



Nasjonal
kommunikasjons-
myndighet

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Oversendes postmottak@jd.dep.no.
Kopi: postmottak@sd.dep.no,
nina.nordby@jd.dep.no,
kurt-arne.sandvik@sd.dep.no.

Vår ref.: 1405898-2 - 008
Vår dato: 19.1.2015

Deres ref.: 14/7082
Deres dato: 4.12.2014

Saksbehandler: Jarle Langeland, Linda Must, Anton
Bolstad, Janne Steen Haugen, Fride Solvik

Ugradert

Hørings svar - forslag til endringer i politiloven og ekomloven

1. Innledning og hovedpunkter

Nasjonal kommunikasjonsmyndighet (Nkom) viser til høringsbrev 4.12.2014 fra Justis- og beredskapsdepartementet, der Post- og teletilsynet inviteres til å kommentere på forslag til endringer i politiloven og ekomloven. Post- og teletilsynet endret 1.1.2015 navn til Nasjonal kommunikasjonsmyndighet.

Nkom fører blant annet tilsyn med bruk av frekvensspekteret, og med at tilbydere av elektronisk kommunikasjonsnett og -tjeneste oppfyller sine sikkerhets- og beredskapsforpliktelser etter lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) og tilhørende forskriftsverk. Herunder fører Nkom tilsyn med at tilbyderne har tilstrekkelige sikkerhetstiltak for å beskytte brukernes kommunikasjon og data, jf. ekomloven § 2-7. Nkom har også en sentral rolle ved håndtering av blant annet utfallshendelser, hvor tilbyderne rapporterer til Nkom ved utfall og større forstyrrelser i nettet, uavhengig av årsaken til forstyrrelsene.

Nkom anser at forslaget til endringer i politiloven og ekomloven for å tillate bruk av støysending og falske basestasjoner reiser vesentlige prinsipielle spørsmål, både hva gjelder frekvensbruk/forstyrrelser og konfidensialitet ved elektronisk kommunikasjon.

Flere av spørsmålene er berørt i høringsnotatet, men viktige hensyn og negative konsekvenser for kommunikasjonens integritet og konfidensialitet kommer etter Nkoms syn ikke klart nok frem

i høringsnotatet. Nkom anser videre at forslaget har uavklarte grenseflater mot annet regelverk, særlig hva gjelder kommunikasjonskontroll.

Nkom støtter at det gis hjemmel for politiet til å benytte støysending (i høringsnotatet og ekomloven omtalt som "jamming") for å avverge utløsning av for eksempel sprengladninger, og anser at lovregulering av dette er å foretrekke fremfor bruk av nødrett. Forslaget går imidlertid meget langt i å åpne opp for både identitetsfangning uten rettskjennelse og støysending i et utall situasjoner, en hittil ukjent rettstilstand i Norge og de nordiske land.

I høringsdokumentet er den forventede praktiske bruken av mobilregulerte soner og støysendere vagt beskrevet. Høringen gjør heller ingen forsøk på å analysere konsekvensene disse tiltakene kan få for brukerne av kommunikasjonsnettene som blir rammet. Det er bekymringsverdig at høringen nærmest ensidig tar opp politiets behov og nytte av tiltakene, uten at ulemper og potensielle skadevirkninger for samfunnet som helhet vies særlig plass og analyse. Nkom viser i denne forbindelse til at utredningsinstruksen¹ stiller krav til grundige konsekvensutredninger, herunder for personvernmessige konsekvenser², noe som Nkom ikke kan se er gjort i dette tilfellet.

Videre understrekes det gjentatte ganger i høringsnotatet at metodene vil benyttes «i et fåtall saker», «...det skal mye til før politiet kan benytte de foreslåtte tiltakene» og lignende. Samtidig er den foreslåtte lovhjemmel i politiloven § 7b meget vidt utformet, og tersklene for bruk etter ordlyden utpreget skjønnsmessige. Nkom har vanskelig for å se hvordan lovgivers eventuelle intensjoner om begrenset bruk skal ivaretas slik de foreslåtte bestemmelser er utformet.

De foreslåtte bestemmelser må naturlig nok praktiseres innenfor rammene av overordnet lovverk. Både Grunnloven og den europeiske menneskerettighetskonvensjon (EMK) vil sette begrensninger for hvor langt de foreslåtte fullmakter kan benyttes. Disse begrensningene vil det imidlertid kunne være vanskelig å identifisere i pressede og tidskrisiske situasjoner. Også dette tilsier etter Nkoms oppfatning at selve hjemlene så langt som mulig bør være utformet slik at disse rammer respekteres i det enkelte tilfellet.

¹ Instruks om utredning av konsekvenser, foreleggelse og høring ved arbeidet med offentlige utredninger, forskrifter, proposisjoner og meldinger til Stortinget, fastsatt ved kongelig resolusjon 18. februar 2000, revidert ved kongelig resolusjon 24. juni 2005.

² Veileder til utredningsinstruksen – vurdering av personvernkonsekvenser – Fornyings- og administrasjonsdepartementet

2. Kort om tidligere prosesser

Ot.prp. nr. 60 (2004-2005) om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre kriminalitet) fra daværende Justis- og politidepartementet, ligger til grunn for at det ble foreslått endringer i ekomloven gjennom Ot.prp. nr. 72 (2006-2007). Førstnevnte fulgte opp Politimetodeutvalgets forslag i NOU 2004:6 Mellom effektivitet og personvern og Lundutvalgets forslag til endringer i straffeprosessloven i NOU 2003:18 Rikets sikkerhet.

Av hovedpunktene i Ot.prp.nr. 60 (2004-2005) går det frem at en ville gi politiet tilgang til to nye etterforskningsmetoder; romavlytting og identifisering av kommunikasjonsanlegg. De øvrige lovforslagene hadde det til felles at de utvidet anvendelsesområdet for dagens etterforskningsmetoder, med det for øyet å bedre politiets muligheter for å gripe inn før en alvorlig straffbar handling ble begått. Forslaget begrenset seg til å gjelde enkelte alvorlige straffbare handlinger som det var særlig viktig for samfunnet å forhindre. Departementet foreslo at det var retten som skulle gi slik tillatelse til bruk av tvangsmidler, og at bruken skulle gjelde som ledd i etterforskning.

For å vurdere hvordan etablering av mobilregulerte soner skulle kunne gjennomføres i praksis, etablerte Samferdselsdepartementet og daværende Justis- og politidepartementet en arbeidsgruppe bestående av Post- og teletilsynet, Politiet, Kriminalomsorgen, Forsvaret og et utvalg av tilbydere. Arbeidsgruppen, som ble ledet av Post- og teletilsynet, skulle levere en utredning innen 1. juli 2007.

Arbeidsgruppen hadde som mandat å klargjøre justismyndighetenes og Forsvarets behov for å kunne etablere mobilregulerte soner og klargjøre konsekvensene ved etablering av mobilregulerte soner. Arbeidsgruppen skulle også gi en anbefaling på hva som med hjemmel i ekomloven burde nedfelles i forskrift når det gjelder praktisk gjennomføring for å etablere mobilregulerte soner. Arbeidet strakk seg over 5 måneder og omfattet en rekke arbeidsmøter. Tilbyderne deltok aktivt på alle møtene og kom med konstruktive innspill. Allerede den gangen ble det påpekt manglende gjennomføring av konsekvensanalyse, og utvidelse av lovforslaget i forhold til det opprinnelige høringsutkastet, til skade for tilbyderne og sluttbrukerne.

Status på forskriftsarbeidet, fra arbeidet i arbeidsgruppen ble avsluttet og frem til i dag, er beskrevet i høringsnotatet, og Nkom kommenterer ikke dette ytterligere. Men det skal bemerkes at ny § 6-2a i ekomloven som ble tilføyd ved lov 14. juni 2013 ga langt videre hjemler til opprettelse av mobilregulerte soner for politiet enn hva den opprinnelige arbeidsgruppen forutsatte. Det foreliggende lovforslaget går sågar enda lenger når det gjelder de foreslåtte

hjemlers rekkevidde, uten at de negative konsekvenser av støysending og identitetsfangning er analysert.

3. Høringsnotatets beskrivelse av gjeldende rett

I høringsnotatets del 2.1 under omtalen av gjeldende rett uttales det at «I tillegg kan politiet med rettens kjennelse avbryte konkrete kommunikasjonsanlegg, enten ved å gi ekomtilbyderen pålegg om å stenge et bestemt kommunikasjonsanlegg eller hindre bruk ved jamming». Nkom viser til at ekomloven § 6-2a første ledd første punktum knytter politiets adgang til å benytte frekvenser tildelt andre til at «vilkårene for identifisering av kommunikasjonsanlegg etter straffeprosessloven § 216a tredje ledd annet punktum, § 216b annet ledd bokstav c eller § 222d er oppfylt, eller vilkårene for bruk av tvangsmidler i forebyggende øyemed etter politiloven § 17d foreligger».

Slik Nkom forstår bestemmelsen, åpnes det dermed i straffeprosessuell etterforskning og avverging kun for frekvensbruk for å identifisere kommunikasjonsanlegg, jf. strpl. § 216a og § 216b bokstav c, mens frekvensbruk ved støysending for å stenge terminaler for kommunikasjon og avbryte samtaler kun er hjemlet ved forebyggende bruk av tvangsmidler etter politiloven § 17d. At det i høringsnotatet gis uttrykk for en annen lovforståelse skaper usikkerhet om hva som er gjeldende rett på området, Nkom anbefaler derfor at departementet avklarer rettssituasjonen.

4. De foreslåtte tiltak

4.1. Systematikk og begrepsbruk

Etter forslaget til ny politilov § 7b bokstav a kan politiet i gitte situasjoner "etablere mobilregulerte soner, jf. ekomloven § 1-5 nr. 19, for et begrenset tidsrom."

Begrepet "mobilregulerte soner" brukes i ekomloven for å beskrive et begrenset geografisk område der offentlig mobilkommunikasjon påvirkes eller hindres. Dette kan etter § 1-5 nr. 19 skje på to måter – ved støysending ("jamming" i ekomlovens begrepsbruk, jf. § 1-5 nr. 21) og ved såkalt identitetsfangning, jf. § 1-5 nr. 20. Det siste skjer i praksis ved bruk av falske basestasjoner, også kalt IMSI-catchere. Ved bruk av falsk basestasjon vil også støysending kunne inngå som en del av denne prosessen.

Nkom bemerker at det ikke gjennomgående i høringsnotatet er skilt klart på disse to metodene. Dette er en ulempe for en balansert fremstilling av lovforslaget, idet de to metodene påvirker mobilbruk i det aktuelle geografiske området på ulike måter. Ved støysending slår en ut all

mobilkommunikasjon i et område, mens en ved identitetsfangning, i tillegg til potensielt å slå ut mobilkommunikasjonen, fanger opp mobilterminaler og i noen tilfeller kommunikasjonen i området, slik at identiteten til brukeren fanges opp og samtaler potensielt kan avlyttes.

Støysending påvirker således nettets integritet, mens identitetsfangning også påvirker konfidensialiteten for terminalenes lokasjon og eventuelt brukers kommunikasjon. Når disse metodene i forslaget blir behandlet og regulert samlet, blir det uklart hvilke fullmakter det i realiteten foreslås å gi politiet. Nkom anbefaler derfor at de to metodene fremstilles og behandles separat i den videre prosessen med lovforslaget. Dette vil også gi mulighet for å utforme mer hensiktsmessige og adekvate kriterier og vilkår for bruken av henholdsvis støysending og identitetsfangning.

4.2. Gjennomføring av identitetsfangning – forholdet til sikkerheten i mobilnett

Identitetsfangning ved hjelp av falske basestasjoner benytter svakheter i underliggende standarder for mobilnett og terminaler til å hente ut informasjon om brukers identitet (gjerne representert ved IMSI-nummer, som i tilbyders databaser er koblet til hver enkelt sluttbruker). Identitetsfangning kan også gjennomføres ved å lytte på samtaler i et område, ved å benytte de samme svakheter i standardene kan man «narre» terminalen til å operere på GSM-nettet med den svakeste krypteringen. Denne krypteringen (A5/1) er det mulig å knekke med relativt enkle midler slik at trafikken kan avlyttes, i motsetning til den krypteringen som normalt benyttes i norske mobilnett.

Nkom har over tid gitt råd og pålegg til tilbyderne av mobilnett om bedre sikring av sine nett mot både uautorisert lokalisering og avlytting. Dette arbeidet vil fortsette med økt styrke. Det fremstår dermed som et paradoks at myndighetene på én side stiller krav til sikring av konfidensialiteten i nettene, og på den annen side aktivt utnytter de samme svakheter ved hjelp av for eksempel falske basestasjoner. Dette tilsier etter Nkoms oppfatning at eventuelle utvidelser av hjemmelsgrunnlaget for bruk bør være særlig godt utredet, og behovene tilsvarende påtrengende.

4.3. Identitetsfangning - konsekvenser for nett og tjenester ved identitetsfangning

Identitetsfangning utføres ved å etablere en falsk basestasjon som er mer «attraktiv» for terminalen enn ekte basestasjoner i et område. Når en terminal kobler seg til et nytt nettverk vil den sende sin IMSI-identifikasjon eller basestasjonen kan be terminalen om å sende IMSI. For at den falske basestasjonen skal kunne fange terminalen må den enten sende med høy effekt, manipulere blant annet reseleksjonsverdier, være fysisk nær terminalen man ønsker å finne identiteten til, eller en kombinasjon av disse. I tillegg kan det være nødvendig med

støysendinger i andre frekvensbånd for å tvinge terminalen over i et frekvensbånd som bruker en teknologi der man kan fange opp IMSI-nummeret og foreta eventuell avlytting. Dersom man ikke gjør dette kan man ikke være sikker på at man identifiserer eller fanger opp den eller de terminalene som er av interesse.

Slik Nkom ser det er det her et vesentlig skille mellom den bruk av falske basestasjoner som er tillatt i dag, der det i all hovedsak eneste lovlige formål er å fange identiteten, og den i høringsnotatet foreslåtte bruk der formålet er å kontrollere all trafikk i et område ved bruk av falske basestasjoner, skissert som et alternativ til støysending. Effektbruken i sistnevnte tilfelle, der total kontroll er målsetningen, vil måtte være vesentlig høyere enn ved ren identitetsfangning der man kan akseptere at identitetsfangningen vil måtte foregå over tid og med noe usikkerhet for om identiteten til den aktuelle terminalen er fanget opp i hvert enkelt tilfelle.

Dersom man er geografisk svært nær terminalen(e) av interesse kan man i begge tilfeller klare seg med en portabel falsk basestasjon som sender med lav effekt. Dersom man antar at det som i høringen er beskrevet som "i det skjulte" betyr at eventuelle falske basestasjoner opprettes et stykke unna stedet politiet skal kontrollere trafikken, så vil både identitetsfangning og støysending måtte foregå med relativt høy sendeeffekt. Dette gjelder spesielt i et bysentrum der man kan risikere at en ekte basestasjon er plassert nærmere området av interesse enn det er mulig for politiet å plassere sin falske basestasjon.

Dersom politiet ikke er kjent med hvilke tilbydere, teknologier og frekvensbånd som mobilterminalen kan koble seg opp mot, og som er tilbudt i området, kan det bli nødvendig å gjennomføre identitetsfangning (eventuelt bruke støysendinger for å tvinge terminalen over i et bestemt bånd) i alle mobilbånd samtidig (800/900/1800/2100/2600). Konsekvensen kan, avhengig av topografi, plassering og andre faktorer, bli at man "fanger" terminaler langt utenfor det tilsiktede området og at man forårsaker utfall og forstyrrelser i mobilnettet i et mye større område enn det som er tiltenkt.

I en slik situasjon vil man også risikere at en falsk basestasjon plassert på gatenivå vil overskride grenseverdiene satt av Statens Strålevern.

Som nevnt ovenfor vil identitetsfangning i en del sammenhenger også innebære støysending som en del av manipuleringen av mobilnettet. I de tilfeller vil kommentarene under også gjelde seg gjeldende for bruk av falske basestasjoner.

4.4. Støysending i frekvenser som benyttes til offentlig mobilkommunikasjon - konsekvenser

For å tjene sitt formål må støysendingen overdøve all mobilkommunikasjon i det definerte området. For å oppnå dette må støysenderne sende med høyere effekt enn de systemer man forsøker å ta ut, eventuelt være fysisk nærmere plassert. Selv om det geografiske området der mobilnettet er helt slått ut er begrenset, så er ikke konsekvensene av støysendinger begrenset til dette området alene. Støysendingen vil kunne slå ut kommunikasjonen, helt eller delvis, i større omkringliggende områder og føre til kapasitetsbegrensninger i et stort område. Mobilnettene er videre nøye planlagte og kalibrerte, naturlig nok med parametere som ikke forutsetter større støykilder innenfor dekningsområdet. Man kan derfor påberegne effekter i nettene som i sin natur er uforutsigbare.

Dersom støysendingen fungerer etter sin intensjon, vil man i det aktuelle området ikke kunne nå nødnumrene. Dette vil også kunne være tilfellet i omkringliggende områder, avhengig av antall og plasseringen til omkringliggende basestasjoner. Generelt vil man, for å være sikker på å blokkere all kommunikasjon i et gitt område, måtte benytte en slik effekt at det signifikant vil påvirke tjenestekvaliteten, også for nødnumre, i et vesentlig større område.

4.5. Støysending i andre frekvensbånd

Som ved støysending på «mobilfrekvenser», kan støysendinger for å hindre annen frekvensbruk også få konsekvenser langt utover det geografiske området som man retter seg inn mot. Avhengig av effekt, kan støysending også «smitte» over i andre, nærliggende frekvensbånd med andre bruksområder enn de man forsøker å hindre.

Det som Nkom ser som de mest sannsynlige frekvensbånd som etter forslaget vil utsettes for støysending, er frekvensbånd som er omfattet av den såkalte fribruksforskriften. Disse frekvensene er tillatt brukt på ikke-interfererende og ikke-beskyttet basis. Det er likevel flere tjenester som opererer i disse båndene som kan kategoriseres som kritiske, blant annet trygghetsalarmer.

Nkom er også bekymret for hvor begrensede støysenderne i realiteten kan være, det vil si hvor fokusert det er mulig å være i støysendingen. En del "fribruksfrekvenser" er naboer til eksempelvis bånd for mobilkommunikasjon.

I høringen ytres det et ønske om at det ikke skal legges noen begrensninger på hvilke frekvensbånd som politiet kan foreta støysendinger i. Argumentasjonen for dette er at det ikke

skal oppstå "friområder" som kriminelle kan kommunisere uhindret i. Nkom har forståelse for dette, men vil likevel sterkt fraråde en «blankofullmakt» til å foreta støysendinger i alle bånd.

Enkelte frekvensbånd er for eksempel helt fundamentale for søk- og redningstjenestene samt for kontroll av trafikk i luftrommet. Noen av frekvensbåndene under er svært viktige og ligger tett opp til frekvensbånd som kan være aktuelle kandidater for støysendinger:

- 406,0-406,1 MHz – nødpeilesendere. Nabobånd til PMR-bruk ("walkie-talkie") i 400 MHz-båndet
- 960-1300 MHz – flere forskjellige radiotjenester for sikker avvikling av luftfart og navigering. Er nabobånd til 900 MHz-båndet for offentlig mobilkommunikasjon.
- 1559-1610 MHz – brukes til satellittnavigasjon og er nabobånd til L-bånd satellittkommunikasjon (for eksempel Inmarsat og Iridium)
- 2700-2900 MHz – luftovervåkingsradarer og er nabobånd til 2600 MHz-båndet til offentlig mobilkommunikasjon

Det presiseres at denne oppstillingen ikke er uttømmende. For å beskytte slike bånd må politiets støysendere, som absolutt minstemål, ha justerbare filter som gjør at de ikke lekker effekt inn i disse båndene. Operatørene av støysendingsutstyr må også ha inngående kjennskap til hvilke frekvensbånd som benyttes for ulike kritiske funksjoner, for å kunne minimere de negative effektene av støysendingen.

5. Utstyrstillatelser

De foreslåtte endringene i ekomloven gjelder endringer i lovens kapittel 6 som gjelder frekvensforvaltning og unntak fra kravet i lovens § 6-2 om at frekvenser ikke kan tas i bruk uten at det foreligger tillatelse fra myndigheten. Kravet i ekomloven § 8-1 annet ledd om at det kreves tillatelse fra myndigheten for bruk av utstyr som ikke omfattes av internasjonal overenskomst som Norge har sluttet seg til, er ikke foreslått endret.

Det følger av ekomloven § 8-1 annet ledd at «Besittelse, omsetning og bruk av radio- og terminalutstyr som ikke omfattes av overenskomst etter første ledd, krever utstyrstillatelse fra myndigheten». Radio- og teleterminalutstyr omfattes av Radio- og teleterminaldirektivet (1999/5/EF) som er gjennomført i norsk rett gjennom Forskrift om EØS-krav til radio- og teleterminalutstyr (R&TTE-forskriften), og utstyr som oppfyller kravene i direktiv og forskrift kan i utgangspunktet besittes, omsettes og tas i bruk. Det følger imidlertid av R&TTE-forskriften § 2

tredje ledd bokstav e) at forskriften ikke gjelder radio- og teleterminalutstyr som bare brukes for å ivareta rikets eller annen offentlig sikkerhet, bare brukes av forsvaret eller for statens tiltak på det strafferettslige området. Radio- og teleterminalutstyr som bare brukes for disse formålene faller altså utenfor forskriftens virkeområde og det kreves at det søkes myndigheten om utstyrstillatelse for lovlig å kunne anvende denne typen utstyr. Det følger av ekomloven § 8-1 annet ledd at «Myndigheten kan nekte tillatelse dersom utstyret ikke oppfyller krav som angitt i første ledd», og at «Det kan stilles vilkår for utstyrstillatelse eller gjøres unntak fra kravet om tillatelse».

Dagens regelverk om mobilregulerte soner som åpner opp for at frekvenser som er tildelt andre i nærmere bestemte tilfeller kan tas i bruk, gir ikke adgang til å ta i bruk utstyr som bare brukes for dette formålet uten at det foreligger utstyrstillatelse fra myndigheten. Dette innebærer at selv om vilkårene i ekomloven § 6-2a og eventuelt de foreslåtte endringene om støysending eller identitetsfangning er oppfylt, så vil det likevel måtte søkes myndigheten om tillatelse til bruk av utstyr for dette formålet.

Nkom har per dags dato ikke innvilget utstyrstillatelse for den type utstyr som det her er snakk om.

Nkom ser at det i den foreslåtte endringen ikke er lagt opp til å gjøre unntak fra kravet om utstyrstillatelse, og tar med dette ikke stilling til hvorvidt bruk av utstyr for formål som fremgår av forslaget til lovendring bør være unntatt kravet om utstyrstillatelse, men gjør oppmerksom på begrensingen som ligger i anvendelsen av utstyr til støysending og identitetsfangning.

Nkom har følgende anbefalinger hva gjelder utstyrstillatelse for utstyr benyttet til støysending og identitetsfangning:

- Det må søkes utstyrstillatelse etter gjeldende rett for eventuelt støysendingsutstyr og falske basestasjoner i bruk i dag.
- Reglene om utstyrstillatelse i ekomloven kapittel 8 bør tilpasses i tråd med endelig forslag.

6. Det foreslåtte hjemmelsgrunnlaget

6.1. Vilkår

I et åpent samfunn som det norske er det en ikke ubetydelig risiko for å bli utsatt for kriminalitet, siden et kontrollnivå i nærheten av det som kreves for å hindre all kriminalitet har blitt ansett for å være uforenelig med et åpent og demokratisk samfunn. Det er derfor en politisk oppgave å

avgjøre hvor stor samfunnets risikoaksept skal være, og når behovet for å avverge slik risiko rettferdiggjør inngripende tiltak overfor borgerne.

Det foreliggende forslaget har meget skjønnsmessige vilkår for når støysending og identitetsfangning kan iverksettes, og overlater slik Nkom forstår forslaget, denne vurderingen til politiet i hvert enkelt tilfelle. Det er heller ikke noe «vilkår at det foreligger en spesifisert og konkret trussel, men det må foreligge en faktisk mulighet for skade på liv og helse eller tungtveiende samfunnsmessige hensyn», jf. høringsnotatets punkt 4.1.2. Nkom forstår derfor inngangsvilkårene, ref. ovenstående, dit hen at de ikke legger noen reell begrensning for bruken av støysending eller identifikasjon av kommunikasjonsanlegg.

Siden disse tiltakene kan ha potensielt store konsekvenser for henholdsvis brukernes mulighet til å kommunisere, og kommunikasjonsutstyrets integritet, anbefaler Nkom at det i en eventuell videre prosess vurderes om inngrepskriteriene kan gjøres mer spesifikke og konkrete fra lovgivers side. Siden støysending i seg selv indirekte kan medføre fare for liv og helse, ved at personer i området for eksempel ikke kan nå nødnumre eller samfunnsviktig trafikk forstyrres, bør det også vurderes om terskelen «fare for liv og helse» bør kvalifiseres.

6.2. De to alternative forslagene

Det bes i høringsnotatet særlig om kommentarer på hvilket av de to foreslåtte alternativer av politiloven § 7b det skal gås videre med. Forslagene skiller seg fra hverandre ved at alternativ 1 har «forebygge og stanse alternative ordensforstyrrelser» som ett av de oppgitte formål, mens det i alternativ 2 foreslås at terskelen for forebygging skal ligge ved straffbare forhold «som etter loven kan medføre straff av fengsel i 3 år eller mer».

Hva som utgjør forebygging av straffbart forhold er ikke klart definert i høringsnotatet, det klargjøres imidlertid at det ikke er krav om mistanke mot bestemte personer. Det klargjøres også at «[i] en konkret situasjon vil ikke politiet nødvendigvis vite sikkert hvilket straffbart forhold som søkes forebygget [...]». Den eneste veiledningen som gis er etter dette at «muligheten for at det skal skje alvorlige straffbare handlinger må være så konkret at det fremstår som nødvendig å ta i bruk mobilregulert sone».

Videre foreslås det at tiltakene skal kunne benyttes i arbeidet med å «iverksette andre politioperative tiltak», som er eksemplifisert, men ikke videre definert.

Disse to formålene er slik Nkom ser det, hver for seg og samlet, så vage og skjønnsmessige at det spiller liten rolle om bestemmelsene setter en konkret strafferamme for forebygging eller ikke. Videre vil bestrebelse for å sikre ro og orden, særlig ved alvorlige ordensforstyrrelser, etter vanlig språkbruk kunne være «politioperative tiltak».

6.3. Forholdsmessighet

Som nevnt ovenfor vil konsekvensene ved bruk av både falske basestasjoner og støysending være vanskelige å estimere. Det er ikke mulig å ha total oversikt over hvilke systemer som rammes av støysending, og dermed skadevirkningen for andre, særlig i tett bebygde/trafikkerte strøk. Identitetsfangning rammer på sin side per definisjon en ubestemt krets av tredjepersoner. Forholdsmessighetsvurderingen vil dermed måtte foretas med en betydelig grad av usikkerhet, uavhengig av den tekniske kompetansen til den besluttende myndighet. Etter Nkoms oppfatning er denne usikkerheten, og de potensielle skadevirkningene, så store at støysending bare bør gjennomføres i helt påtvingende tilfeller. Høringsnotatets forslag om å åpne for forebyggende støysending og bruk av falske basestasjoner, uten konkrete foreliggende farer, samsvarer ikke med dette. Nkom anser at «avverging» av definerte straffbare forhold, som er benyttet blant annet i straffeprosessloven, som vilkår vil samsvare bedre med det reelle innhold i de forholdsmessighetsvurderinger som skal foretas.

Et alternativ og/eller supplement til støysending på frekvenser benyttet til offentlig mobilteneste er at de aktuelle tilbyderne stenger nettet for kommunikasjon i det aktuelle området. Det er mulig å foreta slik stenging slik at bare enten inngående eller utgående samtaler rammes. Hjemmel for slik bruksbegrensning finnes i ekomloven § 2-5 første og annet ledd. I mange tilfeller vil dette være et sikrere tiltak ved for eksempel mistanke om utplassering av eksplosiver, eventuelt i kombinasjon med mer rettet støysending. Siden Nkom og tilbyder i slike tilfeller er informert, oppstår ikke problemstillinger med søk etter støykilder og andre ukoordinerte tiltak. Konsekvensene er imidlertid også her svært store, slik at faren må fremstå som aktuell og konkret før også slike tiltak kan tas i bruk.

6.4. Rettssikkerhetsgarantier

Etter gjeldende rett er identifikasjon av kommunikasjonsanlegg («identitetsfangning») kategorisert som kommunikasjonskontroll etter straffeprosessloven (strpl.), med dertil strenge vilkår for bruk og rettssikkerhetsgarantier. Identifikasjon som foregår ved avlytting av trafikk er å anse som kommunikasjonsavlytting etter strpl. § 216a, og kan bare besluttes av retten ved skjellig grunn til mistanke om straffbart forhold med strafferamme over 10 års fengsel, eventuelt ved avverging eller PSTs forebygging av nærmere bestemte alvorlige straffbare forhold. Identitetsfangning som gjennomføres uten at avlytting finner sted, følger § 216b der det er åpnet for en større gruppe straffebed. Felles for bestemmelsene er at slik kontroll må antas å være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort. Det er også gitt andre særregler for kommunikasjonskontroll for å sikre borgernes rettssikkerhet.

Nkom anser ikke at hensynet til borgernes rettssikkerhet er fulgt tilstrekkelig opp i det foreliggende forslaget, som hverken har krav til identifiserte straffbare forhold eller

domstolskontroll. Det skilles heller ikke mellom identitetsfanging som utelukkende skjer automatisk og identitetsfanging som skjer ved å avlytte et større antall telefonsamtaler, slik straffeprosessloven skiller mellom. Slik forslaget er utformet kan det dermed forstås som om politiet, uten domstolskontroll, identifisert straffbart forhold eller mistankegrunnlag, skal ha mulighet til både «temporært masse-avlytte» og på annen måte å identifisere brukere av for eksempel en mobiltelefon. Det er heller ikke foreslått regler for behandling av overskuddsinformasjon, sml. strpl. § 216i, og sletting av informasjonen når tiltaket er avsluttet.

Nkom anser derfor at forslaget innebærer et brudd med det hittil eksisterende vern av konfidensialiteten for borgernes elektroniske kommunikasjon. Fra et rettssystem der inngrep i borgernes elektroniske kommunikasjon krever klar lovhjemmel og besluttes av domstolene, foreslås det nå at inngrep i denne skal være opp til politiet ensidig å beslutte etter et vagt regelsett med stort rom for skjønn.

6.5. For gjennomføring av andre hemmelige tvangsmidler

Det foreslås at tiltakene etter politiloven § 7b også skal kunne benyttes for å gjennomføre en rekke tvangsmidler i medhold av straffeprosessloven, og at dette skal forankres i politiloven fremfor straffeprosessloven. Som nevnt ovenfor vil støysending og identitetsfanging etter sin natur omfatte utenforstående tredjepersoner, og etter omstendighetene være inngripende overfor disse. Etter Nkoms oppfatning bør det derfor foreligge meget gode grunner for at dette ikke skal underkastes domstolskontroll, på lik linje med andre tvangsmidler. Nkom kan ikke se at slike grunner er nevnt i høringsnotatet.

6.6. Avgjørelsens form og overprøving

Det foreslås at tiltakene skal kunne tas i bruk etter «beslutning» av politimester, visepolitimester, sjef PST og assisterende sjef PST, og at denne myndigheten i særlige tilfeller kan delegeres. Som nevnt over ser ikke Nkom at det er tilstrekkelig underbygget at støysending og identitetsfanging ikke bør underkastes domstolskontroll, med ordinær hastekompetanse for politimester/påtalemyndighet og sjef PST. Skiftende situasjoner og innkommende trusselinformasjon, slik det er referert til i høringsnotatet, kan håndteres innenfor hastekompetansen om nødvendig.

Det fremstår videre som uklart for Nkom hvilken rettslig form beslutningen er tenkt å ha. Det anses naturlig at det er tale om et enkeltvedtak etter forvaltningsloven (fvl.), da støysending og identitetsfanging «generelt eller konkret» vil være bestemmende for rettigheter eller plikter til «en eller flere bestemte personer», jf. fvl. § 2. Dette gjør seg særlig gjeldende i et EMK-perspektiv, da man ellers vil stå uten rett til et effektivt rettsmiddel, jf. artikkel 13, ved inngrep i retten til kommunikasjon og/eller privatliv, jf. artikkel 8.

7. Etterfølgende kontroll

7.1. Kontroll fra ekommyndigheten

Den foreslåtte endring i ekomloven § 6-2a første ledd gjentar inngangsvilkårene fra forslaget til ny politilov § 7 b, hva gjelder at frekvensbruken må være nødvendig for å beskytte liv og helse eller ivareta tungtveiende samfunnsmessige hensyn. Slik Nkom forstår forslaget vil politiets frekvensbruk da kun være lovlig når disse vilkårene er oppfylt, siden frekvensbruk uten tillatelse ellers vil være en overtredelse av ekomloven § 6-2. Det bør derfor avklares nærmere om Nkom, som tilsynsorgan etter ekomloven, skal kunne håndheve brudd på ekomloven § 6-2 som følge av frekvensbruk fra politiet som ikke oppfyller vilkårene i § 6-2a. Nkom vil i så tilfelle måtte ta stilling til politiets vurdering av nødvendigheten av tiltaket for å ivareta de overnevnte hensyn, og innhente nødvendig dokumentasjon i den forbindelse.

Økt lovlig bruk av støysending og identitetsfangning vil også kunne komplisere Nkoms muligheter til å føre kontroll med støy og ulovlig bruk av falske basestasjoner. Dette gjør seg særlig gjeldende der lovlig bruk ikke varsles, se nedenfor.

7.2. Kontrollutvalget for kommunikasjonskontroll og EOS-utvalget

Nkom støtter at all bruk av støysending og identifikasjon av kommunikasjonsanlegg underlegges etterfølgende kontroll fra henholdsvis kontrollutvalget for kommunikasjonskontroll og EOS-utvalget. Slik Nkom oppfatter forslaget og gjeldende praksis, foretas denne kontrollen primært ut ifra et integritetsperspektiv for den enkelte. For å kunne ivareta denne kontrollfunksjonen, ser Nkom det som avgjørende at utvalgene har, eller kan trekke på, tilstrekkelig teknisk kompetanse. Uten slik kompetanse vil det være meget vanskelig å fastslå hvor sterkt det enkelte inngrep i realiteten er, og hvilke konsekvenser inngrep kan medføre.

7.3. Anbefalinger

Nkom har etter dette følgende anbefalinger til bestemmelsens utforming, vilkår og rettssikkerhetsgarantier:

- Lovteksten bør skille mellom støysending og identitetsfangning/bruk av falske basestasjoner, da ulike hensyn gjør seg gjeldende.
- Identifikasjon av kommunikasjonsanlegg, samt støysending for å gjennomføre andre tvangsmidler, bør fortsatt være underlagt domstolskontroll.
- Det må tydeliggjøres om adgangen til identitetsfangning er forutsett å omfatte adgang til såkalt «masse-avlytting», jf. strpl. § 216 a tredje ledd annet punktum.

- Tersklene for å ta i bruk begge tiltak bør kvalifiseres, for eksempel ved å legge til grunn «avverging» i stedet for «forebygging» av straffbare handlinger. Hvilke «politioperative tiltak» det siktes til bør presiseres i lovteksten.
- Øvrige vilkår i bestemmelsen bør gjennomgås, for å sikre bedre samsvar med hva som reelt vil være forholdsmessig bruk av tiltakene. Herunder bør det også i ordlyden tas hensyn til at støysending og enkelte former for identitetsfangning, der andres legitime kommunikasjon stenges ute fra nettet, i seg selv kan utsette liv og helse for fare.
- Det bør synliggjøres at beslutning om støysending og identitetsfangning, dersom dette ikke legges til domstolen, er å betrakte som enkeltvedtak etter forvaltningsloven. Klagerett for de som rammes er etter Nkoms syn påkrevet etter EMK, og bør ivaretas også i nasjonal lovgivning.
- Det bør gis regler om bruk/sletting av eventuell overskuddsinformasjon fra identitetsfangning etter politiloven § 7b, slik det er gjort for annen kommunikasjonskontroll.
- Kontrollutvalgene bør ha tilgang på teknisk kompetanse

8. Varsling

8.1. Erfaringer så langt

Siden bestemmelsene om mobilregulert sone, og tilhørende varslingsplikt, kom til i ekomloven 1.7.2013, har Post- og teletilsynet/Nkom mottatt et svært begrenset antall varslinger. Dette på tross av Post- og teletilsynets brev av 22.5.2014 til Justis- og beredskapsdepartementet, der det ble minnet om varslingsplikten, og denne ble presisert. Brevet ble videresendt Politidirektoratet og Politiets sikkerhetstjeneste med ytterligere presiseringer fra Justis- og beredskapsdepartementet.

Det kan også stilles spørsmål ved om taushetsplikten ved kommunikasjonskontroll, jf. straffeprosessloven kapittel 16a og politiloven § 17f, forhindrer politiet og PST fra å oppfylle varslingsplikten fullt ut ved bruk av frekvenser til mobilregulerte soner. Den forutsetning om informasjonsdeling som det vises til i høringsnotatet punkt 2.5, og som ble tillagt «betydelig vekt» ved avgjørelsen om å tillate identitetsfangning som straffeprosessuelt tvangsmiddel, er dermed ikke nødvendigvis dekkende for den faktiske situasjonen.

8.2. Høringsnotatets forslag

Det foreslås to endringer i varslingsplikten. For det første at kompetansen til å avgjøre unnlatt varsling til tilbyder flyttes fra Post- og teletilsynet/Nkom til politiet. Det åpnes for dette i tilfeller der dette er «av avgjørende betydning for gjennomføring av tiltak som nevnt i politiloven § 7b».

Nkom vil bemerke at slik forslaget er utformet, vil § 6-2a, i motsetning til gjeldende bestemmelse, ikke gi Nkom muligheten til på selvstendig grunnlag å unnlate å varsle rettighetshavere. Slik unnlatt varsling må etter forslaget i alle tilfeller besluttes av politiet. Dette vil typisk ha betydning for varslinger mottatt av NSM, der støysending for å sikre et konkret møterom i en del tilfeller vil ha så liten effekt at det har liten hensikt å varsle tilbyderne. Å måtte kontakte politiet i slike tilfeller fremstår som meget upraktisk for alle parter.

Slik Nkom forstår forslaget, vil politiets mulighet til å beslutte unnlatt varsling til tilbydere videre være avgrenset til støysending og identifikasjon av kommunikasjonsanlegg etter politiloven § 7b, mens identifikasjon av kommunikasjonsanlegg etter straffeprosessloven og politiloven § 17d ikke er omtalt. Det fremstår i det hele tatt som uklart hvordan eventuell varsling etter nevnte hjemmelsgrunnlag er tenkt ivaretatt.

Videre åpnes det for at politiet kan utsette eller unnlate å varsle myndigheten (i praksis Nkom) dersom dette er nødvendig «av hensyn til samarbeidende tjenester», eller det er «helt nødvendig av hensyn til gjennomføringen av tiltak som nevnt i politiloven § 7b». Også her er det usikkert hva som gjelder for identitetsfangning etter strpl. og politiloven § 17. Hvilke situasjoner det i realiteten siktes til er også vagt beskrevet i høringsnotatet. Etter Nkoms syn må et minstemål være at antatte mulige skadevirkninger ved varsling dokumenteres, og at det regelmessig rapporteres om total bruk av disse tvangsmidlene. Nkom behandler i annen sammenheng informasjon gradert etter sikkerhetsloven, og anser at egne rutiner rundt dette er sikre.

Nkom vil også gjøre oppmerksom på at all bruk av identitetsfangning og støysending potensielt kan bli detektert av andre. Noe kan bli detektert av tilbyderne, og noe av Nkoms frekvenskontroll. Nkom leder for tiden en arbeidsgruppe for å bedre tilbyderens mulighet til deteksjon av slikt utstyr, og en heving av Nkoms egne kapasiteter på området er under utredning. Dersom Nkom ikke er varslet, kan dette dermed medføre ukoordinerte tiltak der Nkoms frekvenskontroll potensielt kan gripe inn mot støykilden. Det fremstår også som uheldig at Nkom og tilbyderne skal måtte benytte ressurser for å avdekke lovlige støykilder av denne type, når dette i stor grad kan unngås ved å varsle myndigheten.

8.3. Anbefalinger

Nkom har følgende anbefalinger hva gjelder varslingsplikten:

- Eventuelle eksisterende rettslige hindre for varsling til ekommyndigheten må fjernes før det vedtas ytterligere begrensninger i varslingsplikten.
- Det bør tas en fornyet vurdering av behovet for å unnlate varsling til ekommyndigheten og tilbyderne, og kriteriene for dette bør tydeliggjøres.

- Reglene om unnlatt varsling til rettighetshavere og myndigheten bør underkastes en lovt teknisk gjennomgang, med sikte på intern sammenheng og konsistens.

9. Samarbeid mellom Nkom og politiet

Det vises i høringsnotatet til at Post- og teletilsynet/Nkom kan gi råd til politiet, blant annet ved vurdering av alternative, mindre inngripende tiltak. Nkom stiller seg uforbeholdent til disposisjon for dette. I lys av tidligere erfaringer, spesielt i den tidligere arbeidsgruppe om mobilregulerte soner, antar Nkom likevel at politiet i liten grad vil benytte seg av dette, både på grunn av rettslige uklarheter og ønsker om å skjerme metodebruken.

10. Administrative og økonomiske konsekvenser

Som nevnt flere steder ovenfor vil støysending ha uforutsigbare konsekvenser, i en del tilfeller vil støysending kunne true både liv og helse, samt samfunnets og den enkeltes muligheter til å agere i en krisesituasjon. Dette vil åpenbart også medføre økonomiske konsekvenser som Nkom ikke kan se er vurdert i høringsnotatet.

Vage og skjønnsmessige hjemler for identitetsfangning vil også kunne svekke brukernes tillit til at deres kommunikasjon og lokasjon er konfidensiell. Det kan ikke ses bort fra at et svekket vern for konfidensialiteten vil kunne virke dempende på mobilbruk i samfunnet, og dermed svekke sektorens verdiskapning og positive effekter.

Dersom politiet har gjennomført forebyggende støysending, og denne har hatt negative effekter for annen legitim frekvensbruk, oppstår også spørsmålet om erstatningsansvar dersom det skulle vise seg at støysendingen var gjennomført på feilaktig grunnlag. Nkom kan ikke se at dette er vurdert i høringsnotatet.

Følgende bør etter Nkoms syn ivaretas i det videre arbeidet:

- Politiets erstatningsrettslige ansvar ved bruk av støysendere og identifikasjon av kommunikasjonsanlegg bør klargjøres.
- Både operatører og besluttede ledd i politiet må ha betydelig kompetanse om virkningene av støysending. Detaljerte kompetansekrav kan gis i forskrift.



Nasjonal
kommunikasjons-
myndighet

Med hilsen

Torstein Olsen
direktør

Einar Lunde
avdelingsdirektør

Nasjonal kommunikasjonsmyndighet (Nkom) het tidligere Post- og teletilsynet

Kopi til: Samferdselsdepartementet, Postboks 8010 Dep., 0030 OSLO, Norge

Vedlegg: