Forsvarsdepartementet

12. februar 2019

Høringsinnspill til lov om Etterretningstjenesten

Tekna viser til Forsvarsdepartementets høring om forslag til ny lov om Etterretningstjenesten, og takker for anledningen til å komme med innspill.

Tekna er Norges største fagforening for arbeidstakere med mastergrad innen teknologi, realfag og naturvitenskap. Vi er den største medlemsforeningen i Akademikerne og organiserer 77 000 medlemmer som jobber for å løse samfunnets utfordringer gjennom innovasjon og ny teknologi.

Vi svarer på høringen som oppfølging av vårt innspill til Lysne II-rapporten om digitalt grenseforsvar, som i forslaget til ny lov om Etterretningstjenesten er kalt «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon». Vårt innspill tar et etisk og IKT-faglig utgangspunkt.

Sammendrag

Tekna ser det som udelt positivt at departementet reviderer lov om etterretningstjenesten og gir tydeligere rammer for etterretningstjenestens virksomhet.

Tekna mener at forslaget om «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon» vil ha nytteverdi for etterretningstjenesten. Samtidig vurderer vi det som ressurskrevende å implementere, drifte og videreutvikle et slikt system, og vi ser det som usikkert om nytteverdien vil stå i samsvar med de faktiske kostnadene. Vi er bekymret for tilgangen på kompetanse, sikkerhetsrisikoen ved et slikt system og potensielle negative effekter for norske nettbaserte tjenester og produkter. Vi er også bekymret over de etiske sidene ved forslaget, inkludert personvernimplikasjoner, nedkjølingseffekt, mulig formålsutglidning, hva et slikt verktøy kan brukes til i feil hender, og risiko for svekket tillit til myndighetene.

Tekna kan derfor ikke støtte forslaget om «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon».

Hvis lovutkastet skulle vedtas, mener Tekna at det er særdeles viktig å gi EOS-utvalget tilstrekkelige ressurser til å følge opp sin tilsynsrolle. Vi vil også oppfordre til at loven og alle

systemer som etableres blir gjennomgått og evaluert grundig, med tanke på om de fungerer etter hensikten og er tilstrekkelig tilpasset den teknologiske utviklingen.

En nærmere gjennomgang av Teknas synspunkter følger nedenfor.

Innledning

Tekna er udelt positiv til at departementet reviderer lov om etterretningstjenesten, siden dagens lov er kortfattet og meget generell i sin utforming. Lovutkastet har inkorporert en rekke forhold som ikke er regulert i dagens lov, med lovfesting av både metodebruk og kontroll. Tekna mener at dette vil gi klarere rammer for etterretningstjenestens virksomhet og bidra til mer åpenhet om disse rammene. Den økte demokratiske styring og kontroll som lovutkastet legger opp til, kan bidra til å opprettholde etterretningstjenestens legitimitet og tillit i befolkningen, og styrke etterretnings-tjenestens evne til å ivareta sin samfunnsrolle.

En slik økt grad av lovregulering vil også gi tydeligere rammer, større forutsigbarhet og rettslig trygghet for de ansatte i etterretningstjenesten.

Tekna ser det som naturlig og riktig at lovforslaget adresserer elektronisk/digital etterretning.
Vi mener det er viktig at etterretningstjenesten gis gode verktøy for å oppfylle sitt mandat og sin samfunnsoppgave.

Lovforslaget legger imidlertid opp til en markant, inngripende utvidelse av tilgjengelig metodebruk gjennom kapittel 7 om «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon».

Tekna vil presisere at forslaget teknisk sett gir anledning til å lagre metadata om store deler av det norske folks elektroniske kommunikasjon, eksempelvis e-post, telefonsamtaler, sms-er, meldinger på sosiale medier, webmail, skytjenester for lagring av dokumenter, internett-tilkoblede gjenstander som smart-klokker etc. Slike informasjonsstrømmer vil i praksis ofte krysse grensen. Selv når avsender og eventuelle mottakere sitter i Norge, vil dermed informasjonen bli «innhentet» av etterretningstjenesten. Som poengtert i høringsnotatets punkt 11.13.8.3, er det slik at «systemet for tilrettelagt innhenting vil lagre ikke ubetydelige mengder metadata om norsk-til-norsk kommunikasjon».

Forslaget om «tilrettelagt innhenting» har skapt debatt og motsetninger – også innad i Tekna. Tekna som forening skal fremme utvikling og bruk av teknologi som sikrer liv, helse miljø og verdier, og vi ser at den foreslåtte innhentingen vil gi etterretningstjenesten nyttig informasjon. Innhentingen kan gi informasjon med direkte etterretningsverdi, informasjon som danner grunnlag for ytterligere elektronisk (eller annen) innhenting, og informasjon som kan deles med partnere slik at «norsk etterretningstjeneste får tilsvarende opplysninger fra andre land» (høringsnotatets punkt 7.8).

Samtidig skal Tekna bevisstgjøre til etisk refleksjon. Vi mener at forslaget har flere problematiske sider, både etiske og teknologiske. I sum mener Tekna at de samfunnsmessige ulempene er så store at vi ikke kan stille oss bak det foreliggende lovforslaget.

Etiske betenkninger rundt tilrettelagt innhenting

Det er viktig for befolkningens tillit til etterretningstjenesten – og landets myndigheter i videre forstand – at det er en god balanse mellom nasjonale sikkerhetsbehov og individuelle rettigheter. Lovforslagets § 1-1 (Formål) spesifiserer nettopp at loven skal «bidra til å trygge tilliten til» etterretningstjenesten samt sikre at tjenestens virksomhet «utøves i samsvar med menneske-rettighetene og øvrige grunnleggende rettsprinsipper og verdier i et demokratisk samfunn».

Tekna mener at kapittel 7 ikke ivaretar hensynet til personvern og individuelle rettigheter i tilstrekkelig grad til å oppnå en slik balanse. Selv om informasjonen har verdi for etterretnings-tjenesten, mener vi at inngrepet i befolkningens rettigheter blir uforholdsmessig stort vurdert opp mot den samfunnsmessige nytteverdien. Etter vårt syn står lovforslaget i fare for å svekke, heller enn å styrke, tilliten til etterretningstjenesten og norske myndigheter.

Tekna stiller spørsmål ved om kapittel 7 er forenlig med etterretningstjenestens mandat og ansvars-område, altså utenlandsetterretning. Vi registrerer at kapittel 4 forbyr etterretningstjenesten å «rette» innhenting av informasjon mot norske personer og virksomheter. Ifølge punktene 8.4.3 og 8.6 i høringsnotatet anser ikke Forsvarsdepartementet innhentingsforbudet å gjelde med mindre etter-retningstjenesten har en «overvåkningshensikt» mot konkrete personer eller virksomheter, og mener derfor det bør være anledning til å «innhente» elektronisk kommunikasjon i stor skala. Denne argumentasjonen fremstår noe konstruert og løfter ikke opp det mer grunnleggende, prinsipielle spørsmålet: Bør etterretningstjenesten, som i utgangspunktet skal fokusere på utenlandske forhold, gis adgang til å innhente «ikke ubetydelige mengder metadata om norsk-til-norsk kommunikasjon», eller går tiltaket ut over det ansvarsområdet som etterretningstjenesten er satt til å forvalte?

Det finnes en utbredt oppfatning i samfunnet om at «innhentingen» vil innebære digital masseovervåkning av befolkningen, jf. blant annet Datatilsynets høringsuttalelse og den offentlige debatten. Vi registrerer høringsnotatets argumentasjon for hvorfor «innhentingen» ikke bør regnes som overvåkning, men vi mener at høringsnotatets og politiske myndigheters argumentasjon ikke inneholder gode nok refleksjoner, verken prinsipielt, etisk eller teknologisk, til å dempe den allmenne bekymring for at forslaget innebærer å bygge opp et overvåkingssystem.

Hvis det etableres en oppfatning i befolkningen om at alle overvåkes, kan resultatet bli en nedkjølingseffekt der innbyggerne vil begrense sine ytringer og sin oppførsel i det digitale rom. Dette kan bidra til å svekke demokratiske uttrykk og prosesser i samfunnet, og svekke befolkningens tillit til myndighetene generelt.

Tekna vil også peke på faren for formålsglidning. Det er positivt at lovforslagets § 4-4 setter forbud mot å drive oppgaver med politiformål, og at § 7-12 kun tillater utlevering av «overskuddsinformasjon» som gjelder terror som kan avverges, samt vern av andre grunnleggende nasjonale interesser. Men hvis et slikt system først blir en realitet, vil det fort oppstå økt politisk press om å ta i bruk allerede «innhentede» data til stadig nye formål, noe som kan uthule det individuelle rettsvernet. Det er også en risiko for at teknologisk utvikling som reduserer nytteverdien av «innhentingen» (omtalt lenger nede) kan gi økt politisk press. Resultatet kan bli mandat- og formålsglidning der det introduseres enda mer inngripende metoder for å kompensere for sikrere kommunikasjonsteknologi.

Det er også et moment at ytringsfrihet, pressefrihet og politisk frihet er under press i mange land, inkludert land i Europa. Vi kan ikke utelukke en lignende samfunnsutvikling i Norge i levetiden til et slikt system for «tilrettelagt innhenting». Hvis et fremtidig regime med mindre respekt for demokratiske prinsipper enn dagens får mulighet til å lempe på begrensningene og kontrollmekanismene, vil et allerede operativt system for «tilrettelagt innhenting» kunne bli et drømmeverktøy for overvåkning og kontroll av befolkningen.

I den sammenheng vil vi påpeke at det også i dag kan ha visse problematiske sider å videresende informasjon til utenlandske etterretningsaktører som følger andre rettsprinsipper enn i Norge, selv samarbeidspartnere i allierte land. Deling av informasjon kan øke faren for misbruk av data. Det kan også gjøre det vanskelig å sikre at alle lovutkastets bestemmelser etterleves, for eksempel lagringstid og formål.

Teknologiske betenkninger rundt tilrettelagt innhenting

Den tilrettelagte innhentingen, slik den er skissert i kapittel 7, kommer til å være ressurskrevende. Ifølge Aftenposten 5. februar antyder foreløpige (og usikre) tall fra forsvarsdepartementet at et system for tilrettelagt innhenting vil koste minst 850 millioner kroner. Tekna har ikke forutsetninger for å utarbeide egne kalkyler, men med tanke på systemets omfang og kompleksitet, er vi bekymret for at de reelle kostnadene kan komme til å bli langt høyere.

Tekna stiller også spørsmål ved hvor stort utbyttet vil være. Et viktig moment i så måte er de teknologiske utviklingstrendene: Elektronisk kommunikasjon blir stadig bedre sikret, blant annet ved hjelp av kryptering. Cisco/Gartner anslår at 60–80 % av internett-trafikk i 2019 vil være kryptert (Encrypted Traffic Analytics, Cisco 2019), og andelen er økende. Innføringen av lovforslaget kan tenkes å sette ytterligere fart på overgangen til sikrere elektronisk kommunikasjon i Norge. Vi viser til at «tilrettelagt innhenting» i første omgang dreier seg om metadata, og at metadata «har blitt stadig viktigere i etterretningsarbeidet», jf. høringsnotatets punkt 8.7. Kryptert kommunikasjon inneholder også metadata, for eksempel en avsenders IP-adresse eller hvilket domene en nettleser henter data fra. Metadata kan i mange tilfeller si mye om innholdet i kommunikasjonen og/eller personen som kommuniserer, for eksempel at en kvinne kommuniserer med en abortklinikk. Derfor har Den europeiske menneskerettsdomstol lagt til grunn at også innhenting av metadata er et inngrep i privatlivet, jf. høringsnotatets punkt 4.2.3. Tekna mener at

det vil ha en etterretningsverdi å lagre metadata, men at potensiell nytteverdi vil reduseres etter som stadig mer av kommunikasjonen blir kryptert og det bygges inn stadig flere nivåer av sikkerhet i kommunikasjonstjenestene. Profesjonelle aktører som ønsker å unngå etterretningstjenestens søkelys, vil sannsynligvis være i stand til å kommunisere på måter som legger igjen lite verdifull informasjon i metadata. Hvor stort det faktiske utbyttet dermed blir, kan ingen si sikkert. Vår vurdering, ut fra ordningens omfang og kompleksitet samt våre forventninger om kommende teknologiutvikling, er at systemet vil være ressurskrevende å implementere, drifte og videreutvikle, og at det er ganske usikkert om nytteverdien vil stå i samsvar med de faktiske kostnadene.

Tekna tar det for gitt at etterretningstjenesten ønsker å ta i bruk stordataanalyser og maskinlæring, også omtalt som kunstig intelligens. Vi vil påpeke at disse teknologiene fører med seg mange nye problemstillinger, både etiske og teknologiske. Å introdusere slike teknologier i et miljø som per definisjon har lav transparens, gjør det ekstra vanskelig å adressere og korrigere metodeproblemer og for eksempel skjevheter og innebygde fordommer i datasettene (bias). Noen eksempler på problemstillinger er: Hvilke treningsdata og valideringsdata skal brukes? Hvem skal gis tilgang til disse dataene for å kunne utvikle best mulige algoritmer og modeller? Hva er kravene til treff-sikkerhet/feilrate, og hvordan skal dette måles og korrigeres? Hva er kravene til etterprøvbarhet og begrunnelse av resultater?

Tekna vil også påpeke at innsamling og lagring av store datamengder i seg selv innebærer en forhøyet sikkerhetsrisiko. Det vil introduseres nye sårbarheter hos e-komleverandørene som må tilrettelegge for ukryptert innhenting av informasjon, i datatrafikken fra e-komleverandørene til etterretningstjenesten, og i etterretningstjenestens datalagre. Flere aktører vil være interessert i denne informasjonen. Via hacking eller fysisk tilgang kan informasjon komme på avveie, bli manipulert (for eksempel for å skape en feilaktig situasjonsforståelse) eller misbrukes på annen måte.

Tekna er bekymret for tilgangen på kompetanse. Domstolen som skal kontrollere innhenting, søk og lagring (jf. kapittel 8), tilsynsmyndighetene (EOS-utvalget, jf. § 7-11 m.fl.) og etterretningstjenesten trenger alle teknisk kompetanse på flere områder og nivåer, eksempelvis søk, analyse og IKT-sikkerhet. Det er avgjørende med riktig kompetanse og kapasitet ved etablering av systemet, videre-utvikling og drift. Slik kompetanse må være tilgjengelig fortløpende, over tid. Men vi vet at det er og forventes å være underskudd på slik kompetanse i Norge i lang tid, spesielt IKT-sikkerhets-kompetanse. Dette underbygges blant annet av Nasjonal strategi for digital sikkerhetskompetanse som ble lagt frem for to uker siden. Det er derfor grunn til å frykte at et slikt system for tilrettelagt innhenting vil møte på kompetanseutfordringer. Vi vil derfor understreke at det er viktig at norske myndigheter, både i forbindelse med denne loven og på generell basis, legger til rette for at det utdannes nok nordmenn med nødvendig digital kompetanse.

Kommentarer knyttet til spesifikke kapitler og paragrafer i lovforslaget

§ 7-2 pålegger alle tilbydere av elektroniske kommunikasjonsnett og -tjenester å tilrettelegge for «innhenting» av data. Dette gjelder ikke bare tilbydere etter e-komloven, men også alle «tilbydere

av internettbaserte kommunikasjons- og meldingstjenester». Det fremstår som uklart hvem og hvor mange dette omfatter, men det virker naturlig å forstå dette som at loven innfører en mer omfattende tilretteleggingsplikt enn hva Lysne II-utvalget anbefalte. Også bestemmelsen i punkt d om «link-kryptering eller lignende kryptering» virker å gå lenger enn Lysne II-utvalgets anbefalinger. Dette gjør loven mer inngripende overfor privatpersoner og virksomheter enn forutsatt av Lysne II-utvalget. I tillegg er vi bekymret for at en så omfattende tilretteleggingsplikt vil gjøre norske nettbaserte tjenester og produkter mindre attraktive for både norske og internasjonale kunder. Hvis lovutkastet skulle vedtas, ber Tekna om at omfanget av tilretteleggingsplikten reduseres.

§ 7-5 spesifiserer utvalg og filtrering som skal forhindre at det innhentes informasjon om kommunikasjon mellom nordmenn i Norge. I praksis anser vi det som urealistisk å få til en effektiv og treffende filtrering.

§ 7-7 omhandler metadata. Som nevnt over kan metadata si mye om innholdet i kommunikasjonen og/eller personen som kommuniserer. For øvrig er ikke metadata et entydig begrep, og vi merker oss at etterretningstjenesten selv får rett til å definere hva som kan lagres. Vi vil understreke at EOS-utvalget her har en viktig funksjon i å etterse at denne retten ikke misbrukes. Vi mener for øvrig at en lagringstid på 18 måneder fremstår som lang.

§ 7-8 spesifiserer at personsøk kan inkludere to ledd i kommunikasjonskjeden. Høringsnotatets punkt 11.14.6 referer til en amerikansk studie som estimerer at dette potensielt kan gi tilgang til metadata om 25 000 personer, mens departementet mener anslaget er altfor høyt. Vi vil oppfordre EOS-utvalget til å nøye vurdere omfanget av de søk som faktisk blir foretatt.

§ 7-9 omhandler innholdsdata, eksempelvis innholdet i en e-post. Lagring av innholdsdata krever forhåndsgodkjennelse av domstol. Retten kan ifølge § 8-4 gi tillatelse til målsøking (identifisering av nye etterretningsmål) i ett år og målrettet innhenting (søking etter informasjon om identifiserte etterretningsmål) i seks måneder. Personopplysninger for etterretningsformål er ifølge § 9-1 unntatt fra personopplysningsloven, og skal ifølge § 9-9 slettes «når de ikke lenger er nødvendige å behandle». Dette fremstår for oss langt på vei som en blankofullmakt til å lagre innhentede innholdsdata så lenge etterretningstjenesten selv ønsker. Igjen vil vi understreke at EOS-utvalget har en viktig funksjon i å etterse at etterretningstjenesten håndterer sine fullmakter forsvarlig.

§ 9-9 tillater at «rådata i bulk» (informasjon der etterretningsverdien ikke er vurdert av mennesker) kan lagres i så mye som 15 år før de må slettes – men at sjefen for etterretningstjenesten kan treffe beslutning om å utsette slettingen i fem år om gangen. Det gjøres også unntak for sletting for «historiske, statistiske eller vitenskapelige formål». For øvrig fremstår det lite tillitvekkende at data ikke må slettes endelig, men kun slik at det kreves «avansert teknisk gjenfinningsverktøy» for å rekonstruere de slettede dataene. Hvis lovutkastet skulle vedtas, ber vi om en innstramming av denne paragrafen.

Kapittel 8 om domstolskontroll er viktig som kontrolltiltak. Vi innser at det er nødvendig å holde rettsmøter bak lukkede dører, men vil bemerke at lukket rett med kun advokater som er spesielt klarert, potensielt kan svekke tilliten til kontrollregimet. Igjen må vi peke på at EOS-utvalget er viktig for å skape tillit til prosesser som i utgangspunktet mangler transparens.

Konklusjon

Tekna er positivt til at departementet reviderer lov om etterretningstjenesten og gir tydeligere rammer for etterretningstjenestens virksomhet. Vi mener at forslaget om «tilrettelagt innhenting» vil ha nytteverdi for etterretningstjenesten, men at forslaget har flere problematiske sider, både etiske og teknologiske. I sum mener Tekna at de samfunnsmessige ulempene er så store at vi ikke kan stille oss bak kapittel 7 i forslag til ny lov om Etterretningstjenesten.

Hvis lovutkastet skulle vedtas, mener Tekna at det er særdeles viktig å gi EOS-utvalget tilstrekkelige ressurser til å følge opp sin tilsynsrolle. Vi vil også oppfordre til at loven og alle systemer som etableres blir gjennomgått og evaluert grundig, med tanke på om de fungerer etter hensikten og er tilstrekkelig tilpasset den teknologiske utviklingen.

Med vennlig hilsen
Tekna –Teknisk-naturvitenskapelig forening

Line Henriette Holten
generalsekretær