Tekna –
Teknisk-naturvitenskapelig forening
Postboks 2312 Solli
0201 Oslo

www.tekna.no
Org.nr 971 420 782
post@tekna.no
+47 22 94 75 00

Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo

Vår ref.:	Deres ref.:	Dato:
MKF	2016/2773-185/FD II 6/SIH	27. september 2022

Høringssvar - Forslag om endringer i etterretningstjenesteloven

Tekna – Teknisk naturvitenskapelig forening er den største masterforeningen i Norge, og den største fagforeningen i Akademikerne med over 97 000 medlemmer. Våre medlemmer har mastergrad eller mer fra tekniske og naturvitenskapelige fagområder.

Tekna viser til høringsbrev av 27. juni 2022 om forslag til lov om endringer i etterretningstjenesteloven. Høringsfrist er 27. september 2022.

Tekna har fulgt behandlingen av Etterretningstjenesteloven siden 2019, og har ved gjentatte anledninger uttrykt bekymring for lovens vidtrekkende konsekvenser. Forslagene i dette høringsnotatet gjelder justeringer i § 7-3 i etterretningstjenesteloven. Bestemmelsen gjelder beslutning om tilrettelegging av tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon etter lovens kapittel 7.

Til tross for de forbedringer som er gjort og foreslått, så mener vi at dette forslaget til endringer i ny etterretningstjenestelov ikke svarer ut våre bekymringer. Tekna mener at det foreliggende forslaget i svært liten grad reduserer de alvorlige samfunnsmessige ulempene ved å innføre «tilrettelagt innhenting». Videre mener vi at forslaget ikke er i samsvar med praksis fra EMD og EU-domstolen.

Ikraftsettelsen av § 7-3
Innledningsvis vil vi bemerke Regjeringens ikraftsettelse av § 7-3 knyttet til innhenting og bruk av testdata ved kongelig resolusjon 2. september 2022. Tekna reagerer på at deler av et regelverk som er på høring gjøres gjeldende før høringsprosessen er avsluttet. Tekna mener at dette er så inngripende at regjeringen burde ventet til høringsrunden og stortingsbehandlingen var ferdig før man åpnet for testing.

Forslag til ny § 7-3

Uavhengig forhåndskontroll

Teknas hovedinnvending mot forslaget er at det fortsatt åpnes for innhenting og lagring av metadata i 18 måneder, uten at en uavhengig forhåndskontroll og at mulighetene for å søke i disse opplysningene utvides sammenlignet med gjeldende lov.

Det fremkommer av forslagets § 7-3 første ledd, at sjefen for Etterretningstjenesten treffer beslutning om å speile kommunikasjonsstrømmer etter § 7-2. Dette skal utelukkende benyttes for testing og analyse etter §§ 7-5 og 7-7 fjerde ledd med sikte på å avklare om det foreligger grunnlag for å fremme begjæring om rettens beslutning etter annet ledd. Dette innebærer at det etter § 7-5 kan gjennomføres uttrekk av ufiltrert kommunikasjon fra én eller flere kommunikasjonsstrømmer. Videre fremkommer det av § 7-7 at metadata kan innhentes og lagres i bulk i 18 måneder. Dette vil dreie seg om kommunikasjon som har vært grensekryssende. Når det hevdes at «det bare samles inn metadata», er det viktig å være oppmerksom på at sammenstilling av kontinuerlige strømmer metadata kan gi svært detaljert oversikt over en person. Den største overvåkingseffekten kommer derfor ikke av overvåking gjennom ett selskap, men av sammenstilling av løpende informasjon fra en mengde selskaper, apper og tjenester. Det legger grunnlaget for en omfattende, detaljert kartlegging av befolkningens liv og aktiviteter.

Vi vil videre vise til Datatilsynet sitt høringsinnspill og deres henvisning til at ordlyden «utelukkende skal benyttes for testing og analyse» ikke beskriver formålene med metadatalaget i tilstrekkelig grad. Som de videre skriver så er bestemmelsen i § 7-7 om metadatalageret utformet slik at metadatalageret vil inneholde alle relevante kommunikasjonsstrømmer og brukes til testing og analyse, men også som grunnlag for retrospektive søk – altså søk tilbake i tid før domstolens beslutning og innhenting av kommunikasjonsstrømmer.

Domstolkontrollen

Etter forslagets § 7-3 annet ledd kan retten fatte beslutning om å tillate speiling av kommunikasjonsstrømmer etter § 7-2 som grunnlag for søk og innhenting etter § 7-8 og 7-9. Rettens kjennelse skal ikke gis for lengre tid enn nødvendig, og skal ikke overstige to år. Slik Tekna forstår dette forslaget så kan etterretningstjenesten installere og optimalisere datainnsamlingen parallelt med at de venter på den juridiske godkjenningen. Dette strider imot rettsutviklingen i EMD og EU-domstolen.

I henhold til praksis fra EMD: Big Brother Watch and Others mot Storbritannia (BBW), så skal den uavhengige forhåndskontrollen iverksettes før innhenting. I norsk praksis vil domstolkontrollen kunne foretas så sent som 18 måneder etter at dataen er innhentet.

Tekna er på bakgrunn av dette usikker på hvor reell domstolskontrollen kommer til å være og hvorvidt den vil gi økt rettssikkerhet.

I høringsnotatet er det videre uttalt:

> *«Gitt de teknologiske forutsetninger om at trusselkommunikasjon blander seg med all annen kommunikasjon, og at man ikke på forhånd kan vite hvilken rute en enkelt kommunikasjon vil ta, bør det heller ikke oppstilles for store forventninger knyttet til hvilken rettssikkerhetsgaranti forhåndsautorisasjonen vil utgjøre i praksis. Det må også tas i betraktning at det i mange tilfeller ikke vil være mulig å sondre mellom kommunikasjonsstrømmer av større eller mindre verdi, og at det derfor vil være vanskelig å foreta reelle nødvendighets- og forholdsmessighetsvurderinger i disse tilfellene.»*

Vi tolker lovforslaget dithen at det legges opp til at tingretten skal vurdere mer generelle sikkerhetsvurderinger når de gir tillatelse til søk. Dette er ikke i tråd med praksis fra EU-domstolen (de såkalte La Quadrature du Net-kriteriene) hvor man peker på at det må finnes konkrete sikkerhetstrusler og holdepunkter for å kunne gi tillatelse til søk.

Vi er usikre på om dette lovforslaget vil medføre reell overføring av myndighet fra etterretningstjenesten til domstolen, eller om det vil ha noen faktisk betydning for hvilke selskaper som vil bli pålagt å gi etterretningstjenesten tilgang til datatrafikken sin. Fra vårt faglige ståsted ser det ut som om det mangler gode mekanismer som sørger for en hensiktsmessig bruk av systemet. Vi er skeptiske til effekten av domstolskontrollen, og vil vise til tall fra RIPA (Regulation of Investigatory Powers Act 2000). Dette er en tilsvarende lov i UK som tillater politiet å analysere metadata i visse tilfeller. Vi kan se at fra 2009 til 2011 ble bare 380 av 41.351 anmodninger stoppet. Vi ser det som rimelig å kunne forvente tilsvarende tall med denne loven.

Teknas generelle bekymringer knyttet til etterretningstjenesteloven

Overvåkningens omfang

Tekna er generelt kritiske til omfanget av overvåkningen som loven legger opp til. Lovteksten er formulert på et vis som gjør det vanskelig å trekke opp en klar linje for hvilke selskaper som kan pålegges å overvåke kundenes datatrafikk. § 7-2 sier at dette i tillegg til «tilbydere som omfattes av ekomloven» (bl.a. Telenor), også gjelder «tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten». Mange tilbyr «meldingstjenester» som en del av tjenestene sine, og enda flere tilbyr «internettbaserte kommunikasjonstjenester». Våre eksperter stiller seg spørsmålet om det i det hele tatt er mulig å tilby noe på internett uten at det er en «internettbasert kommunikasjonstjeneste». Videre er vårt inntrykk at mange tror at avlyttingen kun skal skje idet den «krysser grensen», men avlyttingen skjer selvfølgelig i selskapenes server-rom.

Det vises i den forbindelse til Prop 80 L. (2019–2020) kap. 7 hvor det fremgår:

> *«Kommunikasjonsstrømmene vil ikke nødvendigvis speiles og tilgjengeliggjøres på det bestemte punktet hvor de krysser grensen.»*

«ikke ses bort fra at speilingen også vil kunne omfatte norsk innenlandsk kommunikasjon som ikke krysser grensen», men at e-tjenesten skal «søke å forhindre lagring av norsk innenlandsk kommunikasjon gjennom utvalg og filtrering».

Som Tekna har påpekt i flere høringsuttalelser, er det urealistisk å se for seg at man kan filtrere vekk all norsk innenlandsk kommunikasjon. Det er for øvrig interessant å se at lovens § 4-7 eksplisitt sier at «Etterretningstjenesten kan innhente rådata i bulk selv om informasjon om personer i Norge vil kunne følge med».

Risiko for nedkjølingseffekt og formålsutglidning

Tekna er opptatt av å synliggjøre risikoen for at nedkjølingseffekten inntrer idet systemet iverksettes. Vi mener det er en reell sannsynlighet for at innbyggerne begrenser sine ytringer i det digitale rom. Dette vil kunne, legge begrensninger på det offentlige ordskiftet og demokratiske prosesser, samt svekke befolkningens tillit til myndighetene. Vi er også bekymret for at e-tjenesteloven kan svekke forbrukernes tillit til norske virksomheter, siden det er norske selskaper som heretter kan pålegges å overvåke sine kunder.

Tekna vil også peke på faren for formålsglidning. Den nye loven er tydeligere på at overskuddsinformasjon fra overvåkningen kan tilfalle politi og andre myndigheter. Vi er bekymret for at et ytterligere politisk press om å ta i bruk allerede «innhentede» data til stadig nye formål, vil uthule det individuelle rettsvernet.

Skjeve forventninger knyttet til maskinlæring

Tekna er bekymret for e-tjenestens forventede bruk av kunstig intelligens. Maskinlæring er veldig godt egnet til å finne mønstre i data ved å finne korrelasjoner. Dessverre er det slik at maskinlæring ikke kan skille mellom gode, meningsfulle korrelasjoner og «feil» korrelasjoner som skyldes f.eks. problemer med data-sampling, irrelevant informasjon etc. Vi frykter at det trekkes konklusjoner som ikke samsvarer med virkeligheten. For eksempel kan maskinlæringsalgoritmer velge uventede «snarveier» i sin jakt etter svar. Det vil videre være utfordrende å forklare hvorfor en maskinlæringsmodell plukker ut visse datastrømmer og ignorerer andre. Videre å forklare alle faktorer som medvirker til at modellen plukker ut person X som en person med etterretningsverdi og ignorerer andre (forklarbarhet / svart-boks-problematikk). 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).

Tekna har i tidligere høringsrunder løftet frem følgende problemstillinger:

- 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 treffsikkerhet/feilrate, og hvordan skal dette måles og korrigeres?
- Hva er kravene til etterprøvbarhet og begrunnelse av resultater?

Departementets svar i Prop. 80 L (2019–2020) var at de «legger til grunn» at EOS-utvalget «er bevisst på problematikken». Tekna mener at dette er en enorm oppgave å legge på få personer. EOS-utvalget har i sitt høringssvar selv avvist at de kan eller bør være en garantist for at feil ikke skal skje:

> *«Vår kontroll er stikkprøvebasert, og vi har ikke mulighet til en fullstendig gjennomgang av all overvåkingsvirksomhet i E-tjenesten og de andre EOS-tjenestene»*[1].

Det fremstår som svært uklart hvordan man faktisk vil ta i bruk maskinlæring. I et slikt prosjekt er det vanligvis flere forskjellige programvaremiljøer fra utvikling til produksjon, og man trenger data til alle faser, så som utvikling og test. Hvilke data kan brukes, og hvilke tilganger skal gis til hvem? Hvordan skal man teste et sånn system, og hvilke søkebegrensninger vil gjelde for utviklings- og testmiljøer? Hvordan skal man kunne utvikle et velfungerende system og samtidig sørge for at alle personene som trenger tilgang for å utvikle systemet, ikke søker i dataene? Vi lurer også på om man skal bruke tredjeparts applikasjoner eller skytjenester (med økt risiko for at data havner på feil hender).

Sikkerhetsrisiko

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 misbrukt eller manipulert ved eksempelvis å skape en feilaktig situasjonsforståelse.

Tekna etterlyser derfor mer tilgang på kompetanse for å bygge, vedlikeholde, drive og sikre systemet for innsamling og lagring. Nok ressurser med rett kompetanse vil være avgjørende for å begrense sikkerhetsrisikoen og sikre forsvarlig drift av systemet. Ettersom rådata i bulk kan lagres i 15 år, med mulighet for forlengelse, er det betydelige mengder data om befolkningen som skal lagres på ett sted, i lang tid.

Kompetanse

Som en forlengelse av dette, så er vi bekymret for tilgangen på kompetanse. Tekna mener at de fire ekstra årsverkene som Forsvarsdepartementet foreslår

[1] https://fido.nrk.no/0f93889fe52af254e29fcf3ce928ac34265df2829f053c5c7465ff44f4aef2c6/H%C3%B8ringssvar-EOS-utvalget-ny-e-lov.pdf

til kontrollorganet ikke på langt nær vil være tilstrekkelig til å få oversikt over om e-tjenesten bruker den innhentede informasjonen på en måte som ikke bryter loven. EOS-utvalget kan ikke hindre overvåking, men hvis de får tilstrekkelige ressurser, kan de forhåpentligvis bidra til å dempe de mest åpenbare skadevirkningene.

Systemet for tilrettelagt innhenting vil kreve ansettelse av mange fagfolk med topp kompetanse og erfaring, både på drifts- og kontrollsiden. Disse individene må også kunne sikkerhetsklareres. Dette er arbeidskraft mennesker det i dag er mangel på i det norske arbeidsmarkedet. Tekna mener derfor at hvis det dette systemet etableres må det ledsages av en kraftig utbygging av relevant kompetanse på høyt nivå.

Tekna vil også foreslå at det etableres et faglig råd av eksperter som kan evaluere systemets implementasjon, påpeke mangler og sjekke at disse blir rettet.

Vi mener videre at loven og alle etablerte systemer må gjennomgås og evalueres grundig etter to år, for å avdekke på om de fungerer etter hensikten og er tilpasset den teknologiske utviklingen.

Videre må det av sikkerhetshensyn bygges inn en mekanisme for hurtig å avvikle systemet og slette innhentende data i en situasjon der det er fare for at systemet blir misbrukt.

Med vennlig hilsen

Line Henriette Holten
generalsekretær