Det kongelige forsvarsdepartement

Deres ref.: 2016/2773-5/FD II 4/SIH

Oslo, 12.02.2019

Forslag til ny lov om Etterretningstjenesten

Abelia svarer med dette på høring om Lov om Etterretningstjenesten datert 12.11.2018.

Abelia er NHOs landsforening for kunnskaps- og teknologibedrifter, vi har vel 2 100 medlemsbedrifter med omtrent 48 000 årsverk over hele landet. Abelia har medlemmer innenfor blant annet IKT, undervisning, forskning, konsulenttjenester, kreative virksomheter og interesseorganisasjoner

1.0 Innledning

Arbeidet med revisjonen av lov om Etterretningstjenesten er meget omfattende, og Abelia anerkjenner arbeidet som er gjort for å belyse relevante punkter.

Abelia representerer en stor bredde av næringslivet i Norge. En fellesnevner er at digitalisering, tillit, trygghet, forutsigbarhet og sikkerhet er vesentlig for deres virksomheter. Med dette som utgangspunkt vil vi nedenfor fremme hensyn som vi mener bør tas i arbeidet med Lov om Etterretningstjenesten.

Vi ser positivt på revisjonen av lov om Etterretningstjenesten. Tilliten i det norske samfunnet er avgjørende for både det offentliges virke, så vel som for private aktørers mulighet for utvikling og nyskaping. Abelia mener den økte graden av lovregulering av Etterretningstjenestens virksomhet bidrar til mer åpenhet rundt tjenestens formål, rammer og samfunnsoppdrag, og gir økt demokratisk styring og kontroll av virksomheten.

Vi er likevel kritiske til enkelte punkter i høringsbrevet og forslaget til ny lov. Dette gjelder særlig tema som berører det private næringsliv, og hvor ny lov kan medføre negative konsekvenser. Abelia vil kommentere punktene dette gjelder.

2.0 Særlige merknader knyttet til opprettelsen av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

Abelia vil understreke at vi i følgende merknader ikke tar stilling til hvorvidt det bør åpnes for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon som sådan, men har merknader knyttet til innrettingen slik den er forespeilet.

Abelias medlemmer og norsk næringsliv generelt er avhengig av tillit fra befolkningen, både i hvordan de selv opererer og i deres omgang med andre. Norske og utenlandske bedrifter er avhengige av å kunne svare for deres omgang med forbrukernes data og egen opptreden i samfunnet. Internasjonal tillitt til norske selskap er også avhengig av norsk regelverk om tilgang til data som disse forvalter.

For vide, eller uklare, plikter knyttet til informasjonsutveksling med nasjonale etterretningstjenester kunne føre til direkte negative konsekvenser for privat næringsliv i Norge, men også for deres muligheter til eksport av teknologi og tjenester. Kundene forventer at deres data forvaltes trygt, ansvarlig og ikke deles med andre. I de tilfeller hvor det deles med myndigheter, må dette være underlagt strenge, transparente og forutsigbare vilkår.

2.1 Teknisk innretting

Systemet som foreslås av Lysne II-utvalget, og som videreføres som løsning i ny lov om Etterretningstjenesten, består av tre forskjellige datasett som det kan gjøres søk i. Disse tre datasettene kalles korttidslageret, metadatalageret og lageret med spesifiserte innholdsdata.

2.1.1 Korttidslager

Korttidslageret er slik Abelia forstår det ment å lagre "snapshots", og inneholder all data sendt over et kortere tidsrom. Korttidslageret skal kun brukes for utvikling av filtreringsfunksjoner- og seleksjonsmetoder og teknisk vedlikehold, og aldri til søk for etterretningsformål. Lageret vil imidlertid være førende for hvilke data som samles inn i metadata- og innholdsdatalageret, samt inneholde store mengder personinformasjon. Håndteringen av dette lageret er derfor kritisk for både etterretningseffekten og effekten på samfunnet av den tilrettelagte innhentingen. Abelia vil understreke at det er av særlig viktighet at EOS-utvalget gis full oversikt over arbeid med korttidslageret, og følger opp dette.

Vi vil bemerke at det ikke er drøftet hvorvidt det skal tas i bruk maskinlæring eller predikative analyser, og hvilke utfordringer slik teknologibruk vil kunne ha i et kontrollperspektiv. Det bør derfor vurderes om det er mulig og hensiktsmessig at det stilles krav om domstolskjennelse eller lignende forutgående kontroll for innhenting av snapshots og behandlingen av denne dataen. Korttidslageret vil inneholde store mengder informasjon om norske borgere som ligger utenfor Etterretningstjenestens mandat, og risikoen for formålsutglidning syntes derfor å være til stede.

2.1.2 Metadatalageret

Metadatalageret inneholder metadata fra utvalgte protokoller knyttet til utvalgte kommunikasjonstjenester. Lovforslaget legger opp til at data i dette lageret skal slettes etter 18 måneder. Lageret kan åpnes for søk gjennom domstolskjennelse på individer eller modus, og søket kan gå inntil ett år dersom innhentingen gjelder målsøking, og seks måneder når innhentingen gjelder målrettet innhenting. Abelia stiller seg kritiske til tidsperioden søkene i realiteten vil få med tanke på historisk data. Selv om søkeperioden kun skal vare et år, vil det ved målsøking kunne innhentes data fra en periode på totalt to og et halvt år, da også historisk data fra 18 måneder tilbake i tid vil ligge lagret. Vi mener på bakgrunn av dette at lagervarigheten bør settes ned til 12 måneder, eller at målsøkingsperioden og perioden for målrettet innhenting bør begrenses ytterligere.

2.1.3 Innholdsdatalageret

Innholdsdatalageret inneholder både metadata og innholdsdata, og krever i motsetning til metadatalageret rettens kjennelse for at det skal startes lagring her. Abelia ser på dette som fornuftig, da innholdet i dette lageret potensielt vil være av en betydelig mer inngripende karakter enn metadata alene. Vi imidlertid vil bemerke at lovforslaget ikke inneholder eksplisitte regler for sletting av data som innhentes i dette lageret, slik det er foreslått i metadatalageret. Vi mener det bør legges føringer på dette i lov.

Departementet presiserer i høringsnotatet at innhenting og lagring av innholdsdata alltid vil være knyttet til *målrettet innhenting*. Det kommer imidlertid etter vårt syn ikke klart frem hvorfor dette er tilfellet. Slik vi leser forslaget foreligger det ingen eksplisitte regler som tilsier at Etterretningstjenesten ikke kan be retten om at det åpnes for lagring av innholdsdata for målsøking, basert på behov for mer informasjon i målsøknings- eller målutviklingsfasen. Vi mener dette bør presiseres i lov.

2.1.4 Deling av overskuddsinformasjon

Abelia støtter det generelle forbudet mot deling av overskuddsinformasjon, men er kritiske at det åpnes for deling under kapittel 17-18 i straffeloven. Av hensyn til bevisst og ubevisst formålsglidning vil et ubetinget forbud mot deling av overskuddsinformasjon være enklere å praktisere og kontrollere.

2.1.5 Bevisforbud

Abelia støtter bevisforbudet slik det fremkommer i §7-13, og har ingen merknader ut over dette.

2.2 Avgrensninger

2.2.1 Tilretteleggingsplikten

Abelia er svært kritiske til at Departementet her går mye lengre i sitt forslag enn Lysne II-utvalget gjorde, og mener det er avgjørende at tilretteleggingsplikten kun innebefatter tilbydere av fysisk infrastruktur for grenseoverskridende kommunikasjon. Høringsbrevet er etter vårt syn svært uklart både på hvem som vil underlegges tilretteleggingsplikten, og hva denne innebærer.

Departementets beskrivelser i 11.3 og 11.5 antyder at hensikten med formuleringen er et ønske om teknologinøytralitet, men at det i praksis vil gjelde tilrettelegging for søk i kommunikasjon som transporteres i fiberkabler. Under 11.15.2 fremlegges det derimot at "*Det vil i tillegg være behov for tilrettelegging fra tilbydere av innholdstjenester som ikke er omfattet av definisjonen i ekomloven, typisk internettbaserte «over the top-tjenester» (OTT-tjenester) som kan brukes til overføring av tekst, lyd og bilder*". Dette indikerer at tilretteleggingsplikten ikke kun er ment å ramme tilbydere av grenseoverskridende infrastruktur for kommunikasjon (fibereiere og tilbydere på feltet), men alle som tilbyr tjenester som går gjennom infrastrukturen i tillegg. Dette fremkommer også av lovforslaget gjennom inkluderingen av "*tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten*". Departementets nåværende forslag vil i realiteten innebære en tilretteleggingsplikt for store deler av privat næringsliv på området, og vil kunne ramme bedrifter og tjenester som for eksempel Facebook, mailtilbydere, Kahoot, tilbydere av elektroniske signatursystemer og andre. I praksis ser vi få begrensninger i utstrekning med foreslått formulering, og vil sterkt anbefale en omformulering med tydelige begrensninger her. Bekymringer rundt uklarhetene med tanke på utstrekning av plikten forsterkes av at det hverken er lagt opp til forutgående prosesser eller klagemuligheter for berørte bedrifter. Abelia anbefaler at det gis prøvingsrett for bedrifter som Etterretningstjenesten ønsker tilrettelegging fra.

Utfordringene knyttet til omfanget av tilretteleggingsplikten blir forsterket av at det til dels er uklart hva plikten faktisk innebærer. Departementet skriver i sin beskrivelse av lovforslaget i 11.15.3 *" Tilretteleggingsplikten skal derimot ikke innebære en plikt til å bidra til annen omgåelse av kryptering* [enn linkkryptering]*, og departementets forslag går dermed ikke lenger enn Lysne II-utvalgets anbefaling."* Samtidig er lovforslaget mer generelt, og sier *"linkkryptering eller lignende kryptering som tilbyder kontrollerer".* Dette må etter vårt syn sees i sammenheng med forklaringen i 11.15.2 som referert over rundt tilbydere av OTT-tjenester, og presiseringen av at *"Det vil for eksempel kunne være behov for å sørge for tilgang til kommunikasjon uten hinder av kryptering som tjenestetilbyderen kontrollerer."* Hvorvidt lovforslaget slik det er formulert og med denne forklaring åpner for en tilretteleggingsplikt hvor tilbydere

for eksempel pliktes å stille med bakdørsløsninger som gir Etterretningstjenesten full tilgang er uklart. Lysne II-utvalget var tydelige i sin anbefaling på at dette kun skulle gjelde kryptering på lag 2, eller linkkryptering, og vi er svært kritiske til en tilretteleggingsplikt som går lengre enn dette. Den kan henvises til diskusjoner i USA og andre land, og myndighetenes ønske om tilgang på bakdører og lignende i krypterte enheter eller programvare. Utfordringen med denne typen løsninger er at det ikke er fysisk mulig å gi Etterretningstjenesten muligheter til å omgå kryptering, uten å samtidig åpne denne bakdøren for andre. Samtidig er det ikke gitt at for eksempel en innholdsleverandør underlagt tilretteleggingsplikten i det hele tatt har kontroll over krypteringen selv, da de gjerne kan ha kjøpt denne løsningen av en tredjepart. Oppsummert vil derfor en tilretteleggingsplikt for omgåelse av annen kryptering enn linkkryptering være både urimelig, kunne bryte med internasjonale standarder og i mange tilfeller være ikke være praktisk mulig å imøtekomme. Abelia mener derfor ordlyden bør endres til kun å omfatte linkkryptering.

2.2.2 Kostnader ved tilretteleggingsplikten

Abelia ser det som kritisk for at innføringen av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon ikke skal få en utilsiktet konkurransemessig effekt og at utgifter selskapene har dekkes av staten. Effekten av ny etterretningslov er krevende for næringslivet å forutse, blant annet fordi pliktene virksomhetene vil omfattes av er utydelige. Abelia vil understreke viktigheten av at privat næringsliv får kompensert både direkte og indirekte kostnader de måtte ha som følge av tilretteleggingsplikten, herunder utgifter knyttet til personell og fysiske lokaler som stilles til disposisjon for Etterretningstjenestens arbeid. Dette kan innebære lønnskostnader, kostnader til husleie, strøm og annen infrastruktur, i tillegg til utgifter direkte knyttet til innkjøp eller omlegging av utstyr. Vi legger til grunn at tilbydere og andre som får kostnader som følge av tilrettelegging, får disse dekket.

Vi ønsker å påpeke at det vil være svært uheldig dersom praktiseringen av lovverket skulle få utilsiktede, uheldige og unødvendig fordyrende konsekvenser for næringslivet. Abelia forutsetter at konsekvenser for næringslivet, næringslivets kostnader og innovasjonsevne blir førende for det videre arbeidet med forskriftene, og effektueringen av disse. Vi etterlyser også en tydeligere ansvarsklargjøring i tilretteleggingsplikten. Det er for eksempel ikke presisert hvem som har ansvaret eller hva som gjøres dersom et av grensesnittene mellom tilbyder og Etterretningstjenestens systemer skulle svikte eller lekke informasjon, eller dersom bedrifter opplever nedetid på sine tjenester som følge av tilretteleggingsplikten. Abelia ser det som kritisk at Etterretningstjenesten påtar seg juridisk og økonomisk ansvar for systemene som implementeres.

2.3 Kontroll

Abelia vil understreke viktigheten av domstolskontrollordningen skissert i lovforslaget, og mener det bør sikres at dommere og advokater som involverer har eller kan få nødvendig kompetanse til å foreta reell prøving, men har for øvrig ikke andre merknader til dette punktet.

Abelia stiller seg bak utvidelsen av EOS-utvalgets mandat til styrket kontroll med tilrettelagt innhenting, og ønsker å understreke at en slik utvidelse fordrer en betydelig styrking av utvalgets menneskelige ressurser og tekniske kompetanse. I flere av EMD-dommene på tilsvarende systemer i andre land er demokratisk kontroll pekt på som avgjørende i vurderingen av lovligheten til systemet, og det vil derfor være kritisk at EOS-utvalget får mulighet til å føre reell kontroll. Vi har ingen kjennskap til hvilke tekniske verktøy EOS-utvalget benytter i sitt arbeid i dag, men vil påpeke viktigheten av at det også kan være behov oppgradering av disse. EOS-utvalgets mandat og sammensetning bør også vurderes helhetlig, i lys av utvidelsen av utvalgets oppgaver.

2.4 Evaluering

Abelia mener forslaget om opprettelsen av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon slik det er fremlagt inneholder ubesvarte spørsmål, knyttet til personvernshensyn, kommunikasjonsvernshensyn, kostnader og andre utfordringer for næringslivet. Det kan også stilles spørsmålstegn ved den etterretningsmessige gevinsten. Vi mener derfor at dersom Stortinget vedtar en åpning for innhenting av grenseoverskridende elektronisk kommunikasjon, må det gjøres grundige evalueringer av disse problemstillingene i etterkant av opprettelsen. Vi anbefaler at man gjennom EOS-utvalget eller et eget utvalg vedtar et særskilt mandat for evaluering av ordningen, med mål om at det legges frem en ugradert rapport til offentligheten på dette. Den betydelige usikkerheten knyttet til konsekvensene av denne innføringen gjør at vi mener det bør gjennomføres en evaluering innen minst ett, maksimalt tre, år etter ikrafttredelsen. Vi mener også at det bør settes av midler til forskning på eventuell nedkjølingseffekt i samfunnet under evalueringsperioden, for å få et bedre bilde av de bredere samfunnsmessige konsekvensene. Blant annet Datatilsynet har i sitt høringssvar fremhevet de betydelige negative effektene en eventuell nedkjølingseffekt vil ha på samfunnet. Dersom Norge skal kunne møte fremtidens utfordringer er vi avhengige av at befolkningen har tillit til teknologi og teknologiske løsninger, og ikke føler bekymring for å delta i samfunnet og samfunnsdebatten.

2.5 Stoppfunksjoner

Både som sikkerhet for en eventuell ikke-demokratisk maktovertakelse, og som resultat av demokratisk ønske om stopp etter en evaluering, er det avgjørende at det finnes raske metoder for å avvikle systemet med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Dette syntes mangelfullt utredet i høringsnotatet, og Abelia mener det bør legges føringer i lov og forskrift som behandler avvikling.

3.0 Generelle merknader

3.1 Sikkerhetsklarering

Ny lov om Etterretningstjenesten vil i kombinasjon med ny sikkerhetslov og annet arbeid utvilsomt føre til en utvidelse av behovet for mennesker med sikkerhetsklareringer. Både militært og sivilt personell som dommere, advokater og andre må klareres. I EOS-utvalgets årsmelding for 2017 viser utvalget til at de i de seks foregående årsmeldinger har påpekt at saksbehandlingstiden i klareringssaker er altfor lang. Dette gjelder både anmodning om klarering, anmodning om innsyn, klage 1. instans og klage 2. instans. Det er kritikkverdig at kontrollorganet skal måtte påpeke dette over så lang tid, uten at det gjøres nødvendige grep. Abelia mener både personell- og systemkapasiteten til behandling av sikkerhetsklareringer bør utbedres umiddelbart.

Vi ber om at departementet, gjennom sitt arbeid med høringen og omkringliggende aktivitet, sikrer forutsigbarhet, økt transparens i vurderingskriterier og betydelig kortere saksbehandlingstider. Ventetiden på overføring av sikkerhetsklarering fra land Norge samarbeider med bør også være så kort som mulig.

3.2 Kompetanse

Abelia har i flere år påpekt behovet for økt IT-kompetanse generelt i Norge, og økt IT-sikkerhetskompetanse spesielt. Flere rapporter, deriblant Lysne-utvalgets rapport belyser kompetansebehov på sikkerhetsområdet. Vi vil igjen benytte anledningen til å understreke hvor avgjørende det er at vi i Norge evner å heve IT-kompetansen generelt og sikkerhetskompetansen spesielt i samfunnet. Med et relativt lavt antall personer med IT-sikkerhetskompetanse blir vi sårbare som nasjon. Innføringen av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon skaper ytterligere press på IKT-sikkerhetskompetanse, og tiltak for å avlaste dette presset bør prioriteres. Abelia bemerker at regjeringens egen strategi for digital sikkerhet fremhever kompetanse som en utfordring, og forventer at denne blir fulgt opp med konkrete virkemidler. Privat næringsliv etterspør mye av den samme kompetansen som Etterretningstjenesten og kontrollorganer vil ha behov for, og det oppleves sterk konkurranse om de kloke hodene. Abelia mener det er uheldig dersom staten opptrer som lønnsdriver på etterspurt kompetanse, og mener det i større grad må tas høyde for behovet for menneskelige ressurser i statens arbeid med IT-sikkerhet.

3.3 Samarbeid mellom offentlig og privat sektor

Koordinerte ondsinnede angrep, gjerne med internasjonalt opphav blir stadig mer vanlig. Skillet mellom hva som er et angrep mot det norske samfunnet og hva som er et angrep mot enkeltvirksomheter kan være uklart. Angrep kan utføres på tvers av sektorer og konsekvensene kan ramme bredt.

Næringslivet generelt, og IKT-sektoren spesielt, er helt avhengig av støtte fra norske myndigheter i form av løpende informasjonsutveksling for å kunne eliminere eller begrense skadevirkninger i samfunnet. Mange bedrifter, særlig de små- og mellomstore, faller i dag utenfor de eksisterende sektorbaserte ordningene for varsling og håndtering av IKT-hendelser. Abelia mener utveksling av trusselvurderinger og annen sikkerhetsinformasjon må styrkes. Oslo Economics vurderte, i sin rapport om anbefalingene fra IKT-sikkerhetsutvalget, at tilgang på etterretningsinformasjon vil har stor samfunnsøkonomisk betydning. Det er i stor grad private aktører som eier, utvikler og opererer infrastrukturen for håndtering av angrep, og partnerskap på dette feltet er essensielt. Det er viktig at relevante aktører blir informert slik at alvorlige hendelser ikke får et større omfang enn nødvendig på grunn av manglende vilje eller evne fra myndighetene til å dele informasjon.

Abelia vil avslutte med å takke for muligheten til å komme med innspill.

På vegne av Abelia,

Kjetil Thorvik Brun (sign.)

Leder teknologi og digitalisering

Mikal Kvamsdal

Næringspolitisk rådgiver, teknologi og digitalisering