



POLITIET

Politidirektoratet

Postboks 2090 Vika
0125 Oslo

Finnmark politidistrikt

Deres referanse:

21/82791

Vår referanse:

21/127101 - 3

Dato:

07.10.2021

Høringssvar - forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften

Finnmark politidistrikt viser til høringsnotat fra Kommunal- og moderniseringsdepartementet av 02.07.2021 om forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften samt e-post fra Politidirektoratet ved Heidi Venner av 23.09.2021.

I høringsnotatet foreslås en lovhjemmel som gir tilbyderne rett til å kreve fremleggelse av ordinær politiattest av personer som skal ha tilgang til informasjon, ekomnett, tilhørende fasiliteter, utstyr eller systemer med vesentlig betydning for sikkerheten i nett eller tjenester.

Finnmark politidistrikt har gjennom Politiets enhet for vandelskontroll og politiattester ansvaret for utstedelse av politiattester i Norge.

Finnmark politidistrikt støtter begrunnelsen fra Kommunal- og moderniseringsdepartementet. Vi har ingen innvendinger til at politiattesten gjøres ordinær, jf. politiregisterloven § 40. Vi bemerker at det i noen særlover, eksempelvis postloven § 31 første ledd andre setning og tolloven § 12-15 første ledd andre setning, er gitt hjemmel for å kreve uttømmende og utvidet politiattest av personer i særlig betrodde stillinger.

Vi påpeker at ordlyden i forslag til § 3-9 første ledd siste punktum om at politiattesten ikke skal være eldre enn 90 dager er noe upresis. Noen særlover har bestemmelser om at politiattesten ikke skal være eldre enn tre måneder når den leveres til mottaker, jf. eksempelvis forskrift om politiattest i barnehager § 3. Vår vurdering er at slike formuleringer er noe vag da ordlyden ikke tydeliggjør at mottaker av politiattest har ansvar for å kreve at politiattesten som fremlegges er i samsvar med hjemmelsgrunnlaget for krav om politiattest.

Vi foreslår følgende formulering:

"Politiattest som fremvises skal være utstedt med hjemmel i ekomloven § 3-9 og skal ikke være eldre enn 90 dager ved fremvisning".

Videre vil vi påpeke at det etter dagens regelverk ikke er gitt hjemmel for å kreve betaling for innhenting av politiattester.

Finnmark politidistrikt

Post: Postboks 501, 9917 Kirkenes
E-post: post.finnmark@politiet.no

Tlf: (+47) 78 97 20 00

Org. nr: 984000049
www.politiet.no

Økonomiske og administrative konsekvenser

Nye lovhjemler med krav om politiattest, vil potensielt kunne gi en økning i antall søknader om politiattest. Ettersom kravet om politiattest bare gjelder nyansettelser antar vi at endringen vil kunne medføre en økning i antall søknader over tid.

Statistisk sett behandler en saksbehandler ved politiattestkontoret gjennomsnittlig cirka 20 000 politiattester per år. Hvis endringen medfører en økning av innkomne søknader i denne størrelsesorden eller mer, vil det potensielt kunne ha personellmessige konsekvenser. Vi vil likevel understreke at flere mindre lovendringer i ulike regelverk samlet sett kan gi større utslag for den totale saksmengden til politiattestkontoret.

Med hilsen

Ellen Katrine Hætta

Politimester

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:

Gunilla Engenes Hansen

Rådgiver



Politidirektoratet

NCIS Norway

Deres referanse:
21/82791

Vår referanse:
21/82791

Sted, Dato:
Bryn, 1.10.2021

FORSLAG TIL NY EKOMLOV MV. - HØRINGSSVAR FRA KRIPOS

Det vises til Kommunal- og moderniseringsdepartementets (KMD) høringsbrev av 2.7.2021 om høring av forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften mv.

Det vises videre til Politidirektoratets brev vedrørende høringen av 24.8.2021 og vår e-post til direktoratet av 13.9.2021 hvor vi varslet at høringssvar fra Kripos vil foreligge 1.10.2021. Det fremgår av direktoratets brev (side to, første avsnitt) at kommunikasjonsverns-direktivet ikke er EØS-relevant. Til dette vil Kripos gjøre oppmerksom på at ny kommunikasjonsvernsforordning fra EU av departementet er vurdert som EØS-relevant, jf. KMDs foreløpige posisjonsnotat til kommunikasjonsvernforordningen i EØS-notatbasen (<https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2017/juni/forslag-til-kommunikasjonsvernforordning/id2555751/>). Vi vil videre opplyse om at Kripos den 5.-6.10.2021 skal delta på et internasjonalt møte i Hamburg som vi gi informasjon om hvordan den aktuelle EU-reguleringen er implementert i andre europeiske land. Vi vil orientere direktoratet nærmere om dette så snart møtet er gjennomført.

1. Innledning

Kripos er den nasjonale politienheten for bekjempelse av den alvorlige og organiserte kriminaliteten i Norge. Vi er politiets nasjonale kompetansesenter og nasjonalt kontaktpunkt for internasjonalt politisamarbeid. En av våre viktigste oppgaver er å bistå norsk politi innen områder som er særlig teknologi- og kompetansekrevene. Kripos er videre tillagt ansvaret for forvaltning av avtaler med teletilbydere og for teknisk tilrettelegging av politiets skjulte informasjonsinnhenting. Vi har i den anledning regelmessig og tett dialog med tilbydere og Nasjonal kommunikasjonsmyndighet (NKom). Våre ansvarsområder og våre oppgaver gjør at vi stadig

Kripos

Post: Pb. 8163 Dep., 0034 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos

Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no

Org. nr: 974 760 827

involveres i nasjonale og internasjonale problemstillinger knyttet til elektronisk kommunikasjon i nær sagt alle former.

Lov om elektronisk kommunikasjon (ekomloven) er en sentral lov med stor betydning for politiet. For Kripos vil endringer i ekomloven ha betydning både i forbindelse med bistand til og tilrettelegging for politidistriktene og for vår egen etterforskning.

I likhet med departementet registrerer Kripos at nummeruavhengige person-til-person-kommunikasjonstjenester som muliggjør direkte kommunikasjon mellom personer ved hjelp av applikasjoner på mobile enheter, har hatt en betydelig vekst de siste årene. Utbredelsen av denne type tjenester vil etter Kripos'vurdering fortsette å øke - både i antall tilbydere, brukere og dekningsgrad. Denne utviklingen er utfordrende sett fra et kriminalitets-bekjempende perspektiv. En bred tilgjengeliggjøring av avlyttingsfrie og ikke-sporbare kommunikasjonstjenester er bekymringsverdig og vil kunne ha stor betydning for samfunnsvernet, herunder politiets evne til å forebygge og bekjempe kriminalitet. Kripos mener derfor at kompensierende tiltak bør innføres parallelt, og vi finner det problematisk at dette ikke er tydeligere adressert i høringsnotatet. I denne sammenheng viser vi til at den svenske regjeringen nylig besluttet å utrede muligheten for en oppdatert regulering, slik at politiet kan få tilgang til flere og mer relevante opplysninger for å kunne bekjempe straffbare forhold. Spørsmålet om det er mulig å innføre lagringsplikt for apper vil være en sentral del av utredningsoppdraget. Kripos savner lignende initiativ og tiltak fra norsk side.

Det er en omfattende lovpakke som er sendt på høring, hvor det er utfordrende å ha kontroll på alle endringer og konsekvenser av betydning for politiet. Vi vil i det følgende kommentere de forhold som for Kripos fremter som mest relevante. Vi understreker samtidig at det antakelig er forhold her av betydning som vi ikke har hatt kapasitet til å vurdere nærmere.

2. Tilbyderbegrepet

Etter det foreliggende lovforslaget § 1-5 nr. 4 og 11 vil tilbyder av elektronisk kommunikasjonstjeneste være fysiske eller juridiske personer som (normalt) mot vederlag tilbyr andre tilgang til elektronisk kommunikasjonsnett eller kommunikasjonstjeneste slik det er beskrevet i § 1-5 nr. 4 a) – c).

Den foreslåtte definisjonen av elektronisk kommunikasjonstjeneste i § 1-5 nr. 4 er en utvidelse av gjeldende rett og medfører at definisjonen vil bli i tråd med ekomdirektivet artikkel 2 nr. 4. Kripos er positive til denne utvidelsen og særlig prinsippet om at definisjonen blir bestemt ut i fra tjenestens funksjon og ikke de tekniske løsningene som ligger bak.

De tjenestene som er nevnt i § 1-5 nr. 4 bokstav a dekker tilbydere som leverer normal aksess til Internett (ISPer). Siden det er snakk om en "internetttilgangstjeneste" må begrepet også dekke leverandører av datasentertjenester (VPSer) som selger hosting med tilhørende tilgang til internett samt VPN-leverandører som selger tilgang til internett fra servere disse disponerer. Dette selv om slike tjenester leveres på toppen av en normal aksess til internett. Etter Kripos' oppfatning er det viktig at dette blir presisert i merknadene til bestemmelsene for å sikre at VPS- og VPN-leverandører blir underlagt de samme pliktene i den nye ekomloven – på lik linje med ISPer. Det vises i denne sammenheng også til punkt 7 under vedrørende Regjeringens nylig lanserte "Datasenterstrategi"¹.

Kripos anser det som positivt at utvidelsen av begrepet elektronisk kommunikasjonstjeneste også inkluderer tilbydere av en større krets av tjenester, og at det nå også vil kunne omfatte for eksempel Snapchat, Telegram, iMessage/FaceTime, Gmail, Hotmail, Protonmail, Wickr, Teams, Whereby, Zoom, Slack mfl.

Det er viktig at man både i de kommende lovforarbeider og i utformingen av den endelige lovteksten er tydelig på at det er tjenestenes funksjon som er det sentrale og at dette også må være det avgjørende for eventuelle nye tjenester som lanseres. Slike presiseringer vil ha avgjørende betydning for tolking av bestemmelsen, bidra til at den blir mer teknologinøytral og gjøre den mer holdbar mot de stadige teknologiske endringene som utfordrer regelverket.

Samtidig fremstår det for Kripos som utfordrende og uheldig at lovforslaget kun dekker virksomheter som drives med kommersiell interesse, og som dermed direkte eller indirekte tjener penger på kommunikasjonstjenesten. Dette medfører at bruk av vederlagsfrie tjenester kan skje uten mulighet for myndighetskontroll. Dette inkluderer for eksempel tjenester som tilbys helt vederlagsfritt for eksempel Signal og IRC². IRC er en mye brukt plattform for datakriminelle og personer som distribuerer overgrepsmateriale.

En tilsvarende utfordring for politiet er at tjenester som tilbyr kommunikasjon som en sekundær del av tjenesten ikke blir underlagt plikter og kontroll. Tjenester knyttet til spill, publisering, nettforum, kringkasting, transport og finans faller dermed også utenfor. Disse kommunikasjonskanalene sees brukt i svært alvorlige straffesaker, og er derfor sentrale sporsteder. For Kripos fremstår det problematisk at foreliggende lovforslag ikke gir tilgang til informasjon fra disse kommunikasjonsformene.

Når det gjelder kravet til vederlag for å defineres som en elektronisk kommunikasjonstjeneste er det i høringsnotatet bemerket at det ikke er krav om at

¹ <https://www.regjeringen.no/no/dokumenter/norske-datasenter/id2867155/>

² Internet Relay Chat (IRC); en protokoll primært utviklet for kommunikasjon og fildeling på Internett. Dette ved at man bruker en klient som kobler brukeren opp mot ett eller flere nettverk, som består av én eller flere tjenere. Brukeren kobler seg, via nettverket, på kanaler, og kan velge å kommunisere med den gruppen brukere som befinner seg i kanalen, eller gjennom en direkte og privat kontakt med enkeltbrukere.

det er brukeren selv betaler for tjenesten – dette fordi tredjepartsbetaling er foreslått likestilt med direkte betaling. Etter Kripas oppfatning må dette bety at tilbydere som tilbyr en elektronisk kommunikasjonstjeneste som en del av sin kommersielle virksomhet vil være underlagt ekomloven. Dette bør klart fremgå av lovforarbeidene.

3. Tilretteleggingsplikten

Bruk av skjulte etterforskningsmetoder er sentralt i kampen mot den mest alvorlige og organiserte kriminaliteten. For flere av de tilgjengelige metodene er politiets evne helt avhengig av at ekomtilbyderne samarbeider med politiet og bidrar til den tekniske gjennomføringen av metodebruken. Også for tradisjonelle etterforskningsmetoder er informasjon fra tilbyderne av stor betydning, jf. for eksempel reglene om beslag og utleveringspålegg i straffeprosessloven §§ 205 og 210.

Tilretteleggingsplikten er en sentral og viktig del av elektroniske kommunikasjonstjenesters rammevilkår for å drive sin virksomhet i Norge. Det forutsettes at tilbyderne tar hensyn til denne ved utvikling av nye produkter, at de sikrer evne til lovlig tilgang til informasjon og at de kontinuerlig vedlikeholder evnen til å tilrettelegge. Det er viktig å minne om at plikten både er teknologinøytral og tidsuavhengig, og den må derfor også oppfylles ved innføring av ny teknologi og/eller nye tjenester.

Kripas har observert at denne plikten stadig oftere utfordres av tilbyderes kommersielle interesser. Det er svært viktig å sikre at tilretteleggingsplikten ikke blir utvannet.

Ekomtilbyderne har etter gjeldende rett og etter lovforslaget blant annet en tilretteleggingsplikt for kommunikasjonsskontroll i henhold til straffeprosessloven §§ 216 a og b. I praksis betyr dette at ekomtilbyderne sikrer at politiet får en kopi av all kommunikasjon med tilhørende metadata når det gjennomføres kommunikasjonsavlytting, samt bistand til å utlevere trafikkdata (metadata) i henhold til straffeprosessloven § 216 b.

Teknologiutviklingen gjør at det konkrete innhold i plikten til å legge til rette er i stadig endring, og Kripas mener at tilretteleggingsplikten bør konkretiseres slik at de grunnleggende prinsippene sikres og at uklarhet begrenses. Plikten til å tilrettelegge for kommunikasjonsskontroll blir av tilbyderne ofte plassert i et spenningsforhold mot utvikling og kostnader.

I høringsnotatet uttaler departementet på side 38;

Departementet legger til grunn at politimyndigheten og tilbyderne finner praktiske og egnede løsninger for å ivareta tilretteleggingen for politiets lovbestemte tilgang til

informasjon i henhold til forslag til ekomloven § 3-6. Tilretteleggingsplikten må samtidig ikke bli et hinder for innovasjon og teknologisk utvikling.

Kripos mener at denne formuleringen er uheldig idet den kan gi inntrykk av at tilretteleggingsplikten står tilbake for innovasjon og teknologisk utvikling. Utvikling og innovasjon er viktig, men den går ikke foran tilretteleggingsplikten. Politiets lovbestemte tilgang til informasjon er helt avgjørende for etatens evne til å ivareta sitt samfunnsansvar, herunder ansvaret for å bekjempe kriminalitet. Plikten etter dagens lov og forarbeidene forutsetter at nytt utstyr og/eller nye tjenester ikke kan innføres uten at tilbyder samtidig sikrer lovbestemt tilgang til "*informasjon om sluttbruker og elektronisk kommunikasjon*". Dette bør fremkomme klarere i de videre lovforarbeider. Dette prinsippet gjenfinnes enda tydeligere i annen europeisk lovgivning, blant annet i den nederlandske telekommunikasjonsloven artikkel 13.1 hvor det fremkommer at telekommunikasjonsnettverk og kommunikasjonstjenester bare kan gjøres tilgjengelig for sluttbrukere om de kan avlyttes³.

I dagens situasjon er Kripos av den oppfatning at tilretteleggingsplikten jevnlig utfordres av enkelte ekomtilbydere. Ny funksjonalitet eller endring av tjenestetilbudet gjør at politiet og påtalemyndigheten får tilgang til stadig færre opplysninger. Eksempler på dette er manglende tilrettelegging av utenlandske roamingkunder og VoLTE, som også er omtalt i høringsnotatet. I merknader til ny tilretteleggingsbestemmelse i § 3-6 fremkommer det at målet er 100 prosent dekningsgrad for all kommunikasjon hos alle tilbydere. Slik er det også etter dagens bestemmelse, men Kripos' erfaring er at manglende klare uttalelser om hva dette konkret betyr av krav og forventninger til tilbyder gir rom for en praksis hvor tilbyderne enkelt kan definere seg ut av tilretteleggingsplikten.

På dette området har også NKom et sentralt samfunnsansvar og en viktig oppgave gjennom en tilstrekkelig aktiv oppfølging av tilretteleggingsplikten. I forbindelse med tildeling av nye frekvensområder for 5G var ikke krav til tilretteleggingsplikten omtalt i de anbudsrundene tilbyderne måtte innfri. Dette til tross for at 5G som konsept innfører helt nye utfordringer for tilretteleggingsplikten, herunder såkalt network slicing, Multi Edge Computing (MEC) og mulige utfordringer for bruk av IMSI-catcher⁴. Det vises her til vedlagte brev fra Kripos til NKOM av 30.8.19 hvor disse utfordringene er nærmere omtalt⁵. Det er fortsatt uklart for Kripos i hvilken grad og på hvilken måte tilbyderne planlegger å ivareta sin tilretteleggingsplikt med 100 prosent dekningsgrad ved innføring av 5G kjernenett.

Posisjonsnøyaktighet

Et eksempel på uenighet mellom tilbyderne og politiet, er hvilken posisjonsnøyaktighet som skal angis i metadata for kommunikasjonskontroll. Ekomtilbyderne har som følge av teknologiutviklingen fått muligheter til bedre

³ <https://www.government.nl/binaries/government/documents/policy-notes/2012/06/07/dutch-telecommunications-act/telecommunications-act.pdf>

⁴ IMSI-catcher - apparat for telefonavlytting som brukes til å fange opp mobiltrafikkdata og spore bevegelser.

⁵ Brev fra Kripos til NKOM av 30.08.19 – Merknader fra Kripos – Høring om frekvenser til mobilkommunikasjon og 5G

posisjonsnøyaktighet i telenettet blant annet til bruk i forbindelse med nødalarmer – såkalt "beregnet posisjon". Posisjonsnøyaktighet er ofte svært viktig for politiets etterforskning, både for å identifisere bruker av kommunikasjonsenheten, men også for å se hvor vedkommende har beveget seg. Bevismessig kan dette ha stor betydning. Likevel mottar politiet ved for eksempel kommunikasjonskontroll normalt kun informasjon om hvilken basestasjon som er i bruk i forbindelse med samtalen. Kripos kan ikke se gode argumenter for at ikke beste posisjonsangivelse inngår i det som etter tilretteleggingsplikten skal leveres i forbindelse med kommunikasjonskontroll.

Kommunikasjonskontroll knyttet til tjeneste

Som nevnt over utvides definisjonen av hva som skal regnes som en elektronisk kommunikasjonstjeneste til å blant annet omfatte de nummeruavhengige person-til-person kommunikasjonstjenestene i forslaget til ny ekomlov, jf. § 1-5 nr. 4 og 5. Denne utvidelse får også betydning for rekkevidden av tilretteleggingsplikten i forslaget § 3-6.

Utvidelsen av tilretteleggingsplikten medfører at kommunikasjonstjenester som tilbydere av e-post, WhatsApp, Messenger, Teams, Snapchat og Skype blir underlagt en plikt til å tilrettelegge tjenesten slik at "*...lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon sikres*".

Etter gjeldende rett er det ikke anledning til å bruke brukerkonto hos ulike tjenester som identifikator for kommunikasjonskontroll på tvers av de kommunikasjonsenheter som benyttes. Kripos har tidligere tatt til orde for⁶ at det må gjøres endringer i straffeprosesslovens kapittel 16a på dette punkt.

Kripos mener at kommunikasjonskontroll bør tillates direkte mot de aktuelle kommunikasjonstjenestene som brukes og ikke bare til "*..bestemte telefoner, datamaskiner eller andre anlegg for kommunikasjon*", jf. straffeprosessloven § 216a tredje ledd. Løsningen i straffeprosessloven, med å bruke kommunikasjonsenheten som identifikator, fremstår som foreldet sett opp mot dagens kommunikasjonstjenester som er svært fleksible og uavhengige av hvilken kommunikasjonsenhet som benyttes.

Ved å avlytte den mistenktes brukerkonto knyttet til en kommunikasjonstjeneste vil kommunikasjonskontrollen også kunne bli mer målrettet og det vil være mindre muligheter for å fange opp informasjon som ikke er relevant eller datatrafikk som er generert av andre brukere av kommunikasjonsanlegget.

En løsning, som er valgt i Sverige og Finland, er at man i tillegg til å ha kommunikasjonsenheter som identifikatorer for kommunikasjonskontroll også har identifikatorer som for eksempel epostadresse eller annet brukernavn som knytter

⁶ Prop.68L(2015-2016) punkt 7.6.

brukeren som skal avlyttes til den tjenesten han benytter⁷. I Norge er en slik løsning valgt når det gjelder dataavlesing, jf. strpl. § 216o, hvor det etter bestemmelsens fjerde ledd kan benyttes dataavlesing mot "*....bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester*".

Ved behandlingen i 2016 (Prop. 68L) gikk ikke departementet videre med forslaget da de mente dette skilte seg grunnleggende på flere punkter fra dagens regelverk, og at forslaget ikke var tilstrekkelig hørt. Sett i lys av de konsekvenser forslaget til ny lov vil få for hvem som omfattes av tiltretteleggingsplikten mener Kripos en endring av straffeprosessloven § 216a nå bør utredes. Det vises også til det nå gjeldende regelverk om dataavlesing hvor denne type identifikator er valgt. Selv om dette spørsmålet ikke er til særskilt høring nå, mener Kripos at endringer i straffeprosessloven § 216 a vil gi bedre sammenheng i regelverket.

Bistand til gjennomføring av skjulte etterforskningsmetoder

Tiltretteleggingsplikten skal sikre lovbestemt tilgang til tilbyders informasjon om sluttbruker og kommunikasjon. Utviklingen har gjort at de systemer og den kompetanse tilbyderne besitter kan være meget viktig for politiet også ved tvangsmiddelbruk som helt eller delvis har annet formål enn tilgang til tilbyders informasjon om sluttbruker og kommunikasjon. I disse tilfellene etterlyser politiet en klarere og mer omfattende hjemmel for å be tilbydere om hjelp til gjennomføring av tvangsmiddelbruken.

Dataavlesing er et eksempel. Som kjent ble metoden innført som ny etterforskningsmetode i 2016. Kripos' erfaring fra bruk av metoden viser at bistand fra tilbyder til politiet ved gjennomføring av dataavlesing kan være meget nyttig, særlig i tilfelle hvor avlesingen involverer systemer som helt eller delvis administreres av tilbyder. Eksempelvis kan være snakk om å bruke kommunikasjonsstrømmer til å installere programvare for dataavlesing eller gjøre endringer på maskinvare som eies av tilbyderne. Bistand fra tilbyder vil antakelig også i enkelte tilfeller gjøre avlesingen både enklere og sikrere å gjennomføre. Dette fordrer imidlertid en klar hjemmel for bistand der denne går ut over plikten til å legge til rette for informasjon om sluttbruker og kommunikasjon. I dag følger det en plikt for tilbyder til å yte nødvendig bistand ved gjennomføring av kommunikasjonskontroll, jf straffeprosessloven § 216a fjerde ledd andre punktum. Denne gjelder for eksempel ikke ved dataavlesing, romavlytting, samtaleavlytting eller skjult kameraovervåking og teknisk sporing.

Sammenheng og grensesnitt mellom de forskjellige metoder tilsier etter vår vurdering også en klarere og mer omfattende hjemmel for bistand. Som eksempel kan det bero på konkrete omstendigheter i sak om informasjon best og mest målrettet kan innhentes i en kommunikasjonsstrøm (kommunikasjonskontroll) eller der hvor dataene lagres, prosesseres osv (beslag/ransaking/dataavlesing). I slike tilfelle bør

⁷ Svensk lovgivning har følgende beskrivelse for objektet det skal gjennomføres kontroll på: "ett telefonnummer, en kod eller annen teleadress". Det samme oppfattes i finsk lovgivning: "en viss teleanslutning, e-postadress eller någon annan sådan teleadress till eller från teleterminalutrustning gjennom ett sådant allmänt kommunikationsnät....".

valg av metode påvirkes av andre faktorer enn forskjell i mulighet for gjennomføringsbistand.

Anvendelsesområde

Et særtrekk ved de nye tjenestene som vil omfattes av den utvidede definisjonen av tilbyderbegrepet, for eksempel M2M/IoT-nummer, er at tjenestene lettere kan tilbys over landegrensene. Når det legges til rette for at tjenestene kan tilbys fra andre land enn Norge, aktualiseres spørsmålet om reglenes anvendelsesområdet. Dette styrkes også av innføring av fri bruk i utlandet for datasimkort, slik det nå er i store deler av Europa. En sluttbruker kan altså enkelt kjøpe et simkort i et annet land og bruke dette i Norge på lik linje med et norsk nummer. Kripos mener at tilretteleggingsplikten må gjelde for alle tilbydere av ekomtjenester som tilbys til sluttbrukere i Norge. Dette bør presiseres i lovtekst eller i merknader til lovteksten.

Tilretteleggingsplikten, både slik den er utformet i gjeldende rett og slik den er formulert i forslaget til ny § 3-6 må anses som en nasjonal regulering, uavhengig av direktivet. Etter Kripos syn bør dette fremkomme i merknadene for å klargjøre rettstilstanden, og slik at det fremkommer at innholdet og omfanget av tilretteleggingsplikten skal vurderes uavhengig av for eksempel koordineringsrollen som BEREK er tiltenkt etter direktivet.

4. Krav til entydig identifisering av sluttbrukere for sluttbrukere av enkelte IoT-tjenester

Som beskrevet i pkt 2 er Kripos positiv til at tilbyderbegrepet utvides til å også omfatte person-til-person tjenester. Imidlertid hefter det usikkerhet ved hvordan dette skal håndheves for selskaper basert i utlandet, gjerne utenfor europeisk jurisdiksjon. Det vises i denne sammenheng også til pkt 3 vedrørende spørsmålet om anvendelsesområde.

Politiet vil i mange tilfelle umiddelbart ikke kunne identifisere sluttbrukeren av en kommunikasjonstjeneste, og vil i praksis bli stående igjen med en IP-adresse som identifiserer kommunikasjonsbæreren (nett) som er benyttet til kommunikasjonen. Ved overgangen til IoT har bruken av machine-to-machine (M2M) i mange tilfeller erstattet bruken av ordinære abonnementer, og for politiet er det viktig slike abonnementer også omfattes av registreringsplikten. For norske tilbydere vil dette formentlig dekkes av registreringsplikten i nåværende ekomforskrift § 6-2, videreført i forslag til ny ekomforskrift § 7-3. Problemet oppstår imidlertid ved videresalg av tjenester hvor simkortet stammer fra en utenlandsk tilbyder. Kripos mener at departementene ved innføringen av ny ekomlov og forskrift må vurdere om slike videresalg også skal omfattes av registreringsplikt for sluttbrukere.

Selv om M2M primært er tenkt for kommunikasjon mellom enheter, vil M2M som eksemplene under viser også kunne brukes som bærer for person-til-person kommunikasjonstjenester:

1) Kjøretøy

De fleste leverandører av kjøretøy tilbyr nå ulike kommunikasjonstjenester for å kommunisere til/fra kjøretøyet. Siden 31.3.18⁸ har det vært obligatorisk for alle kjøretøy å ha e-call for kommunikasjon med alarmsentral ved ulykker. I tillegg tilbys navigasjonstjenester, fjernstyring av funksjoner i kjøretøy, sporing av kjøretøy mv. og permanent wifi i kjøretøyet⁹. Dette medfører at ett eller flere simkort som er levert fra bilfabrikken vil være databæreren for telefoner, pc'er og tablets for passasjerene i bilen. Den juridiske eieren vil være bilprodusenten som igjen tar betalt for slike tjenester fra bileieren gjennom abonnementer. For politiet er dette en stor utfordring og vil representere en uthuling av den nå vedtatte plikt til lagring av IP-adresser. Om den utenlandske leverandøren av simkort (for eksempel KPN, Vodafone, Movistar, AT&T som er store leverandører av M2M internasjonalt) skulle ha lagret IP-adresser, vil de ikke ha informasjon om hvem sluttbrukeren er utover at bilprodusenten er juridisk eier. Disse produsentene opererer ikke med noen oversikt over sine sluttbrukere. Politiet har da ingen mulighet til å finne ut hvilken reell abonnent som kommunikasjonen stammer fra. Politiet har i stadig større grad sett at kommunikasjon fra kjøretøy har blitt sentralt i etterforskning av straffesaker. Det kan for eksempel være kommunikasjon fra et slikt wifi-anlegg eller sim-kort som har vært i nærheten av et sentralt åsted (basert på basestasjonsregistreringer ved åstedet), men hvor politiet ikke klarer å spore kommunikasjonen til et bestemt kjøretøy. Innføring av en registreringsplikt ved salg av slike abonnementer fra bilforhandlerne, vill derfor ha stor betydning for etterforskning av alvorlig kriminalitet.

2) Anonyme M2M-abonnementer

Et annet eksempel er videresalg av anonyme M2M-kort som også selges i norske butikker¹⁰. Salg av slike utenlandske datasim-kort har samme utfordringer som nevnt for kjøretøy, nemlig at sluttbrukeren av databæreren/sim-kortet ikke kan identifiseres til tross for at de utmerket godt kan brukes til person-til-person kommunikasjon.

Begge disse tilfellene viser at effekten av tilbyders plikt til entydig å identifisere sine sluttbrukere, som ble innført i 2004¹¹, har blitt vesentlig redusert, samtidig som behovene for å kunne identifisere sluttbrukere også for IP-basert trafikk har økt tilsvarende. Dette har også en direkte betydning for effekten av å lagre IP-adresser som nylig ble vedtatt i Stortinget (Prop 167L).

⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0078&from=EN>

⁹ Et eksempel fra BMW: <https://www.bmw.com/en/innovation/wifi-in-the-car.html>. Tilsvarende finnes for de fleste leverandører av kjøretøy.

¹⁰ Eks: <https://www.spyshop.no/uregistrert-data-sim.html>

¹¹ Ekomforskriften § 6-2, første ledd

Kripos foreslår derfor at sluttbrukere også må registreres hos de som videreselger kommunikasjonstjenester/-bærere som *kan* brukes til person-til-personkommunikasjon - på lik linje med eksisterende plikt for ekomtilbyder til å entydig identifisere sine sluttbrukere ved inngåelse endring eller opphør av avtale.

5. Lagring av IP-adresser

Forslaget til ny § 3-4 viderefører gjeldende § 2-8a som ble vedtatt av Stortinget den 18.6.2021. Lovendringen har ikke trådt i kraft.

I tilknytting til det nye tilbyderbegrepet vil lagringsplikten omfatte en betydelig større krets av tilbydere enn hva som var tilfelle under utarbeidelsen av gjeldende § 2-8a. Norge har i lang tid har vært verdensledende når det gjelder digitalisering og er helt i toppen når det gjelder bruk av internett. Denne utviklingen har pågått lenge og den forventes å akselerere ytterligere ved innføring av 5G. Kriminaliteten har utviklet seg tilsvarende og nye arenaer har blitt åsted for kriminalitet. Digital kommunikasjon benyttes også som redskap for å begå kriminalitet, og har medført at mange straffesaker inneholder digitale spor, IP-adresser inkludert. I lys av denne utviklingen har Kripos i mange år engasjert seg sterkt i arbeidet med å få på plass en lagringsplikt.

Vi legger til grunn at de nylig vedtatte reglene om lagring og utlevering av IP-adresser videreføres i ny ekomlov. Samtidig understreker vi betydningen av at de allerede vedtatte endringer i dagens ekomlov blir ikraftsatt raskt. Behovet for lagring er nå klart uttalt fra lovgiver, og det vil være svært uheldig om den vedtatte bestemmelsene nå settes på vent til prosessen med ny ekomlov er slutført.

De vedtatte bestemmelsene er begrenset til lagring og uthenting ved etterforskningsformål. I den forbindelse viser Kripos til den oppfølging som er initiert fra Justis- og beredskapsdepartementet ved skriv av 22.4.2021¹² (vedlagt), hvor man har igangsatt en nærmere utredning av blant annet spørsmålet om uthenting av de samme opplysninger til forebyggingsformål. For Kripos fremstår det naturlig og viktig at denne prosessen fortsetter og koordineres med pågående prosess knyttet til ny ekomlov. Kripos har uttalt seg til behovet for slik uthenting i skriv av 5.8.2021¹³ (vedlagt).

Når det gjelder kostandsmodeller mv. er dette omtalt under i punkt 6.

¹² Deps ref 21/1527-NNO

¹³ Kripos ref 21/53274

6. Kostnadsmodeller

Som redegjort for under pkt 5 vedtok Stortinget den 18.6.21 IP-lagring ved innføring av ny § 2-8a i ekomloven. Bestemmelsens tredje ledd gir følgende føring for kostnadsfordelingen mellom tilbyder og staten;

Tilbyder skal dekke investerings- og driftskostnader som påløper for å oppfylle lagringsplikten. Staten dekker kostnadene for utlevering av informasjon etter § 2-8 b første ledd.

Denne bestemmelsen er nå foreslått inntatt i ny ekomlov § 3-4 annet ledd.

Lovendringen er ikke trått i kraft, men det er lagt opp til at den skal virke sammen med den regel om kostnadsfordeling som følger tilretteleggingsplikten i § 2-8, som i annet ledd fastslår følgende om fordeling av kostnader tilknyttet plikten;

Tilbyders driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten dekkes av staten for de merkostnader som følger av disse tjenestene.

Denne bestemmelsen er nå foreslått inntatt i ny ekomlov § 3-6 annet ledd.

Konsekvensen er at det nå eksisterer to ulike prismodeller i ekomloven som begge er foreslått videreført i ny lov. Dette mener Kripos er uheldig av flere grunner.

Kripos har over flere år påpekt betydelig utglidning og uklarhet knyttet til tolkingen av bestemmelsen i gjeldende lov § 2-8. Fra politiets side har det hele tiden vært lagt til grunn at merkostnadene knyttes til uthentingskostnadene. Samtidig opplever vi at enkelte tilbydere på ulike måter har søkt å skyve kostnader fra investering over på drift. I den senere tiden blant annet gjennom leasingavtaler og ved innføring av begrepet «bortfallskostnader» som utgangspunkt for hva staten skal dekke av tilbyders utgifter. Kripos opplever således at utgangspunktet for kostnadsfordeling etter dagens § 2-8 mer eller mindre kontinuerlig utfordres av enkelte tilbyderne.

Regelen, og den uklare praktiseringen, har lenge vært en utfordring for politiet. Kripos argumenterte derfor sterkt for et klarere regelteknisk utgangspunkt for kostnadsfordeling i forbindelse med prosessen rundt IP-lagring, og vi mener den løsning som er nå er valgt for kostnadsfordeling i den anledning - jf ny § 2-8a - bør gjelde all tilrettelegging for lovbestemt tilgang.

Det kan i den forbindelse vises til argumenter trukket frem i Politidirektoratets høringssvar til departementet av 10.2.2021:

Når det gjelder kostnadsfordelingsmodell uttaler Kripos blant annet følgende: "Kripos' klare utgangspunktet er at kostnader knyttet til lagring, herunder investering i og drift av løsninger, må dekkes av tilbyderne selv. Kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn, og staten bør som er helt klare utgangspunktet kunne pålegge næringer tilretteleggingskrav uten kompensasjon. Kripos kan ikke se at dette tilfellet skiller seg nevneverdig fra for eksempel situasjonen for finansnæringer, som

selv er pålagt å dekke kostnadene knyttet til hvitvaskings-registeret. En utvikling i retning av staten skal måtte betale virksomheter for å legge til rette for ivaretagelsen av grunnleggende samfunnsmessig behov og tjenester, er etter vår oppfatning klart uheldig".

Politidirektoratet tiltrer Kripas sin vurdering.

Politidirektoratet vurderer som Kripas at det er utfordrende å skille mellom investeringskostnader og driftskostnader. Kripas trekker som eksempel fram om det vil bli vurdert som drift eller investering dersom man inngår leasingavtale istedenfor innkjøp av serverpark. Direktoratet mener som Kripas at dersom det velges en løsning hvor staten skal dekke annet enn rene uthentingskostnader, bør man gå for en modell der det ikke skilles mellom investerings- og driftskostnader, jf. modell E. Videre er det direktoratets oppfatning at en fast fordelingsnøkkel mellom tilbyderne blir mest riktig. Det store antallet tilbydere tilsier at individuelle refusjonsavtaler vil være ressurskrevende å drifte.

Kripas peker i sitt innspill på at uthentingskostnader bør begrenses til å gjelde rene kostnader med å hente ut lagrede data og overføre disse til politiet. Videre uttaler Kripas at valget av kostnadsfordelingsmodell ikke må få konsekvenser for om politiet faktisk velger å innhente data, og lage utfordringer for de innarbeidede ordninger som gjelder for innhenting av trafikkdata og tilrettelegging for kommunikasjonskontroll. Politidirektoratet tiltrer Kripas sine vurderinger.

Departementets vurderinger og konklusjon fremgår av I Prop. 167 L (2020–2021) under pkt 10.4, hvor vi vil fremheve følgende uttalelser:

Departementet er enig i at kriminalitetsbekjempelse er et sentralt samfunnsmessig hensyn hvor staten bør kunne pålegge næringer tilretteleggingskrav, og viser til at dette er tilfellet for finansnæringen som er pålagt å dekke kostnadene knyttet til hvitvaskingsregisteret, selv om situasjonen ikke er direkte sammenlignbar med en ordning for lagring av IP-data. Til tross for at det vil være ulikheter mellom finansnæringen og ekomtilbyderne knyttet til henholdsvis hvitvaskingsregisteret og IP-lagringsplikten, viser departementet til at dette trekker i retning av at næringer i visse tilfeller må kunne pålegges tilretteleggingskrav uten kompensasjon. Departementet viser også til at enkelte av våre naboland praktiserer lignende ordninger. I både Sverige og Danmark må tilbyderne bære kostnadene ved å innrette sine systemer slik at de kan levere nødvendig informasjon til politiet, altså dekker de selv investerings- og driftskostnadene.

.....

Departementet legger til grunn at modell A i størst grad ivaretar hensynet til samfunnsøkonomisk kostnadseffektivitet, ved at tilbyderne har størst insentiv til å velge kostnadseffektive løsninger når de selv må bære investerings- og driftskostnadene. Behovet for en egen kontrollenhet/ordning for å ettergå kostnader ved valgte løsninger, bortfaller med modell A, til forskjell fra de andre modellene. Etter en totalvurdering av innspillene som er kommet inn, mener departementet at kostnadsfordelingsmodell A bør velges.

I et konkurranseutsatt marked vil tilbyderne alltid søke å minimere enhver kostnad for å opprettholde god lønnsomhet. Når tilbyderne selv må dekke en kostnad eller en andel av en kostnad vil de derfor selv ha insentiver til å finne kostnadseffektive

løsninger. Kripos har over tid erfart at tilbydere - med utgangspunkt i § 2-8 - har lagt mye arbeid i å minimere driftskostnader ved å flytte dem over på staten. Kripos antar at slike bestrebelser alltid vil forekomme så lenge gjeldende bestemmelser gir muligheter for slike disposisjoner. Dette understreker behovet for å ha både klare og entydige regler.

Dersom man i ekomloven kun legger til grunn en prismodell, lik den nye § 2-8a, vil man ha en gjennomgående modell som er godt beskrevet og begrunnet i et helt oppdatert lovforarbeid. Man vil også bruke en modell som gir vesentlig mindre rom for tolking og utglidning og som hensyntar endringene i finansieringsmodeller. Modellen vil heller ikke virke konkurransedrivende, da den er lik for alle, og i mindre grad kan utnyttes av kreative aktører enn det som har vist seg mulig etter dagens § 2-8. En slik modell vil etter Kripos' vurdering også være i tråd uttalelser i forarbeidene til dagens lov, hvor et hovedpoenget var at staten skulle dekke merkostnadene relatert til uthenting, avgrenset mot blant annet investeringskostnader.

Kripos foreslår etter dette at § 2-8a gjøres gjennomgående for hele ekomloven med grunnlag i de vurderinger som følger av Prop. 167L.

7. Datasenterstrategi

Regjeringen lanserte den 11.8.2021 strategien "[Norske datasenter - berekraftige, digitale kraftsenter](#)". I kapittel 4.1.2 vedr. "Regulering av datasenter" er det opplyst at Regjeringen tar sikte på å høre en rammehjemmel for datasentervirksomhet i forbindelse med forslaget til ny ekomlov. Kripos antar at det i det vesentlige er bestemmelsene i forslaget til ny ekomlov § 3-8 tredje og sjette ledd det siktes til i denne sammenheng.

Regjeringen har i strategien lagt særlig vekt på at Norge har et godt utgangspunkt hva gjelder å være et attraktivt land å investere i når det gjelder etablering av datasentre, og de viser i denne sammenheng særlig til at vi har god og sikker tilgang til fornybar kraft, en solid digital infrastruktur, høy kompetanse og stabile rammevilkår. Regjeringen vil derfor arbeide for økt vekst i datasenternæringen. Det er i strategien videre lagt vekt på at denne utviklingen skal skje på en bærekraftig måte.

Kripos vil påpeke viktigheten av at slik virksomhet må innrettes med tilstrekkelig fokus på kontroll og tilsyn, og at politiet gis reelle muligheter til å håndheve norsk lov. Slik er det ikke nå og det synes heller ikke som om at strategien i tilstrekkelig grad tar hensyn til hvilken risiko som følger med en storstilt etablering av datasentre i Norge.

Kripos har ved flere anledninger opplevd store utfordringer med å innhente tilstrekkelig informasjon fra tilbydere og virksomheter som opererer innenfor eller i tilknytning til datasentertjenester i Norge. Utfordringene har bestått i manglende muligheter for å identifisere virksomheter og ansvarlige personer for hosting- og

kommunikasjonsinfrastruktur og tilhørende tjenester i tilknytning til datasentervirksomhet. Det er etter gjeldende rett ingen krav om identifisering av hverken virksomheter eller ansvarlige personer. Det stilles heller ingen krav i dag til notoritet over hvilke data som er lagret hvor i datasentrene. Dette svekker politiets evne til å forebygge, avverge og etterforske et bredt spekter av digital kriminell aktivitet som kan gjennomføres på og/eller gjennom norsk territorium og i virksomheter underlagt norsk jurisdiksjon.

Med dagens lovverk er norske myndigheter i mange situasjoner forhindret fra å effektivt iverksette fattede beslutninger. Sett fra Kripos' ståsted synes samtidig nasjonale tilsynsmyndigheter å mangle muligheter til effektiv og tilstrekkelig kontroll.

Ved at Norge blir et mer attraktivt marked for datasentre, vil det også tiltrekke seg utenlandske aktører. Vi må påregne at antall anmodninger fra utenlandske samarbeidspartnere om etterforskning av informasjon i norske datasentre vil øke. Et fravær av effektiv kontroll kan medføre at Norge blir en frihavn for IKT-relatert kriminalitet. I ytterste konsekvens kan sågar statlige aktører misbruke norske datasentre i angrep mot tredjeland.

Det opplyses i strategien at regjeringen vil følge opp regulering av datasentre gjennom dialog med datasenternæring og relevante styresmakter. I tilknytning til dette vil Kripos fremheve politiet som en åpenbart relevant styresmakt i denne henseende. Vi konstaterer imidlertid at hverken forarbeidene til ny ekomlov eller den aktuelle datasenterstrategi omtaler disse forhold i særlig grad eller omtaler politiet som sentral adressat for nevnte dialog.

Det er i strategien eksplisitt uttalt at *"Regjeringa vil at datasenter blir vurderte for regulering i ekomregelverket og anna relevant regelverk for å ivareta digital tryggleik og nasjonale tryggleiksinteresser."*, og at *"Regjeringa vil delta aktivt i europeisk samarbeid for å bidra til formålstenlege, og primært felleseuropeiske, løysingar for å vareta digital tryggleik, kamp mot kriminalitet og nasjonale tryggleiksinteresser knytt til datasenterverksemd."* Til det siste er det opplyst at NIS 2-direktivet, som omhandler slike problemstillinger, for tiden er til behandling i europaparlamentet og rådet. Kripos er bekymret for at dette betyr at det ikke vil skje noe med disse utfordringene før arbeidet med NIS 2-direktivet er avsluttet eller i alle fall har fått en tydelig "retning".

Kripos opplever at kriminalitetsbekjempelse tilknyttet datasentervirksomhet i Norge hindres av klare regulatoriske mangler, som eksempelvis manglende mulighet til å spore datatrafikken fra datasenter i Norge.

Dersom det ikke snarlig tas hensyn til disse utfordringene vil datasentre i Norge kunne tiltrekke seg kriminalitet fra hele verden. En datasenterstrategi som ikke i tilstrekkelig grad tar tak i de ovenfor nevnte utfordringer, vil i vesentlig grad kunne forsterke uønsket utnyttelse av datasentervirksomhet i Norge og medføre store utfordringer både nasjonalt og internasjonalt.

Slik Kripos leser forslaget til ny § 3-8 det fokuseres det i det alt vesentlige på datasikkerhetssiden og regelen gir i liten grad rom for tiltak som vil bidra til politiets forebyggende eller kriminalitetsbekjempende arbeid.

8. Særlige merknader

8.1. Ekomlovens formål § 1-1

Kripos har registrert at formålet med den nye loven i stor grad er uforandret, men at departementet i tillegg til å skulle stimulere til næringsutvikling og innovasjon samt ivareta klima og miljø også foreslår enkelte justeringer for å synliggjøre at elektroniske kommunikasjonstjenester skal leveres med forsvarlig sikkerhet. Sett i fra politiets ståsted bør sikkerhetsperspektivet i så måte utvides til også reflektere den innvirkning elektronisk kommunikasjon har på en stor mengde kriminalitet, både som åsted og sporsted for kriminalitet. Etter Kripos' oppfatning bør dette også fremkomme i lovens formål.

8.2. Informasjon til nummeropplysningstjenester

Ekomtilbyderne får tilgang på informasjon om deres sluttbrukere når de registreres. Departementet har på side 112 i høringsnotatet lagt til grunn at det er nødvendig å begrense tilgangen til slike opplysninger og tydeliggjøre rettighetene og pliktene knyttet til utlevering av informasjon til nummeropplysningstjenestene. Det er i denne sammenheng særlig henvist til utlevering av informasjon om brukerens fødselsdato, og krav knyttet til utlevering av nummeropplysningsinformasjon om barn. For politiet er det særlig viktig å kunne få tilgang til fødselsdato, fordi politiet har behov for å identifisere bruker. For politiet er det i alminnelighet enklere å hente slike opplysninger fra nummeropplysningstjenester (som f.eks. Pelle), enn hos den enkelte operatør. Et alternativ, og formentlig en bedre løsning, kan være at vi får tilgang til abonnementsdata via NRDB.

8.3. Nødanrop

Tilgang til telefonnummer, sluttbrukers navn og nødvendige opplysninger om geografisk lokalisering er sentralt for politiet også ved nødanrop. At dette behovet også gjelder ved "E-call" er omtalt i høringsnotatet og det fremkommer på side 135 at tilbyder også plikter å rute "E-call" til valgt mottakssentral for nødanrop med de nevnte opplysninger tilgjengelig. For å ivareta de tilsvarende hensynene knyttet til e-call bør politiet også ha tilgang til knytningen mellom simkort/apparat og kjøretøy. Dette mangler i dag og er heller ikke hensyntatt i lovforslaget.

8.4. Forbud mot jammere

I forslaget til ny ekomlov § 13-2 foreslås en ny bestemmelse om forbud mot radioutstyr mv. som er ment å forstyrre eller hindre elektronisk kommunikasjon. Såkalte "jammere" er en reell problemstilling som politiet har erfaring med og hvor

slik utstyr er benyttet for å sette loggere og utstyr for romavlytting ut av funksjon. Dette er erfaringer som samsvarer med tilsvarende hendelser fra utlandet. Kripes er også kjent med at slikt utstyr på tilsvarende vis har forstyrret andre nødetater og andre kritiske funksjoner. Kripes støtter forslaget.

8.5. Forholdet mellom forvaltningslov og straffeprosesslov

Praksis fra departementet har vist at det kan synes noe uklart hvilket regelsett som kommer til anvendelse ved behandling av innsynsaker hos ekommyndigheten. Dette gjelder situasjoner hvor en part begjærer innsyn i om politiet har begjært opphevelse av taushetsplikt etter ekomloven, i medhold av straffeprosessloven § 118, jf. § 230 og §§ 203 flg. knyttet til etterforskning av straffesak, jf. straffeprosessloven § 224.

Kripes mener at det i merknaden til forslaget § 14-1 bør presiseres at forvaltningsloven ikke kommer til anvendelse i innsynsaker som gjelder opphevelse av taushetsplikt når begjæringen er fremmet av politiet etter straffeprosessloven § 118, jf. § 230 og §§ 203 flg. Her er det straffeprosesslovens regler om innsyn mv. som kommer til anvendelse. Dette får betydning for spørsmål om opphevelse av taushetsplikten etter forslaget § 3-2 tredje og fjerde ledd. Kripes viser til straffeprosessloven § 1 og forvaltningsloven § 4 første ledd litra b) hvor det heter at forvaltningsloven ikke gjelder "*.....saker som forvaltningsorganet selv behandler eller avgjør i medhold av rettspleielovene.....*" Denne formuleringen¹⁴ tar sikte på å få bedre frem at forvaltningslovens saksbehandlingsregler gjelder i tilfeller hvor forvaltningsorganet har en mer avledet tilknytning til saker etter rettspleielovene, f.eks. som part, anmelder eller fornærmet. Dette er nettopp ikke tilfelle når politiet fremsetter denne type anmodninger om opphevelse av taushetsplikt etter straffeprosessloven. For Kripes fremstår dette som klart, men vi har likevel erfart at det i forvaltningen synes uklart hvilket regelsett som kommer til anvendelse.

8.6. Rett til bruk av frekvenser

Det følger av forslaget til ny ekomlov i § 11-13 at politiet, uten tillatelse fra myndigheten, kan ta i bruk frekvenser tildelt andre dersom vilkårene for *identifisering* av kommunikasjonsanlegg er oppfylt. I lov 17. juni 2016 nr. 54 ble det i straffeprosessloven § 216 b annet ledd bokstav c også åpnet for bruk av teknisk utstyr for å *lokalisere* et kommunikasjonsanlegg. Foreslått § 11-13 åpner dermed kun for frekvensbruk i ett av de to tilfelle som aktuell bestemmelse i straffeprosessloven åpner for. Kripes antar at dette ikke er tilsiktet, og ber om at dette rettes i det videre lovarbeidet, typisk ved å innta å tilføye lokalisering i teksten.

I utkastet til § 11-13 fjerde ledd gjøres unntak fra krav om tillatelse for helikoptre fra redningstjenesten, Forsvaret og politiet, av hensyn til gjennomføring av søk og redning. Kripes mener denne bestemmelsen må omformuleres slik at unntaket gjelder etatene redningstjenesten, Forsvaret og politiet. Dette fordi helikopterene ikke i seg selv kan være noe rettssubjekt og fordi tilsvarende behov kan gjøre seg gjeldende i

¹⁴ Ot.prp. nr. 75 (1993-1994) kap. 6.4.

andre sammenhenger, for eksempel for båt. Tilsvarende endring må da gjøres i resten av bestemmelsen.

8.7. Krav til politiattest

I utkastet til § 3-9 foreslås det en ny bestemmelse hvor ekomtilbyderne gis mulighet til å kreve fremlagt *ordinær politiattest* i forbindelse med ansettelse av personer som blant annet vil få tilgang til informasjon med vesentlig betydning for *sikkerheten i nett eller tjenester*. Kripos har tidligere¹⁵ tatt opp behovet for politiattest for ansettelse hos ekomtilbydernes politisvarsentrene, som rutinemessig behandler anmodninger fra politiet om blant annet kommunikasjonskontroll. Vi er positive til at en innhentingsmulighet lovfestes, men mener *ordinær politiattest* ikke er tilstrekkelig i alle situasjoner.

Tidsbegrensningen for *ordinær politiattest* etter politiregisterloven § 40 nr. 5 medfører at mange forhold kun påføres dersom de er ilagt ved dom eller vedtatt forelegg mindre enn tre år før utstedelsen av attesten. For i tilstrekkelig grad å kunne sikre både nett, tjeneste og sensitiv informasjon av annen karakter, mener Kripos at det bør vurderes å sikre tilbyderne en mulighet for å innhente *uttømmende og utvidet politiattest*, jf politiregisterloven § 41. En slik mulighet bør heller ikke begrenses til de "tradisjonelle tilbyderne" slik lovforslaget legger opp til. Det vil etter vårt syn ikke gi et tilstrekkelig fremtidsrettet regelverk. Vi foreslår derfor at formuleringen "*med unntak av nummeruavhengig person-til-person-kommunikasjonstjeneste*" tas ut

Vi kan heller ikke se at formuleringen *vesentlig betydning for sikkerhet i nett eller tjenester* er dekkende for å avhjelpe behovet for attest for ansatte som behandler taushetsbelagt informasjon, for eksempel i tilknytning til politiets skjulte metodebruk. Vårt forslag er at man vurderer et tillegg i lovteksten som synliggjør at også (annen) befatning med taushetsbelagt/sensitiv informasjon i stillingen kan kvalifiserer for innhenting av attest. Dette kan for eksempel gjøres ved å innta følgende tillegg avslutningsvis i første ledd første punktum "*.....eller som av annen grunn er av særlig sensitiv karakter.*"

Politiregisterloven § 37 angir hvilke formål som berettiger bruk av politiattest. Av bestemmelsen fremgår det blant annet at politiattest kun kan brukes for å utelukke fysiske og juridiske personer fra "*....stilling, virksomhet, aktivitet eller annen funksjon*". I tillegg må et av vilkårene i bestemmelsens nr. 1 til 6 være oppfylt. I nr. 1 heter det at bruk av politiattest kan være berettiget dersom "*... lovbruddet gjør en person uegnet, og manglende utelukkelse vil kunne medføre betydelige skadevirkninger*". Kripos mener at det i merknadene til ny bestemmelse bør gis nærmere anvisning på hva som kan eller skal vektlegges for at en person skal kunne anses for uegnet og hva som eventuelt kan vurderes å kunne føre til betydelige skadevirkninger. På et slikt grunnlag kan tilbyderne lettere vurdere om aktuelle kandidater kan inneha stillingen eller utføre de aktuelle oppgavene.

¹⁵ Fellesmøte mellom ekomtilbyderne, Kripos og Nkom 4. april 2019

Norsk politiattest har for øvrig relativt liten verdi dersom person som skal vurderes har en kortvarig tilknytning til Norge. Det bør derfor etter vår vurdering også sikres adgang til å kreve politiattest utstedt i personens hjemland. Politiregisterforskriften § 28-2 første ledd tredje punktum, likestiller politiattest utstedt i annet EØS-land med norsk politiattest i de tilfeller hvor det er hjemlet krav om botid i særlovgivningen, jf. politiregisterloven § 36, annet ledd. Kripes foreslår derfor at det også tas inn et krav om botid i ny bestemmelse om politiattest.

Kripes påpeker samtidig at et slikt forslag bør ha en omtale av personvernkonsekvenser. Når forslaget følges opp i en lovproposisjon bør det således drøftes og synliggjøres hvilke konsekvenser den foreslåtte bestemmelsen vil kunne få for personvernet. Det bør i reguleringen også pålegges plikter med hensyn til rutiner for å slette politiattester når disse ikke lenger er nødvendig å oppbevare, og senest ved tidspunktet vedkommende slutter i den stillingen som ga grunnlaget for vandelskontroll, jf. politiregisterforskriften § 37-2 annet punktum.

8.8. Taushetsplikt

I departementets merknader til ny § 3-2 om taushetsplikt uttales på side 34 at man ber særlig om kommentarer og innspill til konsekvenser endringen av definisjonen av elektronisk kommunikasjonstjeneste vil få for straffeprosessloven § 118, jf. også § 230, og tvisteloven § 22-3. Departementet understreker samtidig at det ikke er utredet eller foretatt en grundig vurdering av om man i norsk rett er forpliktet til å la denne utvidelsen komme til anvendelse også for de prosessuelle bevisforbud.

Å få full oversikt over straffeprosessuelle konsekvenser av denne utvidelsen har for Kripes vært utfordrende. Vi vil imidlertid påpeke at dersom en utvidelse også gis straffeprosessuell anvendelse så vil det medføre at et ytterligere stort antall henvendelser fra politiet om utlevering av infomasjon vil måtte rutes via Nkom for opphevelse av taushetsplikt før disse kan effektueres. Allerede etter dagens tilbyderbegrep medfører dette et omfattende arbeid både for politi/påtalemyndighet og Nkom, og i siste instans retten.

Det kan etter vår vurdering stilles spørsmål ved om dagens ordning er nødvendig og formålstjenlig på et område hvor det rent faktisk er en straffeprosessuell beslutning knyttet til bevisinhenting som ligger til grunn for henvendelsen. Kripos mener det her kan skilles mellom strafferettslige bevisforbud og sivilrettslige bevisforbud. I den videre vurdering av disse spørsmål mener Kripos man derfor bør se på en løsning hvor man unntar tilbyder etter ekomloven fra den opprømsing som foretas i straffeprosessloven § 118 første ledd andre punktum.

Med hilsen

Ketil Haukaas
assisterende sjef

Dokumentet elektronisk godkjent uten signatur.

Saksbehandler
Knut Jostein Sætнан
politiadvokat
Telefon: 99286416

Kopi
Riksadvokatembetet
Det Nasjonale statsadvokatembetet



POLITIET
POLITIDIREKTORATET

Kommunal- og moderniseringsdepartementet

Postboks 8112 Dep
0032 Oslo

NATIONAL POLICE DIRECTORATE

Deres referanse:
21/3980

Vår referanse:
21/82791

Sted, Dato
Oslo, 29.10.2021

**HØRINGSSVAR – FORSLAG TIL NY EKOMLOV, NY EKOMFORSKRIFT OG
ENDRINGER I NUMMERFORSKRIFTEN**

Vi viser til Kommunal- og moderniseringsdepartementets (KMD) høringsbrev av 2. juli 2021 med forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften. KMDs høringsfrist var satt til 15. oktober 2021 som Politidirektoratet etter avtale med departementet har fått forlenget til 1. november 2021.

Politidirektoratet har forelagt høringen for Kripes, Økokrim, Politihøgskolen og politidistriktene Oslo, Nordland, Finnmark, Trøndelag og Innlandet. Politidirektoratet har mottatt høringssvar fra politidistriktene Oslo og Finnmark, samt Kripes. Oslo politidistrikt tiltrer i sitt høringssvar de merknader som gis i høringssvaret fra Kripes. Finnmark politidistrikt gir merknader til forslaget om utstedelse av politiattest. Høringssvarene fra Finnmark politidistrikt og Kripes er vedlagt.

Kort om høringen

KMD har sendt på alminnelig høring en lovpakke med

- forslag til ny lov om elektronisk kommunikasjon (ekomloven),
- forslag til ny forskrift om elektroniske kommunikasjonsnett og - tjenester,
- endringer i forskrift om nummerressurser for elektroniske kommunikasjonsnett og - tjenester (nummerforskriften)
- forslag til ny forskrift om stedlig virkeområde for lov om elektronisk kommunikasjon vedrørende Svalbard, Jan Mayen, Bilandene og Antarktis

KMD foreslår blant annet å gjennomføre EUs ekomdirektiv (2018/1972) som har erstattet EUs regelverksplanke for elektronisk kommunikasjon fra 2002, forordningen om BEREC (2018/1971) og deler av tilgjengelighetsdirektivet (2019/882) som gjelder ekomområdet. I tillegg viderefører lovpakken henholdsvis gjennomføring og inkorporering av en rekke andre EU-rettsakter som er innlemmet i EØS-avtalen. Lenke til ekomdirektivet, BEREC-forordningen og tilgjengelighetsdirektivet ligger tilgjengelig på KMDs høringsside.

Videre har KMD innhentet en vurdering fra Menon Economics og Analysys Mason om ekomdirektivet artikkel 61 nummer 3.

Politidirektoratet

Post: Postboks 2090 Vika, 0125 Oslo
Besøk: Fridtjof Nansens vei 14/16

Tlf: 23 36 41 00
Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no

Org. nr.: 982 531 950
Giro: 7694.05.02388
www.politi.no

Politidirektoratets merknader

Det er et omfattende lovendringsforslag som er sendt på høring hvor en rekke temaer potensielt er av stor betydning for politiet. Kripos har gitt utførlige merknader på en del sentrale forhold for politiet. Politidirektoratet kan fullt ut tiltre disse merknadene. Politidirektoratet vil i det følgende påpeke enkelte særlige forhold.

Nummeruavhengige person til person kommunikasjonstjenester

De nummeruavhengige person til person kommunikasjonstjenestene har som påpekt i høringsnotatet (høringsnotatet pkt. 17.2) hatt en betydelig vekst de siste årene, og denne utviklingen er utfordrende sett fra et kriminalitetsbekjempende perspektiv. En bred tilgjengeliggjøring av avlyttingsfrie og ikke-sporbare kommunikasjonstjenester kan etter direktoratets oppfatning utfordre samfunnsvernet og kriminalitetsbekjempelsen. Det vises nærmere til høringssvaret til Kripos som også påpeker at det bør innføres kompenserende tiltak.

Tilbyderbegrepet

I forslag til ny ekomlov § 1-5 nr. 4 og nr. 11 defineres tilbyder av elektronisk kommunikasjonstjeneste til å være fysiske eller juridiske personer som mot vederlag tilbyr andre tilgang til elektronisk kommunikasjonsnett eller kommunikasjonstjeneste, jf. nærmere § 1-5 nr. 4 a) – c). Politidirektoratet er i likhet med Kripos positive til utvidelsen av definisjonen av elektronisk kommunikasjonstjeneste i § 1-5 nr. 4, og prinsippet om at definisjonen blir bestemt ut fra tjenestens funksjon og ikke de tekniske løsningene som ligger bak.

Direktoratet vil påpeke at begrepet også dekker leverandører av datasentertjenester (VPSer) som selger hosting med tilhørende tilgang til internett samt VPN (Virtual Private Network) - leverandører som selger tilgang til internett fra servere disse disponerer. Dette bør presiseres i merknadene til bestemmelsene for å sikre at VPS- og VPN-leverandører blir underlagt de samme pliktene i ekomloven som ISPer (normal aksess til internett). Det fremstår som utfordrende og uheldig at lovforslaget kun dekker virksomheter som drives med kommersiell interesse, da dette medfører at bruk av vederlagsfrie tjenester kan skje uten mulighet for myndighetskontroll. Som nærmere omtalt vil dette inkludere eksempelvis tjenester som Signal og IRC, hvorav sistnevnte er en mye brukt plattform for datakriminelle og av personer som distribuerer overgrepsmateriale. Det bør videre klargjøres i lovforarbeidene at tilbydere som tilbyr en elektronisk kommunikasjonstjeneste som en del av sin kommersielle virksomhet (herunder tredjepartsbetaling) skal være underlagt ekomloven.

Tilretteleggingsplikten

Bruk av skjulte etterforskningsmetoder er sentralt i kampen mot den mest alvorlige og organiserte kriminaliteten. I likhet med Kripos vil Politidirektoratet fremheve at for flere at de tilgjengelige metodene er politiets evne helt avhengig av at ekomtilbyderne samarbeider med politiet og bidrar til den tekniske gjennomføringen av metodebruken. Tilretteleggingsplikten er her sentral. Informasjon fra tilbyderne er også av stor betydning for tradisjonelle etterforskningsmetoder, som for eksempel beslag og utleveringspålegg etter straffeprosessloven §§ 205 og 210.

Direktoratet registrerer at tilretteleggingsplikten stadig oftere utfordres av tilbydernes kommersielle interesser. Teknologiutviklingen gjør at det konkrete innhold i tilretteleggingsplikten stadig er i endring. Direktoratet tiltre Kripos sin merknad om at tilretteleggingsplikten bør konkretiseres slik at de grunnleggende prinsippene sikres og at uklarhet begrenses. Kripos viser til at formuleringen på side 38 i høringsnotatet er uheldig idet den kan gi inntrykk av at tilretteleggingsplikten står tilbake for innovasjon og teknologisk utvikling. Tilretteleggings-

plikten etter gjeldende rett forutsetter at nytt utstyr/og eller tjenester ikke kan innføres uten at tilbyder samtidig sikrer lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon. Som påpekt av Kripos bør dette fremkomme klarere i det videre lovarbeidet. Videre er det bekymringsverdig om manglende klarhet i hva tilretteleggingsplikten konkret medfører av krav og forventninger til tilbyder gir rom for en praksis hvor tilbydere enkelt kan definere seg ut av tilretteleggingsplikten.

Kripos etterlyser en klarere og mer omfattende hjemmel for politiet til å be om bistand fra tilbydere til gjennomføring av tvangsmiddelbruk. Kripos viser til at etter gjeldende rett er det en plikt for tilbyder å yte nødvendig bistand ved gjennomføring av kommunikasjonskontroll, jf. straffeprosessloven § 216a, men denne bestemmelse gjelder eksempelvis ikke ved dataavlesning, romavlytting, samtaleavlytting eller skjult kameraovervåking og teknisk sporing. Når det gjelder anvendelsesområdet er direktoratet enig med Kripos i at tilretteleggingsplikten må gjelde for alle tilbydere av ekomtjenester som tilbys til sluttbrukere i Norge, og dette bør presiseres i lovtekst eller i merknader til lovteksten.

Krav til entydig identifisering av sluttbrukere

I sitt høringssvar viser Kripos til et par tilfeller hvor effekten av tilbyders plikt til entydig å identifisere sine sluttbrukere har blitt vesentlig redusert. Dette samtidig som behovene for å kunne identifisere sluttbrukere også for IP-basert trafikk har økt tilsvarende - hvilket også har en direkte betydning for effekten av å lagre IP-adresser. Det vises til forslag til ny § 3-4 som viderefører gjeldende § 2-8a som ble vedtatt i juni i år. Kripos foreslår derfor at sluttbrukere også må registreres hos de som videreselger kommunikasjonstjenester/-bærere som kan brukes til person til person kommunikasjon - på lik linje med eksisterende plikt for ekomtilbydere til entydig å identifisere sine sluttbrukere ved inngåelse endring eller opphør av avtale. Politidirektoratet tiltrer merknaden til Kripos.

Kostnadsmodeller

Departementet foreslår å videreføre kostnadsfordelingen i dagens ekomlov § 2-8 hvor det fremkommer at "*Tilbyders driftskostnader knyttet til oppfyllelsen av tilretteleggingsplikten dekkes av staten for de merkostnader som følger av disse tjenestene*". Politiet erfarer at det er noe ulik forståelse av bestemmelsen, noe som er en utfordring for politiet. Videre er dette en annen kostnadsmodell enn den som ble valgt ved IP-lagring i nylig vedtatt § 2-8a i ekomloven, hvor staten dekker kostnadene for utlevering av informasjon, mens tilbyder skal dekke investerings- og driftskostnader. Det er således to ulike prismodeller i ekomloven som begge er foreslått videreført i ny lov. Politidirektoratet tiltrer merknaden fra Kripos om at den kostnadsfordelingen som ble valgt for IP-lagring, bør gjelde for all tilrettelegging.

Forbud mot jammere

I forslaget til ekomlov § 13-2 foreslås et generelt forbud mot radioutstyr mv. som er beregnet på å forstyrre eller hindre lovlig elektronisk kommunikasjon (jammere), med mindre det er eksplisitt tillatt i loven. Politiet vil ha adgang til å jamme i medhold av ekomloven § 11-13 og § 11-14. Politidirektoratet viser til at andres bruk av slikt utstyr vil kunne forstyrre politiets arbeid og utgjøre en trussel mot samfunnet, og vi støtter derfor dette forslaget.

Uskadeliggjøring av droner og andre gjenstander dersom det er fare for liv og helse mv.

I forslaget til ekomlov § 11-13 første ledd siste setning heter det at "*Politiet kan også ta i bruk frekvenser og utstyr som ikke oppfyller kravene i forskrifter gitt med hjemmel i § 13-1 tredje ledd for å uskadeliggjøre droner og andre gjenstander dersom det er fare for liv, helse eller sikkerhet*". Forslaget til lovtekst ivaretar politiets behov. I merknadene til lovforslaget fremgår det uttrykkelig at politiet kan bruke dette virkemiddelet som et operativt tiltak i alle situasjoner

hvor det er nødvendig for å ivareta liv, helse eller sikkerhet. Dette er en hensiktsmessig presisering.

Redningstjenesten

Videre i forslaget til ekomlov § 11-13 fjerde ledd heter det at "*Redningshelikoptrene og Forsvarets og politiets helikoptre kan uten tillatelse fra myndigheten ta i bruk frekvenser som er tildelt andre, til identitetsfanging når det er nødvendig for gjennomføring av søk- og redningsoppdrag*". Formålet med bestemmelsen synes å være at redningstjenesten skal få tilgang til dette virkemiddelet når det er nødvendig for å gjennomføre redningsoppdrag, hvilket tiltres. Direktoratet stiller imidlertid spørsmål ved hensiktsmessigheten av å avgrense hjemmelen til en bestemt kapasitet, nemlig helikoptre. Politiet utøver redningstjeneste også med bruk av andre kapasiteter som for eksempel droner og båter. Dersom også andre kapasiteter er anvendbare i forbindelse med søk- og redningsoppdrag, så bør ikke loven stenge for slik bruk etter direktoratets oppfatning. Det foreslås derfor at lovteksten viser til formål (redningstjeneste) istedenfor særskilte kapasiteter (helikoptre). Videre i forslaget til ekomlov § 11-13 sjette ledd framgår det av sammenhengen at politiets helikoptre skal varsle. Det må være en myndighet som varsler andre myndigheter. Politiets helikoptertjeneste er en del av politiet, og det er derfor tilstrekkelig å vise til at det er politiet som varsler.

Nødanrop

Etter direktoratets oppfatning bør det være en teknologi- og standarduavhengig beskrivelse av tjenester for nødanrop på andre plattformer enn telefonlinjer/GSM-tjenester. OTT-tjenester på internett/bredbånd tilbyr nødanrop fra flere plattformer som for eksempel Applewatch, Skype mv. I tillegg er det sannsynlig at nødanrop vil tilbys til publikum gjennom applikasjoner med videostrømmer fra innringer til nødmeldesentral.

Annet

Kripos gir i sitt høringssvar en rekke særlige merknader. Politidirektoratet tiltrer disse hvor Politidirektoratet særlig har ettergått forslaget om utstedelse av politiattest. Når det gjelder høringssvaret fra Finnmark politidistrikt tiltrer direktoratet merknaden om at det bør presiseres at politiattester som framvises ikke skal være eldre enn 90 dager.

Med hilsen

Kristine Langkaas
seksjonssjef

Morten Rustad
seniorrådgiver

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:

- Høringssvar fra Kripos av 1. oktober 2021
- Høringssvar fra Finnmark politidistrikt av 7. oktober 2021

Kopi: Justis- og beredskapsdepartementet