DEN NORSKE DATAFORENING

Den norske dataforening - IT-politisk råd

6. februar 2019

Forsvarsdepartementet
Via departementets høringsportal

Høringssvar - ny lov om Etterretningstjenesten

Den norske dataforening - IT-politisk råd (DND) viser til Forsvarsdepartementets høring av 21. november 2018 med forslag til ny lov om Etterretningstjenesten.

Som følge av lovforslagets omfang og kompleksitet, og den relativt korte høringsfristen, er det begrenset hvilke tema vi har hatt mulighet til å gå inn på i detalj. Hoveddelen av høringssvaret fokuserer på nødvendigheten av automatisert behandling av data i bulk, kontroll med Etterretningstjenestens metodebruk, og de foreslåtte reglene om tilretteleggingsplikt for tilbydere av kommunikasjonstjenester. Vi vil også vise til enkelte andre områder hvor vi anser at ytterligere presiseringer er nødvendige.

Deler av høringsutkastet er utarbeidet i samarbeid med Elektronisk Forpost Norge, som vil avgi egen høringsuttalelse.

1. Generelt

DND er enige i at det er behov for en oppdatert og mer informativ lov om Etterretningstjenesten. Gjennom Grunnloven § 102, det alminnelige legalitetsprinsippet og Den europeiske menneskerettskonvensjon artikkel 8 er Norge forpliktet til å ha klare, forutsigbare og tilgjengelige lovregler for myndighetenes inngrep i den enkeltes rett til privatliv.

Den gjeldende loven er svært overordnet, og bærer preg av å være en rammelovgivning. Deler av den praksis som beskrives i høringsnotatet, og i EOS-utvalgets særskilte melding om rettsgrunnlaget for Etterretningstjenestens overvåkningsvirksomhet, slik vi ser det, tangerer grensen av hva gjeldende lovgivning tillater. En slik utvikling er naturlig når loven over tid har blitt tolket og praktisert i hemmelighet. Uten offentlig debatt og innsyn i *praktiseringen* av ny lov, er det sannsynlig at også denne over tid vil bli tolket utvidende - gjerne langt utover hva som var lovgivers intensjon. Det er derfor særlig viktig at den nye loven blir presis, og at lovgiver har et bevisst forhold til konsekvensene av de fullmakter som gis til Etterretningstjenesten.

Deler av forslaget bygger på et skille mellom kommunikasjon som krysser norske grenser, og kommunikasjon som fullt og helt foregår i Norge. En slik distinksjon er meningsløs når kommunikasjonen foregår over internett, siden alt fra hjemmelekser til kommunikasjon med forvaltningen i dag rutinemessig tar en sving innom minst ett datasenter eller en ruter plassert utenfor landets grenser. I realiteten vil bortimot all elektronisk kommunikasjon i dag passere landegrensen, enten på grunn av ruting, fordi en bruker en skytjeneste e.l., eller fordi programmene en bruker har interne moduler som lenker mot data utenfor landegrensen.

DEN NORSKE DATAFORENING
Adresse: Møllergaten 24, 0179 Oslo
Telefon: 22 36 48 80
E-post: post@dataforeningen.no
Web: www.dataforeningen.no
Org.nr. NO 871549842 MVA
Bankgiro: 6069.05.18964

2. Aksess til, og behandling av, elektronisk data i bulk

a. Tilrettelegging for aksess

Lysne II-utvalget foreslo aksess til datastrømmen i fiberne som krysser landegrensen, før kryptering på link-laget foretas. I det foreliggende forslaget er tilretteleggingsplikten gjort helt generell og omfatter alle tilbydere av elektroniske kommunikasjonstjenester. Fra å være begrenset til de fysiske kabler som krysser norske grenser beskriver man nå et "sugerør" inn i det norske kjernenett og til potensielt alle tjenesteleverandører. Forslaget kan forstås som at Etterretningstjenesten skal gis tilnærmet fri tilgang til tilbydernes systemer. Forslaget vedrørende "tilrettelagt innhenting" fremstår derfor som vesentlig mer omfattende enn det som ble drøftet og anbefalt i Lysne II-utvalgets rapport.

Forslaget strekker seg også lenger enn hva en finner i Sverige, hvor kun fiber*eiere* berøres av FRA-loven.

b. Kryptering

Krypteringsdebatten fra 1990 tallet har kommet tilbake de siste årene. Sikkerhets- og etterretningstjenester ønsker tilgang uhindret av kryptering. Samtidig er sterk kryptering helt avgjørende for sikkerheten og tilliten til internett som transport for kommunikasjon. Det tok flere år å bygge opp denne tilliten via utvikling av gode produkter for kryptering som måtte sikre den konfidensialitet som må være på plass for å nytte internett kommersielt. Temaet er komplekst og vanskelig.

Vi finner det derfor oppsiktsvekkende at norske myndigheter etter et par siders drøftelse i forslagets punkt 11.15 foreslår å gi tilbyderne av kommunikasjonstjenester en slik vidtgående plikt til å åpne en bakdør for omgåelse av kryptering.

Selve lovhjemmelen for dette er § 7-2, hvor man i bokstav d pålegger tilbyder å

> **"***sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering som tilbyder kontrollerer***"**.

Ved at man i kommentarene setter likhetstegn mellom linkkryptering og *all annen kryptering som tilbyder kontrollerer,* skapes det en stor usikkerhet om hva som er ment. Om forslaget skulle gå igjennom i den form det har nå vil det være et stort feilgrep.

Lovforslaget må presiseres slik at det er klarere hva Etterretningstjenesten gis aksess til.

c. Automatiserte søk og behandling av data i bulk

Bearbeiding av slike datamengder som beskrives i forslaget kan ikke gjøres manuelt. For å tilrettelegge for søk i slike ustrukturerte datamengder som bulkinnsamling gir, bruker man automatiserte teknikker, som kan være ulike former for maskinlæring, automatiserte analyser og "mining" av data. Riktignok er "big data" som begrep blitt noe av en klisje, men med "tilrettelagt innhenting" vil det være tale om virkelig store datamengder blant annet om enkeltpersoners kommunikasjon. Den teknologiske utviklingen for bearbeidelse av store datamengder går fort, og det er liten grunn til å tro at ikke Etterretningstjenesten vil nyttiggjøre seg av den til enhver tid tilgjengelige teknologien som foreligger.

Bruk av automatiserte teknikker er ikke i seg selv galt. Bruk av teknologien reiser imidlertid en rekke prinsipielle og etiske spørsmål, som ikke er belyst i høringsnotatet. Prediktive analyser er et kontroversielt eksempel på dette.

Fra et kontrollperspektiv vil en løsning som tar i bruk slik automatisering og maskinlæring skille seg vesentlig fra et regime hvor søk og analyse gjøres manuelt. Dette problematiseres ikke i høringsnotatet.

d. Korttidslageret

Innhenting av data i bulk vil gi store datamengder selv når det samles inn i korte tidsintervaller. DND anser at korttidslageret er en nødvendig forutsetning for effektiv bulkinnsamling, men at slik lagring *i seg selv* utgjør et betydelig inngrep i retten til privatliv.

e. Metadatalageret

Begrepet "metadata" som brukt i høringsnotatet, er omfattende, og kan kategoriseres som alt som er avledet av innhold. Begrepet metadata i denne konteksten er teknologisk riktig, men representerer noe annet enn når samme begrepet har blitt brukt om for eksempel trafikkdata fra telekommunikasjon. Mengden og typene metadata innhentet ved tilrettelagt innhenting vil langt overgå hva det var tale om å pålegge lagret gjennom datalagringsdirektivet. Som kjent konkluderte konkluderte EU-domstolen i Luxembourg i 2014 at direktivet strider mot forholdsmessighetsprinsippet i europeisk rett og dermed er ugyldig. Konklusjonen var at «direktivet innebærer et meget omfattende og særlig alvorlig inngrep i den grunnleggende rett til respekt for privatlivet og til beskyttelse av personopplysninger, uten at dette inngrepet er begrenset til det strengt nødvendige»

Et søk kan hente ut 15 måneders livshistorie for målet for etterretningsvirksomheten og "to ledd ut" i vedkommendes kommunikasjon. Dette har i liten grad vært diskutert i den offentlige debatten.

3. Kontroll med Etterretningstjenestens metodebruk

Lysne II-utvalget foreslo et kontrollregime langs tre akser, med et tilsyn for løpende kontroll med DGF, etterfølgende kontroll fra EOS-utvalget og domstolskontroll som innehar "etterretningsfaglig kompetanse, teknisk og operativ innsikt i tjenestens virksomhet samt i overordnede myndigheters styrings- og prioriteringsvirksomhet".

Departementet foreslår at domstolskontrollen legges til de ordinære domstoler ved Oslo tingrett, og at det i stedet for et eget tilsyn pålegges EOS-utvalget å føre skjerpet kontroll med tilrettelagt innhenting. Departementet "vurderer at disse endringene styrker ordningen", står det på side 210 i høringsnotatet.

a. Domstolskontroll

Domstolskontrollen i den foreslåtte form vil neppe innebære reell kontroll med Etterretningstjenestens bruk av data fra tilrettelagt innhenting. Dette fordi det vil være nødvendig med betydelig teknisk dybdekunnskap og innsikt for å gjøre en reell vurdering av om vilkårene i loven er oppfylt for søk i de lagrede metadata. Særlig gjelder dette for forholdsmessighetsvurderingen, hvor det er nødvendig å forstå teknikken for å kunne vurdere hvor inngripende et gitt søk er.

Det er heller ikke lagt opp til at domstolen skal få tilgang til slik kompetanse fra andre enn Etterretningstjenesten selv. En ordning med offentlig oppnevnt advokat kan ikke reparere dette, da advokaten - som ikke kan konferere med noen - etter all sannsynlighet vil ha like dårlige forutsetninger for å utfordre Etterretningstjenesten på det tekniske området som domstolen selv.

Domstolskontrollen må derfor styrkes ved at domstolen får tilgang til uavhengig teknisk kompetanse, for eksempel ved at det oppnevnes fagkyndige meddommere når begjæringen fra Etterretningstjenesten skal vurderes.

b. EOS-utvalgets kapasitet

Stortingets Evalueringsutvalg for EOS-tjenesten skriver i sin rapport, side 127 til at

> *Det er imidlertid på det rene at utvalgsmodellen, og det faktum at utvalgsmedlemmene innehar verv som i utgangspunktet skal ivaretas ved siden av fulltids arbeid, begrenser EOS-utvalgets kapasitet og dermed omfanget av kontrollvirksomheten. Særlig for de av medlemmene som har fulltidsstillinger i tillegg til dette vervet, oppleves det som krevende å sette av tilstrekkelig tid. Utvalget har videre opplyst at det ofte opplever tidspress på inspeksjonene og i møtevirksomheten, og gjerne skulle hatt mer tid både til interne drøftelser og til å ta opp saker av eget tiltak.*

Samme rapport, side 162

> *Det er likevel viktig at både omverdenen og EOS-tjenestene kan stole på at det er EOS-utvalget som står for den reelle kontrollen av tjenestenes virksomhet, og ikke utvalgets sekretariat. En forutsetning om dette ligger til grunn for utvalgsmodellen som sådan, dets parlamentariske forankring og sammensetning. EOS-utvalgets eksistens hviler på en forutsetning om at utvalgets avgjørelser skal fattes av utvalgsmedlemmene i fellesskap, og være uavhengige og selvstendige resultater av en kritisk diskusjon av de funn utvalget og sekretariatet har gjort i undersøkelsen av en sak. Selv om sekretariatet besitter særlig faglig ekspertise og kontinuitet, har EOS-utvalgets medlemmer et særlig ansvar for å kontrollere at sakene er tilstrekkelig utredet. Det er utvalget som har det endelige ansvaret for avgjørelsenes innhold og eventuell kritikk som rettes mot EOS-tjenestene.*

Vi ser ikke at EOS-utvalget *som sådan* har kapasitet til å føre en skjerpet kontroll med tilrettelagt innhenting i tillegg til sine eksisterende oppgaver. Evalueringsutvalget foreslo blant annet, av kapasitetshensyn, at EOS-utvalget ikke lenger skulle føre kontroll med sikkerhetsklareringssaker. Dette forslaget ble ikke fulgt opp i Stortinget, slik at kapasitetsutfordringene må antas å være minst like store i dag som da rapporten ble utgitt, og med de forslag som fremmes i lovutkastet vil disse utfordringene antagelig øke i betydelig grad.

c. EOS-utvalgets arbeidsform og rapportering

Departementet er i høringsnotatet inne på at EOS-utvalgets organisering som et organ under Stortinget legger en del føringer for hvordan kontrollen kan gjennomføres. Vi er særlig opptatt av tidsaspektet og av utvalgets myndighet. Det er liten tvil om at EOS-utvalget har gjort grundig arbeid innenfor de gitte rammene. Dersom forvaltningen er uenig i EOS-utvalgets konklusjoner, er prosessen før en endelig avklaring i Stortinget potensielt svært tidkrevende. Dette kan være akseptabelt for områder som EOS-utvalget fører kontroll med i dag, men vil ikke være akseptabelt for et tiltak hvor feil og ulovligheter kan ha så store konsekvenser som ved tilrettelagt innhenting.

d. Kontroll med valget av aksesser

Tilretteleggingsplikten i forslaget er utformet generelt, og vil i prinsippet være gjeldende til enhver tid, jf § 7-2. Dette er til forskjell fra situasjonen i en rekke andre land som har innført bulkaksess, hvor det kreves en beslutning fra politisk hold hver gang det skal etableres en ny

aksess. I angloamerikanske land omtales dette gjerne som en “warrant” fra ansvarlig statsråd.

DND finner det underlig at man i forslaget legger opp til at Etterretningstjenesten fritt kan velge aksesser, uten at for eksempel Forsvarsdepartementet fatter en beslutning i hvert enkelt tilfelle. Slik forslaget er utformet kan man som tilbyder risikere å få e-tjenesten “på døren”, og plikter da å yte omfattende tilrettelegging uten at dette er omfattet av noen forhåndskontroll.

Slik DND ser det vil det være påkrevet at man i det endelige forslaget omarbeider § 7-2 slik at tilretteleggingsplikten er avhengig av en beslutning rettet mot den aktuelle tilbyder. En slik beslutning bør fattes minst ett nivå over Etterretningstjenesten, slik det gjøres i de land det er naturlig å sammenligne seg med.

e. Overgangen mellom tilbyders og Etterretningstjenestens ansvar

Tilbydere av elektroniske kommunikasjonsnett og tjenester er underlagt omfattende forpliktelser til å sikre sine tjenester, og å tilby disse med forsvarlig sikkerhet, jf. ekomloven § 2-10. I en del tilfeller vil også sikkerhetslovens bestemmelser komme til anvendelse.

DND stiller spørsmål ved om grensedragningene mellom tilbyders ansvar for sikkerheten, og Etterretningstjenestens plikt til å sikre konfidensialitet, er tilstrekkelig avklart i forslaget. Tilbyder vil etter forslaget være forpliktet til å gi tjenestens personell adgang til de mest sensitive deler av sin infrastruktur, og være forpliktet til å tåle at det settes opp “fremmed” utstyr i dennes lokasjoner. Tjenestens personell skal kunne komme og gå, og tilbyder er forpliktet til å bidra til at dette kan skje fordekt. For DND virker det som slik aktivitet kan utfordre et etablert sikkerhetsregime med adgangs- og tilgangskontroll.

Et annet spørsmål er hvem som har ansvaret dersom et av grensesnittene mellom tilbyders og Etterretningstjenestens systemer skulle lekke informasjon til en tredjepart. Slike situasjoner er ikke helt ukjente, blant annet har det vært flere mediesaker om at lovlig avlyttingsutstyr plassert hos tilbyder har lekket informasjon til fremmed etterretning.

DND anbefaler at denne grensedragningen gås opp tydeligere i et eventuelt endelig lovforslag.

4. Andre tema

a. Skjerming - forslagets § 11-5

DND har forståelse for at Etterretningstjenesten må fatte tiltak for å skjerme sine operasjoner. DND stiller imidlertid spørsmål ved rekkevidden for forslaget § 11-5, hvor det blant annet fremgår at det “kan (...) tas kontroll over, modifiseres eller utplasseres elektronisk utstyr, for å hemmeligholde og gjennomføre Etterretningstjenestens operasjoner.”

En slik adgang kan være nødvendig, men kan også være farlig. Slik DND ser det er det helt nødvendig at et eventuelt endelig lovforslag er mer detaljert på dette området. Skal Etterretningstjenesten for eksempel ha adgang til å gjøre datainnbrudd for å slette skjermingsverdig informasjon som har kommet på avveie? Gjeldende ordlyd kan synes å åpne for det, men en slik praksis vil være betenkelig i et demokratisk samfunn.

b. Behandling av personopplysninger

DND vurderer det som positivt at det gis egne regler om behandling av personopplysninger for Etterretningstjenesten. Det fremstår imidlertid som uheldig at det skal gjelde en annen definisjon av hva som er personopplysninger for Etterretningstjenesten enn i samfunnet for øvrig. Å operere med avvikende definisjoner av sentrale begreper er rettsteknisk uheldig, og det bør være meget gode grunner for å gjøre dette. Så vidt vi kan se er dette ikke grunngitt i høringsnotatet.

Den norske dataforening v/ IT-politisk Råd

Arve Føyen