



POLITIETS
SIKKERHETSTJENESTE

Postboks 4773 Nydalen
0421 OSLO
post@pst.politiet.no
Tlf.nr. 23 30 50 00
Besøksadresse:
Nydalen allé 35

Kommunal- og moderniseringsdepartementet
Postboks 8112 Dep
0032 OSLO

Deres ref.: 21/3980
Vår ref.: 21/03139-5
Dato: 1. november 2021

Høringssvar - ny ekomlov m.m.

Politiets sikkerhetstjeneste (PST) viser til høringsbrev av 2. juli 2021 vedrørende departementets høringsforslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften.

1. Innledning

PST er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste. PSTs hovedoppgave er å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet, som terror, terrorrelatert kriminalitet og ulovlig etterretningsvirksomhet mot Norge.

PST har gjennom bruk av tvangsmidler og skjulte etterforskningsmetoder regelmessig kontakt med tilbydere av kommunikasjonstjenester. Endringer i ekomloven vil således påvirke PSTs evne til å beskytte borgerne og ivareta grunnleggende nasjonale sikkerhetsinteresser. PST vil i det følgende peke på relevante deler av lovforslaget for tjenesten.

Lovforslaget som er på høring, er omfattende og krevende å sette seg inn i. PST kan ikke utelukke at det kan ligge problemstillinger i dette lovforslaget som treffer vår tjeneste, men som vi ikke har evnet å identifisere innen høringsfristen.

PST har lest bl.a. KRIPOS sin høringsuttalelse¹, som er svært grundig og gjennomarbeidet. De to tjenestene har mange sammenfallende synspunkter på lovforslaget. Som det vil fremgå støtter PST mange av KRIPOS sine synspunkter og forslag.

¹ Høringssvar av 1.10.2021 (KRIPOS`referanse 21/82791) s. 5

2. Tilbyderbegrepet

PST er positive til den utvidelsen av tilbyderbegrepet som forslaget legger opp til, herunder at definisjonen bestemmes ut fra tjenestens funksjon og ikke de bakenforliggende tekniske løsningene.

PST mener lovgiver bør tydeliggjøre at definisjonen av «internetttilgangstjeneste» (ny lov § 1-5 nr. 4 bokstav a) også omfatter leverandører av datasentertjenester (VPS`er) som selger hosting med tilhørende tilgang til internett samt VPN-leverandører som selger tilgang til internett fra servere disse disponerer. Slike leverandører vil da bli registreringspliktige og med krav om å kunne identifisere sluttbrukerne på linje med ISP`ene.

PST ser positivt på utvidelsen av «elektronisk kommunikasjonstjeneste» til også å omfatte tilbydere av en større krets av tjenester og at Snapchat, Telegram, iMessage/FaceTime, Gmail, Hotmail, Protonmail, Wikr, Teams, Whereby, Zoom, Slack m.fl. etter forslaget omfattes av plikter som nevnt.

PST tiltrer KRIPOS når det i deres høringsuttalelse understrekes viktigheten av at lovverket utformes på en slik måte at det fremstår som tydelig at det er tjenestens *funksjon* som er det sentrale for om den omfattes av de plikter som påhviler tilbydere etter den nye ekomloven. Det vil bidra til at loven blir teknologinøytral og mer robust i møtet med fremtidens teknologiske endringer.

Det fremstår som uheldig at lovforslaget kun dekker virksomheter som driver kommersiell aktivitet idet vederlagsfrie tjenester som benyttes av kriminelle, faller utenfor.

Tjenester som tilbyr kommunikasjon som en tilleggsfunksjon til tjenesten, som spill, nettforum, publisering m.m., omfattes ikke av tilbyderbegrepet og faller således utenfor tilbydernes plikter etter lovforslaget. Dette er uheldig idet disse kommunikasjonskanalene sees brukt i flere av PSTs saker. PST ber departementet vurdere å utvide tilbyderbegrepet til å omfatte denne typen tjenester.

3. Taushetsplikt

PST vil samtidig peke på noen uheldige konsekvenser som utvidelsen av tilbyderbegrepet vil ha for bevistilgangen i straffesaker og effektiviteten i avviklingen av straffesaker. Forslaget vil kunne påvirke politiets innhenting av bevis og hvilke bevis som kan fremlegges i retten.

Bevisforbudsreglene i straffeprosessloven § 118 og § 230 (som forbyr retten og politiet å ta imot forklaringer fra personer som er underlagt lovbestemt taushetsplikt) medfører at Nkoms saksmengde (ved behandling av anmodninger om fritak fra taushetsplikten) ventelig vil øke. Det vil igjen kunne skape forsinkelser i straffesaksbehandlingen.

Etter PSTs oppfatning virker forslaget om at Nkom skal frita ansatte i Facebook eller WhatsApp fra deres taushetsplikt, lite praktisk. Dersom PST ønsker

innholdsdata utlevert fra Facebook, må man gå veien om en rettsanmodning til USA, etter at en norsk domstol har funnet at vilkårene for utlevering er tilstede jf. straffeprosessloven § 210. Det er således en amerikansk domstol som vil måtte ta stilling til om utlevering av innholdsdata kan finne sted etter amerikansk rett. For Facebook er innholdsdata beskyttet av amerikansk rett og utlevering skjer i tråd med amerikansk prosess. Tilsvarende vil gjelde for nummeruavhengige tilbydere fra andre land.

I denne forbindelse vil det å innhente fritak for taushetsplikt fra Nkom virke som en unødvendig ekstra runde som medfører en belastning både for PST og for Nkom.

PST antar at man i forhold til straffeprosessloven § 118 må innfortolke at bestemmelsen gjelder overfor norske tilbydere av elektronisk kommunikasjonstjeneste eller i det minste en tilbyder som er undergitt Nkoms tilsynsmyndighet. Den type kommunikasjon vi her snakker om er oftest kryptert og politiet får som oftest tilgang til innholdsdata via beslaglagte telefoner hos en siktet. Dersom det ikke gjøres beslag hos siktede og man ønsker innholdsdata utlevert via tilbyder, betyr forslaget i realiteten at Nkom må forespørres i alle tilfelle der man ønsker et utleveringspålegg jf. straffeprosessloven § 210, fra tilbyder av nummeruavhengig person-til-person chat. Dersom tilbyderen er en utenlandsk tjeneste vil man likevel være henvist til andre lands straffeprosessuelle behandling av saken uten at et fritak fra Nkom da vil være av betydning.

PST, som for øvrig ser en rekke fordeler med å utvide tilbyderbegrepet til å omfatte nummeruavhengige person-til-person-kommunikasjonstjenester, vil likevel be departementet vurdere en regulering som samtidig ikke innskrenker eller forsinker PSTs tilgang til bevis i PSTs forebyggende arbeid og etterforskning av straffesaker.

3.1 Ubetinget utleveringsplikt

I forslaget til ny lov § 3-2 fjerde ledd foreslås følgende bestemmelse: *«Anmodning fra påtalemyndigheten eller politiet om opplysninger som omhandlet i tredje ledd skal etterkommes med mindre særlige forhold gjør det utilrådelig»*. Bestemmelsen er en videreføring av dagens lov uten at det gis noen begrunnelse for hvorfor teletilbyderne skal ha en slik adgang til å nekte utlevering. Som påpekt av Oslo statsadvokatembeter kan en slik nektelsesadgang åpne for misbruk. PST støtter deres forslag om at «med mindre særlige forhold gjør det utilrådelig» tas ut av bestemmelsen. Tilbyderne vil med dette forslaget få en ubetinget utleveringsplikt.

4. Lagringsplikt og utlevering av IP-adresser

PST ser positivt på forslaget om lagringsplikt (ny lov § 3-4) og utlevering av IP-adresser (ny lov § 3-5) som ble vedtatt av Stortinget i juni 2021 og som trer i kraft hhv. 1.1.2022 og 1.1. 2023.

De vedtatte endringene er begrenset til lagring og utlevering av IP-adresser for etterforskningsformål. PST har uttalt seg om PSTs behov for tilgang til slike adresser for forebyggingsformål i vårt brev til Justis- og beredskapsdepartementet av 6.9.2021.² PST ber om at dette arbeidet blir koordinert med den pågående prosessen med ny elov.

Det er i de vedtatte endringene ikke lagt opp til noen regulering av hvilken anledning tilbyderer skal ha til å varsle innehaveren av en IP-adresse m.v. om at PST har anmodet om utlevering av informasjon. Dersom tilbyderer avslører dette vil det potensielt kunne utgjøre en fare for nasjonens sikkerhet. Det vil eksempelvis kunne medføre at trusselaktøren fremskynder f. eks. en terrorhandling. PST advarer derfor mot at en innehavere av en IP-adresse blir gjort kjent med at PST har anmodet om utlevering av IP-adresser fra teletilbydern og ber departementet vurdere en særskilt regulering som ivaretar denne problemstillingen.

PST minner om at lovverket flere steder anerkjenner PSTs behov for å innhente informasjon uten at den berørte gjøres kjent med det. Det gjelder for eksempel i forbindelse med PSTs bruk av tvangsmidler i forebyggende øyemed, hvor den som tvangsmiddelet retter seg mot, ikke har krav på å bli underrettet, jf. politiloven § 17 e annet ledd. Det gjelder heller ikke noen alminnelig innsynsrett for den registrerte i personopplysninger som PST måtte behandle om en person, jf. politiregisterloven § 66 annet ledd.

4.1 Rapporteringsplikt

Departementet foreslår å innføre en årlig rapporteringsplikt om innhenting av IP-adresser til myndigheten, jf. ny lov § 3-5 tredje ledd, med en tilhørende forskriftshjemmel i femte ledd. Forslaget er ikke nærmere begrunnet. Det er på den bakgrunn betimelig å etterspørre begrunnelsen bak forslaget. Uten å forstå behovet for innføringen av en årlig rapporteringsplikt, hvilken myndighet det skal rapporteres til, hvilke opplysninger som skal rapporteres osv. er det vanskelig å gi innspill i denne omgang.

5. Tilretteleggingsplikten

PST vil, i likhet med KRIPOS, advare mot at tilbyderens tilretteleggingsplikt blir utvannet som følge av innovasjon og utvikling av nye produkter. Dagens lov forutsetter at nytt utstyr og/eller tjenester ikke kan innføres uten at tilbyder samtidig sikrer lovbestemt tilgang til «informasjon om sluttbruker og elektronisk kommunikasjon». PST støtter KRIPOS når de i høringssvaret påpeker at *«teknologit utviklingen gjør at det konkrete innhold i plikten til å legge til rette er i stadig endring, og at tilretteleggingsplikten bør konkretiseres slik at de*

² JDs ref. 21/1527-NNO, PSTs ref. 21/01136-7 (uoff.)

grunnleggende prinsippene sikres og at uklarhet begrenses». Handlingsrommet for at tilbyderne kan definere seg ut av tilretteleggingsplikten, bør minimeres.

6. Krav til entydig indentifisering av sluttbrukere for sluttbrukere av enkelte IoT-tjenester

PST viser til høringssvar fra KRIPOS vedr. politiets utfordringer med å identifisere sluttbrukere av kommunikasjonstjenester og beskrivelsen av hvordan utvikling av ny teknologi (eksempelvis knyttet til kommunikasjon til/fra kjøretøy, anonyme M2M-abonnementer) svekker effekten av tilbyders plikt til entydig å identifisere sine sluttbrukere. PST vil understreke viktigheten av at de grunnleggende prinsippene i tilretteleggingsplikten sikres.

7. Datasentre (datahaller)

I Nasjonal trusselvurdering (NTV) 2021 advarer PST mot statlig styrt digital spionasje i form av nettverksoperasjoner fra andre lands etterretningstjenester mot norske myndigheter og private virksomheter. PST advarer mot trusselaktører som benytter globale nettverk av digital infrastruktur mot norske virksomheter. PST ser at etterretningstjenester anonymt leier serverplass i datasentre i Norge. Gitt en økning i antall slike datasentre i Norge den kommende tiden, er det fare for at sentre også her i landet blir brukt til å gjennomføre nettverksoperasjoner.

PST støtter at datasentervirksomheten nå blir regulert. For PST er det vesentlig å kunne identifisere den reelle leietakeren i datasentre og kunne spore datatrafikk knyttet til disse i de saker som ligger under PSTs ansvarsområde.

Som også NSM og KRIPOS påpeker i deres høringsvar ber PST departementet vurdere om det bør innføres krav om entydig identifisering av sluttbrukere også for leie av IKT-struktur, tilsvarende kravet til entydig identifisering av sluttbrukere for person-til-person-kommunikasjon i forslaget til § 2-8.

Partene i Felles cyberkoordineringssenter (FCKS) beskrev allerede i mai 2020 i et brev til de berørte departementene³ hvilke utfordringer og behov for rettslig regulering partene i dette samarbeidet har knyttet til identifisering av sluttbruker av IKT-struktur. I brevet pekte partene blant annet på de utfordringer som knytter seg til fremleie av digital infrastruktur slik at virksomheten som driver datasenteret i Norge ikke kjenner identiteten til sluttbrukeren.

Det haster med å få på plass et rettslig rammeverk rundt datasentre, som blant annet øker myndighetenes innsikt i hvem som leier og disponerer IKT-infrastruktur i Norge, som legger til rette for politiets bruk av tvangsmidler, som sikrer at registreringsplikten overholdes og at oppgitt kontaktperson er underlagt norsk jurisdiksjon. PST ber departementet vurdere om forslaget til forskriftshjemmel i § 3-8 gir tilstrekkelig grunnlag for å regulere de behov som påpekes av NSM, KRIPOS, E-tjenesten og PST, eller om det er nødvendig å

³ NSM, PST, KRIPOS og E-tjenesten i brev til JD av 06.05.2020 (kopi sendt FD og KMD)

lovregulere enkelte av de forpliktelsene som foreslås pålagt tilbydere av datasentre.

8. Rett til bruk av frekvenser tildelt andre

Vi registrerer at det i forslaget til regulering av retten til bruk av frekvenser (ny lov § 11-13) kun er gitt adgang for politiet til å ta i bruk frekvenser tildelt andre dersom vilkårene for *identifisering* av kommunikasjonsanlegg er oppfylt. PST antar det ikke har vært departementets mening å utelate muligheten til å ta i bruk slike frekvenser for å *lokalisere* kommunikasjonsanlegg, jf. straffeprosessloven § 210 b annet ledd bokstav c. PST ber departementet rette dette i det videre lovarbeidet.

PST støtter forslaget om å utvide politiets adgang til bruk av frekvenser som er tildelt andre med det formål å uskadeliggjøre droner og andre gjenstander, dersom det er fare for liv, helse eller sikkerhet, jf. forslaget til endret § 11-13 første ledd, fordi dette er en viktig hjemmel i PSTs terrorforebyggende arbeid.

Selv om høringsnotatet ikke berører reguleringen av politiets rett til bruk av frekvenser ved bruk av tvangsmidler i § 11-13 første ledd første punktum, vil PST likevel be departementet vurdere å endre bestemmelsen. Dagens bestemmelse gir ulik tilgang til bruk av andres frekvenser i forebyggende arbeid, avvergende etterforskning og tradisjonell etterforskning. For tradisjonell etterforskning er politiets tilgang til å bruke andres frekvenser i *etterforskningsøyemed* i dag begrenset til enkelte spesifikke tvangsmidler. Den raske teknologiske utviklingen i samfunnet gjør at frekvensbruk vil bli aktuelt innenfor flere tvangsmidler, bl.a. dataavlesing, også i forbindelse med etterforskning. Ekomlovens regulering av frekvensbruk bør derfor utformes teknologinøytral og rustet for teknologisk utvikling slik at den ikke behøver å endres ved endringer i straffeprosessloven.

9. Forbud mot utstyr som er beregnet på å forstyrre elektronisk kommunikasjon («jammere»)

PST støtter lovforslaget om å forby befatning med jammere som beskrevet i ny lov § 13-2.

12. Krav om politiattest

PST er positiv til forslaget om å innføre rett for tilbyderne til å kreve fremlagt politiattest av personer som skal ha tilgang til informasjon, ekomnett, tilhørende fasiliteter, utstyr eller systemer av vesentlig betydning for sikkerheten i nett eller tjenester.

På bakgrunn av den verdi som tilbyderne forvalter og den betydning elektronisk kommunikasjon har for sentrale nasjonale interesser ber PST departementet vurdere om det bør innføres et lovkrav om at ansatte som skal svare ut

henvendelser fra politiet eller påtalemyndigheten, må være sikkerhetsklarert etter sikkerhetsloven.

Dersom departementet finner at sikkerhetsloven ikke kan anvendes, tiltrer PST forslaget fra KRIPOS med krav om innføring av uttømmende og utvidet politiattest, jf. politiregisterloven § 41, og at det også skal omfatte nummeruavhengig person-til-person-kommunikasjonstjenester. PST støtter også deres forslag om å utvide bestemmelsens nedslagsfelt til å omfatte personer som skal ha tilgang til informasjon, elektroniske kommunikasjonsnett, tilhørende fasiliteter, utstyr eller systemer med «vesentlig betydning for sikkerheten i nett eller tjenester *eller som av annen grunn er av særlig sensitiv karakter*».

PST støtter også KRIPOS sitt forslag om at det i merknadene til ny bestemmelse (ny lov § 3-9) gis nærmere anvisning på hva som kan eller skal vektlegges for at en person skal kunne anses uegnet og hva som eventuelt kan føre til betydelige skadevirkninger.

PST er dessuten enig i KRIPOS sitt forslag om at kravet om politiattest bør omfatte tilgang til politiattest utstedt i personens hjemland.

Roger Berg

Ass. Sjef PST

Dette dokumentet er elektronisk godkjent og har derfor ikke signatur