Stiftelsen SINTEF
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Besøksadresse:
Strindvegen 4
7034 Trondheim

Sentralbord: 40005100
Direkte innvalg: 918 06 193

info@sintef.no

Foretaksregister: NO 948 007 029

Forsvarsdepartementet
Postboks 8126 Dep.
0032 Oslo

Deres ref.:	Vår ref.:	Prosjekt / Sak:	Dato
2016/2773-5/FD II 4/SIH	ABG/akg		2019-02-18

Høringsuttalelse fra SINTEF vedrørende forslag til ny lov om Etterretningstjenesten

Som en sentral bidragsyter innen forskning på digitale teknologier og IKT-sikkerhet, takker SINTEF for muligheten til å gi tilbakemelding på forslaget til ny lov om Etterretningstjenesten. SINTEF er en uavhengig stiftelse, og vår visjon er «Teknologi for et bedre samfunn».

Digitalisering – av mange blinket ut som en bærebjelke for fremtidens verdiskapning – er et av SINTEFs hovedsatsningsområder. I flere år har vi brukt konsepter som Big Data, Internet of Things og kunstig intelligens til å lage nye og innovative løsninger for norske bedrifter og myndigheter. Parallelt har vi i en årrekke drevet forskning innenfor IKT-sikkerhet, blant annet med prosjekter viet kritisk IT-infrastruktur, risikovurderinger og personvern.

Høringsnotatet er en omfattende behandling av bakgrunnen for lovforslaget. Det har ikke vært formålstjenlig for SINTEF å gi en uttalelse hvor vi går i dybden på alle detaljene som høringsnotatet berører. SINTEF understreker derfor at de momenter fra høringsnotatet som ikke er kommentert i dette høringssvaret, hverken bør tolkes som støtte for, eller som kritikk av disse, men som en prioritert avveining av hvilke problemstillinger vi har valgt å fokusere på.

SINTEF ønsker å bidra til en mest mulig opplyst debatt omkring hvilke kortsiktige og langsiktige konsekvenser forslaget vil ha for samfunnet. Vårt utgangspunkt for å kommentere forslaget til ny E-tjenestelov er derfor to fundamentale kjensgjerninger som illustrerer det dilemmaet samfunnet står overfor:

- Den teknologiske utviklingen gjør at E-tjenesten har et behov for tilgang til det digitale rom for å kunne utføre sitt samfunnsoppdrag.
- Konsekvensene av å gi E-tjenesten tilgang som beskrevet i lovforslaget vil gripe langt inn i det norske demokratiets grunnmur.

E-tjenestens legitime behov for å drive informasjonsinnhenting i det digitale rom må derfor tilfredsstilles samtidig som viktige prinsipp som personvern, kildevern og rett til privatliv blir ivaretatt. Dette er utfordrende i en tid der digital teknologi er i ferd med å endre sammenhengene og spillereglene i alle deler av samfunnet.

Sammendrag av SINTEFs syn på lovforslaget

SINTEF mener at forslaget til ny lov om Etterretningstjenesten ikke bør vedtas i sin nåværende form. Etter vårt syn vektlegger forslaget E-tjenestens behov i for stor grad uten å samtidig ta hensyn til de negative konsekvensene forslaget med all sannsynlighet vil ha for samfunnet.

Vi begrunner vårt syn i korthet slik:

- Tilrettelagt innhenting slik det er beskrevet i høringsnotatet utgjør en fundamental endring i hvordan E-tjenesten kan drive informasjonsinnhenting, og har potensielt gjennomgripende konsekvenser for personvernet, som er et av de grunnleggende prinsippene det demokratiske Norge bygger på.
- Konseptet "grenseoverskridende kommunikasjon" brukes som argumentasjon for forslaget og for å legitimere E-tjenestens tilgang. Men det er lite som tilsier at dette skillet er relevant som avgrensning av E-tjenestens mandat i det digitale rom. Dagens nettbaserte tjenester og digitale verdikjeder – også de som i hovedsak tilrettelegger for samhandling i Norge – består, teknisk sett, i stadig større grad av grenseoverskridende kommunikasjon. Resultatet er at så å si all kommunikasjon på nett vil gå via E-tjenestens systemer dersom forslaget blir vedtatt.
- Den teknologiske utviklingen gjør at alle etterhvert vil ha et betydelig digitalt fotavtrykk i form av personopplysninger, vaner og preferanser. For at viktige prinsipper som personvern og ytringsfrihet skal bestå er vi avhengig av at norske borgere opplever at de samme rettighetene eksisterer digitalt som ellers. Lovforslaget legger imidlertid det juridiske grunnlaget for mekanismer og verktøy som potensielt kan gjøre kraftige inngrep i personvernet.
- Vår vurdering er at de sterkeste trusselaktørene har kapasiteter som gjør at de vil kunne omgå systemene som foreslås, samtidig som at adgang til å inspisere kryptert trafikk vil skape usikkerhet hos mange som er avhengige av å ha tillit til konfidensiell kommunikasjon. Dette kan bli en bremsekloss på digitaliseringen av samfunnet.
- Overskuddsinformasjon representerer et problem med mange fasetter. Det kan oppstå et betydelig press for at E-tjenesten skal dele opplysninger som har relevans for f.eks. politiet. Det er også tilfeller der E-tjenesten vil være pliktig å dele slik informasjon. Dette representerer en begynnende formålsutglidning som ikke er godt nok besvart i lovforslaget.
- Personverninngrepene lovforslaget gir adgang til kan bli forsterket etter hvert som teknologien videreutvikles. Både mengden data og hvordan data kan kobles sammen er under stadig utvikling og vil gjennom tilrettelagt innhenting gi økt kapasitet til å inspisere detaljer i enkeltmenneskers privatliv.
- Automatiserte søkealgoritmer som behandler store mengder informasjon risikerer å peke ut uskyldige individer som tilfeldigvis passer til søkekriteriene. Slike kriterier kan inneholde utilsiktet bias og oppleves som diskriminerende. I verste fall kan falske positive treff føre til falsk mistanke og uberettiget påtale.

"Tilrettelagt innhenting" får gjennomgripende konsekvenser for samfunnet

Hovedutfordringen med forslaget om "tilrettelagt innhenting" er at all informasjon som kommuniseres på nett i praksis kan bli tilgjengelig for E-tjenestens systemer. Dette er, uavhengig av hvilke tekniske, juridiske og politiske kontrollmekanismer som implementeres, en grunnleggende endring i hvilken

informasjon E-tjenesten har tilgang til, og hvilken teoretisk kapasitet de vil besitte for å gjøre inngrep i norske borgeres grunnleggende rettigheter.

Nedkjølingseffekt, formålsutglidning og personverninngrep er eksempler på negative konsekvenser slik tilrettelagt innhenting kan ha. Selv om høringsnotatet kommenterer disse er de etter vårt syn ikke tillagt nok vekt i konklusjonen. F.eks. vurderer departementet at det ikke vil oppstå en negativ nedkjølende effekt i Norge, men at tilrettelagt innhenting i stedet vil styrke Etterretningstjenestens evne til å sikre Norge og at det igjen vil skape en følelse av trygghet hos befolkningen[1]. En slik konklusjon gir alvorlig konsekvens for samfunnet, og må begrunnes grundigere.

Grenser i det digitale rom

Prinsippet om at militær etterretning ikke skal bedrive overvåkning av egne borgere er vanskelig å etterleve når det ikke finnes klare digitale grenser som følger de geografiske nasjonsgrensene. Selv om det for bare få år siden var slik at norske nettsider og nettjenester stort sett ble driftet av servere plassert i Norge, er bildet i dag langt mer komplekst. Norske nettsider og datasystemer benytter seg av globale leverandører av skytjenester og serverløsninger. På toppen av alt dette har vi sett en globalisering av selve tjenestene som tilbys på nett. Disse tjenestene består etter hvert av lange digitale verdikjeder som godt kan involvere grenseoverskridende kommunikasjon i flere ledd.

Fraværet av godt definerte grenser i det digitale rom gjør det krevende å definere E-tjenestens mandat til å drive informasjonsinnhenting. Vi mener at man ikke kan bruke grensebegrepet til dette, da resultatet blir et lovforslag som ikke samsvarer med den teknologiske virkeligheten det skal operere i.

Personvern i det digitale rom

Datatilsynet definerer personvern som "retten til et privatliv og retten til å bestemme over egne personopplysninger". Både privatliv og personopplysninger har i dag sin digitale eksistens gjennom enkeltpersoners bruk av digitale tjenester og lagring av personopplysninger av både det offentlige og private aktører. Det er en pågående debatt om hvordan individuelle rettigheter skal forvaltes digitalt og hvem skal ha ansvaret dersom informasjon kommer på avveie. Konsekvensene av sikkerhetsbrudd, id-tyveri og spredning av personopplysninger kan være svært alvorlig for den enkelte, spesielt for utsatte grupper og individer som lever med trusler. Det er et paradoks at E-tjenesten som frem til nå har hatt et strengt forbud mot å overvåke norske borgere, kan ende opp med det kraftigste verktøyet for å samle inn personlig og privat informasjon om Norges innbyggere.

Et grenseforsvar med hull for de med onde hensikter

Det er en kjent sak at trusselaktører i stadig større grad kommuniserer over krypterte kanaler. Tilrettelagt innhenting som foreslått vil ha mulighet til å inspisere også kryptert trafikk, men det vil til enhver tid finnes kryptering som det ikke er mulig å knekke. Sterke trusselaktører vil derfor ta i bruk nye metoder for å kunne kommunisere risikofritt. Tilrettelagt innhenting vil dermed kunne bli en mur med hull for de som har onde hensikter og i tillegg er digitalt kompetente. Dette vil redusere verdien av tilrettelagt innhenting.

Hele hensikten med kryptering for legale formål vil uthules hvis nasjonale aktører har en vedtatt rett til å bryte den. Tilrettelagt innhenting med rett til innsyn i kryptert trafikk, kan tvinge norsk næringsliv samt

[1] Høringsnotatet, side 277, avsnitt 11.13.8.5

forsknings- og innovasjonsmiljøer til å skaffe seg kostbare omveier i jakten på sikre kommunikasjonsløsninger. Da vil digitaliseringen av samfunnet svekkes.

Overskuddsinformasjon og formålsutglidning

Et fundamentalt problem med tilrettelagt innhenting i kommunikasjonskanalene er at E-tjenesten vil fange opp alt av informasjon som går over kabelen. Fra å være en tjeneste som tradisjonelt har hatt strenge juridiske føringer på hvor de har lov til å rette sin signaletterretning, vil E-tjenesten med det nye forslaget være nødt til å behandle store mengder data fra norske borgere – overskuddsinformasjon som E-tjenesten per i dag ikke har lov til å søke i.

Dette inngrepet i personvernet foreslås kompensert med kontrollmekanismer og domstolkontroll for å hindre formålsutglidning. Men det er fortsatt en rekke problemer med en slik løsning, først og fremst relatert til behandlingen av overskuddsinformasjon, eksempelvis:

- Sikker oppbevaring og sletting av informasjon.
- Lovpålagt deling av opplysninger med andre myndighetsorganer.
- Reell, og rettidig klageadgang og klagebehandling.
- Risiko for utvikling av "ukultur" over tid i behandlingen av overskuddsinformasjon.

Mulige fremtidige problemstillinger

Lovforslaget kommer i en tid der den teknologiske utviklingen og digitaliseringen av samfunnet gjør at norske borgere både frivillig og gjennom tvunget omstilling bygger opp en stadig mer detaljert digital identitet. Denne identiteten består av all digital informasjon tilhørende ett enkelt menneske, sammen med hvordan denne informasjonen er knyttet, og kan knyttes, sammen. Det er all grunn til å tro at denne utviklingen vil fortsette og forandre hvordan enkeltmennesker lever sine liv både i det offentlige og private rom – digital og fysisk. Det viktig at et lovforslag tar høyde for teknologiske trender og utviklingstrekk som har lang tidshorisont.

Risiko for falsk mistanke

Datafiltreringen som skal fjerne ikke-relevant data som E-tjenesten ikke har adgang til å søke i, vil måtte implementeres av automatiske algoritmer som filtrerer data basert på kriterier. På samme måte vil E-tjenesten kunne foreta målrettet innhenting basert på kriterier som er forhåndsgodkjent av domstolen. Hvilke algoritmer som brukes og hvilke kriterier de sorterer data etter vil være i konstant utvikling. Det er også et fagområde som er høyaktuelt for maskinlæring og andre avanserte teknikker med *kunstig intelligens* som et paraplybegrep. Det er ved flere tilfeller vist at automatiserte søkealgoritmer er følsomme for bias i søkekriteriene. Dette kan ha flere utilsiktede og diskriminerende konsekvenser. Dette vil kunne oppleves særdeles inngripende for den personen som tilfeldigvis passer inn i et mønster uten å ha gjort seg skyldig i noe som er innenfor E-tjenestens mandat å undersøke. Koblet sammen med utviklingen av en stadig mer omfattende digital identitet, så ligger det i tillegg et potensial for uberettiget påtale, der et individ ikke er i stand til å motbevise det algoritmene har funnet av mønster og sammenhenger. Det er også en fare for at både E-tjenesten og domstolene etterhvert vil få økt tillit til verktøyet og ikke ta høyde for innebygd/skjult bias i algoritmene som kan plukke ut uskyldige personer.

Alternativer til tilrettelagt innhenting

I forbindelse med forslaget fra Lysne II-utvalget om digitalt grenseforsvar, etterlyste flere instanser, deriblant SINTEF, at mer målrettede og mindre inngripende alternativer til masseovervåkning ble vurdert. Dette er delvis redegjort for i nåværende høringsnotat, men dessverre er analysen av alternativene svært begrenset. Den tar etter vår mening primært utgangspunkt i Etterretningstjenestens behov, fremfor å avveie ulike samfunnsbehov.

For å tilstrekkelig sikre et system er det viktig med tidligst mulig deteksjon av angrep og deling av denne informasjonen mellom relevante aktører for å sikre et godt forsvar. Samtidig er det like viktig at systemene er bygd for å motstå et angrep og håndtere at angrep lykkes. Det vil si at kritisk infrastruktur i Norge må utvikles med sikkerhet i fokus, og at en del av dette er å sørge for tilbakefallsløsninger hvor systemer i ytterste konsekvens kan opereres manuelt.

Regjeringen har nylig bevilget[2] 497 millioner NOK til NSM for, blant annet, videreutvikling av Varslingssystem for Digital Infrastruktur – VDI. I SINTEF har vi ikke gjort noen helhetlig analyse av alternativer til tilrettelagt innhenting, men for samfunnets behov fremstår VDI som en velegnet sensor for tidlig deteksjon av angrep mot kritisk infrastruktur. Etablering av tilrettelagt innhenting er estimert i høringsnotatet til å koste ca. 700 millioner NOK, med årlige driftsutgiftene på ca. 150 millioner NOK. Dette er en betydelig årlig merkostnad for et vidt digitalt barriereforsvar. SINTEF etterlyser en mer helhetlig analyse av hva man ville kunne oppnå av økt samfunnssikkerhet ved å bruke disse midlene på alternative sikringstiltak, som f.eks. å styrke VDI ytterligere, redusere medlemsavgiften for deltagelse i VDI, styrke funksjonen for utveksling av trusselinformasjon og innføre en stor satsning på å bedre sikkerheten i kritisk infrastruktur.

Konklusjon

SINTEFs konklusjon og anbefaling er at forslag om ny lov for Etterretningstjenesten, og spesielt forslaget om "tilrettelagt innhenting", ikke bør vedtas i sin nåværende form. Høringsnotatet belyser mange samfunnskritiske sider ved E-tjenestens virksomhet, og behovet E-tjenesten har for å kunne løse sine oppgaver i det digitale rom er utvilsomt reelt. Men det er etter SINTEFs syn ikke gjort nok for å tilpasse lovforslaget til andre vitale samfunnsbehov og rettigheter og de negative konsekvensene et slikt forslag kan ha. E-tjenestens behov for tilgang sett opp mot viktige samfunnsprinsipp og krav om personvern utgjør et dilemma drevet frem av den digitale omstillingen Norge er på vei inn i. Et lovforslag som potensielt kan endre balansepunktet mellom staten og individet må etter vårt syn ta sterkere hensyn til hele dette bildet.

Med vennlig hilsen
SINTEF

Alexandra Bech Gjørv
Konsernsjef

[2] https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/digital-sikkerhet/id2340011/