra 2002 og anti-terrorpakke II fra 2006», datert 9. september 2010. Justitsministeriet innhentet uttalelse fra Politiets Efterretningstjeneste (PET), som ifølge redegjørelsen opplyste følgende om erfaringene med anvendelsen av retsplejeloven § 791 b (side 26–27):

> «Dataaflæsning omfatter bl.a. den situation, hvor politiet ved hjælp af et såkaldt "sniffer-program" modtager kopi af samtlige indtastninger, som brugeren af edb-udstyret foretager, herunder åbning af computeren, oprettelse af nye dokumenter og regnskaber mv., nye indtastninger i allerede eksisterende dokumenter eller visse nærmere angivne indtastninger.
>
> Muligheden for dataaflæsning indebærer således, at politiet ved hjælp af edb-programmer eller andet udstyr løbende kan aflæse ikke offentligt tilgængelige oplysninger.
>
> Ved dataaflæsning får politiet adgang til tekst, herunder elektroniske meddelelser, uanset om teksten har været under forsendelse til eller fra den computer, der er genstand for dataaflæsning. Dataaflæsning udgør således også et alternativ til bl.a. ransagning, og generelt har Politiets Efterretningstjeneste et stort udbytte af de data, som opnås ved dette indgreb.
>
> Politiets Efterretningstjeneste har anvendt og anvender fortsat dataaflæsning i mange tilfælde. Dataaflæsning har vist sig at være et særdeles nyttigt efterforskningsmiddel og er bl.a. anvendt i forhold til målpersonerne i Vollsmose-sagen og Glasvej-sagen.»

I den såkalte Vollsmose-saken ble tre personer dømt i Højesteret til fengsel i henholdsvis tolv år (to personer) og fem år for forsøk på terrorhandlinger mot blant annet Jyllands-Posten, Folketinget og Københavns Hovedbanegård. I «Glasvej-

sagen» ble to personer dømt til fengsel i henholdsvis tolv år og åtte år for forsøk på terrorhandlinger. De to hadde blant annet fremstilt sprengstoff i en leilighet i København.

I redegjørelsen fra 2010 har Justitsministeriet konkludert med at det, på bakgrunn av blant annet tilbakemeldingene fra PET, ikke finner at «der aktuelt er behov for ændring af de regler i retsplejeloven, som blev indført i forbindelse med anti-terrorpakkerne» (side 29). Videre uttales følgende i redegjørelsen (side 29–30):

> «Det bemærkes herved, at formålet med en række af de ændringer af retsplejeloven, der blev indført i forbindelse med anti-terrorpakkerne, var at styrke Politiets Efterretningstjenestes efterforskningsmuligheder. I den forbindelse kan det på baggrund af Politiets Efterretningstjenestes udtalelse konstateres, at de redskaber, som tjenesten har fået stillet til rådighed, generelt er blevet anvendt med positive resultater.»

På side 45 fremgår i samme retning:

> «Det bemærkes i øvrigt, at der i forbindelse med indførelsen af de 2 anti-terrorpakker i høj grad var fokus på at skabe en lovgivning, som kunne sikre en effektiv terrorbekæmpelse uden at kompromittere borgernes grundlæggende rettigheder, og de efterfølgende erfaringer med anvendelsen af reglerne giver efter Justitsministeriets opfattelse ikke anledning til at overveje ændringer af den gennemførte lovgivning ud fra retssikkerhedsmæssige hensyn.»

Metodekontrollutvalget har også henvendt seg til den danske riksadvokaten og etterspurt hans vurdering av metoden på bakgrunn av de danske erfaringene med bestemmelsen om dataavlesing. Om dette heter det i utredningen punkt 23.2.2 side 242–243:

> «[…] Utvalget ba særlig om å få oversendt eventuelt tallmateriale som viser behov og effektivitet, men også eksempler som illustrerer når politiet har hatt behov for metoden og på hvilken måte den har vært avgjørende for den videre etterforsking og iretteføring av straffbare handlinger. Det ble videre bedt om en vurdering av i hvilke situasjoner og for hvilke straffbare handlinger metoden har vist seg å ha særlig betydning. I denne sammenheng ble det opplyst at det var ønskelig om det kunne sies noe om hvilken merinformasjon dataavlesing har fremskaffet i forhold til andre tvangsmiddelbestemmelser, særlig kommunikasjonskontroll og ransaking/beslag.
>
> Riksadvokaten rettet på denne bakgrunn en henvendelse til politiet, herunder det nasjonale IT-Efterforskningscenteret (NITEC) som bistår landets politidistrikter i forbindelse med sikring av elektroniske bevis. Politiet opplyste at det ikke finnes oversikt over antallet dataavlesinger i Danmark, og at det heller ikke kan fremskaffes slike opplysninger fra politiets saksbehandlingssystem. Riksadvokaten har likevel opplyst å være kjent med at dataavlesing har vært anvendt i en rekke konkrete saker, herunder to saker om forsøk på terror. I begge disse sakene ble det gjennomført dataavlesing av de siktedes datamaskiner. Dette frembrakte bevis for at de senere domfelte hadde nedlastet bombemanualer, hadde søkt etter kjemikalier mv. som kunne brukes til bombefremstilling, og hadde kommunisert via datamaskiner i tilknytning til planleggingen av forbrytelsene. I forbindelse med utvalgets besøk ved det nasjonale IT-Efterforskningscenteret (NITEC) fikk utvalget opplyst at dataavlesing også hadde vist seg effektivt ved etterforsking av narkotikasaker og saker om barnepornografi.»

14.3.2 Svensk rett

Også etter svensk rett er det adgang til *kommunikasjonsavlytting* – «hemlig avlyssning av elektronisk kommunikation» i etterforskningsøyemed. Tvangsmidlet er regulert i rättegångsbalken 27 kap. Metoden er beskrevet slik i 27 kap. 18 § 1 mom:

> «Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.»

Formuleringen «meddelanden» som overføres eller har blitt overført i et «elektronisk kommunikationsnät» omfatter alle former for kommunikasjon, herunder overføring av lyd, tekst og bilde (for eksempel innholdet i telefon- og telefakstrafikk, e-post, og ved bruk av chat-programmer).

Kommunikasjonsavlytting forutsetter at noen er «skäligen misstänkt» for en overtredelse som nevnt i rättegångsbalken 27 kap. 18 § 2 mom, og at

inngrepet «är av synnerlig vikt» for etterforskningen, jf. 27 kap. 20 § 1 mom. I tillegg gjelder det et alminnelig forholdsmessighetskrav, idet tvangsmidler bare kan benyttes dersom «skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse», jf. 27 kap. 1 § 3 mom.

Avlytting kan tillates i etterforskningen av lovbrudd som har en minstestraff på minst to års fengsel, jf. 27 kap. 18 § 2 mom. Det samme gjelder ved forsøk, forberedelse eller forbund, dersom slike handlinger er straffbare. I tillegg kan avlytting benyttes i etterforskning av slike samfunnsfarlige lovbrudd som er angitt i 27 kap. 2 § 2 mom. nr. 2 til 7, herunder sabotasje, mordbrann, terrorlovbrudd og spionasje, jf. 27 kap. 18 § 2 mom. Opplistingen er til dels overlappende, siden flere av disse lovbruddene har en minstestraff på minst to års fengsel. Avlytting kan også benyttes ved lovbrudd med en lavere minimumsstraff, såfremt straffeutmålingen i det aktuelle tilfellet kan antas å overstige fengsel i to år. Denne såkalte «straffvärdeventilen» er ment å fange opp alvorlige tilfeller hvor sannsynlig straffenivå i betydelig grad overstiger minstestraffen, og det derfor er særlig viktig med en effektiv etterforskning, jf. prop. 2002/03:74 punkt 6.1 side 33.

Avlyttingen kan rettes mot «telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning» som den mistenkte i det tidsrommet tillatelsen gjelder har eller har hatt rådighet over, eller som han ellers kan antas å ha anvendt eller komme til å anvende, eller tilsvarende utrustning som det «finns synnerlig anledning att anta» at han har kontaktet eller kommer til å kontakte, jf. 27 kap. 20 § 1 mom. nr. 1 og 2.

Avgjørelse om hemmelig avlytting av elektronisk kommunikasjon treffes i utgangspunktet av retten etter begjæring fra påtalemyndigheten, jf. rättegångsbalken 27 kap. 21 § 1 mom. Påtalemyndigheten er imidlertid gitt hastekompetanse i 27 kap. 21 a § 1 mom. I tillatelsen skal tidsrommet for avlyttingen angis. Dette kan ikke overstige én måned. Videre skal det i tillatelsen angis hvilket eller hvilke telefonnummer, annen adresse eller elektronisk kommunikasjonsutrustning tillatelsen gjelder, og hvorvidt tillatelsen også gjelder avlytting utenfor «allmänt tillgängliga elektroniska kommunikationsnät», jf. 27 kap. 21 § 3 mom. Det er opp til domstolen å avgjøre hva tillatelsen skal omfatte. I Prop. 2011/12:55 (punkt 11.4 side 131) er det for eksempel lagt til grunn at en tillatelse til avlytting av elektronisk kommunikasjon via e-post normalt ikke bør knyttes til kommunikasjonsutrustningen (datamaskinen) som mistenkte benytter, men spesifikt til selve e-postadressen.

En tillatelse til kommunikasjonsavlytting etter rättegångsbalken 27 kap. 18 § gir også adgang til å utføre slik «hemlig övervakning av elektronisk kommunikation» som er omtalt i 27 kap. 19 §, jf. 27 kap. 18 § 2 mom.

I rättegångsbalken 28 kap. er det gitt regler om blant annet «*husrannsakan*», som kan foretas i «hus, rum eller slutet förvaringsställe för att söka efter föremål som kan tas i beslag eller i förvar eller annars för att utröna omständigheter som kan vara av betydelse för utredning om brottet», dersom det «finns anledning att anta» at det har blitt begått et lovbrudd som kan føre til fengselsstraff, jf. 28 kap. 1 § 1 mom. Etter svensk rett anses det tillatt å gjennomsøke for eksempel en datamaskin i forbindelse med en husransaking – det kreves da ingen særskilt tillatelse for å ransake datamaskinen, jf. SOU 2013:39 side 134 med videre henvisninger til SOU 1995:47 side 184 og SOU 2011:45 side 295–296. Rättegångsbalken 28 kap. 7 § 4 mom. forutsetter at ransaking skal kunne gjennomføres uten umiddelbar underretning til den ransakingen foretas hos, idet underretning skal gis «så snart det kan ske utan men för utredningen».

I Sverige har *«hemlig dataavläsning»* tidligere blitt utredet og foreslått innført som ny metode av Beredningen för rättsväsendets utveckling (BRU) i SOU 2005:38, «Tillgång til elektronisk kommunikation i brottsutredningar m.m.». Forslaget har ikke blitt fulgt opp, blant annet på grunn av kritiske innspill i høringsrunden, men ble igjen aktualisert i en nyere utredning, SOU 2012:44, hvor det pekes på behov for et slikt tvangsmiddel.

Forslaget i SOU 2005:38 går ut på å innføre en egen, midlertidig lov om hemmelig dataavlesing. I lovforslaget 1 § er «hemlig dataavläsning» definert som «att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål». Ifølge forslaget skal hemmelig dataavlesing kunne gjennomføres blant annet ved at politiet i hemmelighet sender egnet programvare til et informasjonssystem, og så lar programvaren rapportere til politiet om informasjon som finnes i informasjonssystemet og bruken av det. Metoden kan også innebære at maskinvare eller programvare med tilsvarende funksjonalitet plasseres i informasjonssystemet gjennom et fysisk inngrep, for eksempel ved innbrudd i en persons bolig.

Tillatelse til dataavlesing må ifølge lovforslaget 10 § gis av retten etter begjæring fra påtalemyndigheten. Begjæringen skal behandles i retts-

møte, og et «offentligt ombud» (en person oppnevnt av regjeringen som er advokat eller har vært advokat eller «ordinarie domare») skal i utgangspunktet oppnevnes for å ivareta integritetsinteressene til den avlesingen retter seg mot i forbindelse med prøvingen, etter reglene i rättegångsbalken 27 kap. 26 til 30 §§.

Dataavlesing skal ifølge lovforslaget 3 § kunne tillates i etterforskning av lovbrudd med en minstestraff på fengsel i to år, samt overtredelse av enkelte andre, særskilt angitte straffebud, herunder bestemmelser om datainnbrudd, hets mot folkegrupper og barnepornografi. I svensk rett har fastsettelse av minstestraffer vært mer utbredt enn i norsk rett. Som eksempler på lovbrudd som omfattes av bestemmelsen om minstestraff på fengsel i to år nevnes mord, drap, grov menneskehandel, grovt ran, mordbrann, allmennfarlig ødeleggelse, grove brudd mot rikets indre og ytre sikkerhet, grovt narkotikalovbrudd og grov narkotikasmugling. Med unntak for datainnbrudd, hets mot folkegrupper og barnepornografi, er det foreslåtte kriminalitetskravet sammenfallende med det som gjelder for avlytting av elektronisk kommunikasjon etter rättegångsbalken 27 kap. 18 § og hemmelig kameraovervåking etter 27 kap. 20 a §.

I lovforslaget 4 § 1 mom. er indikasjonskravet angitt. Dataavlesing skal ifølge forslaget kunne tillates når noen er «skäligen misstänkt» for en overtredelse som nevnt i forslaget 3 §, og inngrepet «är av synnerlig vikt för utredningen». I tillegg skal det gjelde et forholdsmessighetskrav, ved at det kreves at «skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse». Etter forslaget 4 § 2 mom skal dataavlesing også kunne tillates i tilfeller der ingen er «skäligen misstänkt» for overtredelse som nevnt i forslaget 3 §, dersom inngrepet «syftar til att fastställa vem som skäligen kan misstänkas för brottet», forutsatt at de øvrige vilkår etter forslaget 3 § er oppfylt.

Dataavlesing skal etter forslaget 5 § bare kunne rette seg mot informasjonssystem som det «finns särskild anledning til att anta» at den mistenkte har anvendt eller kommer til å anvende. Dersom informasjonssystemet befinner seg i en annens bopel, skal det gjelde et strengere krav, idet dataavlesing bare kan finne sted dersom det «finns synnerlig anledning att anta» at den mistenkte har anvendt eller kommer til å anvende systemet. Dersom dataavlesingen har som formål å fastslå hvem som kan mistenkes for handlingen, kreves det etter forslaget 6 § at det kan konstateres at informasjonssystemet anvendes eller har blitt anvendt i forbindelse med overtredelsen.

En beslutning om hemmelig dataavlesing skal etter forslaget 11 § være tidsbegrenset. Metoden skal ikke kunne anvendes lengre enn nødvendig, og tillatelse kan ikke gis for mer enn én måned fra dagen for beslutningen. Tillatelsen kan forlenges ved ny beslutning, men det er forutsatt at domstolens prøving da vil bli mer restriktiv – under henvisning til forholdsmessighetskravet, jf. SOU 2005:38 side 388.

I beslutningen om hemmelig dataavlesing kan retten etter forslaget 7 § 3 mom. også gi politiet tillatelse til «att i hemlighet bereda sig tillträde till en plats som annars särskilt skyddas mot intrång i syfte att installera de tekniska hjälpmedlen». I utredningen er dette begrunnet med at effektiv anvendelse av metoden i en del tilfeller forutsetter at det tekniske hjelpemiddelet plasseres i datautstyret gjennom et fysisk inngrep, og at de informasjonssystemene det kan bli tale om å avlese i de aller fleste tilfeller vil være plassert på steder som allmennheten ikke har tilgang til, og som er «skyddade mot intrång» (SOU 2005:38 side 389). En eventuell tillatelse til innbrudd for å installere tekniske hjelpemidler skal i henhold til forslaget 11 § annet ledd angis særskilt i rettens beslutning. Et teknisk hjelpemiddel som har vært installert skal fjernes eller gjøres ubrukelig så snart som mulig etter at fristen for bruk av metoden er utløpt, eller når bruken av metoden ellers har opphørt. Retten skal gis underretning om at dette er gjort, jf. forslaget 13 §.

Kommunikasjon mellom mistenkte og hans forsvarer skal etter forslaget 7 § 2 mom. ikke være gjenstand for hemmelig dataavlesing. Dersom det under avlesingen fremkommer at slik kommunikasjon fanges opp, skal avlesingen avbrytes umiddelbart. Eventuelle nedtegnelser eller opptak av slik kommunikasjon skal umiddelbart tilintetgjøres.

Om det ved hemmelig dataavlesing har fremkommet opplysninger om andre straffbare handlinger enn den eller de som lå til grunn for beslutningen om å tillate metoden anvendt (overskuddsinformasjon), kan disse brukes til å undersøke denne straffbare handling nærmere. Etterforskning kan likevel bare innledes på bakgrunn av slike opplysninger dersom handlingen kvalifiserer til fengsel i ett år eller mer, eller dersom det foreligger særlige grunner. Dersom det har fremkommet opplysninger om forestående straffbare handlinger, kan opplysningene anvendes for å forhindre disse, jf. forslaget 8 §.

Materiale som lagres ved hemmelig dataavlesing må etter forslaget 9 § gjennomgås så snart

som mulig med tanke på om materialet har betydning for den pågående etterforskning. De deler av materialet som har betydning for etterforskningen skal oppbevares til saken er endelig avsluttet. De deler som er av betydning for å forhindre forestående straffbare handlinger, skal oppbevares så lenge det er nødvendig for å forhindre disse. Deretter skal materialet tilintetgjøres, jf. forslaget § 9.

I redegjørelsen for forslaget har BRU pekt på at det er et stort behov for dataavlesing som egen metode. Det uttales at den «snabba tekniska utvecklingen medför att det i dagsläget finns stora problem i brottsutredningar med att få fram uppgifter ur datorer eller avlyssna meddelanden mellan datorer» (SOU 2005:38 side 362), og at dette gjelder særskilt når informasjonen er beskyttet av kryptering eller av annen programvare som skjuler informasjonen. Ifølge BRU påtreffes kryptert informasjon i et «ständig ökande antal brottsutredningar» (samme sted). BRU viser samme sted til at bestemmelsene om kommunikasjonsavlytting og kommunikasjonsovervåking har vært gjeldende over lang tid, og at den teknologiske utviklingen i denne tiden har vært «oerhört kraftig och mycket snabb». Disse tvangsmidlene er ifølge BRU ikke egnet til å overvinne utfordringene knyttet til kryptert informasjon mv. Det konstateres at den utbredte bruken av krypteringsprogrammer og andre tekniske løsninger for å skjule informasjon medfører at det «är mer regel än undantag» at politiet får tilgang til informasjon i datamaskiner under etterforskning av alvorlig kriminalitet (SOU 2005:38 side 364). BRU mener derfor at det er stort behov for dataavlesing som metode, særlig i etterforskning av alvorlig og organisert kriminalitet. BRU uttaler at det ofte er tale om situasjoner der det «i princip inte finns någon möjlighet att på annat sätt skaffa fram avgörande uppgifter och bevisning rörande grova brott» (SOU 2005:38 side 369). Om metodens antatte effektivitet uttales følgende på side 366:

> «Även om det inte har gått att få några precisa uppgifter om tilllämpningen av dataavläsning i Danmark, är alla som vi har talat med helt överens om att rätt använd i det enskilda fallet skulle metoden innebära ett effektivt medel i brottsbekämpningen. Det överensstämmer helt med vår bedömning. Hur metoden bör genomföras på det mest effektiva sättet, t.ex. i valet mellan hård- och mjukvara, blir givetvis beroende av omständigheterna i det enskilda fallet. Vi har fått uppgifter om effektiviteten i olika avseenden med kan av sekretesskäl inte redogöra för dessa. Användning av dataavläsning innebär, precis som för de befintliga hemliga tvångsmedlen, alltid en risk för att verkställigheten röjs. Vi har fått beskrivet även vilka röjningsrisker som finns och sätten att reducera dessa. Inte heller i den delen går det att avslöja några detaljer. Det går ändå att konstatera att de riskerna inte alls är så framträdande att det påverkar effektiviteten i sådan grad att det finns avgörande skäl mot att metoden införs.»

Ifølge BRU er det selvsagt at de nyeste teknologiske mulighetene benyttes som verktøy for å gjennomføre særskilt grov kriminalitet. BRU mener at det er «helt nödvändigt för samhället att myndigheterna inte hamnar hjälplöst efter utan, inom ramen för att ett godtagbart integritetsintrång, får rätt att använda brottsutredande metoder som är effektiva och anpassade till den tekniska situation som råder vid varje givet tillfälle», jf. SOU 2005:38 side 362.

Det fremgår av BRUs utredning at behovet for dataavlesing som «brottsbekämpande metod» er veid mot hensynet til personvern. BRU uttaler at det er en vanskelig oppgave å avveie «integritetsintresset» mot nødvendigheten av å ha effektive metoder for blant annet etterforskning av kriminalitet, og at det «ligger i sakens natur att varje tvångsmedel innefattar ett integritetsintrång» (SOU 2005:38 side 367). Videre peker BRU på at det må tas i betraktning at inngrepet i personvernet ofte er beskjedent sammenlignet med den krenkelsen som ofrene for den alvorlige kriminaliteten må tåle, og uttaler (SOU 2005:38 side 367):

> «Ju allvarligare och ju mer svårutredd som brottsligheten blir, desto mer tvingas statsmakterna tillåta i form av tvångsåtgärder i brottsbekämpningen. Det kan aldrig accepteras att brottsligheten tar överhanden och att statsmakterna kapitulerar inför utvecklingen av en allt mer avancerad och förslagen brottslighet.»

Dataavlesing vil ifølge BRU alltid innebære en viss inntrenging, enten fysisk for å plassere tekniske hjelpemidler, eller elektronisk – ved at programvare sendes til en datamaskin. Det erkjenner at dette, samt den etterfølgende innhentingen av informasjon fra informasjonssystemet og bruken av det, kan representere et vesentlig inngrep i privatlivet, men at det konkrete omfanget vil avhenge av omstendighetene i det enkelte tilfelle. Videre sammenlignes dataavlesing med de eksisterende tvangsmidlene kommunikasjonsavlytting («hem-

lig teleavlyssning») og kameraovervåking (SOU 2005:38 side 368):

> «I allmänhet bör dock kunna sägas att integritetsintrånget i vart fall inte kommer att bli större än vid hemlig teleavlyssning och hemlig kameraövervakning, där samtal avlyssnas och personen är föremål för övervakning genom fjärrstyrda kameror. De sistnämnda tvångsmedlen bör i de flesta fall anses innefatta en mer total kontroll av och insyn i en persons förehavanden än vad dataavläsning innebär. Dessutom bör det i de fallen typiskt sett finnas en större risk för att personer som är ovidkommande för en brottsutredning drabbas av ett integritetsintrång genom att de t.ex. blir avlyssnade vid en telefonkontakt med en misstänkt person eller blir filmade på en plats där kameraövervakning pågår. Det kan tilläggas dels att ett hemligt intrång i en persons bostad eller på en arbetsplats för att placera den utrustning som krävs för dataavläsning inte kan anses mer integritetskänsligt än en s.k. hemlig husrannsakan (se 28 kap. 7 § andra stycket RB), dels att ett samtidigt verkställande av flera tvångsmedel mot samma person givetvis leder till att integritetsintrånget ökar avsevärt, något som måste beaktas när beslut skall fattas om metoden och under verkställigheten av tvångsmedlen.»

Under henvisning til behovet for dataavlesing og metodens antatte effektivitet, mener BRU at det «skulle innebära en så stor vinst för bekämpningen av den allvarliga brottsligheten att det inte är försvarligt att avstå från att införa en möjlighet för de brottsbekämpande myndigheterna att använda metoden», selv om den vil medføre personverninngrep. Det fremheves likevel at reglene bør utformes slik at det ikke gjøres større inngrep enn nødvendig (SOU 2005:38 side 369):

> «En reglering av användning av hemlig dataavläsning måste omgärdas av sådana rättssäkerhetsgarantier som säkerställer att bestämmelserna inte kan missbrukas och att allmänheten kan ha tilltro till de myndigheter som tillämpar regleringen. Tvångsmedelsregleringen måste omgärdas av tydliga och strikta ramar för att det inte skall kunna misstänkas att regelsystemet kommer att utnyttjas utöver vad det skall tillåta. Bestämmelserna måste även utformas på ett sådant sätt att de kan accepteras av allmänheten som ett nödvändigt redskap för de brottsbekämpande myndigheterna i kampen mot den grövre kriminaliteten. Regleringen måste också innefatta ett starkt skydd för den personliga integriteten. Det är av avgörande betydelse att undvika att personer som är ovidkommande för en brottsutredning får sin integritet kränkt. Det är också viktigt att i möjligaste mån begränsa det integritetsintrång som den misstänkte utsätts för.»

Spørsmålet om dataavlesing burde innføres som eget tvangsmiddel er tatt opp igjen i SOU 2012:44, «Hemliga tvångsmedel mot allvarliga brott» (Betänkande av Utredningen om vissa hemliga tvångsmedel). Utvalget understreker at spørsmålet falt utenfor dets mandat, men finner likevel grunn til å henvise til BRUs utredning og forslag, og til å påpeke at det under dets egne undersøkelser har fått opplysninger om den teknologiske utviklingen og kriminelles strategier for å hemmeligholde sin kommunikasjon, som tilsier at dataavlesing bør tillates i Sverige (SOU 2012:44 side 767–768):

> «Det som kommit fram vid kartläggningen ger stöd för att tvångsmedlet hemlig dataavläsning skulle kunna medföra beaktansvärd nytta för de brottsbekämpande myndigheterna. Med den utformning som BRU föreslagit – där avgränsningen av vilken informationsinhämtning som får ske inte är helt klar – skulle tvångsmedlet kunna medföra avsevärda integritetsintrång. Dessa intrång skulle emellertid, på samma sätt som beträffande hemlig rumsavlyssning i vissa fall kunna vara berättigade.»

Utvalget har på denne bakgrunn pekt på at det er «angeläget att frågan utreds» (SOU 2012:44 side 768).

14.3.3 Finsk rett

I Finland er bruken av skjulte tvangsmidler («hemliga tvångsmedel», som brukes «i hemlighet för dem åtgärden riktas mot») i etterforskningsøyemed regulert i tvångsmedellagen (22.07.2011/806) 10 kap. Gjennom endringer som trådte i kraft 1. januar 2015 har reglene i tvångsmedelslagen om bruk av skjulte tvangsmidler i etterforskningsøyemed og reglene i polislagen (22.07.2011/872) om bruk av tilsvarende tvangsmidler for å forhindre, avsløre eller avverge alvorlige lovbrudd, blitt harmonisert og modifisert. Som skjulte tvangsmidler regnes «teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt

inhämtande av information, teknisk observation (teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning), inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp, användning av informationskällor och kontrollerade leveranser», jf. tvångsmedelslagen 10 kap. 1 § 1 mom.

For å benytte et tvangsmiddel i hemmelighet kreves det at det «kan antas att man på det sättet får information som behövs för att utreda ett brott», jf. 10 kap. 2 § 1 mom., og at det «kan antas at vara av synnerlig vikt för utredning av ett brott», jf. samme bestemmelse 2 mom.

Tvångsmedelslagen 10 kap. gir blant annet adgang til «teleavlyssing», som i 3 § er definert som at et «meddelande» som tas imot av eller sendes fra en viss teleadresse eller teleterminalutrustning, gjennom et allment kommunikasjonsnett eller nett som er koblet til et slikt, avlyttes, tas opp eller på annen måte behandles for å undersøke innholdet i meddelelsen og identifiseringsopplysninger knyttet til den. Teleavlytting kan bare rettes mot meddelelser fra eller tiltenkt en person som er «skäligen misstänkt» for et lovbrudd som nevnt i 10 kap. 3 § 2 mom. følgende. Det er her ikke angitt noe generelt strafferammekrav, men opplistet en rekke typer lovbrudd som kan danne grunnlag for avlytting. Opplistingen nevner blant annet folkemord og folkemordrelaterte lovbrudd, lovbrudd mot rikets sikkerhet, forræderi, seksuell utnyttelse av barn, drap, menneskehandel, samt visse vinningslovbrudd og narkotikalovbrudd.

Beslutning om teleavlytting treffes av domstolen på begjæring fra en «anhållningsberättigad tjänsteman» (det vil si politibefal eller tjenestemann med påtalekompetanse), jf. 10 kap. 5 § 1 mom. Tillatelse kan gis for høyst en måned av gangen, jf. 2 mom.

Avlyttingen kan rettes mot «meddelande», hvilket i følge forarbeidene (RP 222/2010 rd side 327) skal forstås som «samtal, elektronisk post, textmeddelande, talmeddelande och annat motsvarande meddelande som i ett kommunikationsnät förmedlas mellan parterna eller till en mottagarkrets som inte är utvald på förhand». Avlyttingen kan rettes mot meddelelser som tas i mot eller sendes fra en viss teleadresse eller teleterminalutrustning. Det er i utgangspunktet bare tillatt å avlytte meddelelser mens de er i den såkalte transportfasen mellom avsender og mottaker, jf. RP 222/2010 rd side 327. Avgrensningen illustreres samme sted med at avlytting ikke kan brukes for å få rede på innholdet i en tekstmelding som har kommet frem til mottakerens mobiltelefon. I slike tilfeller må i utgangspunktet andre tvangsmidler, som for eksempel beslag, benyttes.

I 10 kap. 4 § er adgangen til teleavlytting imidlertid supplert med bestemmelser om «inhämtande av information i stället för teleavlyssning». Etter 10 kap. 4 § 2 mom. kan det gis tillatelse til å rette avlyttingen mot «en personlig teknisk anordning som lämpar sig för att sända och ta emot meddelanden och finns i direkt anslutning til teleterminalutrustning eller mot förbindelsen mellan en sådan anordning och teleterminalutrustning», på samme vilkår som for avlytting etter bestemmelsen om avlytting i 10 kap. 3 §. Slik anordning kan for eksempel være en blue toothhodetelefon («håndfri-sett») som står i forbindelse med en mobiltelefon.

Dersom det er sannsynlig at meddelelser som nevnt i 10 kap. 3 § ikke lenger er tilgjengelige gjennom avlytting etter sistnevnte bestemmelse, kan det på samme vilkår som for avlytting også gis tillatelse til å beslaglegge eller kopiere meddelelsene hos «teleföretag eller sammanslutningsabonnent», jf. 10 kap. 4 § 1 mom.

Videre gir tvångsmedelslagen 10 kap. 16 § og 17 § gir hjemmel for såkalt «teknisk avlyssning», hvilket innebærer at en mistenkt persons «samtal eller meddelande som inte är avsett för utomstående», og som avlytteren ikke deltar i, blir avlyttet, tatt opp eller på annen måte behandlet «med hjälp av en teknisk anordning, metod eller programvara i syfte att ta reda på innehållet i samtalet eller meddelandet eller utreda deltagarna eller den misstänkta verksamheten», jf. 10 kap. 16 § 1 mom.

Vilkårene for «teknisk avlyssning» varierer med hvor den som skal avlyttes befinner seg. Er det tale om sted som ikke benyttes for «stadigvarande boende», kan teknisk avlytting iverksettes ved skjellig grunn til mistanke om lovbrudd med en øvre strafferamme på minst fire års fengsel, samt narkotikalovbrudd, forberedelse til lovbrudd som begås i terrorhensikt, grovt tollrapporteringslovbrudd, forberedelse til gisseltaking eller forberedelse til grovt ran, jf. tvångsmedelslagen 10 kap. 16 § 2 mom. og 3 mom. Avlyttingen kan bare rettes mot steder som den mistenkte med sannsynlighet kan antas å befinne seg på eller besøke.

Sted som benyttes permanent («stadigvarande») som bolig, og der det er sannsynlig at mistenkte befinner seg, kan avlyttes dersom vedkommende med skjellig grunn mistenkes for et lovbrudd som er angitt i tvångsmedelslagen 10 kap. 17 §. Oppregningen omfatter blant annet folkemord, spionasje, ulike former for forræderi, grov seksuell utnyttelse av barn, drap, grov men-

neskehandel, grovt ran, grov sabotasje, terrorisme og grov narkotikakriminalitet.

Gjelder det avlytting av bolig eller avlytting som rettes mot en frihetsberøvet, treffes beslutning av retten, jf. 10 kap. 18 § 1 mom. Annen avlytting kan ifølge 2 mom. besluttes av «anhållningsberättigad tjänsteman». I alle tilfeller kan det gis tillatelse for høyst én måned om gangen, jf. 3 mom.

Ved teknisk avlytting etter tvångsmedelslagen 10 kap. 17 § eller 18 § gis det adgang til å avlytte mer enn bare mistenktes utsagn eller samtaler med andre som befinner seg i samme rom eller på samme sted. I forarbeidene er det forutsatt at teknisk avlytting også dekker det at man «med en teknisk anordning avlyssnar eller upptar vad den andra parten i ett telefonsamtal säger i telefonen när avlyssningen riktas mot de ljudvågor som talet ger upphov til» (RP 222/2010 rd side 340). Lovens formulering «samtal eller meddelande» innebærer at avlyttingsadgangen heller ikke er begrenset til samtale eller meddelelser som skjer muntlig (det var den derimot tidligere). I forarbeidene legges det til grunn at teknisk avlytting også kan omfatte for eksempel overvåking av tastaturet til en datamaskin i forbindelse med sending av e-post, jf. RP 222/2010 rd side 340 og RP 52/2002 rd side 27.

I så måte kan teknisk avlytting utgjøre et praktisk viktig supplement til adgangen til teleavlytting i tilfeller hvor målet er å avdekke innholdet i mistenktes kommunikasjon med andre. I RP 52/2002 rd tilkjennegis følgende om dette (side 26–27):

> «Det ökade behovet av att kunna rikta teknisk avlyssning mot utrymmen som är avsedda för stadigvarande boende beror på att teleavlyssningens användbarhet vid utredning de facto har minskat. När brottslingarna i allt högre grad blir medvetna om risken för att bli avslöjad i samband med telekommunikation kommer de att försöka undvika telekommunikation. Också den ovan nämnda användningen av mobiltelefoner och anonymt förhåndsbetalde teleanslutningar samt ibruktagandet av kryptoteknik försvårar teleavlyssningen. Det enda sättet att ta sig förbi krypteringsarrangemangen kan i praktiken vara att utföra teleavlyssningen vid en teleterminalutrustning. Eftersom det allmänna telenätet anses upphöra vid den s.k. husfördelningen, är det i de kopplingar som görs vid teleterminalutrustningen inte fråga om teleavlyssning utan om teknisk avlyssning.»

Tvångsmedelslagen 10 kap. 23 § gir hjemmel for «teknisk observation av utrustning». Med teknisk observasjon menes det at «en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara på något annat sätt än enbart genom sinnesförnimmelser observeras, upptas eller behandlas på något annat sätt för att utreda omständigheter som är av betydelse för utredningen av ett brott», jf. 1 mom.

Teknisk observasjon kan rettes mot utrustning eller programvare som det er sannsynlig at en mistenkt benytter, og vedkommende med skjellig grunn mistenkes for et lovbrudd som nevnt i 10 kap. 16 § 3 mom. Kriminalitetskravet er altså sammenfallende med det som gjelder for teknisk avlytting av andre steder enn «stadigvarande boende». Beslutning om teknisk observasjon av utrustning treffes av retten, men «anhållningsberättigad tjänsteman» har hastekompetanse dersom «ärendet inte tol upskov», jf. 10 kap. 24 § 1 mom. Tillatelse kan gis for inntil én måned om gangen.

Bestemmelsen om teknisk observasjon ble introdusert ved en lovendring som trådte i kraft 1. januar 2015. Endringen er i forarbeidene begrunnet med behov for å kunne observere teknisk utrustning uavhengig av hvilket sted utrustningen befinner seg på, og at det var et problem med gjeldende rett at «förundersökningsmyndigheten inte kan vara säker på var en anordning används i och med att olika slags bärbara anordningar och andra anordningar som man kan ha med sig blivit så vanliga», jf. RP 222/2010 rd side 346. Det konstateres derfor samme sted at utrustningens fysiske plassering ikke har betydning for adgangen til teknisk observasjon etter 10 kap. 23 §, siden formålet med tvangsmiddelet ikke er å utrede hva som skjer på det sted utrustningen befinner seg.

Bestemmelsen om teknisk observasjon av utrustning gir anledning til å observere bruken av en teknisk anordning og å gjøre seg kjent med filer som måtte være lagret i den. I forarbeidene (RP 222/2010 rd side 346) heter det at man kan «övervaka växelverkan mellan den brottsmisstänkte och den tekniska anordningen», og blant annet utføre såkalt tastetrykksavlesing for å få rede på passord til en server. Metoden kan bare brukes mot anordninger som kan jevnføres med en datamaskin, som for eksempel bærbare elektroniske lagringsmedier og smarttelefoner. En tillatelse til teknisk observasjon av utrustning gir ikke adgang til å innhente opplysninger om innholdet i en meddelelse eller identifiseringsopplysninger som nevnt i 10 kap. 6 §. Kommunikasjonsavlytting må eventuelt gjennomføres med grunnlag i en tillatelse til teleavlytting eller teknisk avlyt-

ting. Det har vært meningen å angi en klar grense mot de andre tvangsmidlene i tvångsmedelslagen 10. kap, jf. RP 222/2010 rd side 347.

I tvångsmedelslagen 10 kap 26 § er det gitt bestemmelser om gjennomføringen av teknisk observasjon, som dekker både teknisk avlytting (10 kap. 16 § og 17 §) og teknisk observasjon av utrustning (10 kap. 23 §). Politiet har adgang til «att fästa en anordning, metod eller programvara som används för teknisk observation på föremål, ämnen, egendom, i utrymmen och andra platser eller informationssystem som åtgärden riktas mot», dersom det er nødvendig for å gjennomføre observasjonen, jf. 10 kap. 26 § 1 mom. For å installere, ta i bruk eller avinstallere anordningen, metoden eller programvaren har politiet da rett til «att i hemlighet ta sig in» på en slik plass eller slikt informasjonssystem som nevnt ovenfor, samt «kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem». Dersom det er behov for å skaffe seg adgang til et sted som benyttes som «stadigvarande boende» kreves det særskilt tillatelse fra retten, jf. 10 kap. 26 § 2 mom.

14.4 Folkerettslige forpliktelser

Som nevnt ovenfor er ikke datavlesing et entydig juridisk begrep, og det betegner heller ikke noen klart avgrenset teknologisk fremgangsmåte. Slik begrepet brukes i proposisjonen her, vil dataavlesing som metode ha paralleller til – og delvis overlappe med – kommunikasjonsavlytting og skjult ransaking.

Det er åpenbart at dataavlesing vil kunne innebære betydelige inngrep i den enkeltes privatliv, familieliv, hjem og korrespondanse, som er vernet etter EMK artikkel 8 nr. 1. Etter omstendighetene kan dataavlesing berøre retten til privatliv så vel som korrespondanse, og gripe inn i både den enkeltes fysiske og psykiske integritet. Metoden kan også tenkes rettet mot det private hjem, hvor vernet etter artikkel 8 nr. 1 er særlig sterkt.

Retten til respekt for privatlivet er likevel ikke absolutt. Etter artikkel 8 nr. 2 kan det gjøres inngrep i rettigheten såfremt dette skjer med hjemmel i lov og er nødvendig i et demokratisk samfunn av hensyn til visse nærmere angitte formål. Departementet er ikke kjent med at EMD i noe tilfelle har vurdert konkret om vilkårene for å gjøre inngrep ved å benytte dataavlesing (som egen metode i den forstand som her legges til grunn) har vært oppfylt. Det kan imidlertid være naturlig å velge en tilsvarende tilnærming som i saker om kommunikasjonsavlytting og romavlytting, og det vises derfor til redegjørelsen i punkt 7.2 og 8.2 ovenfor, samt den generelle redegjørelsen i punkt 5.2.

14.5 Tidligere norske utredninger hvor spørsmålet om dataavlesing bør tillates er vurdert

I NOU 2004: 6 Mellom effektivitet og personvern foreslo *Politimetodeutvalgets* flertall å innføre regler som skulle tillate dataavlesing som forebyggende metode. Det foreslo også å definere dataavlesing slik (punkt 11.8.2 side 233):

> «Med dataavlesing forstås avlesing av opplysninger i et ikke offentlig tilgjengelig elektronisk informasjonssystem ved hjelp av dataprogrammer eller på annen måte.»

Forslaget til bestemmelse om dataavlesing lød slik (punkt 11.1.2 side 250):

> «(1) Politiet kan iverksette dataavlesning overfor person som det er god grunn til å tro forbereder en særlig alvorlig straffbar handling etter § 8-3 (1), men bare av informasjonssystem som det må antas at anvendes i forbindelse med forberedelsen.
>
> (2) Beslutningen skal treffes av retten. Tillatelse kan bare gis når undersøkelsen vil være av avgjørende betydning for å forebygge den straffbare handling, og bare når mindre inngripende metoder ikke vil være anvendelige.
>
> (3) Kontroll kan ikke gjennomføres med hensyn til en persons kommunikasjon med personer som ifølge straffeprosessloven § 119 er utelukket fra å gi vitneforklaring med mindre vedkommende selv er involvert i forberedelsen.
>
> (4) Tillatelsen skal gis for et bestemt tidsrom, som ikke må være lenger enn strengt nødvendig, og ikke lenger enn 8 uker om gangen. I saker som angår § 2-2, kan tillatelse gis for inntil 6 måneder om gangen.
>
> (5) Tillatelse kan likevel ikke gis dersom det etter inngrepets formål, sakens betydning og forholdene ellers vil være et uforholdsmessig inngrep.»

I begrunnelsen for forslaget viste Politimetodeutvalgets flertall til at kommunikasjonskontroll gir politiet mulighet til å kontrollere opplysninger

som kommuniseres mellom datamaskiner, for eksempel e-postforsendelser. Politimetodeutvalget pekte på at bedre tilgang til krypteringsprogrammer medfører at kommunikasjonskontroll som metode gir mindre informasjon enn tidligere. Det viste også til at moderne krypteringsprogrammer har blitt så kompliserte at krypterte meldinger ikke lar seg dekryptere, og at eneste måte å få tak i innholdet på derfor er å fange det opp før meldingen krypteres. Politimetodeutvalgets flertall fremhevet også at dataavlesing ville være en integritetskrenkende metode, men at det burde åpnes for den – på strenge vilkår (NOU 2004: 6 punkt 10.7.11.1 side 207).

Høringen av Politimetodeutvalgets forslag etterlot etter departementets vurdering et klart inntrykk av at dataavlesing var en etterforskningsmetode som det var behov for å vurdere nærmere, jf. Ot.prp. nr. 60 (2004–2005) punkt 11.3 side 141. Departementet konstaterte at dataavlesing kunne virke svært integritetskrenkende, og at det var behov for å gå nærmere inn i kompliserte tekniske spørsmål for å kunne avveie de ulike hensynene på en tilfredsstillende måte. Departementet gikk derfor inn for at spørsmålet burde utredes av Datakrimutvalget før forslag om lovendringer ble fremmet.

Lund-utvalget tok også opp spørsmålet om bruk av spesielle datatekniske metoder i etterforskningsøyemed i NOU 2003: 18 Rikets sikkerhet, Straffelovkommisjonens delutredning VIII, punkt 8.1.2 side 126–127:

> «Det andre spørsmålet er i hvilken grad det bør kunne benyttes spesielle datatekniske metoder i etterforskingen, herunder ulike dataprogrammer – såkalte trojanske hester, ormer, sniffere mv. Dette er dataprogrammer som kan installeres hemmelig i dataanlegg og som kan ha forskjellige funksjoner. For eksempel kan programmene legge «vertsmaskinen» åpen for «innbrudd» utenfra, eller de kan lagre og/eller sende informasjon som ligger på maskinen. Programmene kan også overvåke de enkelte inntastingene underveis, og sende denne informasjonen til politiet før den krypteres. Bruk av slike programmer reiser en rekke tekniske og rettslige spørsmål. Det må legges til grunn at i mange tilfeller vil det være nødvendig med hjemmel utover de som er gitt i gjeldende lovgivning. For å besvare hjemmelsspørsmålet sikkert kreves imidlertid en avklaring av hvilke programfunksjoner som kan være aktuelle, i hvilken grad programmene kan skade vertsmaskinen, om programmene kan forstyrre eller forsinke vertsmaskinens funksjoner, hvor stor plass slike programmer kan oppta på vertsmaskinens harddisk, om programmene kan installeres uten at det medfører datainnbrudd osv. Også andre IKT-relaterte metoder kan visstnok tenkes anvendelige i etterforskingsøyemed, for eksempel avlytting av elektromagnetiske felt.»

Lund-utvalget konkluderte med at det var naturlig å overlate vurderingen av ulike IKT-relaterte metoder til Datakrimutvalget.

Datakrimutvalget konstaterte at dataavlesing var et begrep uten entydig fastlagt innhold, og at det måtte utredes nærmere hva metoden består i. I samråd med departementet valgte Datakrimutvalget å la spørsmålet om innføring av dataavlesing «utstå til det senere utredningsarbeid», jf. NOU 2007: 2 Lovtiltak mot kriminalitet, punkt 4.3.4 side 47. Metodekontrollutvalget ble bedt om å følge opp dette utredningsarbeidet.

14.6 Metodekontrollutvalgets vurderinger og forslag

14.6.1 Innledning

Metodekontrollutvalget presiserer at «dataavlesing» ikke er et entydig juridisk eller teknologisk begrep, men legger til grunn at dataavlesing innebærer «å skaffe seg tilgang til opplysninger i et elektronisk datasystem ved hjelp av dataprogrammer eller på annen måte», jf. NOU 2009: 15 punkt 23.1.4 side 237. I utredningen er det presisert at utvalget har vært særlig opptatt av «å kartlegge behovet for metoden og dens antatte effektivitet», jf. punkt 23.1.3 side 236. Utvalget har utredet og vurdert om det er grunnlag for å foreslå regler som tillater at politiet tar i bruk dataavlesing som metode under etterforskning, og som forebyggende metode. Videre har det tatt stilling til hvordan slike regler eventuelt bør utformes – herunder om dataavlesing bør tillates som en ny selvstendig etterforskningsmetode på lik linje med andre tvangsmidler, eller mer målrettet som en mulig gjennomføringsmåte for informasjonsinnhenting ved bruk av etablerte tvangsmidler, som for eksempel kommunikasjonsavlytting og romavlytting. Om dette heter det i punkt 23.1.4 side 237 i utredningen at:

> «Dataavlesing slik Politimetodeutvalget foreslo, og den løsning som er valgt i Danmark og foreslått i Sverige, jf. nedenfor, innebærer at dataavlesing innføres som en ny selvstendig etterfor-

skingsmetode på linje med andre tvangsmidler som for eksempel kommunikasjonskontroll og romavlytting. En slik form for dataavlesing vil kunne gi tilgang både til informasjon som politiet ved bruk av eksisterende metoder kan få tilgang til, for eksempel gjennom kommunikasjonskontroll eller hemmelig ransaking, og til informasjon som politiet etter gjeldende rett ikke har mulighet til å innhente, nemlig informasjon om den kontinuerlige bruken av informasjonssystemet som for eksempel ikke kommuniseres eller lagres i datasystemet.

Dataavlesing kan alternativt målrettes slik at politiet for eksempel *kun* gis adgang til å bruke fremgangsmåten for å innhente informasjon som politiet allerede i dag kan få tilgang til, men på en måte som ikke hindres av tekniske beskyttelsesinnretninger i det aktuelle datasystemet som bruk av kryptering. En slik regel vil innebære en videreføring av den mulighet allerede eksisterende metoder gir til å fremskaffe informasjon, som for eksempel kommunikasjonsavlytting.

Under enhver omstendighet vil dataavlesing slik utvalget ser det, innebære et ellers straffbart innbrudd i et datasystem etter straffeloven (1902) § 145 annet ledd og straffeloven (2005) § 204, se også § 205.»

Metodekontrollutvalget uttaler samme sted at man «har valgt en mer målrettet og mindre inngripende tilnærming og forslag til løsning av spørsmålet om innføring av dataavlesing som metode enn Politimetodeutvalget hadde, og også den løsning man har valgt i Danmark og foreslått i Sverige.» Utvalget har ikke funnet grunn til å foreslå dataavlesing innført som metode «med det formål å gi politiet mulighet til fortløpende å overvåke all aktivitet i et datasystem». Derimot har utvalget foreslått at dataavlesing innføres «som en mulig gjennomføringsmåte for kommunikasjonskontroll og hemmelig ransaking, slik at politiet settes i stand til å sikre informasjon som er kryptert eller på annen måte er gjort utilgjengelig», jf. punkt 23.1.4 side 237, i utredningen. Utvalgets vurderinger og forslag omtales nærmere nedenfor.

14.6.2 Metodekontrollutvalgets observasjoner om behovet for dataavlesing

Metodekontrollutvalget tar utgangspunkt i at «innføringen av nye tvangsmidler, eller utvidelsen av eksisterende hjemler, må bygge på solid dokumentasjon av behovet», og understreker at det kreves «tungtveiende grunner» for å innføre nye metoder eller gjennomføringsmåter, jf. NOU 2009: 15 punkt 23.2.2 side 240.

Utvalget legger samme sted til grunn at politiets mulighet til å *kontrollere mistenktes kommunikasjon* er «et effektivt og viktig verktøy for politiet i dets arbeid med å avdekke alvorlig kriminalitet». Videre pekes det på at den teknologiske utviklingen fra innføringen av adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen – ved midlertidig lov av 17. desember 1976 – og frem til i dag har «vært enorm» på dette området, både på tilbydersiden og brukersiden (utredningen punkt 23.2.2 side 240 og 241):

«Den teknologiske utviklingen har gjort det mulig å sørge for at innholdet i kommunikasjonen ikke lenger vil være forståelig eller leselig når den kommer til teletilbyderen. Ved bruk av krypteringsprogrammer vil mistenkte for eksempel kunne sørge for at en e-post som hos avsenderen og mottakeren kan leses som ren tekst, vil være kryptert og dermed i utgangspunktet uleselig for politiet dersom den for eksempel hentes ut hos internettilbyderen. Dette betyr ikke nødvendigvis at politiet er helt avskåret fra å lese informasjonen. Dersom politiet klarer å knekke krypteringen eller innehar krypteringsnøkkelen, vil informasjonen kunne dekrypteres, og dermed leses. I dag er imidlertid de fleste krypteringsprogrammer i forbindelse med kommunikasjon så vidt avanserte at krypteringen ikke kan omgås i det hele tatt, og i alle fall ikke innenfor et så kort tidsrom at informasjonen blir etterforskingsmessig relevant.

Alt tyder på at bruken av kryptering av kommunikasjon øker, og vil fortsette å øke i fremtiden. Også opplysninger utvalget har fått fra Nasjonal sikkerhetsmyndighet (NSM), avdeling NorCERT, bekrefter dette. Utviklingen skyldes i hovedsak økt bevissthet om behovet for å beskytte seg både hos tilbydere av teletjenester og hos brukerne, som kan være både enkeltpersoner og bedrifter. I dag kan alle enkelt og billig skaffe seg relativt avanserte krypteringsprogrammer for kommunikasjon. En rekke av de programmer som er tilgjengelige for brukere av teletjenester krypterer i tillegg kommunikasjonen uten at brukeren i og for seg er klar over det, eller i hvert fall ikke trenger å gjøre noe aktivt for det. I tillegg har en rekke offentlige aktører pekt på at også den enkelte bør ta grep for å beskytte seg på Internettet både mot kriminalitet og av personvernhensyn, blant annet ved bruk av

krypteringsprogrammer. For eksempel har Personvernkommisjonen i NOU 2009: 1 på side 87–88 pekt på at alle, av personvernhensyn, i større grad bør kryptere informasjon som går over Internettet.»

Videre bemerker utvalget samme sted at den teknologiske utviklingen har ført til utfordringer for politiet med hensyn til å kunne utnytte kontrolladgangen effektivt:

«Disse samfunnsmessige og markedsmessige tendensene må antas å påvirke også de kriminelle, som vil ha en særlig interesse av å være oppmerksom på forholdet mellom kryptering og politiets arbeidsmetoder. Ved å utnytte kunnskap om politimetodenes svakheter, vil de kriminelle gjennom økt bruk av sterk kryptering kunne sørge for at den kommunikasjonen som tidligere ble fanget opp gjennom kommunikasjonskontroll, ikke lenger tilflyter politiet. På denne bakgrunn legger utvalget til grunn at den økte bevisstheten rundt bruken av kryptering og den økte tilgjengeligheten av slike programmer vil gjøre kommunikasjonskontroll som etterforskingsmetode langt mindre effektiv.»

Metodekontrollutvalget viser også til politiets behov for å kunne foreta *hemmelig ransaking og beslag* i bekjempelsen av alvorlig kriminalitet. Det peker på at den teknologiske utviklingen også i denne sammenheng har gjort at informasjon som politiet tidligere fikk tilgang til ved slik metodebruk, ikke lenger tilgjengelig, og at dette «særlig skyldes […] økt bevissthet knyttet til kryptering av data i forbindelse med lagring», jf. utredningen punkt 23.2.2 side 241. Med hensyn til disse utfordringene har utvalget gjort følgende observasjoner (samme sted side 241–242):

«Politiet kan i dag i prinsippet skaffe seg tilgang til all informasjon for eksempel i en datamaskin, gjennom reglene om hemmelig ransaking og beslag. Dersom vilkårene for det er oppfylt, kan politiet ransake og beslaglegge informasjon på datamaskinen ved å «speile» – det vil si kopiere – aktuell informasjon på harddisken. På den måten vil politiet kunne skaffe seg tilgang til informasjon som både relaterer seg til kommunikasjon og annen usendt, sensitiv eller privat informasjon mv., og til en viss grad også informasjon som mistenkte har ment å slette.

I denne forbindelse er det rapportert at politiet møter utfordringer der informasjonen er kryptert. Informasjonen i et datasystem kan passordbeskyttes på mange måter og på mange nivåer, alt fra oppstarten av enheten til åpning av de enkelte programmer og dokumenter.

Den økte bevisstheten om behovet for å sikre seg mot at andre får tilgang til informasjon som er tilgjengelig på et datasystem har også ført til økt fokus på å beskytte informasjonen. Et typisk eksempel vil være passordbeskyttet oppstart (i BIOS) av en bærbar datamaskin som brukeren har med seg utenfor hjemmet, med den økte risikoen dette har for at den kan bli stjålet eller tapt på annen måte. Det må antas at dette også gjelder de kriminelle. Denne gruppen vil i tillegg ha større grunn til å beskytte alle de datasystemer som brukes i den kriminelle virksomheten, for eksempel også en stasjonær datamaskin.

Det er anført at begge disse hovedutfordringene – kryptering og annen beskyttelse – ved gjennomføringen av dagens metoder, vil kunne møtes mer effektivt dersom politiet gis adgang til dataavlesing. Dataavlesing kan tenkes å gi politiet adgang til for eksempel å avlytte kommunikasjonen før den blir kryptert, alternativt skaffe seg krypteringsnøkkelen på mistenktes datamaskin for så å dekryptere meldingen i transportfasen. Dataavlesing vil også kunne tenkes å åpne for avlesing av mistenktes inntasting av passord, og dermed lettere gi tilgang til den aktuelle informasjonen på maskinen, i programmer eller i dokumenter ved ransaking og beslag. Ransakingen kan videre tenkes å skje uten fysisk tilstedeværelse hos mistenkte, samt muliggjøre fortsatt eller gjentatt ransaking og beslag på en enklere måte.»

Videre har Metodekontrollutvalget konsultert Riksadvokaten, som fremhevet at endrede teknologiske forutsetninger gradvis svekker effektiviteten av tradisjonell kommunikasjonskontroll, blant annet fordi kommunikasjon i stadig større grad skjer med andre midler enn ordinær telefoni (fastlinje eller mobil), og at det stadig oftere brukes løsninger som gjør det umulig å avlytte kommunikasjonen. Riksadvokaten har overfor utvalget presisert at dette er et generelt trekk ved utviklingen av moderne kommunikasjon, og ikke bare ved utveksling av informasjon i kriminell virksomhet. Etter Riksadvokatens oppfatning bør det sørges for at det er praktisk mulig å drive kommunikasjonsavlytting på de vilkår som fremgår av straffeprosessloven § 216 a, og at det derfor er nødven-

dig å slå fast at politiet om nødvendig kan skaffe seg tilgang til kommunikasjonsanlegg for å avlytte kommunikasjon uten hinder av kryptering eller lignende. Riksadvokaten har overfor utvalget anbefalt at dataavlesing tillates for å oppnå dette. Videre viser utvalget til at Riksadvokaten har anbefalt at utvalget vurderer å foreslå at retten kan gi tillatelse til gjentatt ransaking på samme måte som etter dansk rett, og å klargjøre at ransaking av kommunikasjonsanlegg ikke krever fysisk tilgang til anlegget.

Metodekontrollutvalget konstaterer videre at det ikke har vært mulig «på noen måte å få tallfestet eller på annen måte dokumentert behovet for dataavlesing nærmere». Etter utvalgets vurdering skyldes dette i hovedsak følgende (utredningen punkt 23.2.2 side 242):

> «Det finnes ikke rutiner for å rapportere når eksisterende tvangsmidler kommer til kort. Videre vil en pågående etterforsking sjelden eller aldri stoppe helt opp for eksempel fordi politiet per i dag ikke har anledning til å bruke dataavlesing som metode. Politiet innhenter informasjon innenfor de gjeldende rettslige rammer, noe som i de fleste tilfeller er tilstrekkelig. På den annen side er det opplyst for utvalget at politiet i mange saker mener at bevismaterialet er større enn det politiet har klart å bringe på det rene med dagens metoder, noe som igjen vil kunne få betydning for omfanget av tiltalen.»

Metodekontrollutvalget har henvendt seg til den danske riksadvokaten vedrørende vurderingene i Danmark av behovet for dataavlesing og dens effektivitet, på bakgrunn av erfaringene med «dataaflæsning» etter retsplejeloven § 791 b. Om dette heter det følgende i utredningen (punkt 23.2.2 side 243):

> «Riksadvokaten rettet på denne bakgrunn en henvendelse til politiet, herunder det nasjonale IT-Efterforskningscenteret (NITEC) som bistår landets politidistrikter i forbindelse med sikring av elektroniske bevis. Politiet opplyste at det ikke finnes oversikt over antallet dataavlesinger i Danmark, og at det heller ikke kan fremskaffes slike opplysninger fra politiets saksbehandlingssystem. Riksadvokaten har likevel opplyst å være kjent med at dataavlesing har vært anvendt i en rekke konkrete saker, herunder to saker om forsøk på terror. I begge disse sakene ble det gjennomført dataavlesing av de siktedes datamaskiner. Dette frembrakte bevis for at de senere domfelte hadde nedlastet bombemanualer, hadde søkt etter kjemikalier mv. som kunne brukes til bombefremstilling, og hadde kommunisert via datamaskiner i tilknytning til planleggingen av forbrytelsene. I forbindelse med utvalgets besøk ved det nasjonale IT-Efterforskningscenteret (NITEC) fikk utvalget opplyst at dataavlesing også hadde vist seg effektivt ved etterforsking av narkotikasaker og saker om barnepornografi.»

Ifølge Metodekontrollutvalget har det heller ikke i den svenske utredningen SOU 2005:38 vært mulig å tallfeste behovet for dataavlesing eller metodens antatte effektivitet (punkt 23.2.2 side 243).

14.6.3 Grunnleggende prinsipper – personvern og rettssikkerhet

Under punkt 23.2.3 i utredningen peker Metodekontrollutvalget på at eventuelle utvidelser av metodebruken bare kan gjennomføres dersom det er forsvarlig ut fra hensynet til personvern og rettsikkerhet, og at visse grunnleggende prinsipper må ivaretas i denne sammenheng.

For det første peker utvalget på at *legalitetsprinsippet* gjør det nødvendig å etablere klar lovhjemmel for en eventuell adgang til dataavlesing, under henvisning til at dataavlesing vil innebære et ellers straffbart innbrudd i et datasystem etter straffeloven 1902 § 145 annet ledd (straffeloven § 204). I tillegg er det fremhevet (side 243) at «[a]lene det at dataavlesing vil innebære et inngrep i den personlige sfære tilsier at metoden eller gjennomføringsmåten bør reguleres av en klar lovhjemmel», og at dette kan oppnås enten ved å innføre en egen hjemmel til dataavlesing, eller ved å endre eksisterende tvangsmiddelhjemler, slik at det fremgår klart at dataavlesing kan brukes ved gjennomføringen av disse.

For det andre viser utvalget til det personvernrettslige kravet om *formålsbestemthet*, som det er gjort nærmere rede for i utredningen under punkt 6.6. Det innebærer ifølge utvalget at de tillatte formålene med etterforskning som er angitt i straffeprosessloven § 226 må betraktes som en begrensning, og at det i tillegg kan stilles særlige vilkår for å begrense adgangen til dataavlesing, som for eksempel at dataavlesing bare skal kunne utføres som ledd i kommunikasjonsavlytting.

For det tredje peker utvalget på *nødvendighetsprinsippet*, som etter utvalgets vurdering tilsier at dataavlesing bare bør tillates i saker der det av kriminalitetsbekjempelseshensyn anses nødvendig i

den enkelte sak. Utvalget konstaterer i denne forbindelse at dataavlesing vil kunne medføre inngrep i andre enn mistenktes personvern der et datasystem brukes av flere personer, og at metoden «potensielt kan medføre innsamling av store mengder informasjon som ikke er nødvendig i etterforskingssammenheng» (side 243). Dette kan være vektige argumenter mot å tillate metoden, og nødvendighetsprinsippet tilsier etter utvalgets oppfatning at dataavlesingen eventuelt bør innrettes slik at den i minst mulig grad rammer tredjepersoner eller leder til innhenting av irrelevant informasjon. Utvalget viser imidlertid til at dataavlesing også (samme sted) «vil kunne innebære nettopp en mer målrettet informasjonsinnhenting, for eksempel dersom flere brukere (datasystem) deler samme nettverkstilkobling». Metodekontrollutvalget viser også til at *kravet om forholdsmessighet* «utgjør en rettesnor for utvalgets overordnede vurdering av hvilke etterforskingsmetoder politiet bør ha tilgang til» (side 244).

Det fjerde utvalget peker på, er at dataavlesing i lys av *sensitivitetsprinsippet* kan utgjøre et svært kraftig inngrep i enkeltmenneskers personvern. Det viser til at fremgangsmåten vil kunne gi politiet tilgang til innholdet i et datasystem, og ikke bare opplysninger om bruken av det. Ifølge utvalget kan det «i denne sammenheng anføres at politiets kontroll av innholdet i informasjonen som lagres på maskinen uten å være kommunisert til andre, utgjør et større inngrep enn kontroll av innholdet i brukerens kommunikasjon» (side 243). Videre heter det (side 243–244):

> «Dette fordi det som kommuniseres til andre til en viss grad har funnet vegen ut av den personlige sfære og er noe mottakeren av kommunikasjonen selv kunne videreformidlet til politiet. Det samme må gjelde informasjon om handlinger som foretas på Internettet, ettersom man har større grunn til å forvente at slike handlinger registreres og overvåkes. Informasjon som ikke har vært kommunisert til andre eller på Internettet må derimot anses å tilhøre brukerens innerste personlige sfære, og innhenting av slik informasjon vil potensielt kunne være svært integritetskrenkende. Sensitivitetshensyn trenger ikke gjøre seg like sterkt gjeldende når det gjelder bedrifters datamaskiner, men også her kan andres tilgang til informasjonen være svært integritetskrenkende. Typisk vil dette gjelde tilgangen til datasystemer hos legekontor eller andre bedrifter som behandler sensitiv personinformasjon. Det vil også kunne gjelde tilgang til bedriftshemmeligheter og lignende.»

Videre bemerker Metodekontrollutvalget (side 244) at kravet til *informasjonssikkerhet* vil kunne få stor betydning for vurderingen av om politiet bør kunne foreta dataavlesing. Etter utvalgets oppfatning vil eventuelle sikkerhetsrisikoer forbundet med fremgangsmåten tale mot at den bør tillates, og det er fremhevet at det uansett bør stilles krav om at politiet gjennomfører dataavlesing på sikrest mulig måte, og at eventuelle skader som forårsakes blir reparert. I tillegg tilsier *prinsippet om opplysningskvalitet* at opplysningene som innhentes blir oppbevart på en sikker måte, og ikke brukes på en måte som innebærer at de blir tatt ut av sin sammenheng.

Endelig peker utvalget på at også hensynet til rettssikkerhet tilsier at det bør etableres kontrollsystemer for bruken av dataavlesing, som sikrer at det ikke gis tillatelse til innhenting av informasjon som faller utenom hjemmelsgrunnlaget, og at informasjonen blir behandlet «ut fra de formål den er innhentet, samt at uvedkommende ikke får tilgang til den» (side 244). Særlig er det fremhevet at dataavlesing vil skje uten at den mistenkte underrettes, og at det derfor er nødvendig «på annen måte å sikre den kontradiktoriske prosess».

14.6.4 Metodekontrollutvalgets hovedkonklusjoner

Under punkt 23.3.1 i utredningen slår utvalget fast at det på bakgrunn av sin «klare oppfatning om at innføring av nye tvangsmidler, eller utvidelse av eksisterende hjemler, må bygge på solid dokumentasjon av behovet», ikke har funnet «dokumentert et tilstrekkelig behov for å innføre dataavlesing som nytt selvstendig tvangsmiddel» (side 244), i motsetning til det som ble foreslått av Politimetodeutvalget, og den løsning som er innført i Danmark og foreslått innført i Sverige.

Metodekontrollutvalget finner likevel «gode grunner for at dataavlesing bør innføres som en nødvendig teknologisk tilpassing for å kunne opprettholde effektiviteten av enkelte allerede eksisterende metoder» (side 244). Utvalget foreslår derfor en slik tilpassing, og bemerker samtidig at «dette også i noen grad vil kunne innebære en utvidelse av virkeområdet for de eksisterende hjemler» (side 244). Utvalget foreslår innføring av dataavlesing i forbindelse med *kommunikasjonsavlytting* og *hemmelig ransaking og beslag*. Det peker på at forslaget innebærer dataavlesing som

en *gjennomføringsmåte*, som det ikke er tradisjon for å beskrive i detalj under de enkelte tvangsmiddelhjemlene i straffeprosessloven. Likevel er det etter utvalgets vurdering behov for å sikre at hjemmelsgrunnlaget tilstrekkelig klart åpner for de ønskede gjennomføringsmåtene. I denne forbindelse er det også vist til at dataavlesing vil innebære et ellers straffbart datainnbrudd, og at det derfor må gis nødvendig hjemmel for at politiet kan gjennomføre slikt innbrudd i forbindelse med dataavlesing.

14.6.5 Dataavlesing for å muliggjøre kommunikasjonsavlytting

Utvalget finner det «tilstrekkelig dokumentert at kommunikasjonsavlyttingen er, og formodentlig i enda større grad vil bli, vanskeliggjort på grunn av den tekniske utviklingen», og fremhever følgende (punkt 23.3.2 side 245):

> «I den grad kommunikasjonsavlyttingen blir vanskeliggjort på grunn av teknologiske eller andre innretninger, mener også utvalget at det bør gis adgang til bruk av dataavlesing for å kunne gjennomføre kommunikasjonsavlyttingen. Personverninteressene som her må vike er langt på vei de samme som ved tradisjonell kommunikasjonsavlytting. Det nye er at den teknologiske utvikling gjør det nødvendig med en annen fremgangsmåte for at politiet skal kunne skaffe seg den samme informasjonen. Utvalget er oppmerksom på at dataavlesing vil kunne innebære noe større grad av inngrep i tredjepersoners interesser, typisk fordi et datasystem i en husstand gjerne brukes av flere personer, noe som i seg selv er et argument mot en utvidelse. Utvalget finner likevel at dette ikke skiller seg avgjørende fra situasjonen med tradisjonell kommunikasjonsavlytting, for eksempel avlytting av en husstands fasttelefon.»

Utvalget foreslår på denne bakgrunn at det innføres et nytt fjerde ledd i straffeprosessloven § 216 a, hvoretter retten ved kjennelse kan gi politiet «tillatelse til å foreta innbrudd i et datasystem for å kunne gjennomføre kommunikasjonsavlyttingen» (side 245). Utvalgets forslag til ny bestemmelse forutsetter at «kommunikasjonsavlyttingen er vanskeliggjort på grunn av teknologiske eller andre innretninger» (samme sted). I særmerknadene til forslaget har utvalget begrunnet dette med at «[d]et bør kreves at politiet først faktisk har forsøkt å gjennomføre tradisjonell kommunikasjonsavlytting» (punkt 31.1 side 356) og har konstatert at dette har blitt vanskeliggjort på grunn av innretninger, for eksempel kryptering eller andre avlyttingsbarrierer. Utvalget mener imidlertid samme sted at kriteriet vil måtte anses oppfylt også dersom det er godtgjort at forsøk på tradisjonell kommunikasjonsavlytting «klart ikke vil kunne føre til resultater».

Videre understreker utvalget at rammen for dataavlesing i denne sammenheng vil være «kommunikasjonsavlytting», og at også adgangen til kommunikasjonsavlytting ved bruk av eller ved hjelp av dataavlesing vil være begrenset til kommunikasjon mellom «kommunikasjonsanlegg». Utvalget legger til grunn at de «kommunikasjonsanlegg» som kan avlyttes etter straffeprosessloven § 216 a i alminnelighet også vil være «datasystem» (punkt 31.1 side 355). Begrepet er ifølge særmerknadene til forslaget til endringer i straffeprosessloven § 200 a (punkt 31.1 side 352) hentet fra straffeloven § 204, og skal være «teknologinøytralt i den forstand at det ikke spiller noen rolle hvorledes systemet mottar, behandler eller videreformidler informasjon», og at det «således omfatter kommunikasjonsanlegg av ulike slag». Videre forutsetter utvalget samme sted – i relasjon til reglene om ransaking og beslag – at begrepet også omfatter «for eksempel GPS-er, skannere og kopimaskiner mv.»

Utvalget påpeker at plasseringen og formuleringen av forslaget skal understreke at det kun dreier seg om å regulere *gjennomføringsmåten* av en kommunikasjonsavlytting. De alminnelige inngangsvilkårene og begrensningene for kommunikasjonsavlytting vil derfor gjelde, som ved annen kommunikasjonsavlytting (utredningen punkt 23.3.2 side 245):

> «Mistankekravet og kravet til den straffbare handling mv. vil følge av vilkårene for kommunikasjonsavlytting. Bestemmelsene i straffeprosessloven §§ 216c-216k kommer også til anvendelse. Dette innebærer for eksempel at varigheten av inngrepet, begrensningene i forhold til personer uten vitneplikt (bevisforbudsreglene), bestemmelsene om utsatt underretning, kontrollsystemet mv. er de samme som for kommunikasjonsavlytting.»

I utredningen vises det også til at politiet gjennom forslaget vil få rettslig adgang til den informasjonen som kommuniseres til og fra for eksempel mistenktes datasystem i den perioden rettens tillatelse gjelder, men også kan få faktisk adgang til annen informasjon, som for eksempel er lagret i

datasystemet, herunder opplysninger fra eldre kommunikasjon på en e-postkonto eller lignende. Det understrekes (punkt 23.3.2 side 245) at politiet etter forslaget ikke har adgang til å tilegne seg slik informasjon med hjemmel i straffeprosessloven § 216 a. Det samme gjelder manipulasjon av datasystemet for å få fange opp annen informasjon enn den mistenkte sender eller mottar i kommunikasjonen – politiet vil for eksempel ikke ha adgang til å slå på et webkamera, mobiltelefonkamera eller lignende, eller slå på en mikrofon i tilknytning til datasystemet. Det konstateres også samme sted at det etter forslaget heller ikke vil være adgang til å bruke dataavlesing «for å fremskaffe andre opplysninger enn dem som relaterer seg til vanskeliggjøringen av kommunikasjonsavlyttingen». Slik annen informasjon må ifølge utvalgets forslag eventuelt forsøkes innhentet gjennom hemmelig ransaking og beslag. I særmerknadene til utvalgets forslag er det presisert at de opplysningene som foreslås tillatt fremskaffet gjennom dataavlesing er «de som er nødvendig for å gjøre resultatet av kommunikasjonsavlyttingen lesbart for politiet», se utredningen punkt 31.1 side 356–355.

14.6.6 Dataavlesing som gjennomføringsmåte for hemmelig ransaking og beslag

Metodekontrollutvalget legger under punkt 23.3.3 side 245–246 i utredningen til grunn at også adgangen til å foreta hemmelig ransaking og beslag «er et effektivt og viktig verktøy for å bekjempe alvorlig kriminalitet». Utvalget finner det tilstrekkelig dokumentert at det i enkelte saker «vil kunne være et stort behov for dataavlesing for å kunne gjennomføre ransakingen» (samme sted). På denne bakgrunn har utvalget foreslått at dataavlesing ved hemmelig ransaking og beslag tillates i begrenset form, ved at det i straffeprosessloven § 200 a gjøres en tilføyelse om at retten kan gi politiet tillatelse til «samtidig eller senere å foreta innbrudd i et datasystem for å kunne gjennomføre ransaking» etter denne bestemmelsen, jf. forslaget til endringer i straffeprosessloven § 200 a i utredningen punkt 32.1 side 368.

Utvalget har tatt stilling til om det bør være anledning til ransaking og beslag uten politiets fysiske tilstedeværelse, og om det bør være adgang til gjentatt eller fortløpende ransaking.

Utvalget mener at ransaking uten fysisk tilstedeværelse «savner en klar rettskildemessig forankring», men viser til Riksadvokatens opplysninger om at det i underrettspraksis er lagt til grunn at politiet kan ransake og beslaglegge informasjon om mistenktes e-postkonto uten fysisk tilstedeværelse. Ifølge utvalget henger dette formodentlig sammen med at innholdet på en e-postkonto som regel «befinner seg hos en internettilbyder, noe som gjør fysisk tilstedeværelse hos mistenkte upraktisk» (punkt 23.3.3 side 246). Videre er det bemerket samme sted at den teknologiske utviklingen har medført at hemmelig ransaking og beslag nettopp kan gjennomføres uten fysisk tilstedeværelse, og at dette «endatil [vil] kunne være mindre integritetskrenkende enn tradisjonell hemmelig ransaking som krever at politiet skaffer seg fysisk tilgang til anlegget typisk ved å trenge seg inn i en privat bolig eller forretningslokaler». Utvalget peker også samme sted på at oppdagelsesrisikoen og ressursbehovet kan minskes ved ransaking uten fysisk tilstedeværelse, selv om også ransaking ved hjelp av dataavlesing medfører fare for å bli oppdaget, og krever en del ressurser. Utvalgets forslag innebærer at adgang til hemmelig ransaking og beslag uten fysisk tilstedeværelse hjemles uttrykkelig. Etter utvalgets oppfatning må det være opp til politiet å vurdere hvilken gjennomføringsmåte som er mest hensiktsmessig i hvert enkelt tilfelle (23.3.3 side 246).

Med hensyn til *fortsatt eller gjentatt ransaking* legger utvalget det til grunn som «alminnelig antatt» at det ikke foreligger adgang til dette etter gjeldende rett, og at enhver ny ransaking derfor krever ny tillatelse fra retten (punkt 23.3.3 side 246). Det er i denne sammenheng også vist til Politimetodeutvalgets utredning i NOU 2004: 6, hvor det samme er lagt til grunn på side 95 og 98.

Utvalget finner ikke grunnlag for å foreslå adgang til fortsatt eller gjentatt ransaking, og begrunner dette på følgende måte (utredningen punkt 23.3.3 side 246):

> «Slik ransaking vil innebære en klar utvidelse av dagens adgang til bruk av hemmelig ransaking, fordi det vil gi politiet anledning til systematisk å kartlegge mistenktes bruk av et datasystem over tid, herunder opplysninger som ikke blir lagret i datasystemet og dermed ikke vil kunne hentes ut ved tradisjonell hemmelig ransaking. Etter utvalgets syn innebærer dette en for stor integritetskrenkelse i forhold til det anførte behovet. Det kan argumenteres blant annet på bakgrunn av saksforholdet i sakene fra Oslo og Kristiansand tingrett som nevnt ovenfor i punkt 23.2.2, for at det kan være gode grunner til at mistenkte «observeres» over noe tid gjennom en gjentatt eller fortløpende hemmelig ransaking. Rettens kjennelse

vil i et slikt tilfelle kunne angi en tidsperiode ransakingen kan foregå innenfor, slik at det uansett ikke er tale om noen kompetanseoverføring til politi- og påtalemyndigheten. Det kan diskuteres om tillatelsen til slik gjentatt eller fortløpende ransaking bør være et spørsmål under forholdsmessighetsvurderingen som det bør være opp til retten å foreta i den konkrete saken. Det er i utgangspunktet ikke noe i veien for at politiet i dag begjærer hemmelig ransaking flere ganger i løpet av en periode. I så fall vil det være opp til retten å vurdere når en ytterligere ny ransaking vil innebære et uforholdsmessig inngrep. Utvalget er likevel skeptisk til å stille opp en generell adgang til dette, og særlig gjelder dette for en eventuell adgang til fortløpende hemmelig ransaking. En slik adgang vil i praksis innebære at dataavlesing innføres som en selvstendig metode hvor politiet gis adgang til kontinuerlig å overvåke et datasystem og på den måten registrere enhver endring brukeren gjør. Utvalget har som nevnt funnet at det ikke kan anbefale en så stor utvidelse, jf. ovenfor. Dersom politiet mener det er nødvendig med flere ransakinger, bør rettens tillatelse derfor innhentes på nytt for hver gang.»

Videre peker utvalget på at forslaget innebærer at retten kan gi tillatelse til at politiet benytter seg av dataavlesing som alternativ til tradisjonell hemmelig ransaking (uten bruk av dataavlesing), dersom det viser seg at det sistnevnte er praktisk vanskeligere enn først antatt. Ifølge utvalget må det da (samme sted) «være greit at retten har gitt tillatelse til at politiet alternativt kan gjennomføre ransakingen ved innbrudd i datasystemet. Det er i så fall tale om samme ransaking.»

Utvalget bemerker ellers samme sted at det ikke har ansett det nødvendig med endringer i straffeprosessloven § 208 a (utsatt eller unnlatt underretning om beslag) for at politiet skal ha adgang til å ta beslag i materialet som innhentes ved ransaking ved hjelp av dataavlesing.

14.6.7 Dataavlesing i forebyggende øyemed

Etter Metodekontrollutvalgets vurdering gjør utfordringene på etterforskningsstadiet seg også gjeldende på forebyggingsstadiet, og utvalget foreslår derfor også å tillate at dataavlesing kan benyttes tilsvarende av Politiets sikkerhetstjeneste i dens forebyggende virksomhet etter politiloven § 17 d. Om dette heter det i utredningen punkt 23.3.4 side 247:

«Etter politiloven § 17d kan Politiets sikkerhetstjeneste bruke skjulte tvangsmidler i sin forebyggende virksomhet «dersom det er grunn til å undersøke» om noen forbereder enkelte nærmere bestemte straffbare handlinger. Det er dermed ikke noe krav om at de skjulte tvangsmidlene brukes mot noen som kan mistenkes for å ha begått en straffbar handling. På den annen side er kravet til den straffbare handling skjerpet i forhold til bruk av skjulte tvangsmidler under etterforskingen. Utvalget finner derfor å kunne tilråde at en tilsvarende utvidelse som beskrevet ovenfor også gjelder for PSTs forebyggende virksomhet. Utvalget presiserer likevel at forholdsmessighetsvurderingen etter straffeprosessloven § 170a i alminnelighet vil være strengere i det forebyggende sporet enn ved bruk av tvangsmidler under etterforskingen.

Forslaget vil ikke kreve noen endring av politiloven § 17d første ledd, ettersom det her vises til straffeprosessloven § 200a og § 216a som etter utvalgets forslag vil gi adgang til innbrudd i et datasystem.»

Utvalget har også vurdert forholdet til Grunnloven § 102. Det viser til redegjørelsen i utredningen punkt 13, og bemerker for øvrig følgende (utredningen punkt 23.3.4 side 247):

«*Utvalgets flertall* mener Grunnloven § 102 innebærer at det på det forebyggende stadiet ikke kan gis adgang til å gå inn i noen av de vernede områder (privat bolig) for å plassere utstyr, for eksempel hardware, som er nødvendig for å gjennomføre innbrudd i et datasystem. Dette gjelder tilsvarende for plassering av utstyr til å foreta romavlytting, og utvalget viser til de vurderinger som er gjort av dette under punkt 13.3. *Utvalgets flertall* mener denne begrensningen bør komme uttrykkelig frem av loven.

Utvalget er oppmerksom på at forslaget om at også PST kan foreta innbrudd i et datasystem i det forebyggende sporet vil innebære en utvidelse i forhold til politiloven § 17d, ved at bestemmelsen i dag ikke tillater ransaking av «noens private hjem», jf. tredje ledd annet punktum. Dette innebærer at PST ikke har anledning til å foreta en hemmelig ransaking i noens hjem, og i forbindelse med en slik ransaking for eksempel kopiere en harddisk. Gjennom forslaget om at PST skal ha adgang til å foreta innbrudd i et datasystem, vil PST få adgang til å gjennomføre slik kopiering ved hjelp av dataavlesing.

At PST ikke har anledning til å foreta ransaking av noens private hjem etter politiloven § 17d, ble begrunnet med at departementet ikke ønsket å «trå Grunnloven for nær», jf. Ot.prp. nr. 60 (2004–2005) side 132. Som det fremgår av kapittel 13, finner utvalget at det ikke er problematisk i forhold til Grunnloven § 102 å tillate dataavlesing i det forebyggende sporet, likevel med den reservasjon som er gjort ovenfor. Etter utvalgets vurdering bør det derfor åpnes opp for at PST også kan foreta hemmelig ransaking ved innbrudd i et datasystem etter politiloven § 17d.»

14.6.8 Gjennomføringen av dataavlesing

Under punkt 23.3.5 side 247 i utredningen viser utvalget til at gjennomføringen av dataavlesing vil fordele seg på forskjellige faser, som «installering av programvaren eller montering av hardware, selve avlesingen, tilgjengeliggjøring for politiet, samt avinstalleringen eller fjerning av hardware».

Utvalget peker på at det neppe er hensiktsmessig eller mulig å beskrive mulige gjennomføringsmåter av dataavlesing i detalj, verken i forbindelse med kommunikasjonsavlytting eller hemmelig ransaking og beslag. Det vises til at de tekniske mulighetene er «mange og forskjelligartede», og at den teknologiske utviklingen «formodentlig vil innebære at en slik beskrivelse raskt blir utdatert». Politiet må etter utvalgets oppfatning vurdere hvilken gjennomføringsmåte som er mest hensiktsmessig i hvert enkelt tilfelle, ut fra en samlet vurdering av taktiske og teknologiske forhold. Utvalget har sett for seg to hovedgjennomføringsmåter, som er beskrevet slik (utredningen punkt 23.3.5 side 247–248):

> «Med en softwarebasert løsning får politiet installert et program typisk i mistenktes datamaskin som gjør politiet i stand til å hente ut informasjon fra datasystemet. Dette kan for eksempel gjøres ved at politiet utnytter et sikkerhetshull i datasystemet eller sender en e-post som inneholder et skjult vedlegg med det aktuelle programmet, at politiet installerer programmet i forbindelse med en hemmelig ransaking eller etter å ha utført innbrudd i datasystemet.
>
> Med en hardwarebasert løsning installeres komponenter typisk på mistenktes datamaskin, som gjør politiet i stand til å skaffe seg tilgang til informasjonen. For eksempel kan utstyr som leser av tastetrykkene monteres i tastaturet (key-logging), eller at det monteres utstyr i overgangen mellom tastaturet og selve datamaskinen, for eksempel i en usb-port, som leser av informasjonen som går fra tastaturet til maskinen, eller at det monteres utstyr i et headsett eller mikrofon som gjør det mulig å fange opp lydsignalene ved kommunikasjon over Internettet. En rekke andre gjennomføringsmåter kan tenkes, uten at utvalget – for lovforslaget – finner behov for å gå inn på disse.»

Videre er det bemerket at det «neppe er til å unngå» at gjennomføringen av dataavlesingen vil kunne fange opp opplysninger som ikke var ment kommunisert eller lagret, og som ikke ville ha blitt fanget opp ved tradisjonell kommunikasjonsavlytting eller hemmelig ransaking og beslag. Om dette heter det videre (utredningen punkt 23.3.5 side 248):

> «For eksempel vil såkalt key-logging, altså det at tastetrykkene på et tastatur registreres, ikke kunne skje uten en viss usikkerhet knyttet til om opplysningene ellers ville kunne fanges opp ved de eksisterende metoder. I så fall vil innføring av dataavlesing som gjennomføringsmåte slik utvalget foreslår også kunne innebære en utvidelse av eksisterende hjemler. Utvalget presiserer derfor at dataavlesingen må innrettes slik at det ikke fanges opp opplysninger ut over det som er nødvendig for å kunne gjennomføre en kommunikasjonsavlytting eller en hemmelig ransaking og beslag. Dersom det er nødvendig for politiet å skaffe seg mistenktes oppstartspassord til et datasystem, må gjennomføringen av eventuell key-logging innrettes slik at det er tastetrykkene i oppstartsfasen som registreres, ikke en fortløpende registrering av alle tastetrykk over en lengre periode som derved gir informasjon ut over det som er nødvendig.»

Med hensyn til politiets *tilegnelse* av informasjonen som dataavlesingen frembringer, forutsetter utvalget samme sted at programvaren enten kan lagre dataene på datautstyret eller «sende dem ut via Internettet eller annet tilgjengelig eller installert nettverk/radioutstyr som politiet råder over». Tilgang til de avleste dataene kan ifølge utvalget (samme sted) oppnås «for eksempel ved å hente dem ut av datautstyret ved fysisk tilstedeværelse (beslag eller ransaking), å hente dem ut via bakdør til programvaren fra Internettet, eventuelt ved et nytt innbrudd i datasystemet, å fange dem opp via kommunikasjonskontrollen, eller via utplassert datautstyr som mellomhopp på Internettet».

Etter Metodekontrollutvalgets oppfatning bør det legges opp til at programvare som er installert i mistenktes datasystemer for å gjennomføre dataavlesing, blir avinstallert når avlesingen er avsluttet (punkt 23.3.5 side 248). Videre peker utvalget samme sted på at politiet må være i stand til å dokumentere hva slags programvare eller maskinvare som er benyttet, «herunder angivelse av leverandør, leverandørens programnavn og/eller produktnavn, versjonsangivelse, og påtegninger av hvilke modifikasjoner eller tilpasninger som er gjort med programvaren eller hardwaren dersom man ikke benytter programvaren eller hardwaren slik den leveres av leverandøren».

Videre gir utvalget uttrykk for at dataavlesingen «må innebære så liten sikkerhetsrisiko for mistenktes datasystemer som mulig» (punkt 23.3.5 side 248). Det pekes på at dette til en viss grad vil regulere seg selv, siden ødeleggelse eller forstyrrelse av elementer i brukerens datasystemer ved dataavlesingen vil medføre økt oppdagelsesrisiko, og dermed økt risiko for at metodebruken avsløres og at etterforskningen blir skadelidende.

Med hensyn til eventuelle «sikkerhetshull», gjør utvalget samme sted gjeldende at disse må tettes «så snart som mulig etter at de er oppstått». Det pekes på at politiet må iverksette nødvendige tiltak for å hindre at uvedkommende utnytter svakheter i den programvaren politiet benytter, og at overføring av informasjon tilbake til politiet ikke avlyttes av andre. Utvalget vurderer sikkerhetsrisikoen, herunder faren for at andre utnytter svakheter eller sikkerhetshull som oppstår ved dataavlesingen, som «liten, og uansett innenfor et akseptabelt nivå». Faren for misbruk må etter utvalgets oppfatning inngå som et element i forholdsmessighetsvurderingen i hvert enkelt tilfelle.

14.6.9 Kontrollen med inngrepet

I utredningen kapittel 11 peker utvalget på at bruk av de evaluerte tvangsmidlene bare kan aksepteres dersom kontrollen med inngrepet er forsvarlig. Dette standpunktet er gjentatt under punkt 23.3.6 side 249 med hensyn til dataavlesing som gjennomføringsmåte for kommunikasjonsavlytting, hemmelig ransaking og beslag. Etter utvalgets oppfatning kreves det «skjerpet kontroll med og dokumentasjon av bruken av et slikt tvangsmiddel», fordi dataavlesing kan etterlate seg sikkerhetshull, og fordi det eksisterer en misbruksfare ved at dataavlesingen kan gi tilgang til informasjon som politiet ikke har hjemmel til å innhente.

I henhold til utvalgets forslag vil bruken av dataavlesing ved kommunikasjonsavlytting, hemmelig ransaking og beslag, være underlagt kontroll av Kontrollutvalget for kommunikasjonskontroll, som etter straffeprosessloven § 216 h skal føre kontroll med politiets og påtalemyndighetens behandling av saker etter straffeprosessloven kapittel 16 a. Utvalgets forslag inkluderer en henvisning i straffeprosessloven § 200 a første ledd om at § 216 h skal gjelde tilsvarende ved hemmelig ransaking.

Utvalget vurderer det som nødvendig å etablere et «loggesystem (protokoll)» for bruken av dataavlesing, og at dette bør gjennomføres gjennom bestemmelser etter lignende modell som kommunikasjonskontrollforskriften § 7. Utvalget foreslår derfor en ny § 7 a i forskriften, jf. punkt 32.4 side 376. Om dette heter det under punkt 23.3.6 side 249 i utredningen at:

> «Det er etter utvalgets mening nødvendig å sikre notoritet rundt hjemmelen for det aktuelle innbruddet i datasystemet, påtalemyndighetens begjæring eller eventuelle bruk av hastekompetanse, rettens kjennelse, begjæringer om bistand fra andre organer i gjennomføringen, angivelse av hvilket datasystem som har vært gjenstand for innbrudd, når innbruddet fant sted, eventuelle forlengelser, innbruddets opphør, alle relevante parametere i datasystemet før og etter innbruddet, hvilken programvare eller hardware som har vært benyttet, hvilke risiki datasystemet kan ha vært utsatt for og hva som har vært foretatt for å avverge skade på datasystemet og andres utnyttelse av eventuelle sikkerhetshull, eventuelle skader på datasystemet, hvilke ressurser som har medgått, hvilke opplysninger som er fremskaffet og betydningen (effektivitet) i den konkrete saken, sletting av innholdsdata, samt lagringsperiode for metadata. Det påligger vedkommende departement som forskriftsmyndighet å påse at forskriften dekker registrering/logging av alle relevante parametre vedrørende gjennomføringen av dataavlesing på en slik måte at notoritet og manipulasjonssikkerhet ivaretas. Det er en forutsetning at disse forhold også ivaretas gjennom det datasystem politiet benytter ved gjennomføringen av dataavlesing.»

Videre foreslår utvalget et nytt femte punktum i kommunikasjonskontrollforskriften § 10 første ledd (jf. punkt 32.4 side 377), som innebærer at politimestrenes innberetning til Riksadvokaten med opplysninger om kommunikasjonskontroll, og Riksadvokatens innrapportering til Justis- og

beredskapsdepartementet, også skal inneholde opplysninger om de sakene hvor kommunikasjonsavlyttingen har funnet sted ved innbrudd i et datasystem.

14.6.10 Evaluering

Under punkt 23.3.6 side 249 i utredningen, peker Metodekontrollutvalget på at det kan være grunn til å gi de foreslåtte lovendringene en virkeperiode på for eksempel fem år, for å «sikre at en slik evaluering faktisk finner sted».

14.7 Høringsinstansenes syn

14.7.1 Behovet for dataavlesing

Flere av høringsinstansene peker på at den teknologiske utviklingen – herunder økt bruk av og kunnskap om kryptering og andre former for informasjonsbeskyttelse – har medført at bruken av skjulte tvangsmidler, som kommunikasjonsavlytting og skjult ransaking, ikke gir like godt informasjonsutbytte som tidligere. Metodenes effektivitet er *redusert*, og det er anført at en utvidet adgang til bruk av datateknologi, herunder skjulte innbrudd i datasystemer som brukes av mistenkte, er nødvendig.

Kripos uttaler blant annet følgende:

> «Kripos kan bekrefte at det brukes krypterte nettforbindelser og nettsesjoner i saker hvor kommunikasjonskontroll har vært benyttet, og at det ofte forekommer krypterte autentiseringsdata (passord og adgangskoder til internettjenester) som politiet ikke kan dra nytte av pga krypteringen. Etterforskningen er ofte vesentlig tyngre uten slike data i lesbar form.
>
> Det som uten tvil vanskeliggjør kommunikasjonskontroll er kryptering av hele nettforbindelsen eller nettsesjonen, og de fleste krypteringsprotokollene som brukes i dag for kommunikasjon benytter vilkårlige nøkler som skiftes ut jevnlig. Den populære tjenesten Google Mail er et eksempel hvor nettsesjonen (alle datapakkene mellom Googles server og brukerens dataanlegg) krypteres uten at brukeren gjør dette valget selv.
>
> […]
>
> Det er utvilsomt at politiet kan ransake og ta beslag i en datamaskin eller annet informasjonssystem, eksempelvis en kopimaskin, når vilkårene etter strpl §192 og §203 foreligger. De påfølgende datatekniske undersøkelsene vil være avgjørende for hvor stor del av innholdet av den beslaglagte datamaskinen eller informasjonssystemet politiet kan dekode og gjøre lesbart. Store deler av innholdet kan være kryptert. Det er altså ikke tilgangen til beslaget som er problematisk, men i hvor stor grad den teknologiske utviklingen hindrer at beviset kan fremkalles. Dersom politiet hadde funnet en universalmetode for å fremkalle alle tenkelige dataspor ved å knekke en hver kryptering, ville bestemmelsene om ransaking og beslag hatt like stor betydning som tidligere. Slik er det imidlertid ikke. Den teknologiske utviklingen har gjort at elektroniske bevis er mindre tilgjengelige nå enn før.
>
> Elektroniske bevis er utvilsomt av stor betydning. Bruken av elektroniske hjelpemidler har økt drastisk de siste tiårene. Mye av det som tidligere forelå i papirform foreligger nå elektronisk. Det sendes ikke lenger brev, men e-post. Notater skrives ikke på notatlapper, men på en datamaskin. Det innhentes ikke plantegninger over bankhvelv, men viktig informasjon finnes via internett eller mottas elektronisk på et annet lagringsmedium. Når dette blir gjort uttilgjengelig for bevissikring ved at det er kryptert, har effekten av ransaking og beslag som metoder blitt vesentlig redusert.
>
> […]
>
> Det er vanskelig for politiet å ha en begrunnet oppfatning av hvilken informasjon en ikke får tilgang til når krypteringen ikke kan brytes. Det kan være andre grunner for å kryptere informasjon enn for å skjule kriminalitet. Stadig mer informasjon i datasystemer blir kryptert av programvaren uten at brukeren selv er klar over det. Uavhengig hva som er årsaken til at informasjonen blir mindre tilgjengelig, er det uansett en utvikling som utvilsomt gjør metodene ransaking og beslag mindre anvendelige. Det en kan slå fast med sikkerhet er at mye informasjon som tidligere var tilgjengelig ved en fysisk ransaking nå lagres elektronisk, som nærmere beskrevet ovenfor. Slik sett er det ikke vanskelig å begrunne behovet for at politiet må gis adgang til å bruke metoder som er egnet til å bryte en elektronisk kryptering, på samme måte som nødvendige metoder kan benyttes for å bryte opp en safe.»

Behovet for å kunne benytte dataavlesing som gjennomføringsmåte for kommunikasjonsavlytting, ransaking og beslag bekreftes også av *Riksadvokaten*, *Politiets sikkerhetstjeneste (PST)*, *Økokrim* og *Det nasjonale statsadvokatembetet for bekjempelse av organisert og annen alvorlig krimi-*

nalitet (NAST). *Økokrim* uttaler blant annet at det «deler utvalgets konklusjon om at bruken av kryptering øker», og at embetet i flere saker har opplevd at kryptering har vanskeliggjort etterforskningen. Etter Økokrims oppfatning er dataavlesing «en svært effektiv måte å få tilgang til informasjon uten hinder av krypteringen». De ovennevnte høringsinstansene uttrykker støtte til utvalgets forslag om å tillate dataavlesing, men flere har også pekt på at dataavlesing bør innføres som selvstendig tvangsmiddel, eller på annen måte tillates i større utstrekning enn det utvalget har foreslått. *PST* uttaler i denne sammenheng følgende:

> «Vi finner det imidlertid nødvendig at også dataavlesing som selvstendig metode for å gjennomføre kommunikasjonskontroll, innføres. Vi viser i den forbindelse til vårt brev til Riksadvokaten, sendt Metodekontrollutvalget til orientering, av 19. desember 2008 vedrørende dette.
>
> Som poengtert i vårt brev er det vanskelig å se noen prinsipielle motforestillinger mot selve informasjonstilgangen dataavlesing som selvstendig metode kan medføre. Politiet har allerede hjemler til inngripende tvangsmidler med virkning fremover i tid. Ved tilgang på informasjon gjennom dataavlesning kan politiet i et idealtilfelle, gjennom spisset og effektiv informasjonsinnhenting, på kortere tid og ved mindre integritetskrenkelser settes i stand til bedre å bekjempe de alvorligste straffbare handlingene.
>
> Dataavlesing fremstår som den sentrale metode for å gjennomføre kommunikasjonskontroll i fremtiden. Det eneste som kan avgi en helhetlig bilde av kommunikasjonen osv, mellom de kriminelle er i brukergrensesnittet mellom maskin og bruker, dvs. mellom apparatet og objektet.
>
> Dataavlesing som selvstendig metode synes per nå å representere den eneste tekniske muligheten for å gjennomføre slik avlytting/avlesing. Gjennom dataavlesing kan objektets produksjon av viktige dokumenter, herunder krypterte filer, avdekkes. Dette kan gjelde dokumenter som kanskje ikke finnes på det tidspunktet en ransaking av pc-en finner sted, og som kanskje aldri blir sendt elektronisk og derfor heller ikke vil bli fanget opp i forbindelse med en kommunikasjonskontroll. En eventuelt gjentatt ransaking av samme objekt – kanskje flere ganger – gir ingen garanti for at slike dokumenter avdekkes. Eneste mulighet for å gi politiet tilgang til slik informasjon er derfor gjennom dataavlesing.»

NAST peker på generelle svakheter ved lovens skille mellom hemmelig ransaking og kommunikasjonskontroll «i lys av den teknologiske utvikling» (omtales nærmere nedenfor under punkt 14.7.3), og mener at dataavlesing bør innføres som selvstendig metode. NAST kan ikke se at det vil være mer integritetskrenkende enn for eksempel kommunikasjonskontroll. I denne sammenheng uttales:

> «Det er behov for metoden for å fange opp dekrypteringsnøkler, slik at politiet kan utnytte kryptert informasjonsfangst uavhengig av om den stammer fra data som er lagret eller som har vært innhentet ved kommunikasjonskontroll.
>
> Metodekontrollutvalget har tatt utgangspunkt i at metodene skal møte etterforskingsbehovet stilt overfor «miljøer preget av elementer som sterk intern justis, profesjonalitet, organisering, mobilitet og internasjonale kontakter.» (utredningen s. 110).
>
> Utgangspunktet er altså mennesker i bevegelse, flere som samarbeider og følgelig utnytter elektroniske kommunikasjonstjenester, profesjonelle som vet å beskytte kommunikasjonen ved kryptering.
>
> Hvis lovens formål er å gi politiet mulighet til å følge med på kommunikasjonen mellom kriminelle, er det både behov for kommunikasjonskontroll som i dag, og for gjentatt hemmelig ransaking som kan følge med på en epostkonto eller annen brukerkonto i nettet. Metodene dekker samme formål. Utvalget har drøftet *gjentatt ransaking* under merkelappen «dataavlesing» og kommet til at man ikke vil anbefale metoden, «fordi det vil gi politiet anledning til systematisk å kartlegge mistenktes bruk av et datasystem over tid, herunder opplysninger som ikke blir lagret i datasystemet og dermed ikke vil kunne hentes ut ved tradisjonell hemmelig ransaking. Etter utvalgets syn innebærer dette en for stor integritetskrenkelse i forhold til det anførte behovet.» (s. 246).
>
> Første del av begrunnelsen er ikke lett å forstå sammenlignet med at man aksepterer bruk av kommunikasjonskontroll. Det ville gitt bedre sammenheng i regelverket om utvalget hadde utformet en *ransakingsregel som ga politiet adgang til å foreta informasjonsinnhenting*

fra brukerkontoen/datasystemet et ubegrenset antall ganger, også med bruk av dataprogram som automatisk rapporterer om endringer, innenfor en nærmere bestemt tidsperiode.

Andre del av begrunnelsen i sitatet gjelder data som ikke blir lagret, noe som i praksis er passord for tilgang og dekryptering. At dette er nødvendige data for politiet også for *enkeltstående* tilfeller av ransaking, bør være hevet over tvil, så også denne delen av begrunnelsen er vanskelig å forstå. Det er følgelig behov for å utnytte automatiske metoder for *å kopiere lagret innhold og rapportere om bruk av datamaskinen (tastetrykk), samt å kopiere trafikk mellom kommunikasjonsanlegg*, og alt dette bør reguleres i samme bestemmelse.»

Også *Kripos* gir uttrykk for at dataavlesing bør tillates i videre utstrekning enn det utvalget foreslår – særlig i forbindelse med ransaking, som etter Kripos' oppfatning må tillates utført fortløpende for at metoden ikke skal miste sitt anvendelsesområde for elektroniske spor. Det vises til den danske løsningen, hvor dataavlesing er innført i en egen bestemmelse, men understrekes at den lovtekniske løsningen ikke er avgjørende. Kripos' synspunkter knyttet til dataavlesing ved ransaking og behovet for å kunne gjennomføre fortløpende eller kontinuerlig ransaking omtales nærmere nedenfor under punkt 14.7.3. Kripos er kritisk til avgrensningene i adgangen til å benytte dataavlesing etter utvalgets forslag, «til tross for at utvalget også anerkjenner at bruken av kryptering av kommunikasjon øker, og vil fortsette å øke i fremtiden».

Politidirektoratet har «klare innvendinger mot at dataavlesning ikke foreslås innført som egen metode». Under henvisning til Kripos' redegjørelse mener direktoratet at «utvalget ikke i tilstrekkelig grad tar innover seg den teknologiske utviklingen og de utfordringer politiet møter i så måte».

Oslo politidistrikt gir uttrykk for at metoden «dataavlesing» må «forstås på samme måte som i den danske retsplejeloven § 791 b», og uttaler følgende:

«Oslo politidistrikt konstaterer at i Danmark fikk man hjemmel til dataavlesning allerede i 2002. Utvalget har ikke funnet å kunne anbefale metoden, bl.a. begrunnet i at det ikke er dokumentert tilstrekkelig behov for dette. Oslo politidistrikt finner grunn til å bemerke at det forutsettes at dataavlesning kun skal benyttes ved mistanke om alvorlig, oftest organisert, kriminalitet og at bruken vil være begrenset. Vi mener utvalget i alt for stor grad er opptatt av at man kan påvise et nærmere behov for en metode som vi ikke har hatt anledning til å benytte, og at det tydeligvis ikke legges vekt på den tekniske utvikling som gjør at politiet hele tiden kommer på etterskudd i forhold til de muligheter lovbrytere kan gjøre seg nytte av.

Metoden skulle være tilstrekkelig utredet, og det blir da opp til de politiske myndigheter å treffe et valg om politiet skal få adgang til et nyttig redskap ved etterforskning i alvorlige straffesaker. Vi mener at det bør innføres en lovhjemmel til dette tilsvarende den danske.»

Økokrim uttaler at det oppfatter utvalgets forslag som en «pragmatisk mellomløsning», som vil gi tilstrekkelige muligheter til å ivareta Økokrims behov i dagens situasjon. Økokrim peker likevel på at:

«[…] dersom dataavlesing innføres i tråd med utvalgets forslag (det kun tillates i tilknytning til kommunikasjonskontroll og hemmelig ransaking), vil enkelte mulige sporsteder forbli utilgjengelig for politiet. Alt som produseres i informasjonssystemer uten å lagres (eller som lagres utilgjengelig dvs. kryptert eller skjult på annen måte som steganografi), eller som ikke kommuniseres ut via avlyttbare kanaler, kan forbli utilgjengelig. En kan også tenke situasjoner hvor to personer i samme rom ikke snakker sammen, men bruker en datamaskin til å kommunisere uten at noe noen gang lagres eller kommuniseres. I slike tilfeller vil ikke romavlytting gi noen informasjon, og dataavlesing ville ha vært eneste mulighet til å dokumentere hva som "blir sagt".»

Utvalgets forslag om å tillate dataavlesing som gjennomføringsmåte for kommunikasjonsavlytting og hemmelig ransaking og beslag støttes av *Norges politilederlag*, *Telemark politidistrikt*, *Hordaland politidistrikt* og *Fornyings-, administrasjons- og kirkedepartementet*.

Oslo statsadvokatembeter viser til utvalgets redegjørelse om utfordringene med å fremskaffe dokumentasjon eller tallmateriale som belyser behovet for dataavlesing, og uttaler at det «kan synes overraskende at utvalget fremmer forslag som er så vidt vidtgående når utvalget selv poengterer at det ikke har fått tilstrekkelig dokumentasjon for behovet for å innføre fremgangsmåten». Videre heter det i høringsuttalelsen:

> «Når utvalget likevel foreslår å åpne for skjult dataavlesning, er dette begrunnet med at det er nødvendig for å opprettholde effektiviteten av dagens kommunikasjonskontroll og for å kunne gjennomføre en hemmelig ransakning. Etter det man forstår er begrunnelsen å videreføre de i dag tilgjengelige metoder «en digital verden.» Derimot forstår man utvalget slik at de ikke foreslår å tillate gjentatte ransakinger på en og samme beslutning. Dette ville i prinsippet åpne for en sammenhengende «overvåkning» av datamaskinene.
>
> Oslo statsadvokater er i prinsippet enig i denne avgrensing. Likevel oppstår det flere vesentlige og vanskelige spørsmål. Et moment i denne sammenheng vil være at man kan etablere tilfredsstillende kontrollsystemer som sikrer mot misbruk eller påstander mot misbruk.»

Advokatforeningen uttaler at utvalgets forslag ikke «foranlediger […] særskilte merknader fra Advokatforeningens side».

Flere høringsinstanser mener at dataavlesing ikke bør tillates, verken som gjennomføringsmåte for eksisterende tvangsmidler eller som selvstendig tvangsmiddel.

Datatilsynet gir uttrykk for at dataavlesing – selv som en videreføring av eksisterende metoder – vil innebære at «tanker, assosiasjoner og ønsker som kanskje engang aldri var tenkt kommunisert til noen andre blir gjenstand for politiets behandling». Datatilsynet mener at man «[b]illedlig kan [...] si det slik at det ikke bare er ens kommunikasjon som avlyttes, men ens dagbok», og at metoden «er så inngripende at den ikke bør innføres, selv som et virkemiddel for å gjennomføre andre metoder».

Norsk forening for kriminalreform (KROM) siterer utvalgets uttalelse på side 248 i utredningen om at det neppe er til å unngå at gjennomføringen av dataavlesingen vil kunne fange opp opplysninger som ikke var ment kommunisert eller lagret, og som ikke ville blitt fanget opp ved kommunikasjonsavlytting eller hemmelig ransaking og beslag uten bruk av dataavlesing. KROM viser til at dette «kan gjelde uskyldige tredjepersoners bruk av maskinen, men også rent personlige tanker, tanker som vedkommende mistenkt ikke har tenkt lagret eller å bli konfrontert med senere», og at dataavlesing derfor må «utredes ytterligere før det innføres som en yttereligere metode for skjulte etterforskningsskritt». KROM mener videre at «dekrypteringsmetoder vil være et mer adekvat satsingsområde enn å åpne for dataavlesing».

NRK støtter heller ikke utvalgets forslag om å tillate dataavlesing ved gjennomføringen av kommunikasjonskontroll og hemmelig ransaking. NRK uttaler at «[s]elv om politiet *rettslig* sett kun har tilgang til det som kommuniseres til og fra datamaskinen, vil politiet faktisk kunne skaffe seg tilgang til alt som ligger på datamaskinen, eksempelvis eldre kommunikasjon på e-post mellom kilde og journalist, og denne faktiske tilgangen vil i seg selv være tilstrekkelig til å medføre en «chilling effect»».

Forsvarergruppen av 1977 mener at utvalgets forslag om å tillate dataavlesing som gjennomføringsmåte ved kommunikasjonsavlytting og hemmelig ransaking og beslag, men ikke som metode for fortløpende overvåking av all aktivitet i et datasystem, er en «fornuftig tilnærming». Forsvarergruppen støtter likevel ikke forslaget, under henvisning til «de betenkeligheter som gjør seg gjeldende overfor informasjon som ikke er ment kommunisert til noen, samt overfor tredjepersoners bruk av for eksempel felles datamaskin i husstand». Etter Forsvarergruppens oppfatning gjør dette dataavlesing «særlig integritetskrenkende».

14.7.2 Dataavlesing for å muliggjøre kommunikasjonsavlytting

Kripos gir uttrykk for at utvalgets forslag på dette punkt «i de fleste tilfeller vil løse politiets utfordringer som vanskeliggjør kommunikasjonskontroll – i særlig grad kryptering». Kripos uttaler videre:

> «Utvalgets forslag betyr at avlyttingspunktet flyttes fra teletilbyderen («den lukkede transportfasen») og inn til mistenktes kommunikasjonsanlegg før den krypteres og gjøres uleselig for politiet («den åpne transportfasen»). Kripos er enig i at noe annet ville føre til at kommunikasjonskontroll som metode gradvis vil ha mindre verdi.»

NAST uttaler derimot at:

> «NAST har problem med å forstå utvalgets begrunnelse for å innføre dataavlesing i form av adgang til å foreta datainnbrudd for å foreta kommunikasjonskontroll, jf. forslag til nytt femte ledd i strpl. § 216a. Kommunikasjonskontroll utføres vanligvis med bistand fra tilbyder, en situasjon som ikke gir behov for å begå datainnbrudd for å gjennomføre tilegnelsen av innholdsdata. Dersom kommunikasjonen er kryptert er det imidlertid behov for å få tilgang

til *dekrypteringsnøkler* fra tilbyder, slik at kommunikasjonen kan konverteres til klartekst. Slik forslaget til strpl. § 216a nest siste ledd er utformet, omfattes ikke denne situasjonen, jf. at det gir tillatelse til «å foreta innbrudd i et datasystem», noe som strengt tatt ikke gjelder kommunikasjonskontroll, men ransaking. Det burde imidlertid fremgå av loven at tillatelse til kommunikasjonskontroll med bistand fra tilbyder *gir politiet rett til å motta kommunikasjonen i klartekst dersom tilbyder er i stand til å dekode innholdet.»*

Flere høringsinstanser er kritiske til utvalgets forslag om at tillatelse til dataavlesing bare skal gis dersom kommunikasjonsavlyttingen «er vanskeliggjort». *Kripos* uttaler at dette er et «lite hensiktsmessig vilkår», og det bør være nok at tradisjonell kommunikasjonskontroll er vurdert og funnet utilstrekkelig, samt at det gis en særskilt begrunnelse for dette. Kripos begrunner dette slik:

«Ellers vil politiet risikere å miste viktig informasjon i en periode hvor man gjør et forsøk på tradisjonell kommunikasjonskontroll, til tross for at politiet har grunn til å tro at mistenkte benytter krypterte tjenester eller andre beskyttelsestiltak som vanskeliggjør kommunikasjonskontroll. Denne informasjonen kan eksempelvis ha fremkommet gjennom kommunikasjonskontroll av mistenktes telefon eller fra annen etterforskning.»

Lignende synspunkter tilkjennegis av *Riksadvokaten*, som uttaler at det bør overveies om det kan være tilstrekkelig at tradisjonell kommunikasjonsavlytting «antas vanskeliggjort». Riksadvokaten peker på at det i så fall bør presiseres i motivene at det kreves mer enn en løs antakelse om at dette er situasjonen, «for eksempel at det godtgjøres at politiet har erfaring for at det i det aktuelle miljøet er vanlig å benytte kommunikasjon som ikke kan avlyttes ved tradisjonelle midler».

14.7.3 Dataavlesing som gjennomføringsmåte for hemmelig ransaking

Kripos gir for det første uttrykk for at straffeprosessloven § 200 a allerede gir adgang til hemmelig ransaking uten politiets fysiske tilstedeværelse, og at datainnbrudd kan være en gjennomføringsmåte ved ransaking av datasystem etter beslutning om ransaking i medhold av straffeprosessloven § 192, eventuelt med utsatt underretning etter straffeprosessloven § 200 a. Etter Kripos' oppfatning kan politiet «bryte seg inn i et datasystem på samme måte som man kan bryte seg inn i en leilighet, som ellers ville være et straffbart innbrudd etter strl § 147». Det vises i denne sammenheng til at det ikke er tradisjon for å beskrive gjennomføringsmåter for de enkelte tvangsmidler i detalj i straffeprosessloven, og at dersom det likevel skulle være behov for å presisere adgangen i loven, bør dette gjøres i straffeprosessloven § 200.

Videre peker Kripos på at ransaking av datasystemer innebærer utfordringer som følge av den teknologiske utviklingen. Dersom mistenkte beskytter lagret innhold i datasystemet med kryptering, eller ikke lagrer informasjonen («flyktige data»), er den eneste måten å få tilgang til informasjonen å slå til mens den ligger åpen hos mistenkte, altså mens mistenkte selv har åpnet krypteringen. Kripos begrunner dette med at «krypteringsnøklene som beskytter informasjonen som regel er flyktige, og ikke lagret, det er ikke snakk om et brukernavn og passord». Det understrekes at «et teknologisk kappløp med krypteringsløsninger» ikke er gjennomførbart.

Kripos er også kritisk til utvalgets tilnærming til elektroniske bevis, og uttaler:

«Utvalget drøfter i pkt 23.2.3 dataavlesing opp mot *sensitivitetsprinsippet*. Kripos' utgangspunkt er at ransaking av et datasystem er likestilt med ransaking for øvrig. Enhver ransaking etter strpl §192 stiller politiet overfor de samme problemstillinger som utvalget drøfter, nemlig at politiet må søke gjennom en rekke ting/gjenstander/informasjon for å finne ting som *«antas å ha betydning som bevis»* etter strpl §203. Det innebærer at politiet ved en tradisjonell ransaking av en bolig går gjennom tidvis meget personsensitiv informasjon som håndnotater, dagbøker, bilder av personlig karakter, brev, forretningshemmeligheter mv. Deretter gjøres det en vurdering av hva som har bevisverdi i den konkrete saken. Typen opplysninger som gjennomgås i forbindelse med en tradisjonell ransaking skiller seg ikke fra opplysninger som forefinnes i et datasystem. Det er i begge tilfeller opplysninger som kan være av meget personlig karakter, og som ikke er ment for andre enn besitteren. Det er som oftest opplysninger som ikke er tenkt kommunisert til andre. Likevel kan politiet vurdere at opplysningene har betydning som bevis.

Utvalgets vurderinger stiller elektroniske bevis i en unaturlig stilling til tross for at de etter Kripos oppfatning ikke skiller seg fra øvrige opplysninger som kan fremskaffes ved

tradisjonell ransaking. Det er den teknologiske utviklingen som har gjort at opplysningene nå forefinnes elektronisk og ikke som fysiske bevis, eksempelvis som e-post i stedet for brev. En tilnærming hvor ransaking av datasystemer sidestilles med ordinær ransaking taler for at dataavlesing bør tillates.

Utvalget nevner særskilt datasystemer som inneholder særlig sensitiv informasjon, eksempelvis et datasystem på et legekontor. Kripos er enig i at denne type informasjon står i en særstilling, men dette kan reguleres med unntaksbestemmelser slik det er gjort for kommunikasjonskontroll, se strpl §216c annet ledd.»

Etter Kripos' oppfatning skiller dataavlesing seg fra tradisjonell ransaking fordi den må gjennomføres fortløpende eller kontinuerlig dersom det skal være gjennomførbart i krypterte systemer. Det må derfor tas stilling til om fortløpende ransaking av datasystem skal tillates, «for at ransaking som metode skal ha samme effekt som tidligere». Det pekes på at dette vil være et større inngrep enn en enkeltstående ransaking, og et større inngrep i personvernet enn tradisjonell ransaking, mens gjentatt ransaking vil stå i en mellomstilling.

Med hensyn til *gjentatt ransaking* mener Kripos at det «kan stilles spørsmål ved om dagens ransakingshjemler gir adgang til å gi tillatelse til mer enn én ransaking av samme objekt om gangen», og uttaler:

«Det er på det rene at en og samme ransakingsbeslutning kan omfatte flere mistenkte/flere objekter. Det er ikke noe vilkår at ransakingen utføres på et bestemt tidspunkt, og heller ikke at ransaking mot samtlige objekter finner sted samtidig. Det er også tillatt å ta seg inn på åstedet flere ganger, dersom ransakingen av praktiske grunner må avbrytes før den er ferdig gjennomført. Da dreier det seg fortsatt om samme ransaking. Det er videre på det rene at samme objekt kan ransakes flere ganger i samme sak, dersom vilkårene er til stede hver gang og det gis ny beslutning for hver gang.

Spørsmålet er om samme objekt også kan ransakes flere ganger med grunnlag i en og samme beslutning, dersom retten etter en konkret vurdering finner at vilkårene er tilstede over en gitt tidsperiode. Lovens ordlyd er ikke til hinder for dette. Rettstilstanden synes imidlertid uavklart. I NOU 2004: 6 s 93 andre spalte sier utvalget at *«kommunikasjonsavlytting kan gjelde et bestemt tidsrom, mens en ransakingstillatelse er begrenset til én undersøkelse»,* uten å problematisere dette nærmere. Dette er også lagt til grunn av metodekontrollutvalget i utredningen s 246, 1. spalte 4. avsnitt.»

Ifølge Kripos kan det at ransakingsbestemmelsen tradisjonelt har vært forstått og praktisert slik at det kun besluttes én ransaking av samme objekt om gangen, blant annet skyldes at gjentatt ransaking er lite aktuelt i en åpen etterforskning. Det pekes på at en åpen ransaking «etter sin art er avslørende», og at det derfor normalt er lite hensiktsmessig å foreta en ny ransaking når den første er gjennomført, og åstedet er frigitt. Etter Kripos' oppfatning er situasjonen en annen ved skjult etterforskning, og det gis uttrykk for at den tradisjonelle forståelsen av straffeprosessloven § 197 derfor ikke forhindrer at bestemmelsen «i et gitt tilfelle vurderes annerledes når man står overfor en hemmelig ransaking med hjemmel i §200a». Kripos gir følgende illustrasjon i denne sammenheng:

«Som eksempel på hemmelig ransaking av et fysisk rom kan nevnes et tilfelle hvor politiet besitter informasjon om at en bestemt leilighet vil bli brukt som depot for et narkotikaparti som skal innføres til Norge. Man vet imidlertid ikke når partiet vil ankomme. Kommunikasjonskontroll kan gi politiet en pekepinn om dette. Men det vil uansett være et behov for å gå inn og sjekke leiligheten med jevne mellomrom. Dette kan selvsagt løses ved at retten tar stilling til spørsmålet hver eneste gang politiet skal inn og undersøke. Men det er som nevnt intet ved ordlyden i § 200a, jfr §197 som hindrer retten i å gi politiet tillatelse til å undersøke samme leilighet flere ganger over en gitt tidsperiode.

Det samme behovet for fortsatt ransaking gjelder for et virtuelt rom i cyberspace. I forbindelse med skjult etterforskning er det ofte behov for gjentatt ransaking av elektroniske lagringsmedier fordi innholdet endres. En epostkonto hvor det jevnlig tilkommer nye bevis av vesentlig betydning for saken vil det eksempelvis være nødvendig å ransake med jevne mellomrom. Teknisk sett kan politiet gjennomføre ransakingen ved bruk av dataprogrammer. At retten i et slikt tilfelle gir tillatelse til flere ransakinger i samme beslutning er som nevnt forenlig med lovens ordlyd.»

Etter Kripos' oppfatning er hyppigheten av ransakinger, og den totale tidsperioden det gis tillatelse til ransakinger i, spørsmål som «hører

naturlig inn under forholdsmessighetsvurderingen i strpl §170a». Det pekes på at også objektet for ransakingen vil være et relevant vurderingsmoment, og at det eksempelvis må anses mer inngripende å ransake mistenktes bolig enn «å ransake en e-postkonto som er opprettet med det formål å tjene som informasjonskanal for de mistenkte som ledd i den straffbare handling». I tillegg vises det til at omfanget av beslutningen også vil avhenge av mistankens styrke og hvor sentralt ransakingsobjektet synes å være, og at det kan være naturlig å gi en éngangsbeslutning først, og eventuelt en videre beslutning etter hvert, dersom ransaking «avdekker et mønster som viser at det jevlig tilkommer nye bevis av vesentlig betydning».

Videre peker Kripos på at spørsmålet om gjentatt ransaking hjemles i dagens regelverk ikke er avklart av Høyesterett, men at høringsinstansen kjenner til at problemstillingen «ved enkelte anledninger har vært prøvd av både tingrett og lagmannsrett». Videre uttaler Kripos:

> «Som eksempel nevnes en skjult etterforskning ved Kripos for noen år tilbake (som ikke lenger er taushetsbelagt) hvor tingretten ga tillatelse til å ransake en e-postkonto. Etterforskningen viste at de mistenkte benyttet kontoen til å utveksle informasjon om det straffbare forhold, særlig om forestående møtevirksomhet. Siden de mistenkte var svært forsiktige i sin telefonbruk, var hemmelig ransaking av e-postkontoen et nødvendig supplement til den øvrige etterforskningen. KK-bestemmelsen ga som kjent ikke hjemmel til å sikre dette bevismaterialet, siden det ikke var snakk om e-post som ble sendt fra et kommunikasjonsanlegg til et annet. Informasjonen ble derimot utvekslet ved at mistenkte skrev utkast til meldinger, som ble lagret på kontoen. Enhver med tilgang (passord) kunne logge seg inn og lese utkastet. Kontoen fungerte følgelig som en slags oppslagstavle, hvor beskjeder ble formidlet uten å bli sendt fra A til B. Politiet hadde i dette tilfellet riktig passord. Det tilkom jevnlig ny informasjon på kontoen, og det var derfor behov for flere ransakinger. Tingretten ga på denne bakgrunn tillatelse til gjentatt ransaking. Kjennelsen ble ikke påanket av §100a-forsvareren.»

Kripos antar på denne bakgrunn at straffeprosessloven § 197 gir hjemmel for å tillate flere ransakinger av samme objekt innenfor en avgrenset tidsperiode – i én beslutning, og at dette kan skje som ledd i skjult etterforskning dersom vilkårene i § 200 a er oppfylt. Etter Kripos' oppfatning er det en forutsetning at politiet forlater stedet eller det virtuelle rommet hver gang en ransaking er gjennomført. I motsatt fall «er det snakk om en kontinuerlig overvåkning («fortløpende ransaking»), som åpenbart ikke hjemles i dagens ransakingsbestemmelser».

Kripos peker videre på at gjentatt ransaking ikke er tilstrekkelig for å sikre «flyktige opplysninger» – altså opplysninger som ikke lagres – i elektroniske informasjonssystemer. Som eksempler nevnes krypteringsnøkler, passord og «annet som kan brukes til å bryte kryptering». Etter Kripos' oppfatning er det i mange situasjoner «avgjørende […] å ha anledning til å bevissikre disse» gjennom fortløpende eller kontinuerlig ransaking. Dette utdypes slik:

> «Dersom en gjennomfører ransaking på et tilfeldig tidspunkt i håp om at mistenkte har åpnet de krypterte filene vil det være mer eller mindre tilfeldig hvilken informasjon som er tilgjengelig. Hyppig gjentakelse i den fysiske verden kan betraktes som sneglefart i et elektronisk datasystem. I praksis kan de flyktige opplysningene eller de åpne krypterte filene kun bevissikres ved en kontinuerlig tilstedeværelse. Det frekvensbeskrivende begrepet «gjentatt» gir i praksis ikke en slik grad av tilstedeværelse. Det må i så fall gjennomføres et stort antall «stikkprøve»-ransakinger som i praksis blir lite gjennomførbart og antakeligvis ikke mulig. Det gir også sikringsmuligheten et tilfeldighetspreg. Adgangen til fortløpende ransaking vil derfor være eneste praktiske løsning på krypteringsproblemet.»

Kripos mener derfor at «dataavlesing må innføres som en gjennomføringsmåte også for ransaking, slik at denne metoden ikke skal miste sitt anvendelsesområde for elektroniske spor». Det er etter Kripos' oppfatning av mindre betydning om dette lovteknisk gjennomføres ved at dataavlesing defineres som egen metode, eller som gjennomføringsmåter for henholdsvis kommunikasjonskontroll og ransaking. Det vises imidlertid til den danske løsningen, hvor dataavlesing er inntatt i en egen bestemmelse.

Politidirektoratet støtter Kripos' synspunkter, og uttaler:

> «Et grunnleggende utgangspunkt, som utvalget synes enig i, må være at politiet gis de samme forutsetninger for å gjennomføre en ransaking med tanke å innhente bevis (infor-

masjon) som er lagret elektronisk, som ved en tradisjonell ransaking. Direktoratet anser i så henseende at den teknologiske utviklingen (økt grad av kryptering) har ført til at politiet ikke har de samme muligheter til å innehente/beslaglegge informasjon som er lagret elektronisk som fysisk. Direktoratet viser her til at Kripos *«mener det som skiller dataavlesing fra tradisjonell ransaking, er at det av teknologiske årsaker må gjennomføres fortløpende (kontinuerlig) om det skal være gjennomførbart i krypterte systemer»*. Som Kripos peker på videre er det vanskelig å ha en begrunnet oppfatning om hvilken informasjon politiet ikke får tilgang til når krypteringen ikke kan brytes. Den omstendighet at det ligger informasjon der som politiet ikke klarer å få tilgang til er i seg selv klart uholdbart. Politidirektoratet støtter derfor Kripos tilrådning om at det må vurderes nærmere om fortløpende ransaking av datasystem skal tillates.

Politidirektoratet viser ellers til Kripos' utførlige merknader på dette punkt, som direktoratet i det vesentlige kan slutte seg til.»

Også *Riksadvokaten* slutter seg langt på vei til Kripos' vurderinger av hva det i praksis er behov for:

«For riksadvokaten er det overordnede krav til ny lovgivning at den gir tilstrekkelige hjemler til at det rent faktisk blir mulig å få tilgang til kommunikasjonen på samme måte som ved for eksempel tradisjonell avlytting av telefonsamtaler. Hva som kreves for å gjennomføre dette i praksis er et utpreget teknisk spørsmål og en viser her til høringsuttalelsen fra Kripos. Det kan formentlig være hensiktsmessig om departementet i det videre arbeid med spørsmålet orienterer seg noe nærmere om de tekniske muligheter og begrensninger.

Riksadvokaten har som det fremgår av utredningen tilrådd at hemmelig ransaking og beslag kan gjennomføres uten fysisk tilstedeværelse. Utvalget må forstås slik at det slutter seg til dette på side 246 første spalte og særlig tydelig i sammendraget (side 27). Det er formentlig tilstrekkelig at dette uttales klart i lovforarbeidene uten at det nedfelles i en egen bestemmelse.»

NAST har som nevnt ovenfor under punkt 14.7.1 pekt på at lovens skille mellom hemmelig ransaking og kommunikasjonskontroll er en svakhet, den teknologiske utviklingen tatt i betraktning. Det vises til at ransaking tradisjonelt har vært knyttet til fysiske rom og personer, mens kommunikasjonskontroll gjelder elektronisk kommunikasjon. NAST konstaterer derfor at opplysningsgrunnlaget er «artsforskjellig, nemlig fysiske objekter vs. elektroniske data». Videre pekes det på at det lenge har vært klart at også datasystemer kan være gjenstand for ransaking, og at opplysningsgrunnlaget da er av samme art som ved kommunikasjonskontroll, nemlig elektroniske data. Forskjellen er ifølge NAST bare at ved kommunikasjonskontroll er dataene under overføring, mens ved ransaking er de lagret. I begge tilfeller er opplysningsverdien avhengig av at dataene er tilgjengelige i klartekst – altså at dataene er dekryptert eller i utgangspunktet ukryptert. NAST konstaterer derfor at «teknologiutviklingen har ledet til at ransaking og kommunikasjonskontroll kan rette seg mot samme type objekt (elektroniske data), og kan stå overfor samme utnyttelsesproblem på grunn av kryptering».

Videre gir NAST uttrykk for at «[n]este aspekt av problemet er den rettslige definisjonen av objektet for kommunikasjonskontroll, nemlig «samtaler eller annen kommunikasjon til og fra bestemte telefoner, datamaskiner eller andre anlegg for elektroniske kommunikasjon», jf. strpl. § 216a tredje ledd. I korthet er det tale om elektronisk kommunikasjon, dvs, data under overføring». NAST viser til at definisjonen er bygd ut «i takt med ekomlovgivningen», men at kommunikasjonskontroll opprinnelig gjaldt avlytting av samtaler mellom to forskjellige samtaleparter – noe som «fulgte med nødvendighet av det gamle fasttelefonisystemet». De strenge vilkårene for kommunikasjonskontroll «reflekterte følgelig det fundamentale vernet om kommunikasjonsfortroligheten, ikke bare for siktede, men også for den annen part i kommunikasjonen». Etter NASTs oppfatning har teknologiutviklingen ledet til at den tradisjonelle forutsetningen om at kommunikasjonen går mellom forskjellige parter ikke kan opprettholdes bare fordi datastrømmen går mellom forskjellige kommunikasjonsanlegg. Årsaken er ifølge NAST at «datastrømmen like gjerne kan skyldes personens kontakt med egne data som er lagret på en server i «internettskyen», og at det dermed er et «annet aspekt av privatlivets fred enn kommunikasjonsfortroligheten» som berøres.

NAST mener at områdene for kommunikasjonskontroll og ransaking er i ferd med å gli over i hverandre, «også fordi det ikke lenger kan legges til grunn at data ikke er *vernet* av kommunikasjonsfortroligheten, bare fordi de er *lagret*». Som et «velkjent eksempel fra praksis» trekker NAST

frem kriminelles bruk av en e-postkonto til å skrive beskjeder til hverandre uten at meldingene sendes. Hver deltaker logger seg inn med brukernavn og passord, og leser de lagrete meldingene. Det er ifølge NAST ikke tvilsomt at informasjonsoverføringen representerer kommunikasjon, men metoden som står til rådighet er likevel ikke kommunikasjonskontroll, men derimot ransaking, eller utleveringspålegg overfor tilbyder. Videre uttaler NAST:

> «Slik utviklingen går, er det naturlig å anse stadig mer av datamengden som kommunikasjon, fordi informasjonen forvaltes i nettverk. For eksempel er det vanlig å forvalte sin informasjon via servere utenfor sin egen personlige datamaskin (kommunikasjonsanlegg). Man er heller ikke avhengig av å disponere en egen datamaskin, fordi informasjonen kan lagres, hentes og spres via servere i «internettskyen» ved bruk av offentlige terminaler, for eksempel på internettkafe eller bibliotek. Videre blir lagrete data ofte (videre)sendt, for eksempel som vedlegg til epost, og representerer derfor kommunikasjon.
>
> Det er neppe gitt hva som er hensiktsmessig eller korrekt metodebruk, kommunikasjonskontroll eller hemmelig ransaking, og politiet vil ende opp med å begjære begge deler for å være på den sikre siden. Kommunikasjonskontroll kan imidlertid være «feil» tvangsmiddel dersom det gjelder en forutsetning om forskjellige samtaleparter. Ransaking er på den annen side utilstrekkelig dersom det ikke er adgang til *regelmessig nedlasting* fra brukerkontoen, slik at politiet kan følge med på informasjonsutvekslingen. Så vidt forstås er gjeldende lære at ransakingsbestemmelsen i strpl. 200a ikke gir adgang fil dette. Tolkningen følger ikke eksplisitt av ordlyden, men viser vel at konseptet «ransaking» er forankret i åpen metodebruk i det fysiske rom. I slike tilfeller har det ikke vært behov for ransaking flere ganger under samme tillatelse, fordi siktede alt første gang ble gjort oppmerksom på etterforskingsskrittet og har kunnet innrette seg deretter. Men ved hemmelig metodebruk er gjentatt ransaking hensiktsmessig, *både* for fysiske og virtuelle rom.»

NAST mener at teknologiutviklingen har ledet til at «et rettslig skille mellom lagrede data og data under overføring blir kunstig», og at lovgiver derfor bør vurdere å lage én dekkende regel for hemmelig tilgang til elektroniske data.

Videre gjør NAST gjeldende at det bør være adgang til gjentatt ransaking – både fysisk og virtuelt. Om dette uttaler NAST at «[s]elv om det ikke kan ses at ordlyden i gjeldende ransakingsregler er til hinder for hemmelig gjentatt ransaking, fysisk og virtuelt, hersker det en usikkerhet som påkaller behov for rettslig avklaring». I tillegg peker NAST på at ransaking av virtuelle rom innebærer bruk av dataprogram – altså en automatisert ransakingsprosess – hvilket i seg selv tilsier at det bør være adgang til gjentatt automatisert ransaking.

Enn videre mener NAST at det er behov for dataavlesing som selvstendig metode, for å utnytte automatiske metoder for å kopiere lagret innhold og rapportere om bruk av datamaskinen (tastetrykk), samt å kopiere trafikk mellom kommunikasjonsanlegg – altså en form for fortløpende ransaking.

Telemark politidistrikt mener også at gjentatt ransaking under én beslutning bør tillates. Distriktet uttaler følgende:

> «Utvalget vil ikke foreslå en adgang til fortløpende eller gjentatt ransaking av kommunikasjonsanlegg. Påtalemyndigheten må etter utvalgets forslag be om rettens kjennelse for hver ny ransaking. Argumentet er hovedsakelig at en slik adgang vil innebære en for stor integritetskrenkelse. Det er etter mitt skjønn vanskelig å se den prinsipielle forskjellen mellom en rettslig kjennelse for hemmelig ransaking av et dataanlegg i en periode, eller flere kjennelser om det samme i den samme perioden. I de saker hvor slik hemmelig ransaking vil være mest aktuelt, vil det kunne være en slik overvåking over tid som er relevant for etterforskningen. Flere av de andre skjulte etterforskningsmetodene brukes over til dels lang tid for å avdekke kriminelle nettverk og de ulike aktørenes roller.»

Oslo statsadvokatembeter mener derimot at gjentatte ransakinger under én beslutning ikke bør tillates, fordi det «i prinsippet [ville] åpne for en sammenhengende «overvåkning» av datamaskinene».

14.7.4 Gjennomføringen av dataavlesing

Forsvarergruppen av 1977 viser til at utvalget har konstatert at det neppe er til å unngå at gjennomføringen av dataavlesing vil kunne fange opplysninger som ikke var ment kommunisert, og at det derfor er viktig at dataavlesingen innrettes slik at

det ikke fanges opp opplysninger ut over det som er nødvendig for å gjennomføre kommunikasjonsavlytting eller ransaking. Forsvarergruppen uttaler under henvisning til dette:

> «På denne bakgrunn mener Forsvarergruppen at, dersom forslaget vedtas, departementet umiddelbart bør igangsette et arbeid for å utarbeide datafaglige/tekniske retningslinjer ift hvordan slik dataavlesning skal innrettes, med klare føringer om å sikre å motvirke at dataavlesning får slike konsekvenser som beskrevet. At for eksempel nedtegnelser av private tanker, fantasier eller lignende som mistenkte (eller tredjepersoner) aldri har ment satt ut i livet/kommunisert eller lignende, skal komme i hende på politiet, og i verste fall bli misbrukt, finner Forsvarergruppen at vil representere en så alvorlig krenkelse at kostnadene ved dette virkemiddelet vil overstige gevinsten ved det, jfr også sensitivitetsprinsippet og kravet om formålsbestemthet (utredningens kap. 6).»

Oslo statsadvokatembeter peker på at det er liten grunn til å tro at politiet vil anvende hardwarebaserte fremgangsmåter i særlig utstrekning, fordi disse «i de fleste tilfeller vil være operativt vanskelige». Videre uttales det at en «softwareløsning vil være vesentlig enklere å anvende», men at «behovet for kontroll og etterprøvbarhet er størst ved anvendelse av denne fremgangsmåten samtidig som den er vanskelig å få gjennomført».

14.7.4.1 Kontrollen med inngrepet

Kripos viser til utvalgets uttalelser om at kravet til rettssikkerhet medfører at det må stilles krav til kontrollsystemer for bruken av dataavlesing, og sier seg enig i dette. Videre uttaler Kripos at innføring av dataavlesing «stiller krav til at omfang og gjennomføringsmåte må dokumenteres», og at det er hensiktsmessig å regulere dette i egne retningslinjer eller i forskrift.

Forsvarergruppen av 1977 gir sin «ubetingede støtte» til utvalgets forslag om at reglene skal evalueres, og til å gi lovendringen en bestemt virkeperiode «for å sikre at slik evaluering faktisk finner sted».

Oslo statsadvokatembeter peker på at dataavlesing som fremgangsmåte «gir en betydelig mengde overskuddsinformasjon», og uttaler:

> «Dette kan gjelde personlige forhold, men også knyttet til den enkeltes økonomiske forhold. Politiet vil ved anvendelse av metoden få tilgang til den enkeltes passord ved utførelse av banktjenester, varekjøp m.v., og passord som anvendes i forhold til det offentlige og dets tjenester. Videre må det fremheves at metoden ikke gir en særlig god notoritet som kan sikre mot misbruk. Rett nok har utvalget skissert på en detaljert liste tiltak som kan sikre notoritet på oppkopling og avkopling, men det bør understrekes at det kan være van[s]kelig å sikre notoritet og kontroll på det materialet som innhentes. Det må i den forbindelse understrekes at datamaskiner kan inneholde en stor mengde tekst og bilde/filmateriale og at gjennomgangen og kontrollen kan være svært ressurskrevende.
>
> Politiet må i alle tilfelle registrere og dokumentføre det materialet som lastes ned. Dette gjelder også selv om materialet bedømmes som irrelevant av politiet. En sletting i en tidlig fase vil alltid åpne for påstander fra forsvareren om at politiet har slettet materiale som taler til fordel for siktede. En nøyaktig registrering av nedlastet materiale vil åpenbart kunne bli ressurskrevende for politiet.»

Videre gir Oslo statsadvokatembeter uttrykk for at innføringen av dataavlesing som gjennomføringsmåte bør forutsette at man kan «etablere tilfredsstillende kontrollsystemer som sikrer mot misbruk eller påstander mot misbruk». Dette kan «være av avgjørende betydning for å gi «legitimitet» for de regler som innføres». Oslo statsadvokatembeter understreker «at man i prinsippet gir politiet tilgang til samtlige datamaskiner som befinner seg i Norge og i en viss utstrekning utenfor landets grenser», og uttaler videre at dette «innebærer at den innebyggede kontrollmekanisme som fordrer fysisk medvirkning fra utenforstående (teleselskaper/internettleverandører) blir delvis borte». Oslo statsadvokatembeter mener at det «åpenbart [er] av sentral betydning» at eventuelle nye regler om utsatt underretning også blir vurdert i denne sammenheng.

14.8 Departementets vurderinger

14.8.1 Grunnleggende forutsetninger for departementets vurderinger

Politiets adgang til skjult tvangsmiddelbruk skal ikke være videre enn det som er nødvendig for å møte behovet for effektiv kriminalitetsbekjempelse. Det er heller ikke gitt at politiet skal ha

anledning til å benytte metoder som i art og omfang er så vidtfavnende at de dekker behovet fullt ut. I denne sammenheng legger departementet særlig vekt på at bruken av tvangsmidler ikke bare kan utgjøre inngrep overfor mistenkte, men også tredjepersoner som på ulike måter kan bli berørt av metodebruken. Selv om utvidelser av tvangsmiddelhjemlene eller innføring av nye tvangsmidler kan gi en stor samfunnsmessig gevinst i form av mer effektiv kriminalitetsbekjempelse, er det ikke grunnlag for å foreslå utvidelser som kan virke uforholdsmessig inngripende overfor mistenkte eller tredjepersoner. Et avgjørende moment i denne vurderingen vil være om behovet for effektiv kriminalitetsbekjempelse kan tilfredsstilles med mindre inngripende midler.

Videre er det avgjørende at eventuelle utvidelser innrettes slik at den enkeltes krav på materiell og prosessuell rettssikkerhet ivaretas. Inngrep skal bare kunne skje med grunnlag i tilstrekkelig klar lovhjemmel og på vilkår som sikrer at inngrepet ikke går ut over det som er nødvendig for å tjene det forhåndsbestemte formålet, altså kriminalitetsbekjempelse. Inngrepshjemlene må ledsages av objektive kontrollmekanismer for å hindre at noen utsettes for uforholdsmessig eller unødvendig belastning som følge av tvangsmiddelbruken og for å hindre misbruk av tvangsmiddeladgangen. I denne sammenheng er det etter departementets oppfatning vesentlig at bruken av skjulte tvangsmidler som hovedregel skjer med grunnlag i en forutgående tillatelse fra retten. I tilfeller hvor det er aktuelt å gi påtalemyndigheten hastekompetanse til å beslutte at inngrep skal foretas, må det skje en etterfølgende domstolskontroll.

Bruken av skjulte tvangsmidler innebærer også at den inngrepet rettes mot først i ettertid, og i noen tilfeller heller ikke da, får vite om at det er benyttet tvangsmidler. Det er derfor nødvendig å sørge for at mistenktes interesser ivaretas av andre. Departementet peker i denne forbindelse særlig på bestemmelsen i straffeprosessloven § 100 a om oppnevning av offentlig advokat for mistenkte ved behandlingen av saker om bruk av skjulte tvangsmidler. I tillegg mener departementet at det er nødvendig å sørge for at egnede kontrollorganer fører et mer helhetlig tilsyn med bruken av skjulte tvangsmidler, slik kontrollutvalget for kommunikasjonskontroll og EOS-utvalget gjør. For departementet er det en forutsetning at også bruken av eventuelle nye skjulte tvangsmidler underkastes et tilsvarende kontrollregime.

14.8.2 Behovet for dataavlesing – tradisjonelle tvangsmidler og ny teknologi

Både Metodekontrollutvalget og flere av høringsinstansene har pekt på den raske teknologiske utviklingen i samfunnet. Moderne løsninger for elektronisk behandling og formidling av informasjon legger til rette for effektiv kommunikasjon og stor bevegelsesfrihet. Departementet ser også at det er en økende bevissthet om viktigheten av informasjonsbeskyttelse i samfunnet generelt, og allmenhetens kunnskaper om – og evne til – slik beskyttelse virker å være større enn tidligere. Etterspørselen etter løsninger som verner mot at utenforstående skaffer seg uberettiget tilgang til informasjon som bearbeides og kommuniseres med elektroniske hjelpemidler, synes å være stor. En rekke av de løsningene som er i utbredt bruk i dag leveres med sterk informasjonsbeskyttelse som «standardoppsett». Først og fremst er det tale om *kryptering*. Det vil si at brukeren av informasjonsbærende utstyr produserer eller bearbeider informasjonen «åpent», men at den sendes eller lagres kryptert. Krypteringen kan skje ved at brukeren aktivt benytter krypteringsprogrammer og «lukker» informasjonen når den overføres eller lagres, eller ved automatisk kryptering gjennom løsninger som tjenesteleverandøren har implementert. Det sistnevnte skjer uten at den enkelte bruker tar et bevisst valg om å kryptere.

Bedre informasjonsbeskyttelse er en fordel, så lenge beskyttelsen har som formål å verne lovlig aktivitet. Beskyttelsesmulighetene kan imidlertid også benyttes for å hindre utenforstående innsyn i informasjon og kommunikasjon som gjelder kriminelle handlinger. Kriminelle miljøer vil ofte ha kunnskap om politiets arbeidsmetoder, og kan ha både vilje og betydelig evne til å benytte tilgjengelige teknologiske løsninger for å skjule informasjon som knytter seg til den kriminelle virksomheten. Høy informasjonsteknologisk kompetanse er heller ingen absolutt forutsetning i så måte. Kriminelle kan på lik linje med andre benytte seg av kommersielle standardløsninger for kryptering av kommunikasjon og lagret informasjon.

Fremveksten av krypteringsløsninger og andre metoder for informasjonsbeskyttelse fører utvilsomt til utfordringer for politiet. I forbindelse med forebygging, avverging og etterforskning av alvorlig kriminalitet, kan politiet ha behov for å skaffe seg tilgang til kommunikasjon eller informasjon som finnes lagret i elektronisk utrustning som disponeres av mistenkte, uten den mistenktes viten. Etter departementets oppfatning viser utredningen og høringen at de eksisterende

skjulte tvangsmidlene har tapt mye av sin effekt som følge av den teknologiske utviklingen, herunder fremveksten av ulike løsninger for informasjonsbeskyttelse. Adgangen til meningsinnholdet i informasjonen er rettslig sett uendret, men i praksis vanskeliggjort.

Kommersielle krypteringsløsninger baseres på svært komplekse krypteringsalgoritmer. Forsøk på å «knekke» kryptering krever meget store ressurser i form av tid, datakraft og kompetanse, og det er beskjedne utsikter til å lykkes. Det synes ikke å være en praktisk gjennomførbar løsning for politiets utfordringer per i dag. I utgangspunktet er politiet derfor avhengig av å kunne tilegne seg den aktuelle informasjonen «i klartekst» på annen måte. I noen tilfeller kan det være mulig å skaffe seg tilgang til kryptert informasjon gjennom innhenting og bruk av passordene eller kodene som brukes som krypteringsnøkler. Det forutsetter at politiet får tak i disse opplysningene gjennom annen metodebruk, eller at mistenkte eller andre oppgir disse til politiet. Kjennskap til passord og lignende vil imidlertid i mange tilfeller være utilstrekkelig. Flere av høringsinstansene har påpekt at krypteringsnøklene, som beskytter informasjonen, som regel er flyktige, og at det nettopp ikke er snakk om et fast brukernavn eller passord. De har gitt uttrykk for at det derfor er behov for å gi politiet tilgang til informasjonen når den ligger åpen – for eksempel når en mistenkt har åpnet et tekstdokument for behandling på sin datamaskin, eller når lyden fra en ip-basert telefonsamtale overføres fra mikrofonen eller til høyttaleren på mistenktes smarttelefon eller datamaskin.

Et annet sentralt trekk ved utviklingen innen elektronisk kommunikasjon synes å være at det i stadig større utstrekning benyttes kommunikasjonstjenester som ikke er bundet til et bestemt kommunikasjonsanlegg eller en bestemt nettverksforbindelse, men derimot til en *virtuell brukerkonto* som innehaveren med et brukernavn og passord, og eventuelt tilpasset programvare, kan benytte fra en rekke plattformer – for eksempel smarttelefoner, nettbrett og bærbare datamaskiner. Disse enhetene er mobile og kan benytte flere typer av både faste og trådløse nettverksforbindelser. Spekteret av tilgjengelige kommunikasjonstjenester er vidt, og én og samme tjeneste kan gi tilgang til mange varianter av nettverksbasert kommunikasjon. Ett eksempel er *Skype*, hvor en bruker blant annet kan føre telefonsamtaler, også gruppesamtaler (ringe til andre skype-brukere gjennom ip-telefoni, ringe til mobiltelefoner og fasttelefoner), føre videosamtaler med én person eller en gruppe, sende og motta videobeskjeder, direktemeldinger («chat»), tekstmeldinger (SMS) og dele filer og skjermbilder.

I den straffeprosessuelle reguleringen av skjulte tvangsmidler går det et skille mellom informasjon som er lagret, og informasjon som overføres mellom en avsender og en mottaker. Ransaking og beslag, eventuelt utleveringspålegg, må benyttes for tilgang til elektronisk lagret informasjon, mens kommunikasjonsavlytting er det tilgjengelige tvangsmiddelet for å fange opp informasjon under overføring mellom ulike kommunikasjonsanlegg. Dette skillet settes på prøve av fleksible løsninger for elektronisk informasjonshåndtering. Disse tjenestene fungerer naturligvis ubundet av den straffeprosessuelle sondringen mellom kommunikasjon og lagret informasjon.

Utfordringene blir etter departementets oppfatning særlig tydelige når en ser på bruken av for eksempel internettbaserte e-post- og fildelingstjenester. Tjenestene åpner for at flere – ved å dele tilgangen til én og samme brukerkonto – kan gå sammen om å opprette, lese og redigere dokumenter eller andre filtyper som lagres på tjenestetilbydernes servere, uten at informasjonen utveksles direkte mellom de involvertes kommunikasjonsanlegg. Et kjent eksempel, som flere av høringsinstansene har pekt på, er kriminelle som fra hver sine kommunikasjonsanlegg «logger seg på» samme e-postkonto for å utveksle informasjon. Informasjonen blir da ikke sendt mellom ulike e-postadresser. Dette er utvilsomt en form for kommunikasjon, i hvert fall i faktisk forstand, men det er likevel ikke gitt at kommunikasjonsavlytting etter straffeprosessloven § 216 a gir tilgang til informasjonen som utveksles.

Bestemmelsen om kommunikasjonsavlytting gir riktignok adgang til å avlytte signalstrømmen mellom den enkelte brukers kommunikasjonsanlegg og tjenesteleverandørens kommunikasjonsanlegg, men dette vil normalt ikke gi et fullstendig bilde av informasjonen som utveksles mellom de involverte personene. I tillegg kommer det at den enkelte brukers kontakt med brukerkontoen ikke er bundet til et bestemt kommunikasjonsanlegg. Brukeren kan benytte ulike enheter, som nettbrett, datamaskin og smarttelefon, og veksle mellom flere internettforbindelser, for eksempel offentlig tilgjengelige trådløse nettverk på ulike steder. I denne sammenheng er det også av betydning at meningsinnholdet i informasjonen som utveksles, ofte er gjort utilgjengelig for utenforstående gjennom krypteringsløsninger som beskytter informasjonen når den er under overføring. Det vil derfor uansett kunne være svært vanskelig å gjennomføre effektiv kommunikasjonsavlytting.

Politiet kan eventuelt anvende tvangsmidlene skjult ransaking og beslag for å tilegne seg elektronisk lagret informasjon knyttet til en e-postkonto eller tilsvarende, for på den måten å danne seg et bilde av informasjonsutvekslingen mellom de involverte. Ransakinger forutsettes imidlertid gjennomført som enkeltstående handlinger. Politiet skaffer seg tilgang (hvilket kan være en stor praktisk utfordring), gjennomsøker objektet for ransakingen og beslaglegger eventuell informasjon som kan ha betydning som bevis, og trekker seg deretter ut. En ransakingstillatelse gir derimot ikke adgang til å overvåke ransakingsobjektet (for eksempel forbli pålogget på en e-postkonto eller datamaskin) over tid for å fange opp ny aktivitet eller ny informasjon som produseres fortløpende av mistenkte eller andre. Selv om det hyppig begjæres og gjennomføres nye ransakinger av samme objekt, vil hver enkelt ransaking bare gi øyeblikksbilder, og ikke nødvendigvis noen tilfredsstillende oversikt over den informasjonsutvekslingen som faktisk finner sted mellom de involverte. Mellom hver ransaking kan ny informasjon ha blitt tilført og slettet.

Metodekontrollutvalget har konstatert at det ikke har vært mulig «å tallfeste behovet for dataavlesing». Departementet ser heller ikke at det er mulig å foreta noen slik tallfesting. Utredningen og høringen viser likevel et klart behov for å supplere bestemmelsene om kommunikasjonsavlytting og hemmelig ransaking, med bestemmelser som er bedre tilpasset det rådende teknologiske virkelighetsbildet. Dette behovet er etter departementets oppfatning enda sterkere i dag enn da Metodekontrollutvalget presenterte sin utredning. Det er nødvendig med endringer for å gjenopprette den effekten disse metodene hadde tidligere, men også for å gjøre politiet bedre rustet til å møte de utfordringene den teknologiske utviklingen kan forventes å gi fremover i tid.

De utfordringene som kryptering og mobilitet skaper for politiets faktiske informasjonstilgang ved kommunikasjonsavlytting, kan etter departementets oppfatning forsøkes møtt med å legge til rette for å flytte «avlyttingspunktet» tettere på den mistenkte – inn i det kommunikasjonsanlegget mistenkte benytter seg av. Det gir rom for å fange opp innholdet i kommunikasjonen når den ligger åpen (ukryptert) i mistenktes anlegg. Bruk av spesiell programvare kan for eksempel legge til rette for at politiet tar del i de ukrypterte lydsignalene fra en ip-basert telefonsamtale før de krypteres på vei ut på linjen, og dekryptert etter at de har kommet inn fra linjen. Slike fremgangsmåter kan også legge til rette for mer målrettet avlytting, hvor faren for å fange opp utenforståendes kommunikasjon reduseres. Politiet bør også få anledning til å benytte nye fremgangsmåter for å møte utfordringene som kryptering og andre beskyttelsestiltak skaper for tilgangen til annen elektronisk fremstilt og lagret informasjon. Departementet viser i denne sammenheng til uttalelsene fra flere av høringsinstansene innen politiet og påtalemyndigheten, hvor det gis uttrykk for at hjemlene for skjult ransaking og beslag ikke holder tritt med den teknologiske utviklingen.

I det følgende vurderer departementet om behovet bør dekkes ved å endre de eksisterende hjemlene for kommunikasjonsavlytting og skjult ransaking, eller ved å innføre et nytt, selvstendig tvangsmiddel.

14.8.3 Dataavlesing som gjennomføringsmåte for kommunikasjonsavlytting og hemmelig ransaking

Metodekontrollutvalget har foreslått at dataavlesing skal kunne benyttes for å gjennomføre kommunikasjonsavlytting etter straffeprosessloven § 216 a og hemmelig ransaking av datasystemer etter § 200 a.

For kommunikasjonsavlytting har utvalget foreslått et nytt fjerde ledd i § 216 a. Etter forslaget skal retten kunne gi politiet tillatelse til «å foreta innbrudd i et datasystem for å kunne gjennomføre kommunikasjonsavlyttingen», dersom denne er vanskeliggjort på grunn av teknologiske eller andre innretninger. Kommunikasjonsavlyttingen kan tenkes gjennomført ved bruk av programvarebaserte løsninger, der det installeres et program i mistenktes kommunikasjonsanlegg som gjør politiet i stand til å hente ut informasjonen mens denne er tilgjengelig i ukryptert form. Denne og andre varianter kan etter departementets oppfatning innebære en viss forskyvning av avlyttingspunktet sammenlignet med «tradisjonell» kommunikasjonsavlytting, siden det kan være aktuelt å fange opp for eksempel lydstrømmen i en ip-telefonsamtale når den passerer mellom mikrofon og operativsystemets drivere, og mellom operativsystemets drivere og høyttaler på en datamaskin.

For hemmelig ransaking har utvalget foreslått en tilføyelse i § 200 a første ledd om at retten skal kunne gi politiet tillatelse til «samtidig eller senere å foreta innbrudd i et datasystem for å kunne gjennomføre ransaking etter bestemmelsen her».

Utvalget har lagt til grunn at det ikke er hensiktsmessig eller mulig å beskrive gjennomføringsmåten i detalj, verken i forbindelse med

kommunikasjonsavlytting eller hemmelig ransaking og beslag. Det har pekt på at «de tekniske mulighetene er mange og forskjelligartede», og at «den teknologiske utviklingen formodentlig vil innebære at en slik beskrivelse raskt blir utdatert» (utredningen punkt 23.3.5 side 247). Utvalget ser for seg at politiet blant annet skal kunne installere programvare i mistenktes datamaskin som gjør politiet i stand til å hente ut informasjon fra datasystemet, og at dette kan gjøres ved å utnytte sikkerhetshull i datasystemet, sende programmet som skjult vedlegg til e-post, eller installere programmet i forbindelse med en hemmelig ransaking «eller etter å ha utført innbrudd i datasystemet». Utvalget har også pekt på muligheten for å bruke maskinvarebaserte løsninger, der det fysisk installeres komponenter på mistenktes datamaskin som gjør politiet i stand til å skaffe seg informasjon. Som eksempel på dette nevnes utstyr for tastetrykksregistrering og oppfanging av lydsignaler ved kommunikasjon over internett.

Departementet er enig i at det bør tas høyde for nye teknologiske løsninger og ser også teknologinøytrale beskrivelser som en fordel. Spekteret av fremgangsmåter som utvalget vil tillate, synes imidlertid å være mer vidtfavnende enn det som faller naturlig inn under den foreslåtte formuleringen «innbrudd i et datasystem». Utvalgets forslag til lovtekst kan derfor etterlate en viss usikkerhet om yttergrensene for fremgangsmåtene politiet skal kunne benytte. Dette gjelder særlig for den tiltenkte adgangen til å installere og benytte program- og maskinvare i datasystemet. Med tanke på ransaking er det også grunn til å peke på straffeprosessloven § 200 annet ledd siste punktum, hvor det er bestemt at det «kan åpnes adgang med makt» dersom det er nødvendig for å gjennomføre ransaking. Bestemmelsen gjelder både åpen og skjult ransaking, og den er åpenbart utformet med ransaking av fysiske rom for øye. Det samme gjelder ransakingsbestemmelsene for øvrig, men det legges like fullt til grunn at de også hjemler både åpen og skjult *elektronisk* ransaking. Det kan derfor være rimelig å hevde at også straffeprosessloven § 200 annet ledd siste punktum er anvendelig ved elektronisk ransaking, og følgelig allerede gir politiet hjemmel for å bryte beskyttelse i datasystemer i den utstrekning det er nødvendig for å gjennomføre ransaking av disse. Likevel er det etter departementets vurdering behov for en tydeligere hjemmel for å gjøre innbrudd i datasystemer i forbindelse med skjult ransaking, både med hensyn til slike fremgangsmåter som allerede er hjemlet i straffeprosessloven og eventuelle utvidelser.

Utvalget har ikke funnet grunnlag for å innføre dataavlesing som nytt selvstendig tvangsmiddel, fordi det «finner […] at det ikke er dokumentert et tilstrekkelig behov» for dette (utredningen punkt 23.3.1 side 244). Det er presisert at forslagene innebærer at dataavlesing bare skal kunne benyttes i den utstrekning det er nødvendig for å kunne gjennomføre henholdsvis kommunikasjonsavlytting og hemmelig ransaking, og at bruken for øvrig må skje innenfor rammene av de respektive tvangsmiddelhjemlene. Samtidig pekes det på følgende (utredningen punkt 23.3.5 side 248):

> «Det er neppe til å unngå at gjennomføringen av dataavlesingen vil kunne fange opp opplysninger som ikke var ment kommunisert eller lagret, og som dermed ikke ville blitt fanget opp ved tradisjonell kommunikasjonsavlytting eller hemmelig ransaking og beslag. For eksempel vil såkalt key-logging, altså det at tastetrykkene på et tastatur registreres, ikke kunne skje uten en viss usikkerhet knyttet til om opplysningene ellers ville kunne fanges opp ved de eksisterende metoder. I så fall vil innføring av dataavlesing som gjennomføringsmåte slik utvalget foreslår også kunne innebære en utvidelse av eksisterende hjemler. Utvalget presiserer derfor at dataavlesingen må innrettes slik at det ikke fanges opp opplysninger ut over det som er nødvendig for å kunne gjennomføre en kommunikasjonsavlytting eller en hemmelig ransaking og beslag. Dersom det er nødvendig for politiet å skaffe seg mistenktes oppstartspassord til et datasystem, må gjennomføringen av eventuell key-logging innrettes slik at det er tastetrykkene i oppstartsfasen som registreres, ikke en fortløpende registrering av alle tastetrykk over en lengre periode som derved gir informasjon ut over det som er nødvendig.»

Så vidt departementet kan se, tar utvalget med forslagene sikte på å overvinne krypteringsproblemet ved henholdsvis kommunikasjonsavlytting og hemmelig ransaking og beslag. Innføringen av dataavlesing som gjennomføringsmåte innenfor rammene av de eksisterende tvangsmiddelhjemlene, og med de begrensningene som er gjengitt ovenfor, medfører at det trekkes opp et tydelig skille med hensyn til hvilken type informasjon som kan innhentes gjennom dataavlesingen, avhengig av om den i det enkelte tilfelle hjemles i straffeprosessloven §§ 216 a eller 200 a. Dersom dataavlesingen skjer for å gjennomføre kommuni-

kasjonsavlytting, kan politiet etter forslaget fange opp kommunikasjonen før den krypteres eller etter at den er dekryptert. Utvalget forutsetter også at politiet skal kunne fange opp krypteringsnøkler som så benyttes for å dekryptere kommunikasjonen i transportfasen. Derimot gir en tillatelse til å benytte dataavlesing for å gjennomføre kommunikasjonsavlytting ikke anledning til å fange opp annen informasjon, som for eksempel krypteringsnøkler som kan være nødvendige for en senere ransaking og dekryptering av *lagret* informasjon.

Når det gjelder hemmelig ransaking, skal dataavlesing ifølge utvalget kunne benyttes for å gjennomføre dette uten fysisk tilstedeværelse, for eksempel over internett. Forslaget innebærer at politiet skal kunne benytte dataavlesing for å skaffe seg tilgang til det datasystemet som skal ransakes. Utvalget forutsetter imidlertid også at politiet skal ha anledning til å fange opp krypteringsnøkler som er nødvendige for å dekryptere lagret informasjon, for eksempel ved bruk av tastetrykksavleser eller tilsvarende. Selv om utvalget presiserer at det ikke skal være anledning til å følge med på annen aktivitet, eller fange opp annen informasjon, forutsetter dette en viss overvåking av den fortløpende bruken av datasystemet. Samtidig mener utvalget at det ikke bør gis tillatelse til gjentatt eller fortløpende hemmelig ransaking, fordi det ville «innebære en klar utvidelse» sammenlignet med dagens ransakingsregler, og «fordi det vil gi politiet anledning til systematisk å kartlegge mistenktes bruk av et datasystem over tid, herunder opplysninger som ikke blir lagret i datasystemet og dermed ikke vil kunne hentes ut ved tradisjonell hemmelig ransaking». Etter utvalgets syn ville det innebære «en for stor integritetskrenkelse i forhold til det anførte behovet» (utredningen punkt 23.3.3 side 246).

Ransaking, herunder hemmelig ransaking etter straffeprosessloven § 200 a, forutsettes etter gjeldende rett utført som en enkeltstående og tidsmessig avgrenset handling. Når politiet har skaffet seg adgang til objektet og innledet ransakingen, skal inngrepet avsluttes så snart objektet er gjennomsøkt. Ransakingsbestemmelsene gir ikke anledning til vedvarende overvåking fremover i tid. Etter departementets oppfatning står utvalgets forslag om å tillate fortløpende overvåking av datasystemet for å fange opp tilgangskoder mv. (for å kunne gjennomføre ransaking) i et motsetningsforhold til utvalgets forutsetning om hemmelig ransaking som en enkeltstående handling.

Utvalgets forslag angir ikke hvor lenge politiet skal ha anledning til å følge med på datasystemet for å fange opp tilgangskoder mv. i forbindelse med hemmelig ransaking. Ved kommunikasjonsavlytting følger det av straffeprosessloven § 216 f første ledd første punktum at retten kan gi tillatelse for inntil 4 uker om gangen. Rettens angivelse av tidsperiode vil dermed også være bestemmende for hvor lenge dataavlesingen kan foregå. Avlyttingen skal også stanses før utløpet av fristen dersom vilkårene for avlytting ikke lenger antas å være til stede, eller dersom kontroll ikke lenger anses hensiktsmessig, jf. § 216 f annet ledd. Ved hemmelig ransaking gir rettens tillatelse ingen tilsvarende angivelse av hvilken tidsperiode ransakingen skal kunne strekke seg over. Følgelig vil det etter utvalgets forslag ikke gjelde noen uttrykkelig begrensning med hensyn til hvor lenge politiet skal kunne overvåke et datasystem for å fange opp tilgangskoder mv. som er nødvendige for å gjennomføre ransaking. De alminnelige begrensningene i straffeprosessloven § 170 a, at et tvangsmiddel bare kan brukes når det er tilstrekkelig grunn til det og det ikke ville virke uforholdsmessig, gjelder likevel. Politiet vil i så måte uansett ha plikt til å avslutte dataavlesingen dersom det ikke lenger er behov for den, eller dersom den har pågått så lenge at en fortsettelse ville virke uforholdsmessig inngripende. Etter departementets oppfatning medfører utvalgets forslag likevel en usikkerhet som kan være problematisk sett hen til kravet om tilstrekkelig klar lovhjemmel. Videre kan fraværet av en uttrykkelig tidsbegrensning gjøre det vanskelig for retten å foreta en reell forholdsmessighetsvurdering når en begjæring om hemmelig ransaking ved hjelp av dataavlesing skal vurderes.

Flere av høringsinstansene har dessuten tatt til orde for at skjult elektronisk ransaking bør tillates gjennomført fortløpende over tid. I denne sammenheng pekes det blant annet på at kriminelle bruker skylagringstjenester og e-postkontoer for å kommunisere i forbindelse med sin virksomhet, jf. også omtalen av dette ovenfor. Dette er en form for kommunikasjon som politiet ikke får tilfredsstillende tilgang til i medhold av bestemmelsene om kommunikasjonsavlytting. De aktuelle objektene kan riktignok ransakes, men det vil være mer eller mindre tilfeldig om informasjonen fortsatt er tilgjengelig på tidspunktet for ransakingen. Det pekes på lignende utfordringer ved ransaking av for eksempel en datamaskin. Informasjon kan være slettet på tidspunktet for ransakingen, eller mistenkte kan ha beskyttet lagret innhold med kryptering eller ikke lagret informasjonen i det hele tatt («flyktige data»). Ifølge Kripos vil det i mange tilfeller være avgjørende å kunne slå til

mens informasjonen ligger åpen hos mistenkte, altså mens mistenkte selv har åpnet krypteringen. Ofte vil en adgang til å benytte tastetrykksregistrering eller lignende for å fange opp passord ikke være tilstrekkelig, fordi krypteringsnøklene som beskytter informasjonen som regel er flyktige. Det hevdes derfor at utbyttet av en enkeltstående ransaking vil være preget av tilfeldigheter og mer fungere som en «stikkprøve».

Departementet ser at skjult ransaking av for eksempel datamaskiner og e-postkontoer medfører særskilte utfordringer sammenlignet med tradisjonell fysisk ransaking. Utvalgets forslag om å tillate dataavlesing som gjennomføringsmåte innebærer i utgangspunktet ingen endring av de øvrige rettslige rammene for hemmelig ransaking. Forslaget vil derfor trolig ikke fullt ut løse de problemene som flere av høringsinstansene har pekt på, særlig med hensyn til flyktige data og krypteringsnøkler, mistenktes sletting av informasjon og kommunikasjonsformer som ikke kan fanges opp gjennom kommunikasjonsavlytting. Politiets adgang til å tilegne seg innholdet i fortrolig elektronisk informasjon bør ikke være avhengig av hvilken konkret teknologisk løsning mistenkte velger å benytte.

14.8.4 Bør dataavlesing innføres som eget tvangsmiddel?

Dataavlesing etter utvalgets forslag, som gjennomføringsmåte innenfor rammene av etablerte tvangsmiddelhjemler (kommunikasjonsavlytting og skjult ransaking), kan utfordre de alminnelige skrankene for bruk av disse tvangsmidlene. Departementet mener dessuten at politiet bør gis adgang til å benytte dataavlesing i videre utstrekning enn det som følger av utvalgets forslag. Utvalgets forslag synes ikke å ta høyde for utfordringene politiet har med hensyn til effektiv avlytting av kommunikasjon som foregår i former som straffeprosessloven § 216 a ikke gir egnet grunnlag for å kontrollere. Etter departementets vurdering bør dataavlesing heller innføres som et selvstendig tvangsmiddel. Departementet foreslår derfor et nytt kapittel 16 d i straffeprosessloven, med to nye bestemmelser som hjemler dataavlesing – straffeprosessloven §§ 216 o og 216 p.

Dataavlesing som metode bør gi politiet anledning til å skaffe seg tilgang til opplysninger i et datasystem, herunder opplysninger om bruken av datasystemet over tid. Det er en forutsetning at avlesingen kan skje uten samtidig underretning til mistenkte eller andre, på lignende måte som ved for eksempel romavlytting, kommunikasjonsavlytting og hemmelig ransaking. Etter departementets oppfatning bør en hjemmel for dataavlesing gi politiet anledning til å foreta innbrudd for å skaffe seg adgang til datasystemet som skal avleses. Politiet bør ha forholdsvis stor valgfrihet med hensyn til hvilke fremgangsmåter som benyttes for å skaffe adgang til datasystemet og til å gjennomføre avlesingen. Politiet bør blant annet kunne installere og benytte egnet programvare og teknisk utstyr, utnytte eksisterende sikkerhetshull eller sårbarheter i datasystemet og bruke andre tilgjengelige teknikker for å besørge nødvendig program- eller maskinvare installert i datasystemet, som for eksempel å sende programmet som skjult vedlegg til e-post eller fordekt i et annet vedlegg, bruke tilgjengelige nettverksforbindelser til å hente ut informasjonen som avdekkes, samt å foreta innbrudd for å installere og fjerne programvare eller maskinvare dersom det er nødvendig for å kunne gjennomføre dataavlesingen.

I likhet med utvalget mener departementet at det ikke er hensiktsmessig eller mulig å beskrive gjennomføringsmåtene i detalj. Til det er de tekniske mulighetene for mange og den teknologiske utviklingen for rask og uoverskuelig. Politiet bør også av taktiske årsaker levnes en viss mulighet til å utvikle og benytte fremgangsmåter som i hvert fall ikke umiddelbart, og ikke i detalj, blir kjent.

Et 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 dataavlesing. Det er informasjon som genereres i og av datasystemet, og mistenktes *bruk* av datasystemet, som skal kunne kontrolleres gjennom dataavlesing. Departementet understreker at en tillatelse til dataavlesing derimot ikke skal gi politiet adgang til å manipulere datasystemet for å drive andre former for skjult overvåking. 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. Slik overvåking må eventuelt hjemles i henholdsvis straffeprosessloven § 216 m (romavlytting) og kapittel 16 a (skjult kameraovervåking).

Med hensyn til *hvilke typer informasjon* politiet bør kunne gjøre seg kjent med ved dataavlesing, mener departementet at metoden for det første må omfatte tilgang til samme type elektronisk informasjon som politiet ellers har rettslig adgang til gjennom kommunikasjonsavlytting og hemmelig ransaking og beslag. Ett av de viktigste formålene med å innføre dataavlesing som metode er

nettopp å kompensere for det effekttapet henholdsvis kommunikasjonsavlytting og hemmelig ransaking har hatt, som følge av den teknologiske utviklingen. Ved dataavlesing bør politiet imidlertid ikke være bundet av noen tilsvarende sondring mellom elektronisk lagret informasjon og kommunikasjon, jf. også punkt 14.8.2 ovenfor.

Skrankene for bruken av dataavlesing bør fastsettes med utgangspunkt i en vurdering av hvordan og hvor mye metoden kan gripe inn i privatlivets fred og kommunikasjonsfortroligheten. Langt på vei er det snakk om å introdusere nye og mer effektive fremgangsmåter for å skaffe politiet tilgang til informasjon som det allerede har rettslig adgang til gjennom kommunikasjonsavlytting og hemmelig ransaking og beslag. Dataavlesing kan likevel hevdes å innebære en noe større integritetskrenkelse enn tradisjonell kommunikasjonsavlytting og hemmelig ransaking, siden gjennomføringen kan forutsette innbrudd og en form for «tilstedeværelse» over tid i datasystemet. Departementet mener like fullt at det ikke vil være snakk om så alvorlige inngrep at det i seg selv utelukker slik metodebruk i bekjempelsen av alvorlig kriminalitet. Det må også tas i betraktning at inngrepet kan være beskjedent sammenlignet med den krenkelsen som ofrene for den alvorlige kriminaliteten må tåle.

Det bør også understrekes at dataavlesing åpner for mer målrettet informasjonsinnhenting enn de eksisterende hjemlene for henholdsvis kommunikasjonsavlytting og hemmelig ransaking og beslag. Ved «tradisjonell» avlytting av elektronisk kommunikasjon vil avlyttingspunktet ofte være på internettforbindelsen (i transportfasen), hvor politiet samler inn materialet med bistand fra tele- eller internettilbyder. Ved avlytting av ip-basert kommunikasjon innebærer dette at politiet i utgangspunktet kontrollerer all kommunikasjon over internettforbindelsen. Mistenkte kan dele både kommunikasjonsanlegget (for eksempel datamaskin) og internettforbindelsen med familiemedlemmer eller andre utenforstående husstandsmedlemmer, som dermed også kan bli kontrollert. Bruk av dataavlesing åpner for å rette avlyttingen mot for eksempel en spesifikk datamaskin eller smarttelefon som det er grunn til å tro at mistenkte benytter, eller en bestemt brukerkonto (for eksempel til e-post eller en annen kommunikasjonstjeneste) som disponeres av vedkommende. Tredjepersoner kan dermed i en del tilfeller skjermes bedre mot personverninngrep.

Etter departementets oppfatning tilsier det ovennevnte at dataavlesing i en del tilfeller kan lede til at overvåkingen kan gjennomføres på en mer skånsom måte enn det straffeprosessloven § 216 a i dag åpner for. Videre vil metoden kunne brukes for å gjennomføre hemmelig ransaking av datasystemer uten fysisk tilstedeværelse, i flere tilfeller enn det gjeldende rett gir praktisk rom for. Den kan derfor også medføre at det blir mindre behov for å gjøre fysisk innbrudd, og dermed legge til rette for en mindre integritetskrenkende gjennomføringsmåte.

Med forslaget om å tillate dataavlesing vil departementet imidlertid også åpne for at politiet fortløpende gjør seg kjent med andre opplysninger knyttet til bruken av et datasystem som det ikke har anledning til å innhente etter gjeldende rett. Dette inkluderer opplysninger om inntastinger på et tastatur, bruk av programvare og behandling av ulike filer som ikke resulterer i data som blir lagret eller kommunisert, eller som senere blir utilgjengelig for politiet fordi dataene da lagres eller kommuniseres i kryptert form. Etter departementets oppfatning er en slik utvidelse nødvendig for å kunne møte utfordringene knyttet til kryptering og moderne kommunikasjonstjenester på en tilstrekkelig effektiv måte, herunder for å dekke det anførte behovet for å kunne gjennomføre «fortløpende ransaking», se særlig punkt 14.7.3 og 14.8.2 ovenfor.

Enkelte av høringsinstansene har, i sine begrunnelser for hvorfor dataavlesing ikke bør tillates, pekt særskilt på at dataavlesingen vil kunne fange opp opplysninger som ikke var ment kommunisert til noen, og som heller ikke var ment å skulle lagres. Dette vil ifølge høringsinstansene fremstå som særlig integritetskrenkende. Departementet er enig i at det å gi politiet mulighet til å tilegne seg kunnskap om enkeltindividers personlige betraktninger, medfører et vesentlig personverninngrep. Slike inngrep er imidlertid ikke noe nytt i forbindelse med politiets tvangsmiddelbruk. Bestemmelsene om ransaking og beslag er eksempler på dette. Politiet kan søke etter og beslaglegge personlige notater, for eksempel skriftlige dagbøker, dersom de antas å kunne ha betydning som bevis. Informasjonen kan ha både sensitiv og privat karakter, men er like fullt rettslig sett gjort tilgjengelig for politiet, med de begrensninger som følger av bestemmelsene om avlyttings- og beslagsforbud. Dette gjelder selv om mistenkte ikke har ment eller sett for seg at andre skulle kunne få innsyn i materialet. Politiet kan også gjøre seg kjent med materiale som den mistenkte har forsøkt å slette eller tilintetgjøre (forutsatt at det er praktisk mulig å rekonstruere det). Rettslig sett skilles det heller ikke mellom dagboknotater i mistenktes fysiske dagbok og tilsva-

rende notater ført i et tekstbehandlingsprogram på en datamaskin. Hvorvidt informasjonen er lagret fysisk eller elektronisk, bør i utgangspunktet ikke ha noe å si for nivået av rettslig beskyttelse mot inngrep. Forslaget om dataavlesing innebærer i så måte ikke at det åpnes for mer vesentlige inngrep, i form av innsyn i personlig informasjon som er lagret elektronisk, enn adgangen som allerede følger av gjeldende rett.

Som metode vil dataavlesing imidlertid også gi et visst rom for innsyn i personlige betraktninger eller lignende som brukeren ikke har tenkt å lagre (og langt mindre å dele med andre). Forutsetningen for at denne situasjonen skal oppstå må vel i så fall være at mistenkte eller andre benytter en datamaskin, og for eksempel et tekstbehandlingsprogram, til å formulere betraktninger eller tilsvarende, uten å lagre det som er formulert. Det kan ikke utelukkes at noen vil bruke et datasystem på denne måten for å «tenke høyt», men departementet legger til grunn at det er heller uvanlig. Departementet mener uansett at en slik beskjeden risiko for å avdekke personlige betraktninger og formulerte tanker som verken blir lagret eller kommunisert, ikke kan veie tyngre enn de viktige samfunnsinteressene som søkes vernet ved å gi politiet anledning til å benytte effektive virkemidler i bekjempelsen av alvorlig kriminalitet. En adgang til å føre en viss fortløpende kontroll med bruken av nærmere angitte datasystemer, betinget av at strenge vilkår er oppfylt, er etter departementets oppfatning en nødvendig forutsetning for at virkemidlene skal kunne bli tilstrekkelig effektive.

Dataavlesing kan bidra til at politiet klarer å tilegne seg kunnskap om innholdet i kommunikasjon og elektronisk lagret personlig informasjon i flere tilfeller enn det klarer i dag (på grunn av kryptering og andre teknologiske utfordringer). I denne forbindelse er det imidlertid snakk om å gi politiet adgang til å bruke praktiske midler for å gjennomføre den informasjonsinnhentingen som det allerede har en befestet og akseptert rettslig adgang til etter gjeldende rett. At dataavlesing kan bidra til at politiet i større utstrekning faktisk lykkes med informasjonsinnhentingen, kan etter departementets oppfatning ikke brukes som argument mot å tillate dataavlesing. Nivået for beskyttelsen mot personverninngrep må fastlegges ut fra en rettslig avveining av de motstående interessene. Selve beskyttelsen må sikres gjennom passende vilkår for bruk av metoden. Dersom vilkårene for bruk først er oppfylt, må målsetningen være at metoden også er effektiv i praksis. Verken mistenkte eller andre kan bygge noen berettiget forventning om vern på en forutsetning om at politiet ikke vil lykkes med den praktiske gjennomføringen av et lovlig inngrep.

All bruk av skjulte tvangsmidler tillates med grunnlag i en forventning om at politiet evner å respektere de skrankene som lovgiver og retten angir for bruken. Departementet kan ikke se at politiet ikke bør vises den samme tilliten i forbindelse med dataavlesing. På samme måte som ved bruk av andre tvangsmidler er det likevel en forutsetning at det gis retningslinjer for den praktiske gjennomføringen av metoden og at det etableres rutiner for å kontrollere at den ikke benyttes utenfor lovens rammer. Departementet legger til grunn at dataavlesing vil etterlate få ytre spor, og at det derfor er særlig viktig at politiets bruk av metoden dokumenteres på en måte som setter kontrollorganene i stand til å vurdere om det som er utført ligger innenfor de lovlige rammene, og så vidt mulig også til å konstatere at det ikke har blitt utført noe annet eller noe mer enn det som oppgis. Dette omtales nærmere under punkt 14.8.8 og 14.8.10 nedenfor.

Fremgangsmåtene som det kan være aktuelt for politiet å benytte seg av for å foreta dataavlesing, innebærer også en viss risiko for at det utilsiktet voldes skade på datasystemet og for at andre enn politiet settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller opplysninger som behandles i systemet. For eksempel kan det tenkes at det ved gjennomføringen skapes sikkerhetshull eller oppstår fare for at andre kan «overta» eller utnytte programvaren som politiet benytter. Metodekontrollutvalget omtaler disse problemstillingene slik under punkt 23.3.5 (side 248) i utredningen:

> «Utvalget har vært opptatt av at dataavlesingen må innebære så liten sikkerhetsrisiko for mistenktes datasystemer som mulig. Utvalget er av den oppfatning at dette til en viss grad vil regulere seg selv. Dersom programvaren som brukes i forbindelse med dataavlesingen ødelegger eller forstyrrer elementer i brukerens datasystemer, vil oppdagelsesrisikoen øke, med den mulige virkning at metodebruken avsløres og etterforskingen spoleres. Det er dermed i politiets egen interesse å utvikle sikre programvareløsninger. Skulle datasystemet i større eller mindre grad bli ødelagt av politiets metodebruk, anser utvalget det klart at politiet vil være erstatningsansvarlig for dette.
>
> Utvalget er videre opptatt av at eventuelle sikkerhetshull må tettes så snart som mulig etter at de er oppstått. All programvare innehol-

der feil eller mangler som i større eller mindre grad kan utgjøre en sårbarhet for det aktuelle datasystemet. Ved politiets installasjon av programvare for å muliggjøre dataavlesing kan slike svakheter utnyttes. Det innebærer at også andre kan utnytte de samme svakhetene. I tillegg vil politiets programvare kunne inneholde svakheter som kan utnyttes av andre. Ved installasjon av hardware- eller softwarebaserte avlyttingsløsninger som skal kommunisere data tilbake til politiet over en eller annen form for kommunikasjonsnettverk, som for eksempel kan være radio, Internettet eller GSM-nettet, vil det være nødvendig å sette inn tiltak for å hindre uvedkommende i å fange opp disse dataene, eller overta og kontrollere avlyttingsløsningen. Det er for utvalget opplyst at selv kriminelle som foretar innbrudd i datasystem regelmessig tetter de sikkerhetshull som er utnyttet, for å verne om det datasystemet de har skaffet seg kontroll over. Det samme vil selvsagt også politiet kunne gjøre.

Utvalget mener etter dette at sikkerhetsrisikoen, herunder faren for at andre utnytter sikkerhetshull som er oppstått i forbindelse med dataavlesingen er liten, og uansett innenfor et akseptabelt nivå. Spørsmålene må imidlertid bli en del av forholdsmessighetsvurderingen i den enkelte sak. Ettersom gjennomføringsmåten må tilpasses den enkelte sak, og metodebruken vil utvikle seg i takt med den teknologiske utviklingen, er det ikke mulig generelt å gi føringer på denne forholdsmessighetsvurderingen. Påtalemyndigheten må foreta en vurdering av dette spørsmålet i forbindelse med begjæringen til retten om tillatelse til å bruke metoden, og samtidig gjøre domstolen i stand til å foreta en selvstendig vurdering av dette. Det vil til slutt være opp til retten å vurdere om sikkerhetsrisikoen i den enkelte sak er akseptabel.»

Langt på vei kan departementet slutte seg til utvalgets vurderinger ovenfor. Politiet vil være tjent med å velge løsninger som gir minst mulig oppdagelsesrisiko. Etter departementets oppfatning er likevel denne konstateringen isolert sett utilstrekkelig som vern mot skade på datasystemet. Det bør stilles krav til politiets valg av fremgangsmåter for å minimere risikoen for skade og misbruk. Kravene bør fremgå av selve lovhjemmelen for dataavlesing. I denne sammenheng bør det også settes som vilkår at dataavlesing bare skal kunne utføres av personell som har tilstrekkelig kompetanse til å ivareta et slikt krav til forsvarlighet. Departementet viser til den nærmere omtalen av lovforslaget under punkt 14.8.8 nedenfor.

Departementet legger videre til grunn at det, til tross for at det stilles krav til kompetanse og gjennomføringsmåte, vil kunne oppstå noen tilfeller hvor datasystemet påføres skade som følge av dataavlesingen. Etter departementets vurdering kan dette imidlertid ikke tjene som grunnlag for en prinsipiell motforestilling mot metoden, så fremt det i loven oppstilles vilkår for bruken av dataavlesing som er tilfredsstillende med hensyn til å avverge unødvendig skaderisiko. Politiet vil, som ved annen bruk av tvangsmidler, også kunne pådra seg erstatningsansvar etter de alminnelige erstatningsreglene og de særskilte bestemmelsene i straffeprosessloven kapittel 31.

14.8.5 På hvilke områder bør det åpnes for dataavlesing?

Hvor dataavlesing brukes med sikte på strafforfølgning, foreslår departementet å gjøre det til et vilkår at den dataavlesingen retter seg mot med skjellig grunn kan mistenkes for å ha begått eller forsøkt å begå en alvorlig straffbar handling, jf. forslaget til straffeprosessloven ny § 216 o første ledd. Dataavlesing i forebyggende og avvergende øyemed omtales under punkt 14.8.11 nedenfor.

Spørsmålet er hvilke straffbare handlinger mistanken må knytte seg til for at dataavlesing skal kunne iverksettes. I proposisjonen punkt 14.8.11 går departementet inn for at adgangen til å benytte skjulte etterforskningsmetoder fremdeles skal være knyttet til det enkelte straffebuds øvre strafferamme. Departementet mener at det samme bør gjelde for dataavlesing.

Som det er påpekt ovenfor, skal dataavlesing som metode blant annet kompensere for at hjemlene for kommunikasjonsavlytting og hemmelig ransaking bare i begrenset utstrekning er effektive ved avlytting av elektronisk kommunikasjon og ransaking av elektroniske lagringsmedier. Departementet mener derfor, som et utgangspunkt, at det bør vurderes å gi dataavlesing anvendelse i etterforskningen av samme typer saker som kommunikasjonsavlytting og hemmelig ransaking. Det alminnelige strafferammekravet for anvendelse av kommunikasjonsavlytting og hemmelig ransaking fremgår av henholdsvis straffeprosessloven §§ 216 a første ledd bokstav a og 200 a første ledd. Tvangsmidlene kan som hovedregel iverksettes dersom noen med skjellig grunn mistenkes for å ha begått en handling eller forsøk på handling som kan medføre fengsel i ti år eller mer. Forhøyelse av maksimumsstraffen ved

gjentakelse eller sammenstøt av forbrytelser kommer ikke i betraktning. Ved å sette grensen ved strafferammer på minst ti år, vil de mest alvorlige forbrytelsene bli omfattet. Departementet viser for så vidt til punkt 6.1.4.

Dataavlesing vil som metode også ha likhetstrekk med kommunikasjonsavlytting og hemmelig ransaking når det gjelder karakteren til de integritetsinngrepene metodebruken innebærer. Som påpekt under punkt 14.8.4 ovenfor kan dataavlesing etter omstendighetene også fremstå som noe mer inngripende enn kommunikasjonsavlytting og hemmelig ransaking. Departementet mener derfor at det alminnelige strafferammekravet ikke kan være *lavere* enn for kommunikasjonsavlytting og hemmelig ransaking, og foreslår at det i straffeprosessloven ny § 216 o første ledd i utgangspunktet settes et tilsvarende vilkår om at noen med skjellig grunn kan mistenkes for å ha begått en handling eller forsøk på handling som kan medføre fengsel i ti år eller mer.

Likevel kan visse andre lovbrudd medføre etterforskningsmessige utfordringer som tilsier at dataavlesing bør tillates benyttet, selv om det ordinære strafferammekravet ikke er oppfylt. For kommunikasjonsavlytting og hemmelig ransaking har slike ekstraordinære behov kommet til uttrykk i henholdsvis straffeprosessloven §§ 216 a første ledd bokstav b og 200 a første ledd. Begge nevner straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum og 129 om lovbrudd mot statens selvstendighet og sikkerhet i form av etterretningsvirksomhet, avsløring av statshemmeligheter, deltagelse i voldelig sammenslutning mv. (straffeloven 1902 § 90, § 91, § 91 a, §§ 94 jf. 90, §§ 104 a annet ledd jf. første ledd annet punktum), straffeloven § 136 a om kvalifiserte former for deltakelse i terrororganisasjon (straffeloven 1902 § 147 d), samt straffeloven §§ 231, 332 jf. 231, 335 jf. 231, 337 jf. 231, og 340 jf. 231 om narkotikaforbrytelser og heleri og hvitvasking av utbytte fra narkotikaforbrytelser (straffeloven 1902 §§ 162 eller 317, jf. § 162). Straffeprosessloven § 216 a første ledd bokstav b nevner i tillegg eksportkontrolloven § 5 om overtredelser av forbudet mot utførsel av varer mm. av strategisk betydning.

I proposisjonen her foreslås det at kommunikasjonsavlytting etter straffeprosessloven § 216 a også skal kunne anvendes ved skjellig grunn til mistanke om overtredelse av straffeloven § 136 om oppfordring, rekruttering og opplæring til terror (straffeloven 1902 § 147 c), § 254 om frihetsberøvelse (straffeloven 1902 § 223), § 311 om overgrepsbilder av barn (straffeloven 1902 § 204 a) og § 257 om menneskehandel (straffeloven 1902 § 224), samt utlendingsloven § 108 femte ledd om grov menneskesmugling se punkt 7.4 ovenfor. Dette er sakstyper hvor det det kan være behov for særskilte etterforskningsmetoder. Ved menneskesmugling, menneskehandel og overgrepsbilder av barn er den kriminelle virksomheten ofte godt organisert og utført på måter som gjør den vanskelig å avdekke. De fornærmede har dessuten sjelden vilje eller evne til å bidra til oppklaring og iretteføring. Frihetsberøvelse står i en noe annen stilling, men departementet konstaterer at det er behov for å kunne benytte kommunikasjonsavlytting også i slike saker.

Departementet bemerker at anvendelsesområdet for inngripende tvangsmidler ikke kan fastlegges alene med grunnlag i samfunnets behov for beskyttelse mot kriminalitet. Personvernhensyn kan tilsi at bruk av slike tvangsmidler bør være utelukket i en del situasjoner, selv om det kan påvises et reelt behov for metoden. Utvalget av straffbare forhold som kan etterforskes ved hjelp av kommunikasjonsavlytting og hemmelig ransaking bygger etter departementets oppfatning på en slik vurdering. Departementet mener at de hensynene som begrunner anvendelse av kommunikasjonsavlytting og hemmelig ransaking i disse sakene også gjør seg gjeldende for dataavlesing. Et vesentlig siktemål med forslaget om å tillate dataavlesing som metode er, som nevnt ovenfor, å innføre et virkemiddel for informasjonsinnhenting som kan være effektivt i tilfeller hvor kommunikasjonsavlytting etter § 216 a ikke kan ventes å føre frem.

Departementet kan i utgangspunktet ikke se at det vil være vesentlig mer inngripende å benytte dataavlesing i slike saker enn det vil være å benytte kommunikasjonsavlytting eller hemmelig ransaking, eller å benytte begge de sistnevnte tvangsmidlene parallelt. Derfor foreslår departementet at det også åpnes for dataavlesing etter straffeprosessloven ny § 216 o når noen med skjellig grunn kan mistenkes for handlinger som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136, 136 a, 231, 254, 257, 311, 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231 (straffeloven 1902 §§ 90, 91, 91a, 94 jf. 90, 104 a første ledd annet punktum, 104 a annet ledd jf. første ledd annet punktum, § 162 eller § 317, jf. § 162, § 204 a, 223, 224), eller av eksportkontrolloven § 5 eller utlendingsloven § 108 femte ledd.

Det er grunn til å understreke at adgangen til bruk av dataavlesing vil være underlagt en vesentlig tilleggsbegrensning. I henhold til straffepro-

sessloven § 170 a kan et tvangsmiddel bare brukes når det er tilstrekkelig grunn til det, og inngrepet etter sakens art og forholdene ellers ikke vil være uforholdsmessig. Forholdsmessighetskravet vil kunne ha særlig betydning for adgangen til dataavlesing i saker som gjelder forbrytelser med en vesentlig lavere strafferamme enn fengsel inntil 10 år. Departementet viser i denne sammenheng særlig til det som er sagt om kommunikasjonsavlytting ved mistanke om simple narkotikaforbrytelser og besittelse av overgrepsbilder av barn under henholdsvis punkt 7.4.2.4 og 7.4.8.3 ovenfor.

14.8.6 Andre vilkår for å iverksette dataavlesing

Departementets forslag til nye §§ 216 o og 216 p i straffeprosessloven regulerer politiets adgang til å foreta dataavlesing. Grunnvilkåret for å tillate dataavlesing skal være at noen med skjellig grunn må kunne mistenkes for å ha begått eller forsøkt å begå en av handlingene som det er redegjort for under punkt 14.8.5 ovenfor. Departementet har med andre ord valgt å bygge på det tradisjonelle mistankekravet som gjelder for bruk av de mest inngripende tvangsmidlene i straffeprosessloven. Kravet innebærer at retten må anse det som mer sannsynlig at den inngrepet vil rette seg mot har begått eller forsøkt å begå en slik handling, enn at vedkommende ikke har det. Det må altså foreligge sannsynlighetsovervekt. Dette reduserer risikoen for at overvåkingen vil berøre personer som likevel ikke kan knyttes til kriminelle handlinger.

Som det er redegjort for under punkt 14.8.1 ovenfor, bør dataavlesing bare tillates i saker hvor det er et reelt behov for slik metodebruk, for eksempel fordi det må antas at mindre inngripende etterforskningsmetoder vil komme til kort. Departementet går derfor inn for at tillatelse til dataavlesing bare kan gis dersom det må antas at dataavlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort, jf. ny § 216 o tredje ledd. Tilsvarende vilkår gjelder for kommunikasjonsavlytting, jf. straffeprosessloven § 216 c første ledd, og for hemmelig ransaking, jf. § 200 a annet ledd.

Departementet har også vurdert om det burde være et vilkår for dataavlesing at andre konkret angitte tvangsmidler først har blitt forsøkt benyttet, men ikke har ført frem. Departementet har kommet til at det ikke er grunnlag for noen slik begrensning. Det legges til grunn at de konkrete omstendighetene i hvert enkelt tilfelle vil være avgjørende for om dataavlesing vil fremstå som mer eller mindre inngripende enn for eksempel kommunikasjonsavlytting etter § 216 a eller hemmelig ransaking etter § 200 a (eller eventuelt begge brukt parallelt), jf. også punkt 14.8.4 ovenfor. Et absolutt krav om at andre tvangsmidler først må ha vært forsøkt brukt, kunne derfor ha virket mot sin hensikt.

Departementet antar likevel at det kan være krevende for retten å gjøre konkrete vurderinger av hvorvidt andre tvangsmidler vil kunne gi tilfredsstillende resultater, og i så fall om dette ville virke mindre inngripende enn å benytte dataavlesing. Departementet understreker derfor at påtalemyndigheten, når den begjærer tillatelse til dataavlesing, må gi retten informasjon som er tilstrekkelig til at retten kan foreta en reell vurdering av behovet for tvangsmiddelbruken.

Forholdsmessighetsprinsippet i straffeprosessloven § 170 a vil som nevnt ovenfor gjelde for dataavlesing. Dersom dataavlesing vil være et uforholdsmessig inngrep, kan det ikke tillates selv om de øvrige vilkårene er oppfylt. Denne begrensningen bidrar til å sikre at bruken av dataavlesing i praksis finner sted innenfor rammene av EMK artikkel 8 om retten til privatliv.

For ytterligere å målrette hjemmelen for dataavlesing, foreslår departementet at straffeprosessloven § 216 c annet ledd skal gjelde tilsvarende ved dataavlesing. Det innebærer at tillatelse til avlesing av datasystemer som er tilgjengelig for et større antall personer bare kan gis når det foreligger særlige grunner. Det samme gjelder dersom det er spørsmål om å avlese datasystemer som tilhører advokat, lege, prest eller andre som erfaringsmessig benytter slikt datasystem til å behandle opplysninger av svært fortrolig art, eller som tilhører redaktør eller journalist, såfremt vedkommende ikke selv er mistenkt i saken.

Departementet legger i sitt lovforslag opp til at dataavlesing skal kunne besluttes selv om straff ikke kan idømmes på grunn av bestemmelsene i straffeloven § 20 første ledd (straffeloven §§ 44 eller 46). Det samme skal gjelde når tilstanden har medført at den mistenkte ikke har utvist skyld. Tilsvarende bestemmelser finnes blant annet i straffeprosessloven § 196 (ransaking), § 216 a annet ledd (om kommunikasjonsavlytting) og § 216 m annet ledd (romavlytting).

14.8.7 Hvilke datasystemer skal kunne avleses?

Departementet foreslår for det første at politiet skal kunne få tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et «datasys-

tem», jf. forslaget til straffeprosessloven ny § 216 o første ledd. Departementet har dermed valgt å benytte betegnelsen «datasystem» for å angi de objektene som skal kunne avleses. Denne betegnelsen brukes også flere steder i straffe- og straffeprosesslovgivningen, se straffeprosessloven § 199 a, straffeloven 1902 §§ 145 b og 145 c og straffeloven §§ 201, 204 og 206. Begrepet bygger, slik det er brukt i disse bestemmelsene og i forslaget her, på definisjonen av «computer system» i Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi artikkel 1 bokstav a:

> ««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.»

Datasystem skal i henhold til konvensjonen forstås som enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer, jf. blant annet Ot.prp. nr. 22 (2008–2009) punkt 16.2 side 400. Departementet mener at dette også passer godt for det tilsiktede virkeområdet for dataavlesing, i det «datasystem» blant annet vil omfatte smarttelefoner, datamaskiner og andre anlegg for elektronisk kommunikasjon som foretar behandling av data ved hjelp av dataprogrammer. I informasjonsteknologisk terminologi brukes begrepet datasystem også for å betegne flere terminaler (gjerne datamaskiner) som er knyttet sammen med nettverksforbindelser, jf. alternativet «group of interconnected or related devices» i definisjonen ovenfor. Slik uttrykket brukes i forslaget her, er det imidlertid ikke noen betingelse at den aktuelle innretningen er tilknyttet noe slikt nettverk. Derfor omfattes også innretninger for databehandling som ikke brukes til kommunikasjon, som for eksempel datamaskiner uten nettverksforbindelse. Uttrykket «datasystem» er forholdsvis teknologinøytralt, hvilket departementet anser som en fordel med hensyn til den forventede teknologiske utviklingen.

Etter departementets forslag skal en tillatelse til dataavlesing gi adgang til å avlese «bestemte» datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester, jf. forslaget til ny § 216 o fjerde ledd. I formuleringen «bestemte» ligger det et krav om at datasystemet eller brukerkontoen som skal avleses må identifiseres i politiets begjæring (og i politiets beslutning, dersom hastekompetansen benyttes) og i rettens kjennelse. Angivelsen må være så spesifikk som mulig for å unngå tvil om hvilke objekter som tillates avlest. Er det aktuelle datasystemet en mobiltelefon, vil for eksempel telefonens IMEI-nummer kunne brukes. Brukerkontoer kan identifiseres med brukernavn, eller e-postadresse dersom det er snakk om en e-postkonto. Ellers må identifiseringen også kunne skje ved at utstyrets fabrikat opplyses, eller ved angivelse av det geografiske sted hvor utstyret befinner seg og av hvem som har rådighet over det.

Departementets forslag innebærer som nevnt at dataavlesing også skal kunne rettes mot brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester. Fellestrekket ved slike tjenester er at utnyttelsen ikke er bundet til bestemte datasystemer. Hver bruker har et virtuelt avgrenset område som er identifisert ved et brukernavn, og som kan benyttes fra et hvilket som helst passende datasystem med nødvendig nettverksforbindelse og programvare, ved å oppgi brukernavnet og som regel et passord eller en annen form for tilgangskode. Dersom mistenkte bruker slike tjenester via mange ulike nettverkstilkoblinger (for eksempel trådløse internettsoner) og flere forskjellige datasystemer, kan politiet være avskåret fra effektiv kontroll gjennom dataavlesing rettet mot bestemte datasystemer. Politiet bør derfor ha en viss adgang til å gjøre seg kjent med mistenktes bruk av en slik brukerkonto, uavhengig av hvilke datasystemer den mistenkte benytter for å skaffe seg tilgang til kontoen. Avlesing som begrenser seg til en bestemt brukerkonto kan også være mindre inngripende enn avlesing av for eksempel all aktivitet på en datamaskin.

Adgangen til å avlese bestemte brukerkontoer forutsetter at politiet har eller får kjennskap til de nødvendige tilgangsopplysningene (normalt brukernavn og passord), og skaffer seg tilgang til brukerkontoen via politiets egne datasystemer og nettverkstilkoblinger. Dersom det er nødvendig å gå via datasystem som brukes av mistenkte for å oppnå tilgang til brukerkontoen, må politiet fortsatt innhente tillatelse til å avlese det aktuelle datasystemet.

Dataavlesing skal etter departementets forslag bare kunne rettes mot datasystemer eller brukerkontoer som den mistenkte «besitter eller kan antas å ville bruke», jf. forslaget til ny § 216 o fjerde ledd første punktum. Tilsvarende gjelder for kommunikasjonsavlytting, jf. straffeprosessloven § 216 a tredje ledd, og departementet forutsetter at kriteriet skal forstås på samme måte etter forslaget til ny § 216 o fjerde ledd. Med «bruke» siktes det til den direkte bruken av for eksempel

en datamaskin, smarttelefon eller andre typer terminaler. Det er bare datasystemer som er i slik bruk av mistenkte, eller som det kan antas at han vil bruke, som kan avleses. En tillatelse til å avlese et bestemt datasystem, for eksempel en datamaskin, gir anledning til å avlese all informasjon som er tilgjengelig fra maskinen, uavhengig av om informasjonen er lagret lokalt i maskinen eller et annet sted. Det samme gjelder ved avlesing av en bestemt brukerkonto. Derimot er det ikke adgang til å foreta direkte avlesing av eksempel servere hos tjenesteleverandører mv. som mistenkte bare indirekte gjør bruk av. Tilgangen til opplysningene må skaffes gjennom mistenktes datasystem eller brukerkonto.

Det bør kreves at det med grunnlag i objektive kriterier kan konstateres en viss sannsynlighet for at mistenkte vil bruke det datasystemet eller den brukerkontoen som ønskes avlest. Etter departementets oppfatning bør det ikke kreves sannsynlighetsovervekt, men det må være objektive holdepunkter for at mistenkte vil bruke det aktuelle datasystemet. Rene formodninger er altså ikke tilstrekkelig.

14.8.8 Bestemmelser om gjennomføringen av dataavlesing

Som påpekt under punkt 14.8.4 mener departementet at det ikke er mulig å gi noen uttømmende og samtidig hensiktsmessig beskrivelse av fremgangsmåtene ved dataavlesing i lovteksten. Departementets forslag innebærer derfor at politiet får forholdsvis stor frihet til å velge hvilken praktisk fremgangsmåte som skal benyttes for å gjennomføre dataavlesing i hvert enkelt tilfelle. I forslaget til straffeprosessloven ny § 216 p første ledd annet punktum heter det følgelig at dataavlesing kan foretas «ved hjelp av tekniske innretninger, dataprogram eller på annen måte». Meningen er at politiet skal kunne benytte tekniske hjelpemidler, programvare og kunnskap for å gjennomføre dataavlesingen. Adgangen til å benytte tekniske hjelpemidler og dataprogram innebærer at politiet blant annet skal kunne installere egnet programvare eller fysiske komponenter i datasystemet som skal avleses. Det samme gjelder maskinvare som kan knyttes til datasystemet, men som ikke er en nødvendig del av det. Eksempler på slik maskinvare er tilbehør som tastaturer og hodetelefoner, samt eksterne lagringsmedier – herunder «minnepinner». At dataprogrammer og tekniske innretninger også kan installeres i slikt tilbehør foreslås presisert i § 216 p første ledd.

For at avlesingsadgangen skal kunne benyttes i praksis, er det nødvendig at politiet gis anledning til å skaffe seg *tilgang* til datasystemet, både for å kunne iverksette avlesingen og for å hente ut den informasjonen som fremkommer ved avlesingen. Å skaffe tilgang til datasystemet kan formodentlig by på utfordringer, all den tid forutsetningen er at avlesingen skal skje uten mistenktes kunnskap og medvirkning. Departementet foreslår derfor blant annet at straffeprosessloven § 199 a skal gjelde tilsvarende ved dataavlesing, slik at enhver som har befatning med datasystemet kan pålegges å gi politiet nødvendige opplysninger for å gi tilgang til det datasystemet som skal avleses. Politiet må også ha anledning til å bryte eller omgå beskyttelse i datasystemet (foreta datainnbrudd). Dette foreslås presisert i ny § 216 p første ledd.

I tillegg mener departementet at politiet bør kunne foreta fysisk innbrudd for å plassere og fjerne utstyr og programvare som er nødvendig for å gjennomføre avlesingen. Dette er særlig viktig i tilfeller hvor datasystemet befinner seg i lukkede rom, og det ikke synes mulig å gjennomføre dataavlesingen «over nettet», enten fordi systemet ikke er koblet til internett eller annet nettverk, eller fordi det av andre årsaker ikke er mulig for politiet å foreta avlesingen uten fysisk tilgang til datasystemet. Politiet har etter gjeldende rett tilsvarende adgang til å foreta innbrudd for å gjennomføre hemmelig ransaking etter straffeprosessloven §§ 200 a, jf. 200 annet ledd tredje punktum, og for å foreta romavlytting, jf. § 216 m femte ledd. I sistnevnte bestemmelse heter det at når retten ikke bestemmer noe annet, kan politiet foreta innbrudd for å plassere eller fjerne utstyr som er nødvendig for å gjennomføre avlyttingen. Departementet foreslår at adgangen til å foreta innbrudd for å gjennomføre dataavlesing formuleres på lignende måte i ny § 216 p første ledd, slik at politiet – når retten ikke bestemmer noe annet – kan foreta innbrudd for å plassere eller fjerne tekniske innretninger og programvare som er nødvendig for å gjennomføre dataavlesingen. Dersom politiet også skulle ønske å ransake stedet hvor datasystemet befinner seg, må det derimot innhente særskilt tillatelse til dette etter reglene om ransaking.

Kravet om at utstyret må være nødvendig for å gjennomføre avlesingen innebærer at retten ikke bør gi tillatelse til å foreta innbrudd dersom politiet vil kunne gjennomføre avlyttingen på en annen og tilfredsstillende måte uten at det blir behov for innbrudd. Det følger for øvrig også av forholdsmessighetsprinsippet i straffeprosessloven § 170 a at politiet plikter å vurdere om avle-

sing kan skje uten at det er nødvendig å begå innbrudd. Retten må i lys av samme bestemmelse også vurdere om innbrudd medfører at avlesingen vil utgjøre et uforholdsmessig inngrep.

Departementet legger til grunn at effektiv gjennomføring av dataavlesing krever særskilt kompetanse. Bruk av metoden kan også skape risiko for skade på datasystemene som avleses, og for at uvedkommende kan misbruke datasystemene, se også punkt 14.8.4 ovenfor. Dataavlesing bør derfor bare kunne utføres av personell med tilstrekkelig informasjonsteknologisk kompetanse. Et slikt kvalifikasjonskrav kan også bidra til å forebygge og redusere risiko for skade på eller misbruk av datasystemene som avleses. Departementet foreslår derfor at det i straffeprosessloven ny § 216 p første ledd settes som krav at dataavlesingen må foretas av personell som er særlig skikket til det og som er utpekt av politimesteren, sjef PST eller den som bemyndiges.

Videre foreslår departementet at det i straffeprosessloven ny § 216 p annet ledd stilles krav til politiets valg av fremgangsmåter for å minimere risikoen for skade og misbruk. Med dette menes det for det første at politiet ved gjennomføringen av dataavlesing bør være forpliktet til å velge løsninger som ikke skaper unødig fare for skade eller driftshindringer på datasystemet som skal avleses. Enhver fare for skade eller driftshindring kan imidlertid ikke utelukke at dataavlesing likevel gjennomføres. Politiets forpliktet er i denne sammenheng å påse at det ikke *unødig* voldes fare for skade eller driftshindring. I dette ligger det at politiet i valget mellom flere alternativer kan ha plikt til å velge mer omstendelige fremgangsmåter, og til å foreta grep som strengt tatt ikke er nødvendig for å lykkes med gjennomføringen, dersom det reduserer faren for skade eller driftshindring. Videre bør politiet – så langt det er praktisk mulig – være forpliktet til å sørge for at gjennomføringen av avlesingen ikke setter uvedkommende i stand til å skaffe seg uberettiget tilgang til datasystemet, for eksempel ved å utnytte sårbarheter eller «sikkerhetshull» som oppstår som følge av politiets fremgangsmåte. Derimot kan politiet ikke være forpliktet til å utbedre sårbarheter eller sikkerhetshull som allerede eksisterer i datasystemet.

For å understreke viktigheten av at det ikke gjøres større inngrep i noens privatliv enn nødvendig, foreslår departementet videre at det i straffeprosessloven ny § 216 p annet ledd sies uttrykkelig at avlesingen må innrettes slik at det ikke unødig fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Avlesingen skal altså være så målrettet som mulig. Dette har særlig betydning i tilfeller hvor mistenkte deler datasystemet med andre – for eksempel der en datamaskin også brukes av andre medlemmer av husstanden.

Videre bør det kreves forholdsvis nøyaktig registrering av hva politiet foretar seg ved dataavlesing. Notoritet med hensyn til hvilke skritt politiet har tatt, er en forutsetning for å sikre tilfredsstillende kontroll med politiets metodebruk. Det bør derfor kreves at det føres protokoll med opplysninger om metodebruken i hver enkelt sak. I kommunikasjonskontrollforskiften § 7 er det gitt bestemmelser om protokollføring ved kommunikasjonskontroll etter straffeprosessloven §§ 216 a og 216 b. Bestemmelsene får også anvendelse ved romavlytting etter § 216 m. Etter departementets vurdering bør det gis særskilte bestemmelser om logg- eller protokollføring ved dataavlesing, som er tilpasset denne metodens særpreg.

14.8.9 Øvrige prosessuelle bestemmelser

Kompetansen til å gi tillatelse til dataavlesing bør etter departementets oppfatning legges til retten. Rettens avgjørelse bør begrunnes, og det foreslås derfor at avgjørelsen skal treffes ved kjennelse. Selv om tillatelse i utgangspunktet skal gis av retten, mener departementet at påtalemyndigheten bør gis kompetanse til å beslutte dataavlesing i saker hvor rettens kjennelse ikke kan avventes uten stor fare for at etterforskningen vil lide. I slike saker bør ordre fra påtalemyndigheten kunne tre i stedet for rettens kjennelse, slik regelen også er ved kommunikasjonsavlytting, jf. straffeprosessloven § 216 d, og ved hemmelig ransaking, jf. § 200 a sjette ledd. Departementet foreslår derfor at straffeprosessloven § 216 d skal gjelde tilsvarende ved dataavlesing. Dette innebærer også at det er påtalemyndigheten som har kompetanse til å avgjøre om det skal begjæres tillatelse til dataavlesing eller treffes hastebeslutning etter § 216 d første ledd. I utgangspunktet er det politimesteren eller visepolitimesteren som skal avgjøre spørsmålet, jf. § 216 d annet ledd første punktum.

Dataavlesing skal kunne gjennomføres fortløpende over noe tid, men ikke lenger enn strengt nødvendig. Rettens tillatelse må derfor angi en tidsperiode som dataavlesingen skal kunne foregå innenfor. Ved kommunikasjonskontroll er hovedregelen at tillatelsen ikke kan gis for mer enn fire uker om gangen, jf. straffeprosessloven § 216 f første ledd annet punktum. Kontrollperioden kan forlenges etter ny begjæring fra påtalemyndighe-

ten. Dersom mistanken gjelder overtredelse av straffeloven kapittel 17 (straffeloven 1902 kapittel 8 eller 9), kan tillatelsen likevel gis for inntil åtte uker om gangen dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter fire uker vil være uten betydning, jf. § 216 f første ledd tredje punktum. Departementet foreslår at de samme reglene skal gjelde ved dataavlesing, men likevel slik at retten ikke skal kunne tillate dataavlesing for mer enn to uker om gangen. Begrunnelsen for dette er at dataavlesing etter omstendighetene *kan* fremstå som et større integritetsinngrep enn kommunikasjonsavlytting, hvilket tilsier at det legges til rette for en hyppigere prøving av om det er grunnlag for å fortsette avlesingen.

Videre foreslår departementet at straffeprosessloven § 216 f annet ledd skal gjelde tilsvarende ved dataavlesing etter ny § 216 o. Det innebærer at dataavlesingen skal stanses før utløpet av fristen som er satt i rettens kjennelse, dersom vilkårene for kontroll ikke lenger antas å være til stede, eller dersom avlesing ikke lenger anses hensiktsmessig. Bestemmelsen vil for eksempel være aktuell dersom politiet, etter at avlesing er iverksatt, mottar opplysninger som viser at det ikke lenger er skjellig grunn til mistanke mot den som avlesingen er rettet mot. En tilsvarende begrensning kan nok sies å følge allerede av forholdsmessighetsprinsippet som kommer til uttrykk i straffeprosessloven § 170 a, men departementet mener at det er hensiktsmessig å synliggjøre dette ytterligere gjennom en henvisning til § 216 f annet ledd.

Departementet foreslår også at straffeprosessloven § 216 e skal gjelde tilsvarende, slik at sak om dataavlesing kan bringes inn for tingretten på det sted hvor det mest praktisk kan skje. Avgjørelsen treffes uten at den mistenkte eller den som avgjørelsen ellers rammer, gis adgang til å uttale seg. Kjennelsen blir heller ikke meddelt dem.

Etter straffeprosessloven § 100 a skal retten, når den behandler begjæringer om bruk av skjulte tvangsmidler, oppnevne offentlig advokat. Advokaten skal vareta den mistenktes interesser i forbindelse med rettens behandling av begjæringen. I proposisjonen foreslår departementet at det lovfestes i § 100 a annet ledd at advokaten også skal vareta eventuelle tredjepersoners interesser, se punkt 6.6.5 ovenfor. Departementet mener at det må oppnevnes offentlig advokat til å vareta den mistenktes og eventuelle tredjepersoners interesser også i forbindelse med behandling av begjæringer om tillatelse til dataavlesing. Det foreslås derfor at straffeprosessloven ny § 216 o inkluderes i oppregningen i § 100 a første ledd første punktum.

Etter departementets oppfatning bør også en rekke av de øvrige prosessuelle reglene om kommunikasjonskontroll gis tilsvarende anvendelse ved dataavlesing. Med hensyn til underretning til mistenkte og den som har rådighet over datasystemet, mener departementet at bestemmelsene om underretning ved kommunikasjonskontroll, med de endringene som foreslås i punkt 6.10 ovenfor, bør gjelde tilsvarende ved dataavlesing. Hovedregelen vil da være at mistenkte og den som har rådighet over datasystemet skal underrettes om dataavlesingen når den er avsluttet, men likevel slik at retten kan beslutte utsatt eller unnlatt underretning på de vilkårene som fremgår av forslaget til endringer i § 216 j.

Videre foreslår departementet at straffeprosessloven § 216 i om taushetsplikt og bruk av opplysninger som fremkommer ved kommunikasjonskontroll (og ved romavlytting, jf. § 216 m) skal gjelde tilsvarende for opplysninger som fremkommer ved dataavlesing.

Bruk av dataavlesing vil sannsynligvis medføre at det også blir fanget opp informasjon som ikke er relevant for etterforskningen, selv om avlesingen skal innrettes slik at dette unngås så langt det er praktisk mulig. Det er også tilfellet ved kommunikasjonskontroll. For å ivareta personvernhensyn inneholder straffeprosessloven § 216 g regler om sletting av overskuddsmateriale fra kommunikasjonskontroll. Bestemmelsen ble endret ved lov 21. juni 2013 nr. 86, og foreskriver nå at materiale som ikke er fremlagt som bevis skal slettes ved rettskraftig dom dersom det åpenbart er uten betydning for saken, og ellers sperres. Dersom saken henlegges, skal materiale fra kommunikasjonskontroll som hovedregel slettes. Påtalemyndigheten kan likevel beslutte at materialet i stedet skal sperres dersom det er grunn til å regne med at siktede vil kreve erstatning i anledning av forfølgning eller at materialet kan få vesentlig betydning for senere etterforskning eller forebygging. Opplysninger som er omfattet av vitneforbud eller -fritak etter straffeprosessloven §§ 117 til 120 og 122 skal slettes så snart som mulig. De omtalte lovendringene har foreløpig ikke trådt i kraft. Departementet foreslår at § 216 g skal gjelde tilsvarende for materiale som innhentes ved dataavlesing.

14.8.10 Etterfølgende kontroll

Politiets og påtalemyndighetens behandling av saker om dataavlesing må etter departementets

oppfatning være gjenstand for etterfølgende kontroll. Kontrollutvalget for kommunikasjonskontroll fører slik kontroll med politiets og påtalemyndighetens bruk av kommunikasjonskontroll og romavlytting, jf. straffeprosessloven §§ 216 h og 216 m siste ledd. Det er gitt nærmere regler om kontrollutvalgets oppgaver og saksbehandling i kommunikasjonskontrollforskriften kapittel 2.

Departementet foreslår at straffeprosessloven § 216 h skal gjelde tilsvarende for dataavlesing etter straffeprosessloven nytt kapittel 16 d, slik at kontrollutvalget også skal føre kontroll med bruken av dataavlesing. Etter departementets oppfatning kan det være grunn til å gi særskilte forskriftsbestemmelser om kontrollutvalgets oppgaver og saksbehandling i saker om dataavlesing, som tilpasses metodens særpreg.

Departementet understreker for øvrig at det må legges til rette for at kontrollutvalget kan utføre en effektiv og reell kontroll med bruken av dataavlesing. Metodens karakter tilsier at utvalget vil være avhengig av å ha høy teknologisk kompetanse tilgjengelig. I denne sammenheng viser departementet også til Metodekontrollutvalgets utredning punkt 11.10.2 side 140, hvor det konstateres at kontrollutvalget «må ha tilgjengelig tilstrekkelig teknologisk kompetanse, og at uavhengighetshensyn og kontinuitetshensyn kan tilsi at slik kompetanse finnes blant utvalgsmedlemmene og ikke for eksempel innleies fra eksterne.» Departementet legger til grunn at det kan være nødvendig å styrke kontrollutvalgets budsjett som følge av den her foreslåtte utvidelsen av dets ansvarsområde og det økte behovet for teknologisk kompetanse, se punkt 15.9 nedenfor.

PSTs bruk av skjulte tvangsmidler i forebyggingssaker og etterforskningssaker kontrolleres av EOS-utvalget, jf. lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-loven) og Stortingets instruks om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-instruksen). EOS-utvalgets kontroll vil følgelig omfatte PSTs bruk av dataavlesing.

14.8.11 Dataavlesing i avvergende og forebyggende øyemed

Etter departementets oppfatning bør dataavlesing også kunne benyttes i avvergende øyemed som ledd i etterforskning, på lik linje som kommunikasjonsavlytting og hemmelig ransaking. Departementet foreslår derfor at straffeprosessloven ny § 216 o tas med i oppregningen av tvangsmidler som kan benyttes etter § 222 d første og annet ledd. Tillatelse til å benytte dataavlesing bør bare kunne gis når særlige grunner tilsier det, jf. § 222 tredje ledd.

Departementet er av samme oppfatning med hensyn til PSTs adgang til å benytte tvangsmidler i sin forebyggende virksomhet etter politiloven § 17 d. Det foreslås derfor at straffeprosessloven ny § 216 o også tas med i oppregningen av tvangsmidler i politiloven § 17 d første ledd, og at tillatelse bare skal kunne gis når særlige grunner tilsier det, jf. § 17 d annet ledd.

15 Økonomiske og administrative konsekvenser

15.1 Innledning

Lovforslaget vil medføre økte utgifter til Kontrollutvalget for kommunikasjonskontroll. Det årlige behovet anslås å øke fra 0,7 mill. kroner til 6,0 mill. kroner. Merutgiftene vil dekkes innenfor Justis- og beredskapsdepartementets gjeldende budsjettrammer.

Det foreligger ikke detaljerte data for medgåtte ressurser knyttet til eksisterende lovgivning om politiets bruk av skjulte tvangsmidler. Det er derfor vanskelig å tallfeste merkostnadene ved lovendringer. Generelt vil en bedret evne til effektiv kriminalitetsbekjempelse kunne lede til flere behandlede straffesaker og derved økte kostnader. Men den preventive effekt som følger av at iretteføring av straffbare forhold finner sted, vil også kunne lede til færre straffbare handlinger på sikt. Forslagene kan derfor gi en samfunnsøkonomisk gevinst. Eventuelle merutgifter dekkes innenfor gjeldende budsjettrammer.

15.2 Fellesspørsmål

Når det gjelder økonomiske og administrative konsekvenser knyttet til kapittel 6 om fellesspørsmål, vil enkelte sider av forslaget by på merutgifter, mens andre sider vil medføre innsparinger. Dersom Stortinget beslutter at spørsmålet om utsatt underretning ved jevne mellomrom må prøves også for kommunikasjonskontroll og romavlytting, vil dette bety enkelte merutgifter både når det gjelder domstoler, offentlige advokater og politi. Dersom det gis mulighet for å utsette underretning i inntil fire måneder om gangen, vil imidlertid dette kunne redusere utgiftsøkningen noe. Dessuten vil det antakelig ligge en ikke ubetydelig innsparing i forslaget om å la påtalemyndigheten beslutte utsatt underretning ved beslag og utleveringspålegg i inntil åtte uker. Det kan synes noe usikkert om dette innebærer et «nullsumspill».

Selv om det er en del ulikheter mellom EOS-utvalget og KK-utvalget med hensyn til oppgavenes art og kompleksitet, har Metodekontrollutvalget merket seg at det er stor forskjell på tilgjengelige budsjettressurser for de to kontrollutvalgene, jf. utredningen punkt 11.10.2 side 140. KK-utvalget hadde for året 2007 en budsjettramme på kr 300 000. Samme år hadde EOS-utvalget en budsjettramme på kr 6 193 000. Da det er en nær sammenheng mellom budsjettmidler og faktisk gjennomførte kontroller både i omfang og innhold, tilrår utvalget at budsjettet for KK-utvalget styrkes vesentlig. Budsjettrammene for KK-utvalget og EOS-utvalget var i 2015 henholdsvis på kr 700 000 og 13,0 mill. kroner. Departementet mener at dette, i tillegg til nye kontrolloppgaver, underbygger at det er behov for å styrke KK-utvalgets budsjett, jf. nedenfor i punkt 15.9.

15.3 Kommunikasjonskontroll

Departementet foreslår å utvide politiets adgang til å iverksette kommunikasjonskontroll til å gjelde ved noen flere kriminalitetstyper enn i dag. Hvorvidt metoden rent faktisk skal benyttes i en straffesak, må vurderes av politiet ut fra forholdsmessighet, hensiktsmessighet og behov. I utgangspunktet er dette en prioritering som må foretas innenfor gjeldende budsjettrammer. Det er likevel ikke usannsynlig at endringene vil medføre at kommunikasjonskontroll vil benyttes i noe større utstrekning enn i dag, slik at mer politiressurser brukes på dette. Dette vil også kunne gi en økning i arbeidsmengde for Kontrollutvalget for kommunikasjonskontroll. Samtidig kan utvidelsene også føre til en effektivisering av etterforskningen av de aktuelle sakstypene, og dermed gi ressursbesparelser.

For politiet vil forslagene gi tilgang til enkelte nye virkemidler i etterforskningen for å kunne lokalisere kommunikasjonsanlegg. Bruk av disse virkemidlene vil kunne kreve ressurser, både i form av personell og muligens også i form av teknisk utstyr. Samtidig vil forslagene kunne føre til en effektivisering av politiets etterforskningsarbeid, og dermed ha ressursmessige gevinster. Det foreligger ingen plikt for politiet til å benytte seg av de foreslåtte fremgangsmåtene. Hvorvidt man i den enkelte straffesak skal ta i bruk slike virkemidler,

vil være opp til politiet selv og må vurderes ut fra blant annet budsjettmessige prioriteringer. Samlet antas forslaget for politiets del å kunne gjennomføres innenfor gjeldende budsjettrammer.

For nett- og tjenestetilbydere vil forslaget om utvidet adgang til å kreve utlevering av posisjonsopplysninger føre til visse merkostnader, som følge av at tilbyderne plikter å bistå politiet ved å utlevere de relevante opplysningene. Den utvidede utleveringsadgangen vil også kunne medføre administrative konsekvenser i form av merarbeid knyttet til flere utleveringsbegjæringer. Kostnader knyttet til slik utlevering dekkes imidlertid av politiet i henhold til gjeldende regler om dette. Heller ikke for tilbyderne antas derfor forslaget å ha nevneverdige økonomiske konsekvenser.

15.4 Romavlytting

I proposisjonen foreslår departementet å fjerne kravet om tilknytning til organisert kriminalitet ved bruk av romavlytting i drapssaker. Endringen kan medføre at romavlytting benyttes i noen flere saker enn i dag. Antallet drapssaker i Norge hvert år er imidlertid lavt, og det antas at økonomiske konsekvenser ved forslaget vil være marginale. Bruk av metoden vil måtte skje innenfor gjeldende budsjettrammer.

15.5 Teknisk sporing

Det foreslås å gi adgang til bruk av teknisk sporing i saker om grov ulovlig befatning med våpen mv. Videre foreslås å åpne for bruk av personnær teknisk sporing i saker om frihetsberøvelse. Forslagene kan medføre en viss økning i bruken av teknisk sporing, men kan samtidig medføre en ressursgevinst ved at etterforskningen av de nevnte sakstypene gjøres mer effektiv. Endringene antas å kunne gjennomføres innenfor gjeldende budsjettrammer.

15.6 Postbeslag og postkontroll

Endringene som foreslås i kapittel 10 om utleveringspålegg, ransaking, beslag, postbeslag og postkontroll vil ikke ha økonomiske eller administrative konsekvenser av betydning.

15.7 Skjult kameraovervåking

Departementet foreslår en utvidelse av hvilke områder som kan overvåkes ved hjelp av skjult kameraovervåking. Dette kan føre til en viss økning i politiets bruk av metoden. Hvorvidt skjult kameraovervåking faktisk skal iverksettes i en konkret straffesak, må imidlertid vurderes av politiet ut fra blant annet ressurshensyn. Videre vil bruk av metoden etter omstendighetene kunne effektivisere bruken av andre etterforskningsmidler, noe som kan gi en viss ressursbesparelse. Samlet antas endringene ikke å medføre økonomiske eller administrative konsekvenser av betydning.

15.8 Tvangsmidler i avvergende og forebyggende øyemed

Departementet foreslår at politiets adgang til å benytte skjulte tvangsmidler for å avverge drap utvides, slik at det ikke lenger skal være krav om at dette begås som ledd i organisert kriminalitet eller motarbeiding av rettsvesenet. Videre foreslås det at PST gis adgang til å bruke skjulte tvangsmidler for å avverge offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, samt til å bruke romavlytting for å avverge angrep mot myndighetspersoner. PST gis dessuten adgang til å bruke tvangsmidler for å forebygge ulovlig omgang med masseødeleggelsesvåpen.

Den utvidede adgangen til å benytte tvangsmidler for å avverge drap, vil neppe ha nevneverdige økonomiske konsekvenser. Derimot kan det ikke utelukkes at PSTs bruk av tvangsmidler for å avverge terrorrelaterte handlinger, øker noe. Bruken av tvangsmidler vil imidlertid måtte skje ut fra en prioritering innenfor gjeldende budsjettrammer. Departementet legger til grunn at de øvrige lovendringene ikke vil ha økonomiske eller administrative konsekvenser av betydning.

15.9 Dataavlesing

Departementet foreslår at dataavlesing innføres som nytt tvangsmiddel med hjemmel i straffeprosessloven nye §§ 216 o og 216 p. Politiet må, som ellers, gjøre konkrete vurderinger av om det er behov for å benytte seg av denne metoden i den enkelte sak. Departementet legger til grunn at gjennomføring av dataavlesing kan vise seg å kreve betydelige ressurser, særlig under henvis-

ning til at avlesingen forutsettes utført av personer med særskilt teknologisk kompetanse, og at avlesingen skal kunne foregå løpende over en viss tid. Videre antar departementet at politiet kan finne det nødvendig å gjøre investeringer i programvare og annet utstyr for å benytte seg av metoden. Departementet peker imidlertid også på at dataavlesing kan erstatte kommunikasjonsavlytting eller hemmelig ransaking i enkeltsaker. I utgangspunktet er det snakk om prioriteringer som må gjøres innenfor de gjeldende budsjettrammene.

Likevel vil departementet fremheve at bruken av dataavlesing forutsettes kontrollert av KK-utvalget, eller EOS-utvalget ved PSTs bruk av metoden. Med dette utvides KK-utvalgets kontrollportefølje til å omfatte bruken av et nytt tvangsmiddel, hvilket tilsier at utvalgets arbeidsmengde vil øke. Videre legger departementet til grunn at utvalgets evne til å føre en reell og tilfredsstillende kontroll med denne typen tvangsmiddelbruk forutsetter at det har tilgang til passende teknologisk kompetanse.

KK-utvalget uttaler følgende i e-post 23. mai 2014 til departementet:

> «Dersom det åpnes for dataavlesning, er jeg enig i at kontrollen av denne metodebruken naturlig bør ligge inn under KK-utvalgets arbeidsoppgaver, men utvalgets organisering og ressurssituasjon må da særlig vurderes. Det er ikke mulig å utføre ytterligere kontrolloppgaver med dagens opplegg. Med utvidet kontrollområde der det forventes rask saksbehandling, er det vanskelig å se for seg et forsvarlig arbeid uten at det etableres et sekretariat i egnede, sikre lokaler (jf. at de fleste dokumentene er gardert strengt fortrolig) med heltidsansatte jurister hvorav en også er sekretariatsleder, dataekspert minst i halv stilling, arkivleder osv. Utvalget som sådan kan fortsatt være basert på sidegjøremål slik at den brede kompetansen og kontrollen utenfra beholdes. Et slikt opplegg vil nok anslagsvis kunne medføre kostnader i størrelsesorden kr 4 – 5 millioner per år for at hensikten med endringen skal oppnås.»

Departementet henvendte seg til KK-utvalget og ba om ytterligere dokumentasjon av kostnadene. I brev 23. februar 2015 gis det blant annet uttrykk for følgende:

> «Med utvidet kontrollområde der det forventes og bør skje rask saksbehandling, er det vanskelig å se for seg et forsvarlig kontroll- og oppfølgingsarbeid uten at det etableres et utvalgssekretariat i egnede, sikre lokaler. Utvalget som sådan bør fortsatt være uavhengige personer som har vervet som sidegjøremål, men de daglige, løpende kontroll oppgavene må utføres av kompetente heltidsansatte. For KK-utvalget med de arbeidsoppgaver som kan forventes i overskuelig fremtid, kan det skisseres følgende kostnader per år:

(a)	utvalget som sidegjøremål – godtgjøring	kr	1 000 000
(b)	to jurister hvorav én sekr.leder inkl. sos.	kr	2 000 000
(c)	dataekspert (ev. innleid) inkl. utstyr	kr	1 000 000
(d)	kontorleder inkl. arkivledelse inkl. sos.	kr	700 000
(e)	medarbeider/post inkl. sos.	kr	500 000
(f)	sikrede lokaler, møterom og dok.lager	kr	800 000
SUM	anslag	kr	6 000 000»

Departementet legger på bakgrunn av ovennevnte til grunn at årlige tildelinger til Kontrollutvalget for kommunikasjonskontroll må økes fra 0,7 mill. kroner til om lag 6 mill. kroner, jf. punkt 15.1. Merutgiftene vil dekkes innenfor Justis- og beredskapsdepartementets gjeldende budsjettrammer.

16 Merknader til de enkelte bestemmelsene

16.1 Til endringene i straffeprosessloven

Til § 100 a

I *første ledd første punktum* er straffeprosessloven § 202 a annet ledd om skjult kameraovervåking på privat sted og § 216 o om dataavlesing lagt til i opplistingen av sakstyper hvor det skal oppnevnes offentlig advokat. Se proposisjonen punkt 6.6.7 og 14.8.9.

Annet ledd første punktum er endret slik at den offentlige advokaten også skal ivareta interessene til tredjeperson. Dette samsvarer med Metodekontrollutvalgets forslag, se nærmere punkt 6.6.5. I *annet ledd annet punktum* fremgår det at samme advokat så langt det er mulig skal oppnevnes ved begjæring om forlengelse av bruken av tvangsmidler og ved begjæring om andre tvangsmidler mot mistenkte som er oppregnet i paragrafens første ledd. Regelen samsvarer med Metodekontrollutvalgets forslag, se nærmere punkt 6.6.2. *Annet ledd tredje punktum* viderefører tidligere annet punktum, og presiserer dessuten at den offentlige advokaten har krav på tilstedeværelse under rettsmøte til behandling av begjæringen. Bestemmelsen samsvarer med Metodekontrollutvalgets forslag, se NOU 2009: 15 side 352. *Annet ledd fjerde punktum* bestemmer at påtalemyndigheten skal fremme begjæring om forlengelse så tidlig at advokaten kan få varsel senest dagen før rettsmøtet holdes. Bestemmelsen er ny og svarer til Metodekontrollutvalgets forslag, se nærmere punkt 6.6.3.

Fjerde ledd nytt annet punktum bestemmer at et forbud etter fjerde ledd første punktum for den offentlige advokaten mot å ta forsvareroppdrag senere i saken ikke strekker seg lenger enn til det tidspunktet da mistenkte gjennom dokumentinnsyn får de samme opplysningene som forsvareren. Bestemmelsen er ny og svarer innholdsmessig til Metodekontrollutvalgets forslag, se nærmere punkt 6.6.6.

Til § 200 a

Tilføyelsen av straffeloven §§ 136, 254, 257 og 311 (straffeloven 1902 §§ 147 c, 204 a, 223 og 224) samt lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd i § 200 a *første ledd* innebærer at det åpnes for hemmelig ransaking i saker om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, frihetsberøvelse, menneskehandel, grov menneskesmugling og befatning med overgrepsbilder av barn – forutsatt at øvrige vilkår for slik metodebruk er oppfylt. Se proposisjonen punkt 10.4, jf. 7.4.

Tredje ledd og fjerde ledd erstatter tidligere tredje ledd, og innebærer en rekke endringer i reglene om underretning til mistenkte om den skjulte ransakingen.

Etter *tredje ledd første punktum* kan underretning utsettes dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. Vilkåret erstatter det tidligere «strengt nødvendig»-vilkåret og samsvarer med metodekontrollutvalgets forslag, se nærmere punkt 6.10.5.1.

Tredje ledd annet punktum bestemmer at retten i saker om overtredelse av straffeloven kapittel 17 (straffeloven 1902 kapittel 8 og 9) kan beslutte at underretning kan utsettes for inntil seks måneder om gangen. Dette samsvarer med tidligere fjerde punktum og utvalgets forslag, se nærmere punkt 6.10.5.4.

Tredje ledd tredje punktum viderefører ordningen med at utsatt underretning i alle andre saker, som ikke gjelder overtredelse av straffeloven kapittel 17 (straffeloven 1902 kapittel 8 eller 9), kan besluttes for inntil åtte uker om gangen. Også dette samsvarer med utvalgets forslag.

Regelen i *tredje ledd fjerde punktum* om at retten kan beslutte at underretning kan utsettes i inntil fire måneder dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter åtte uker vil være uten betyd-

ning, er ny og var heller ikke foreslått av utvalget. Regelen samsvarer med straffeprosessloven § 185 første ledd fjerde punktum om prøving av fengslingsspørsmålet, se nærmere punkt 6.10.5.4.

Fjerde ledd første punktum bestemmer at underretning senest skal gis når tiltale tas ut eller saken henlegges og fristen etter § 75 annet ledd første punktum har gått ut. Det første alternativet er en videreføring av tidligere tredje punktum, mens alternativet om underretning ved henleggelse er nytt. Bestemmelsen samsvarer med utvalgets forslag, likevel slik at den presiserer at henleggelse først foreligger når omgjøringsfristen etter straffeprosessloven § 75 annet ledd første punktum har gått ut. Se nærmere punkt 6.10.5.5.

Fjerde ledd annet punktum bestemmer at retten likevel kan bestemme at underretning helt kan unnlates dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. En hjemmel til helt å unnlate underretning gjaldt også tidligere for saker etter straffeloven 1902 kapittel 8 og 9, men det er nytt at dette gjelder for alle sakstyper hvor det foretas skjult ransaking. Bestemmelsen skiller seg dermed fra utvalgets forslag, som ikke gikk inn for at underretning helt skulle kunne unnlates. Bakgrunnen for bestemmelsen er nærmere behandlet i punkt 6.10.6.

Fjerde ledd tredje punktum bestemmer at enkelte regler i straffeprosessloven kapittel 16 a om kommunikasjonskontroll gjelder tilsvarende ved skjult ransaking. Henvisningen til § 216 e annet ledd er en videreføring av tidligere tredje ledd første punktum, og innebærer at mistenkte eller andre som rammes av avgjørelsen om utsatt underretning ikke skal underrettes om kjennelsen. Henvisningen til § 216 f annet ledd er en videreføring av tidligere femte punktum, og medfører at underretning må gis før fristen for utsatt underretning løper ut, dersom vilkårene for utsettelse ikke lenger er oppfylt. Henvisningen til § 216 j sjette ledd første til fjerde punktum er ny, og innebærer at underretning skal kunne gis på begjæring, selv om det er besluttet at underretning kan utsettes eller helt unnlates. Noen lovregulert ordning om underretning på begjæring fantes ikke tidligere for skjult ransaking, men det fantes heller ikke regler som var til hinder for dette, se nærmere punkt 6.10.6.1. Henvisningen til § 216 j syvende ledd innebærer at Kongen kan gi forskrift om underretning ved skjult ransaking som skjer på begjæring fra utenlandske myndigheter.

Til § 202 a

Første ledd gjelder kameraovervåking på eller fra offentlig sted som nevnt i straffeloven § 10 første ledd (straffeloven 1902 § 7 første ledd). Forslaget viderefører det som i dag følger av straffeprosessloven § 202 a om overvåking på offentlig sted, men presiserer at skjult kameraovervåking også kan skje fra offentlig sted mot privat sted. Slik overvåking vil typisk kunne rettes mot inngangsparti, gårdsrom, hage mv. som er synlig fra offentlig sted. Overvåkingen kan under ingen omstendighet rettes mot privat beboelsesrom. Tillatelse til å iverksette skjult kameraovervåking på eller fra offentlig sted gis av retten ved formløs beslutning. Det vises til proposisjonen punkt 12.5 og 12.7.

I *annet ledd* foreslås at politiet, på strenge vilkår, gis adgang til å iverksette skjult kameraovervåking på privat sted. I motsetning til skjult overvåking på eller fra offentlig sted etter første ledd, treffes avgjørelsen ved kjennelse. Adgangen gjelder ikke overvåking i eller mot privat hjem, jf. *fjerde ledd i.f.* Kravet til den straffbare handling som kan gi grunnlag for overvåking er tilsvarende som for kommunikasjonsavlytting etter straffeprosessloven § 216 a. Videre kan overvåking bare iverksettes når det må antas å være av vesentlig betydning for å oppklare saken og oppklaring ellers i vesentlig grad vil bli vanskeliggjort. Kravet er strengere enn etter første ledd, hvor det bare kreves at overvåkingen vil være av vesentlig betydning for etterforskningen. Se for øvrig punkt 12.6 og 12.7.

Etter *tredje ledd* kan skjult kameraovervåking iverksettes selv om mistenkte ikke kan dømmes til straff på grunn av reglene i straffeloven § 20 første ledd (straffeloven 1902 §§ 44 eller 46).

I *fjerde ledd* angis hva kameraovervåkingen etter første og annet ledd kan bestå i. Formuleringen er hentet fra personopplysningsloven § 36, og skal forstås på samme måte som denne bestemmelsen. Bestemmelsens siste punktum presiserer at skjult kameraovervåking etter straffeprosessloven § 202 a ikke under noen omstendighet kan rettes mot private hjem. Kameraovervåkingen kan likevel rettes mot beboelsesrom hvor personer oppholder seg over kortere perioder, slik som fritidsboliger, hotellrom og lignende, eller mot såkalte dekkboliger. Den konkrete avgrensningen må skje i samsvar med Grunnloven § 102, jf. også politiloven § 17 d annet ledd siste punktum. Ste-

dets private karakter vil for øvrig være et sentralt moment i forholdsmessighetsvurderingen etter straffeprosessloven § 170 a.

Femte ledd fastsetter at skjult kameraovervåking bare kan skje på privat sted hvor det må antas at den mistenkte vil oppholde seg. Videre oppstilles en begrensning i adgangen til å overvåke steder hvor visse yrkesgrupper regulært fører samtaler som nyter et særskilt vern. Bestemmelsen skal forstås på samme måte som § 216 c annet ledd annet punktum.

Etter *sjette ledd* skal tillatelse til skjult kameraovervåking gis for et bestemt tidsrom, som ikke kan være lengre enn fire uker om gangen.

I *syvende ledd* foreslås at påtalemyndigheten gis kompetanse i hastesaker. Paragraf 216 d gjelder tilsvarende.

Åttende ledd gir politiet hjemmel til å foreta innbrudd for å plassere eller fjerne utstyr som er nødvendig for å gjennomføre kameraovervåkingen.

Etter *niende ledd* treffes avgjørelse om skjult kameraovervåking uten at den mistenkte eller den som avgjørelsen ellers rammer, gis adgang til å uttale seg. Avgjørelsen blir heller ikke meddelt dem. Ved avgjørelse om skjult kameraovervåking på privat sted etter annet ledd, skal likevel mistenkte og den som har rådighet over stedet som hovedregel underrettes når overvåkingen er avsluttet. «Den som har rådigheten» vil kunne være person som eier, leier, låner eller på annen måte disponerer det lokalet som avlyttes. Paragraf 216 j gjelder tilsvarende. Bestemmelsen er et ledd i forslaget om enhetlige regler om underretning ved bruk av skjulte tvangsmidler, jf. punkt 6.10 og 12.10.

Til § 202 b

Tilføyelsen av straffeloven § 254 (straffeloven 1902 § 223) i § 202 b *første ledd første punktum* innebærer at det åpnes for teknisk sporing i saker om frihetsberøvelse.

Til § 202 c

Tilføyelsen av straffeloven §§ 136 og 254 (straffeloven 1902 §§ 147 c og 223) i § 202 c *første ledd første punktum* innebærer at det åpnes for personnær teknisk sporing i saker om frihetsberøvelse og offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, jf. også punkt 7.4.6 og 7.4.11.

Sjette ledd og *nytt syvende ledd* erstatter tidligere sjette ledd, og innebærer en rekke endringer i reglene om underretning til mistenkte om den personnære tekniske sporingen. Det vises til merknadene til § 200 a tredje og fjerde ledd.

Hva gjelder personnær teknisk sporing skal det likevel nevnes at loven tidligere ikke ga regler om utsettelsens lengde i saker om overtredelse av straffeloven kapittel 17 (straffeloven 1902 kapittel 8 og 9), mens det nå – tilsvarende som ved skjult ransaking – kan gis utsettelse for inntil seks måneder om gangen, se *sjette ledd annet punktum*. Til forskjell fra tidligere, ligger dessuten utsettelsesmyndigheten hos retten og ikke hos påtalemyndigheten, se punkt 6.10.5.3.

Det er også grunn til å fremheve at *sjette ledd femte punktum* bestemmer at tredje ledd gjelder tilsvarende. § 202 c tredje ledd regulerer hvem som har kompetanse til å begjære rettens kjennelse for sporingen og gir regler om hastekompetanse. Noen tilsvarende bestemmelse har en ikke hatt for begjæring om utsatt underretning om sporingen, selv om det åpenbart har vært ment at de samme kompetansereglene skulle gjelde her. Gjennom henvisningen til tredje ledd er dette nå rettet opp.

Til § 202 e

Annet ledd første punktum er endret tilsvarende § 200 a tredje ledd første punktum. Det vises til kommentarene til denne. Utover å presisere «strengt nødvendig»-vilkåret, har departementet – i likhet med utvalget, se NOU 2009: 15 side 354 – ikke gått inn for andre endringer i reglene om båndlegging av formuesgoder.

Til § 208 a

Første og annet ledd er betydelig endret som følge av nye regler om underretningsplikt.

Første ledd første punktum gir påtalemyndigheten myndighet til å beslutte at underretning om beslaget kan utsettes for inntil åtte uker, såfremt underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. Sistnevnte erstatter det tidligere «strengt nødvendig»-vilkåret, se punkt 6.10.5.1. At påtalemyndigheten gis myndighet til å beslutte utsatt underretning for inntil åtte uker, er nytt og var heller ikke foreslått av utvalget. Se nærmere om bakgrunnen for regelen i punkt 6.10.5.3. Som tidligere må det foreligge skjellig grunn til mistanke om en handling eller forsøk på en handling som kan medføre høyere straff enn fengsel i seks måneder.

Første ledd annet og tredje punktum gir retten myndighet til ved kjennelse å beslutte ytterligere utsettelse dersom påtalemyndighetens utsettelse i inntil åtte uker ikke anses tilstrekkelig og vilkårene i første punktum er oppfylt. *Annet punktum* gir retten myndighet til å beslutte at underretning kan utsettes ytterligere for inntil seks måneder om gangen i saker om overtredelse av straffeloven kapittel 17 (straffeloven 1902 kapittel 8 og 9). *Tredje punktum* gjelder for alle andre saker, og bestemmer at retten her kan gi utsettelse for inntil åtte uker om gangen.

Fjerde punktum oppstiller et unntak fra tredje punktum, ved at retten gis myndighet til å beslutte utsatt underretning i inntil fire måneder dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter åtte uker vil være uten betydning, se merknad til § 200 a tredje ledd fjerde punktum.

Femte punktum er en ren videreføring av tidligere første ledd annet punktum.

Annet ledd svarer til § 200 a fjerde ledd. Det vises til merknadene til denne.

Til § 210

I *annet ledd første punktum* er formuleringen «kjennelse» endret til «beslutning». Av bestemmelsen følger i dag forutsetningsvis at rettens avgjørelse treffes ved kjennelse. Dette beror på en inkurie, se punkt 10.2. Beslutnings form er tilstrekkelig.

Til § 210 a

Første ledd er endret tilsvarende § 208 a første ledd første til fjerde punktum. Det vises til merknadene til disse bestemmelsene.

Til § 210 c

Første ledd er endret tilsvarende § 208 a første ledd første til fjerde punktum, og *annet ledd* er endret tilsvarende § 208 a annet ledd. Det vises til merknadene til § 208 a.

Femte ledd er endret slik at den viser til § 216 d. At bestemmelsen tidligere viste til § 216 e annet ledd og ikke § 216 d, antas å skyldes feilskrift, se Ot.prp. nr. 64 (1998–99) side 154 og NOU 2009: 15 side 355.

Til § 216 a

I *første ledd bokstav b* foreslås straffeloven §§ 136, 254, 257 og 311 (straffeloven 1902 §§ 204 a, 223 og 224) samt lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd, lagt til i opplistingen. Endringen medfører at kommunikasjonsavlytting kan benyttes i etterforskningen av saker om offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger, befatning med overgrepsbilder av barn, frihetsberøvelse, menneskehandel og grov menneskesmugling – forutsatt at øvrige vilkår for slik metodebruk er oppfylt. Se proposisjonen punkt 7.4.

Til § 216 b

I *annet ledd bokstav c* foreslås det presisert at kommunikasjonskontroll etter § 216 b kan gå ut på å bruke teknisk utstyr for å lokalisere et kommunikasjonsanlegg. Dette kan for eksempel skje ved bruk av en såkalt IMSI-catcher eller annet egnet utstyr. Henvisningen til anlegg som nevnt i bokstav a, innebærer at det er forutsetning at lokaliseringen gjelder kommunikasjonsanlegg som den mistenkte besitter eller kan antas å ville bruke. Slik metodebruk vil kunne gi politiet informasjon om hvor det aktuelle anlegget befinner seg og dermed mistenktes oppholdssted, noe som i sin tur – og i kombinasjon med andre etterforskningsmetoder – vil kunne bidra til å identifisere mistenkte. Forslaget har sin bakgrunn i Høyesteretts ankeutvalgs kjennelse inntatt i Rt. 2009 side 394, der utvalget konkluderte med at det etter gjeldende rett ikke er adgang til å iverksette kommunikasjonskontroll etter § 216 b med sikte på å avdekke brukerens identitet. Det vises til punkt 7.7.

I *annet ledd bokstav d* foreslås et tillegg som gir politiet hjemmel til å innhente fra netteier eller tjenestetilbyder opplysninger om den geografiske plasseringen til et bestemt kommunikasjonsanlegg, uavhengig av om anlegget er i bruk til kommunikasjon. Henvisningen til anlegg som nevnt i bokstav a, innebærer at det er forutsetning at lokaliseringen gjelder kommunikasjonsanlegg som den mistenkte besitter eller kan antas å ville bruke. Med opplysninger om «den geografiske posisjonen til et slikt anlegg» menes lokaliseringsdata med så høy nøyaktighetsgrad som mulig. Det påhviler nett- og tjenestetilbyder å yte den bistand som er nødvendig for å gjennomføre tiltaket, jf. straffeprosessloven § 216 a fjerde ledd annet punktum jf. § 216 b tredje ledd. Bistandsplikten medfører imidlertid ikke noen plikt for tilbyder til å iverksette selvstendige tiltak, for eksempel ved å konfigurere systemene slik at lokaliseringsdata genereres oftere eller med høyere nøyaktighetsgrad enn det som er nødvendig for tilbyders egne formål. Det er likevel uten betydning for utleve-

ringsplikten hvor i tilbyders systemer de aktuelle opplysningene hentes ut fra.

Annet ledd ny bokstav e gir politiet adgang til i hemmelighet å overføre signaler til et bestemt kommunikasjonsanlegg, for å effektivisere tiltak som nevnt i bokstav c og d. Bestemmelsen gir blant annet hjemmel for bruk av såkalt stille SMS. Signalene som genereres ved overføringen kan nyttiggjøres for eksempel ved å begjære basestasjonsopplysninger utlevert fra nett- og tjenestetilbyder. Ved bruk av stille SMS påhviler det nett- og tjenestetilbyder å yte den bistand som er nødvendig for å gjennomføre tiltaket, jf. straffeprosessloven § 216 a fjerde ledd annet punktum jf. § 216 b tredje ledd. Dette innebærer blant annet at tilbyderne plikter å åpne sine nett for sending av skjulte signaler fra politiet.

Til § 216 j

Bestemmelsen gir nye regler om underretning om kommunikasjonskontrollen. Mens bestemmelsen tidligere bare åpnet for underretning på begjæring, er nå hovedregelen at det skal underrettes om kommunikasjonskontrollen uten at det er nødvendig at mistenkte eller andre begjærer dette. Samtidig er det gitt hjemler for å utsette og unnlate underretning. Bestemmelsen samsvarer dermed innholdsmessig i stor grad med de øvrige hjemlene for utsatt underretning i §§ 200 a, 202 c, 208 a, 210 a og 210 c. Bestemmelsen svarer et stykke på vei til utvalgets forslag, men er langt mer utbygd for at den skal henge sammen med de bestemmelsene om underretningsplikt som gjelder for de øvrige skjulte tvangsmidlene. Bakgrunnen for endringene er nærmere omtalt i punkt 6.10.2.

Første ledd første punktum bestemmer at mistenkte og den som har rådigheten over kommunikasjonsanlegget skal underrettes om kommunikasjonskontrollen når den er avsluttet. Noen tilsvarende bestemmelse er ikke foreslått av utvalget, som likevel klart forutsetter at underretning til mistenkte er hovedregelen. Med «den som har rådigheten over kommunikasjonsanlegget» siktes til den personen som eier, låner, leier eller på annet grunnlag besitter den aktuelle telefonen eller datamaskinen mv., for det tilfellet at dette er en annen enn mistenkte. Det kan for eksempel være at mistenkte regelmessig bruker sin samboers datamaskin. Også samboeren skal da som utgangspunkt underrettes om kommunikasjonskontrollen når denne er avsluttet. For øvrig må bestemmelsen ses i sammenheng med annet ledd, som gir påtalemyndigheten en frist på to uker til å fremsette begjæring om utsatt underretning. Se nærmere punkt 6.10.2 og 6.10.5.2.

Første ledd annet til femte punktum svarer til § 200 a tredje ledd første til fjerde punktum og § 202 c sjette ledd første til fjerde punktum. Det vises til merknadene til § 200 a tredje ledd første til fjerde punktum.

Annet ledd første punktum bestemmer at utsatt underretning må begjæres innen to uker etter at kontrollen er avsluttet, mens *annet ledd annet punktum* bestemmer at retten uten ugrunnet opphold skal ta stilling til begjæringen. Tilsvarende presiseringer var ikke foreslått av utvalget. Se nærmere om begrunnelsen for reglene i punkt 6.10.5.2.

Tredje ledd første og annet punktum svarer til § 200 a fjerde ledd første og annet punktum og § 202 c syvende ledd første og annet punktum, se merknadene til § 200 a fjerde ledd første og annet punktum.

Tredje ledd tredje punktum bestemmer at § 216 e gjelder tilsvarende. Det var også tidligere vist til denne i § 216 j – se for så vidt også nytt sjette ledd fjerde punktum som gjelder når underretning begjæres av mistenkte eller andre.

Fjerde ledd bestemmer at mistenkte og den som har rådigheten over kommunikasjonsanlegget skal underrettes om kjennelsen og om kontrollen når fristen for utsatt underretning er utløpt og ikke forlenget. Bestemmelsen har ingen parallell i utvalgets forslag, men tilsvarende regel er gitt i de fleste øvrige hjemler for skjult metodebruk, og ville uansett kunne sluttes ut fra første ledd. Departementet har likevel funnet det hensiktsmessig med en uttrykkelig lovregulering av dette.

Femte ledd gir regler om personell kompetanse når politiet ber om rettens samtykke til å utsette eller unnlate underretning eller selv beslutter utsatt underretning i kraft av hastekompetanse. Noen slik regulering er ikke tatt inn i utvalgets lovforslag, men lignende bestemmelser gjelder for de øvrige metodene hvor underretning kan utsettes. Ettersom det er tale om inngripende metodebruk, fordrer bruk av hastekompetanse at det ved opphold er *stor* fare for at etterforskningen vil lide. Bruk av hastekompetanse synes imidlertid mindre praktisk, ettersom politiet etter avsluttet kontroll i praksis har to uker på å områ seg, jf. annet ledd. Det kan vel imidlertid tenkes at toukersfristen går mot slutten og mistenkte planlegges underrettet, men at det så oppstår forhold i etterforskningen som likevel ikke gjør dette tilrådelig, og en heller ikke rekker å overholde toukersfristen for fremsettelse av begjæring til retten

etter annet ledd. Tilsvarende kan tenkes å oppstå mot slutten av en utsettelsesperiode. I slike tilfelle kan hastekompetansen tenkes brukt.

Sjette ledd første punktum bestemmer at enhver kan begjære underretning om hvorvidt han eller hun har vært undergitt kommunikasjonskontroll, selv om det er besluttet at underretning kan utsettes eller unnlates. Metodekontrollutvalget drøfter ikke om adgang til utsatt eller unnlatt underretning bør suppleres med en adgang til å få kjennskap til metodebruken på begjæring.

Sjette ledd annet punktum bestemmer at underretning skal gis med mindre det foreligger omstendigheter som nevnt i første ledd annet punktum. Politiet må dermed på nytt ta stilling til om vilkårene for utsettelse er til stede, selv om begjæringen kommer i en periode hvor det er gitt tillatelse til at underretning ikke skal gis. At det må foretas en fornyet vurdering, korresponderer med tredje ledd tredje punktums henvisning til § 216 f annet ledd, som innebærer at underretning må gis før fristen for utsatt underretning løper ut, dersom vilkårene for utsettelse ikke lenger er oppfylt. Politiet må derfor uansett vurdere dette kontinuerlig.

Sjette ledd tredje punktum bestemmer at avslag på begjæringen kan bringes inn for retten, som avgjør spørsmålet ved kjennelse.

Sjette ledd fjerde punktum bestemmer at § 216 e gjelder tilsvarende, og medfører at saken bringes inn for tingretten på det sted hvor det mest praktisk kan skje, og at avgjørelsen treffes uten at den mistenkte eller den som avgjørelsen ellers rammer gis anledning til å uttale seg eller meddeles kjennelsen. Bestemmelsen samsvarer med tidligere § 216 j tredje ledd annet punktum.

Sjette ledd fjerde punktum om at underretning bare kan gis om kommunikasjonskontroll som er besluttet etter at § 216 j trådte i kraft (det vil si etter 21. april 1995), er en ren videreføring av tidligere § 216 j første ledd tredje punktum.

Bakgrunnen for sjette ledd er nærmere omtalt i punkt 6.10.6.1.

Syvende ledd gir Kongen hjemmel til å gi nærmere regler om underretning ved kommunikasjonskontroll som skjer på begjæring fra utenlandske myndigheter. Forskriftshjemmelen har bakgrunn i høringen, se punkt 6.10.8.

Til § 216 m

I *første ledd bokstav b* er henvisningen til straffeloven § 79 bokstav c (straffeloven 1902 § 60 a) fjernet hva gjelder drap etter straffeloven § 275 (straffeloven 1902 § 233). Endringen medfører at politiet i etterforskningen av drap kan anvende romavlytting, uten krav om at handlingen kan knyttes til organisert kriminalitet.

For grovt ran og særlig grov narkotikaforbrytelse etter straffeloven § 328 og § 232 annet ledd (straffeloven 1902 henholdsvis §§ 268 jf. 267 og § 162 tredje ledd), foreslås kravet om tilknytning til organisert kriminalitet opprettholdt. Disse lovbruddene er derfor flyttet til *første ledd bokstav c*. Som følge av endringen i kriminalitetskravet med hensyn til drap, blir *nåværende bokstav c* overflødig. Se proposisjonen punkt 8.4.

I *sjette ledd* er det tilføyd at etterfølgende underretning skal gis til mistenkte og den som har rådigheten over det stedet som avlyttes. Tilføyelsen må ses i lys av at § 216 j gjelder tilsvarende for romavlytting, og at det dermed som utgangspunkt skal underrettes også i saker om romavlytting, se nærmere § 216 j med merknader. «Den som har rådigheten» vil kunne være mistenkte selv, men også andre som eier, leier, låner eller på annen måte disponerer det lokalet som avlyttes.

Til § 216 o

Bestemmelsen er ny, og den åpner for at retten ved kjennelse kan gi politiet tillatelse til å foreta dataavlesing, se kapittel 14.

I *første ledd* er dataavlesing omtalt som avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem. Med «datasystem» menes enhver innretning, bestående av maskinvare og programvare, som foretar behandling av data ved hjelp av dataprogrammer, se punkt 14.8.7. For eksempel omfattes datamaskiner, nettbrett og smarttelefoner. Metoden gir politiet anledning til å overvåke den fortløpende bruken av datasystemet, og til å hente ut informasjon som er lagret eller genereres i systemet, se merknadene til § 216 o fjerde ledd nedenfor og punkt 14.8.4 og 14.8.8.

Kompetansen til å gi tillatelse til dataavlesing foreslås lagt til retten. Dersom det ved opphold er stor fare for at etterforskningen vil lide, kan ordre fra påtalemyndigheten likevel tre i stedet for rettens kjennelse (se nedenfor om henvisningen i femte ledd til straffeprosessloven § 216 d).

Tillatelse til dataavlesing kan bare gis når det foreligger skjellig grunn til mistanke om at noen har begått eller forsøkt å begå en handling som nevnt i første ledd bokstav a eller b. Begrepet «skjellig grunn» skal her forstås på samme måte som ellers i straffeprosessloven, se for eksempel § 216 a om kommunikasjonsavlytting. Også de øvrige vilkårene for dataavlesing er langt på vei

sammenfallende med de som gjelder for kommunikasjonsavlytting.

Etter *første ledd bokstav a* kan dataavlesing iverksettes når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i ti år eller mer. Se punkt 14.8.5 om betydningen av gjentagelse og sammenstøt av lovbrudd.

I *første ledd bokstav b* åpnes det for at retten også kan tillate dataavlesing i forbindelse med etterforskning av handlinger eller forsøk på nærmere angitte handlinger som ikke oppfyller strafferammekravet etter første ledd bokstav a, men hvor det likevel er behov for å kunne bruke dataavlesing. Opplistingen av straffebud er sammenfallende med den som foreslås for kommunikasjonsavlytting etter § 216 a, se punkt 14.8.5 og punkt 7.4.

Annet ledd gjør det klart at dataavlesing kan besluttes selv om straff ikke kan idømmes på grunn av bestemmelsene om tilregnelighet i straffeloven § 20 første ledd (straffeloven 1902 §§ 44 eller 46), og selv om tilstanden har medført at den mistenkte ikke har utvist skyld. Regelen er den samme ved kommunikasjonsavlytting og romavlytting, se henholdsvis §§ 216 a annet ledd og 216 m annet ledd.

Etter *tredje ledd* skal tillatelse til dataavlesing bare kunne gis dersom det må antas at avlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort. Disse vilkårene skal forstås på samme måte som de tilsvarende vilkårene i §§ 200 a annet ledd (hemmelig ransaking), 216 c første ledd (kommunikasjonskontroll) og 216 m tredje ledd (romavlytting). Det sentrale er at dataavlesing bare skal kunne tillates dersom det må antas at avlesingen vil gi et vesentlig bidrag til oppklaring av saken, og bare når det må antas at mindre inngripende etterforskningsmetoder vil komme til kort. Hvorvidt bruk av en annen metode vil være mer eller mindre inngripende, kan avhenge av de konkrete omstendighetene – se punkt 14.8.6.

Vilkårene i tredje ledd suppleres av det alminnelige forholdsmessighetsprinsippet som gjelder for all bruk av tvangsmidler. Etter § 170 a kan et tvangsmiddel bare brukes når det er tilstrekkelig grunn til det, og ikke når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep.

Etter *fjerde ledd første punktum* kan det bare gis tillatelse til å avlese bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller kan antas å ville bruke. Det sistnevnte alternativet sikter til brukerkontoer knyttet til for eksempel internettbaserte e-posttjenester og skylagringstjenester, se nærmere om dette i punkt 14.8.7. I formuleringen «bestemte» ligger det et krav om at datasystemet eller brukerkontoen som skal avleses må identifiseres i politiets begjæring og i politiets beslutning, dersom hastekompetansen benyttes, samt i rettens kjennelse. Angivelsen må være så spesifikk som mulig for å unngå tvil om hvilke objekter som tillates avlest, for eksempel en telefons IMEI-nummer, et brukernavn tilhørende en brukerkonto eller en e-postadresse tilhørende en e-postkonto, eventuelt en angivelse av det geografiske sted hvor utstyret befinner seg og av hvem som har rådighet over det.

Videre følger det av *fjerde ledd annet punktum* at § 216 c annet ledd gjelder tilsvarende ved dataavlesing. Det innebærer at det må foreligge særlige grunner for å tillate avlesing av datasystem som er tilgjengelig for et større antall personer, eller som tilhører advokat, lege, prest mv. eller redaktør eller journalist.

I *fjerde ledd tredje punktum* er det angitt at dataavlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen. I praksis kan det være overlapp mellom kategoriene. Meningen er for det første at politiet fortløpende skal kunne tilegne seg innholdet i kommunikasjon til, fra og i datasystemet eller brukerkontoen, uavhengig av om tilegnelsen skjer mens informasjonen er under overføring, eller først etter at informasjonen er sendt eller mottatt. Videre kan politiet sikre annen informasjon som er lagret i datasystemet eller brukerkontoen. Med «andre opplysninger om bruk av datasystemet eller brukerkontoen» siktes det til all informasjon knyttet til bruk av systemet – både informasjon som brukeren selv produserer og informasjon som datasystemet genererer automatisk. Avlesingsadgangen omfatter også signalstrømmen mellom selve datasystemet og tilknyttet utrustning, som skjerm, tastatur, kamera, mikrofon og høyttaler. Avlesingsadgangen gjelder opplysninger som knytter seg til bruken av datasystemet. Det innebærer at politiet ikke kan aktivere et tilknyttet kamera for å utføre kameraovervåking, eller slå på en tilknyttet mikrofon for å utføre romavlytting med hjemmel i bestemmelsen om dataavlesing. Slik tvangsmiddelbruk må eventuelt vurderes opp mot vilkårene i bestemmelsene om kameraovervåking og romavlytting og fordrer slik tillatelse fra domstolen.

Av *femte ledd* følger det at bestemmelsene i §§ 216 d til 216 k gjelder tilsvarende ved dataavle-

sing, men likevel slik at tillatelse til dataavlesing bare kan gis for høyst to uker om gangen, se nærmere omtale i punkt 14.8.9 og 14.8.10. Eventuelt utstyr som er benyttet for å gjennomføre dataavlesingen skal fjernes snarest mulig etter avlesingsperiodens utløp.

Til § 216 p

Bestemmelsen er ny, og angir rammer for hvordan politiet kan gå frem ved gjennomføring av dataavlesing etter § 216 o.

Av *første ledd første punktum* følger det at dataavlesing bare kan foretas av personell som er særlig skikket til det og som utpekes av politimesteren, sjef PST eller den som bemyndiges. Meningen er at dataavlesingen bare skal kunne utføres av personell med tilstrekkelig høy informasjonsteknologisk kompetanse, se også punkt 14.8.8.

I *første ledd annet punktum* er det angitt at dataavlesing kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. Politiet har stor frihet med hensyn til valg av fremgangsmåte og hjelpemidler, se punkt 14.8.8. Videre følger det av *første ledd tredje punktum* at § 199 a gjelder tilsvarende ved dataavlesing, slik at politiet kan pålegge enhver som har befatning med datasystemet å gi nødvendige opplysninger for å gi tilgang til datasystemet.

I *første ledd fjerde punktum* er det presisert at politiet har anledning til å foreta datainnbrudd dersom det er nødvendig for å gjennomføre dataavlesingen.

Av *første ledd femte punktum* følger det at adgangen til å benytte tekniske hjelpemidler og dataprogram innebærer at politiet blant annet skal kunne installere egnet programvare eller fysiske komponenter i datasystemet som skal avleses. Det er presisert at slike innretninger og programvare også kan installeres i maskinvare som kan knyttes til datasystemet, men som ikke er en nødvendig del av det. Eksempler på slik maskinvare er typisk tilbehør som tastatur og hodetelefoner, eller flyttbare lagringsmedier – se punkt 14.8.8.

Etter *første ledd sjette punktum* kan politiet også foreta fysisk innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen, med mindre retten angir noe annet i kjennelsen. Tilsvarende gjelder ved romavlytting, jf. § 216 m femte ledd. Retten bør ikke gi tillatelse til innbrudd dersom politiet vil kunne gjennomføre avlesingen tilfredsstillende ved hjelp av fremgangsmåter som ikke krever at det gjøres fysisk innbrudd. Første ledd femte punktum gir bare anledning til å foreta innbrudd og til befatning med det datasystemet som skal avleses. Øvrig ransaking av det sted hvor datasystemet er plassert, krever særskilt tillatelse.

Annet ledd angir plikter for politiet med hensyn til å begrense ulemper som dataavlesing kan medføre, se punkt 14.8.8.

Til § 222 d

I *første ledd bokstav b* fremgår det at drap, uavhengig av hvilken sammenheng det inngår i, er en så alvorlig og uavvendelig krenkelse av menneskelivet at politiet har anledning til å benytte tvangsmidler for å søke det avverget. Det er således ikke lenger et vilkår at drapet vil utføres som ledd i virksomheten til en organisert kriminell gruppe, jf. straffeloven § 79 bokstav c (straffeloven 1902 § 60 a), eller som ledd i motarbeidelsen av rettsvesenet, jf. straffeloven §§ 157-159 (straffeloven 1902 § 132 a).

I *første ledd bokstav c* fremgår det at politiet fortsatt skal ha adgang til å bruke skjulte tvangsmidler for å avverge grove narkotikaforbrytelser og grovt ran som ledd i organisert kriminalitet.

Begrepet «rimelig» inntas i bestemmelsens *annet ledd første punktum*. Dette er ikke ment å innebære noen realitetsendring av mistankekravet.

I *annet ledd bokstav a* inntas straffeloven §§ 127 og 136 (straffeloven 1902 §§ 94 første ledd og 147 c) i oppregningen. Dette innebærer at PST kan gis adgang til å benytte tvangsmidler for å avverge henholdsvis forbund om krenkelse av Norges selvstendighet og forfatning og offentlig oppfordring, rekruttering eller opplæring til terrorhandlinger.

I *annet ledd bokstav d*, som gir PST utvidet myndighet til å benytte tvangsmidler for å avverge integritetskrenkelser, fjernes henvisningen til straffeloven § 275 (straffeloven 1902 § 233) om drap. PST vil kunne benytte tvangsmidler for å avverge drap generelt etter § 222 d første ledd bokstav b, og det stilles således ikke lenger krav om at handlingen retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater. Henvisningen til straffeloven § 253 om tvangsekteskap fjernes, da faren for at ovennevnte gruppe utsettes for slikt lovbrudd anses begrenset. Videre inntas en henvisning til § 256 om forbund om grov frihetsberøvelse, som ble utelatt ved ikraftsetting av straffeloven, jf. Prop. 64 L (2014–2015) punkt 6.7.10 side 87, der straffeloven 1902 §§ 222 og 223 ved en inkurie kun ble

foreslått erstattet med straffeloven §§ 251, 253 og 254, til tross for at § 256 tilsvarer straffeloven 1902 § 223 tredje ledd. Det fremgår av nevnte proposisjon punkt 2.4 side 14 at departementet så langt som mulig søkte å erstatte aktuelle henvisninger til straffeloven 1902 med henvisninger til tilsvarende bestemmelser i straffeloven.

I *tredje ledd annet punktum* inntas en henvisning til straffeprosessloven §§ 202 a annet ledd og 216 o. Dette innebærer at tillatelse til å benytte tvangsmidlene skjult kameraovervåking på privat sted og dataavlesing i avvergende øyemed bare kan gis når særlige grunner tilsier det.

I tredje ledd tredje punktum inntas en henvisning til handlinger som rammes av straffeloven §§ 251, 254, 256, 263, 273 eller 275 (straffeloven 1902 §§ 222, 223, 227, 229, 231 eller 233) og som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater. Dette innebærer at PST kan gis adgang til å benytte romavlytting for å avverge trusler eller angrep mot myndighetspersoner.

16.2 Til endringene i politiloven

Til § 17 d

I *første ledd* gis PST adgang til å benytte tvangsmidlene fremtidig utleveringspålegg med utsatt underetning og dataavlesing som ledd i sin forebyggende virksomhet, se punkt 13.5.5.4.

Henvisningen i *første ledd bokstav c* til straffeloven § 142 (straffeloven 1902 § 152 a) innebærer at PST kan benytte tvangsmidler for å forebygge ulovlig omgang med radioaktivt materiale, biologiske eller kjemiske våpen eller en kjernefysisk eller radioaktiv anordning (masseødeleggelsesvåpen).

I *første ledd bokstav d* fjernes henvisningen til straffeloven § 253 om tvangsekteskap, da faren for at medlemmer av de høyere statsmakter utsettes for slikt lovbrudd anses begrenset. Videre fjernes henvisningen til § 274 om grov kroppsskade. Det følger av Prop. 64 L (2014–2015) om lov om ikraftsetting av straffeloven punkt 2.4 side 14 at departementet legger til grunn som et utgangspunkt at det i tilfeller hvor henvisningen skal omfatte både det såkalte grunndeliktet og det grove deliktet ved graderte lovbrudd, er det tilstrekkelig å vise til grunndeliktet.

Tilføyelsen av straffeprosessloven §§ 202 a annet ledd og § 216 o i *annet ledd annet punktum* innebærer at PST bare kan gis tillatelse til å nytte tvangsmidlene kameraovervåking på privat sted og dataavlesing når særlige grunner tilsier det.

I § 17 d *annet ledd tredje punktum* nedsettes det forbud mot bruk av romavlytting i private hjem i forebyggende øyemed.

I § 17 d *annet ledd fjerde punktum* åpnes det for innbrudd for å legge til rette for dataavlesing og skjult ransaking i private hjem for å forebygge terrorhandlinger. Det understrekes at sjefen eller den assisterende sjefen for PST, som fremmer beslutning om å begjære bruk av tvangsmidler i forebyggingsøyemed, og domstolen i tillegg må foreta en forholdsmessighetsvurdering i den enkelte sak, og blant annet se hen til hvor sikre holdepunkter en har for at en terrorhandling vil kunne bli begått og hvor alvorlige konsekvensene vil kunne bli.

Henvisningen i *tredje ledd første punktum* til første ledd bokstav a innebærer at PST gis hastekompetanse til å benytte tvangsmidler for å forebygge terrorhandling, jf. straffeloven §§ 131–134 (straffeloven 1902 § 147 a). Henvisningen til bokstav d er en konsekvens av at attentatsaker nå inntas i bokstav d i stedet for c, fordi ulovlig omgang med masseødeleggelsesvåpen er inntatt som ny bokstav c.

Justis- og beredskapsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i straffeprosessloven mv. (skjulte tvangsmidler).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i straffeprosessloven mv. (skjulte tvangsmidler) i samsvar med et vedlagt forslag.

Forslag
til lov om endringer i straffeprosessloven mv. (skjulte tvangsmidler)

I

I lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker gjøres følgende endringer:

I § 100 a første ledd første punktum tilføyes §§ «202 a annet ledd» og «216 o» i opplistingen.

§ 100 a annet ledd skal lyde:

Advokaten skal vareta den mistenktes *og eventuelle tredjepersoners* interesser i forbindelse med rettens behandling av begjæringen. *Samme advokat skal så langt det er mulig oppnevnes ved begjæring om forlengelse av bruken av tvangsmidler og ved begjæring om andre tvangsmidler mot mistenkte som nevnt i første ledd.* Advokaten skal gjøres kjent med begjæringen og grunnlaget for den, har etter anmodning krav på innsyn i sakens dokumenter med de begrensninger som følger av §§ 242 og 242 a, har krav på varsel til *og tilstedeværelse under* rettsmøte til behandling av begjæringen og har rett til å uttale seg før retten treffer avgjørelse. *Påtalemyndigheten skal fremme begjæring om forlengelse så tidlig at advokaten kan få varsel senest dagen før rettsmøtet holdes.* Advokaten kan anke rettens kjennelse. Kapittel 26 gjelder så langt reglene passer.

§ 100 a fjerde ledd nytt annet punktum skal lyde:

Forbudet gjelder frem til mistenkte gjennom dokumentinnsyn får de samme opplysningene som forsvareren.

§ 200 a første ledd skal lyde:

Når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre straff av fengsel i 10 år eller mer, eller som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, *136,* 136 a, 231, *254, 257, 311,* 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231 *eller av lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd* kan retten ved kjennelse beslutte at ransaking kan settes i verk uten underretning til den mistenkte eller andre.

§ 200 a tredje og fjerde ledd skal lyde:

Retten kan ved kjennelse beslutte at underretning om ransakingen og resultatet av den også i ettertid kan utsettes dersom *underretning vil være vesentlig til skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. I saker om overtredelse av straffeloven kapittel 17 kan retten beslutte at underretning kan utsettes for inntil 6 måneder om gangen. I andre saker kan retten beslutte at underretning kan utsettes for inntil 8 uker om gangen. Dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 8 uker vil være uten betydning, kan retten beslutte at underretning kan utsettes i inntil 4 måneder.*

Underretning skal senest gis når tiltale tas ut eller saken henlegges og fristen etter § 75 annet ledd første punktum har gått ut. Retten kan likevel bestemme at underretning kan unnlates helt dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. § 216 e annet ledd, § 216 f annet ledd og § 216 j sjette ledd første til fjerde punktum og syvende ledd gjelder tilsvarende.

§ 200 a nåværende fjerde til syvende ledd blir femte til nytt åttende ledd.

Kapittel 15 a overskriften skal lyde:

Kapittel 15 a. Skjult *kameraovervåking* og teknisk sporing

§ 202 a skal lyde:

Når det foreligger skjellig grunn til mistanke om en eller flere straffbare handlinger som etter loven kan medføre høyere straff enn fengsel i 6 måneder, kan politiet iverksette skjult *kamera-*

overvåking på eller fra offentlig *sted når* slik overvåking vil være av vesentlig betydning for etterforskningen. *Beslutning treffes av retten.*

Retten kan ved kjennelse gi politiet tillatelse til å iverksette skjult kameraovervåking på privat sted når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling

a) som etter loven kan medføre straff av fengsel i 10 år eller mer

b) som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136, 136 a, 231, 254, 257, 311, 332 jf. 231, 335 jf. 231, 337 jf. 231 eller 340 jf. 231 eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5 eller av lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd.

Tillatelse kan bare gis dersom det må antas at slik overvåking vil være av vesentlig betydning for å oppklare saken, og oppklaring ellers i vesentlig grad vil bli vanskeliggjort.

§ 196 gjelder tilsvarende.

Som kameraovervåking regnes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkingskamera eller annet lignende utstyr som er fastmontert. Som kameraovervåking anses både overvåking med og uten mulighet for opptak av lyd- og bildemateriale. Det kan ikke gis tillatelse til å overvåke noens private hjem etter bestemmelsen her.

Tillatelse etter annet ledd kan bare gis for sted hvor det må antas at den mistenkte vil oppholde seg. Tillatelse til overvåking av sted hvor advokat, lege, prest eller andre erfaringsmessig fører samtaler av svært fortrolig art eller av redaksjonslokale eller tilsvarende sted hvor redaktør eller journalist fører samtaler av yrkesmessig art, kan bare gis når det foreligger særlige grunner, såfremt vedkommende ikke selv er mistenkt i saken.

Tillatelse til skjult kameraovervåking etter bestemmelsen her gis for et bestemt tidsrom, som ikke må være lengre enn strengt nødvendig og høyst 4 uker.

Dersom det ved opphold er stor fare for at etterforskningen vil lide, kan ordre fra påtalemyndigheten tre istedenfor rettens avgjørelse. § 216 d gjelder tilsvarende.

Når retten ikke bestemmer noe annet, kan politiet foreta innbrudd for å plassere eller fjerne utstyr som er nødvendig for å gjennomføre kameraovervåkingen.

Avgjørelse om skjult kameraovervåking treffes uten at den mistenkte eller den som avgjørelsen ellers rammer, gis adgang til å uttale seg, og avgjørelsen blir ikke meddelt dem. Ved tillatelse etter annet ledd skal likevel mistenkte og den som har rådighet over stedet, underrettes om overvåkingen når den er avsluttet. § 216 j gjelder tilsvarende.

§ 202 b første ledd første punktum skal lyde:

Når noen med skjellig grunn mistenkes for en handling eller forsøk på handling som etter loven kan medføre straff av fengsel i 5 år eller mer, eller som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 198 eller *254,* kan påtalemyndigheten beslutte at teknisk peileutstyr plasseres på kjøretøy, gods eller andre gjenstander for å klarlegge hvor den mistenkte eller gjenstandene befinner seg (teknisk sporing).

§ 202 c første ledd første punktum innledningen skal lyde:

Når noen med skjellig grunn mistenkes for en handling eller forsøk på handling som etter loven kan medføre straff av fengsel i 10 år eller mer, eller som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, *136*, 136 a *eller 254*, eller som rammes av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5, kan retten ved kjennelse gi politiet tillatelse til å

§ 202 c sjette og nytt syvende ledd skal lyde:

Retten kan ved kjennelse beslutte at underretning om sporingen og resultatet av den også i ettertid kan utsettes dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. I saker om overtredelse av straffeloven kapittel 17 kan retten beslutte at underretning kan utsettes for inntil 6 måneder om gangen. I andre saker kan utsatt underretning besluttes for inntil 8 uker om gangen. Dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 8 uker vil være uten betydning, kan retten beslutte at underretning kan utsettes i inntil 4 måneder. Tredje ledd gjelder tilsvarende.

Underretning skal senest gis når tiltale tas ut eller saken henlegges og fristen etter § 75 annet ledd første punktum har gått ut. Retten kan likevel bestemme at underretning kan unnlates helt dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder

eller omstendighetene for øvrig gjør det strengt nødvendig. § 216 e annet ledd, § 216 f annet ledd og § 216 j sjette ledd første til fjerde punktum og syvende ledd gjelder tilsvarende.

§ 202 e annet ledd første punktum skal lyde:

Dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, kan retten beslutte at varsel som nevnt i første ledd skal unnlates og underretning om kjennelsen utsettes.

§ 208 a første og annet ledd skal lyde:

Når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre høyere straff enn fengsel i 6 måneder, kan *påtalemyndigheten* beslutte at underretning om beslaget til den mistenkte eller andre som rammes av beslaget, kan utsettes *for inntil 8 uker, dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. I saker om overtredelse av straffeloven kapittel 17 kan retten ved kjennelse på samme vilkår beslutte at underretning kan utsettes ytterligere for inntil 6 måneder om gangen. Tilsvarende kan retten i andre saker beslutte at underretning kan utsettes ytterligere for inntil 8 uker om gangen. Dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 8 uker vil være uten betydning, kan retten beslutte at underretning kan utsettes i inntil 4 måneder.* § 196 gjelder tilsvarende.

Underretning skal senest gis når tiltale tas ut eller saken er henlagt og fristen etter § 75 annet ledd første punktum har gått ut. Retten kan likevel bestemme at underretning kan unnlates helt dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. § 216 e annet ledd, § 216 f annet ledd og § 216 j sjette ledd første til fjerde punktum og syvende ledd gjelder tilsvarende.

§ 210 annet ledd første punktum skal lyde:

Dersom det ved opphold er fare for at etterforskningen vil lide, kan ordre fra påtalemyndigheten tre istedenfor *beslutning* av retten.

§ 210 a første ledd skal lyde:

Når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling som etter loven kan medføre høyere straff enn fengsel i 6 måneder, kan *påtalemyndigheten* beslutte at underretning om utleveringspålegg etter § 210 til den mistenkte eller andre som rammes av utleveringspålegget, kan utsettes *for inntil 8 uker, dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. I saker om overtredelse av straffeloven kapittel 17 kan retten ved kjennelse på samme vilkår beslutte at underretning kan utsettes ytterligere for inntil 6 måneder om gangen. Tilsvarende kan retten i andre saker beslutte at underretning kan utsettes ytterligere for inntil 8 uker om gangen. Dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 8 uker vil være uten betydning, kan retten beslutte at underretning kan utsettes i inntil 4 måneder.*

§ 210 c første og annet ledd skal lyde:

Påtalemyndigheten kan beslutte at underretning til den mistenkte om utleveringspålegg etter § 210 b kan utsettes *for inntil 8 uker, dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. I saker om overtredelse av straffeloven kapittel 17 kan retten ved kjennelse på samme vilkår beslutte at underretning kan utsettes ytterligere for inntil 6 måneder om gangen. Tilsvarende kan retten i andre saker beslutte at underretning kan utsettes ytterligere for inntil 8 uker om gangen. Dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 8 uker vil være uten betydning, kan retten beslutte at underretning kan utsettes i inntil 4 måneder.*

*Underretning skal senest gis når tiltale tas ut eller saken er henlagt og fristen etter § 75 annet ledd første punktum har gått ut. Retten kan likevel bestemme at underretning kan unnlates helt dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforsk-

ningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. § 216 e annet ledd, § 216 f annet ledd og § 216 j sjette ledd første til fjerde punktum og syvende ledd gjelder tilsvarende.

§ 210 c femte ledd skal lyde:

§ 216 *d* gjelder tilsvarende.

§ 211 og 212 oppheves.

§ 216 a første ledd bokstav b skal lyde:

b) som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, *136,* 136 a, 231, *254, 257, 311*, 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231, eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5 *eller av lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd.*

§ 216 b annet ledd bokstav c, d og ny e skal lyde:

c) å identifisere *eller lokalisere* anlegg som nevnt i bokstav a ved hjelp av teknisk utstyr,
d) at eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjonen, skal gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg som nevnt i bokstav a, andre data knyttet til kommunikasjon*, og den geografiske posisjonen til et slikt anlegg,*
e) *å overføre skjulte signaler til anlegg som nevnt i bokstav a, i forbindelse med tiltak som nevnt i bokstav c og d.*

§ 216 j skal lyde:

Mistenkte og den som har rådighet over kommunikasjonsanlegget skal underrettes om kommunikasjonskontrollen når den er avsluttet. Retten kan likevel ved kjennelse beslutte at underretning kan utsettes dersom underretning vil være til vesentlig skade for etterforskningen i saken eller en annen verserende sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. I saker om overtredelse av straffeloven kapittel 17 kan retten beslutte at underretning kan utsettes for inntil 6 måneder om gangen. I andre saker kan retten beslutte at underretning kan utsettes for inntil 8 uker om gangen. Dersom etterforskningens art eller andre særlige omstendigheter tilsier at fornyet prøving etter 8 uker vil være uten betydning, kan retten beslutte at underretning kan utsettes i inntil 4 måneder.

Utsatt underretning må begjæres innen to uker etter at kontrollen er avsluttet. Retten skal uten ugrunnet opphold ta stilling til begjæringen.

Underretning skal senest gis når tiltale tas ut eller saken henlegges og fristen etter § 75 annet ledd første punktum har gått ut. Retten kan likevel bestemme at underretning kan unnlates helt dersom saken henlegges og underretning vil være til vesentlig skade for fremtidig oppklaring av saken eller etterforskning av en annen sak om en lovovertredelse hvor det kan besluttes utsatt underretning, eller hensynet til politiets etterforskningsmetoder eller omstendighetene for øvrig gjør det strengt nødvendig. § 216 e og § 216 f annet ledd gjelder tilsvarende.

Når tidsfristen for utsatt underretning er utløpt og ikke forlenget, skal mistenkte og den som har rådigheten over kommunikasjonsanlegget underrettes om kjennelsen og om kontrollen.

Når politiet ber om rettens samtykke etter denne bestemmelsen, gjelder § 216 d annet ledd tilsvarende. Dersom det ved opphold er stor fare for at etterforskningen vil lide, kan ordre fra påtalemyndigheten tre istedenfor kjennelse av retten, men ikke utover 24 timer. § 197 tredje ledd og § 216 d gjelder tilsvarende.

Selv om det er besluttet at underretning kan utsettes eller unnlates, kan enhver begjære underretning om hvorvidt han eller hun har vært undergitt kommunikasjonskontroll etter dette kapitlet. Underretning skal gis med mindre det foreligger omstendigheter som nevnt i første ledd annet punktum. Avslag på begjæringen kan bringes inn for retten, som avgjør spørsmålet ved kjennelse. § 216 e gjelder tilsvarende. Underretning kan bare gis om kommunikasjonskontroll som er besluttet etter at denne bestemmelsen er trådt i kraft.

Kongen kan gi nærmere regler om underretning ved kommunikasjonskontroll som skjer på begjæring fra utenlandske myndigheter.

§ 216 m første ledd bokstav b og c skal lyde:

b) straffeloven *§ 275*,
c) *straffeloven §§ 232 annet ledd eller 328, jf. § 79 bokstav c.*

§ 216 m sjette ledd skal lyde:

Bestemmelsene i §§ 216 d til 216 k gjelder tilsvarende, likevel slik at rettens tillatelse ikke kan gis for mer enn to uker om gangen *og etterfølgende underretning gis til mistenkte og den som har rådigheten over det stedet som avlyttes.*

Nytt kapittel 16 d skal lyde:

Kap 16 d. Dataavlesing

§ 216 o. Retten kan ved kjennelse gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing) når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling

a) som etter loven kan medføre straff av fengsel i 10 år eller mer
b) som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136, 136 a, 231, 254, 257, 311, 332 jf. 231, 335 jf. 231, 337 jf. 231, eller 340 jf. 231, eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5 eller av lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd.

Dataavlesing kan besluttes selv om straff ikke kan idømmes på grunn av bestemmelsene i straffeloven § 20 første ledd. Det gjelder også når tilstanden har medført at den mistenkte ikke har utvist skyld.

Tillatelse etter første ledd kan bare gis dersom det må antas at dataavlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort. § 216 c annet ledd gjelder tilsvarende.

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

§§ 216 d til 216 k gjelder tilsvarende, likevel slik at rettens tillatelse ikke kan gis for mer enn to uker om gangen. Eventuelt utstyr som er benyttet for å gjennomføre dataavlesingen skal fjernes snarest mulig etter avlesingsperiodens utløp.

§ 216 p. Dataavlesing etter § 216 o kan bare utføres av personell som er særlig skikket til det og som utpekes av politimesteren, sjef PST eller den som bemyndiges. Avlesingen kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. § 199 a gjelder tilsvarende. Politiet kan bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen. Tekniske innretninger og dataprogram kan installeres i datasystemet og i annen maskinvare som kan knyttes til datasystemet. Når retten ikke bestemmer noe annet, kan politiet også foreta innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen.

Dataavlesingen skal innrettes slik at det ikke unødig fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Avlesingen skal utføres slik at det ikke unødig voldes fare for driftshindring eller for skade på utrustning eller data. 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.

§ 222 d første til tredje ledd skal lyde:

Retten kan ved kjennelse gi politiet tillatelse til som ledd i etterforsking å nytte tvangsmidler som nevnt i kapittel 15, 15 a, 16, 16 a, 16 b og 16 d når det er rimelig grunn til å tro at noen kommer til å begå en handling som rammes av

a) straffeloven §§ 131 eller 134,
b) straffeloven *§ 275, eller*
c) *straffeloven §§ 232 annet ledd eller 328, jf. § 79 bokstav c.*

Politiets sikkerhetstjeneste kan også gis slik tillatelse når det er *rimelig* grunn til å tro at noen kommer til å begå en handling som rammes av

a) straffeloven §§ 111, 113, 115, 117, 119, 123, 126, *127*, 128 første punktum, 129, 133, 135, *136,* 136 a eller 142,
b) lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5,
c) straffeloven §§ 139, 140, 192, 194, 238, 239, 240, 241, 242, 355, 356, 357 eller 358 og som begås med sabotasjehensikt, eller
d) straffeloven §§ *251, 254, 256,* 263 *eller 273 og* som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater.

Tillatelse kan bare gis dersom det må antas at inngrepet vil gi opplysninger av vesentlig betydning for å kunne avverge handlingen og at avverging ellers i vesentlig grad vil bli vanskeliggjort. Tillatelse til å nytte tvangsmidler som nevnt i §§ 200 a, *202 a annet ledd*, 202 c, 216 a, 216 m *og 216 o* kan bare gis når særlige grunner tilsier det. Politiets sikkerhetstjeneste kan bare gis tillatelse til å romavlytte, jf. § 216 m, når det er grunn til å tro at noen kommer til å begå en handling som rammes av straffeloven §§ 121, 123, 125, 126, 131, 133, 134 eller 142, *eller av §§ 251, 254, 256, 263, 273 eller 275 og som retter*

seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater.

II

I lov 4. august 1995 nr. 53 om politiet gjøres følgende endringer:

§ 17 d første og annet ledd skal lyde:

Retten kan ved kjennelse gi Politiets sikkerhetstjeneste tillatelse til som ledd i sin forebyggende virksomhet å nytte tvangsmidler som nevnt i straffeprosessloven §§ 200 a, 202 a, 202 c, 208 a, 210 a, *§ 210 c,* 211, 212, 216 a, 216 b, 216 m *eller 216 o* dersom det er grunn til å undersøke om noen forbereder en handling som rammes av

a) straffeloven §§ 131, 133 og 134,
b) straffeloven §§ 121 til 126,
c) *straffeloven § 142,*
d) straffeloven §§ 251, 254, 256, 263, 273 eller 275 og som retter seg mot medlemmer av Kongehuset, Stortinget, regjeringen, Høyesterett eller representanter for tilsvarende organer i andre stater.

Tillatelsen kan bare gis dersom det er grunn til å tro at inngrepet vil gi opplysninger av vesentlig betydning for å kunne forebygge handlingen, at forebygging ellers i vesentlig grad vil bli vanskeliggjort og inngrepet etter sakens art og forholdene ellers ikke fremstår som uforholdsmessig. Tillatelse til å nytte tvangsmidler som nevnt i straffeprosessloven §§ 200 a, *202 a annet ledd,* 202 c, 216 a, 216 m *og 216 o* kan bare gis når særlige grunner tilsier det. *Det kan ikke gis tillatelse til å romavlytte noens private hjem etter bestemmelsen her. Det kan bare gis tillatelse til å ransake eller ved dataavlesing å gjøre innbrudd i noens private hjem etter bestemmelsen her når det er grunn til å undersøke om noen forbereder en handling som nevnt i første ledd bokstav a.*

§ 17 d tredje ledd første punktum skal lyde:

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, kan ordre fra sjefen eller den assisterende sjefen for Politiets sikkerhetstjeneste tre i stedet for kjennelse av retten, bortsett fra ved romavlytting som nevnt i straffeprosessloven § 216 m.

III

I lov 21. juni 2013 nr. 86 gjøres følgende endringer:

Endringen i straffeprosessloven § 202 a nytt fjerde ledd blir nytt tiende ledd.

Endringen i straffeprosessloven § 202 c nytt syvende ledd blir nytt åttende ledd.

V

Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.

Bestilling av publikasjoner

Offentlige institusjoner:
Departementenes sikkerhets- og serviceorganisasjon
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 00 00

Privat sektor:
Internett: www.fagbokforlaget.no/offpub
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: 07 Xpress AS – 03/2016