Til Evalueringsutvalget

Oslo, 21.11.2025

Vi viser til invitasjonen til å gi skriftlig innspill til evalueringen av etterretningstjenesteloven.

Ved behandlingen av etterretningstjenesteloven våren 2020 besluttet Stortinget at loven skal være gjenstand for en uavhengig, offentlig evaluering senest fire år etter full ikrafttredelse. Evalueringen skal omfatte lovens virke og muligheten for effektiv kontroll, herunder ressurser, kompetanse og virkemidler hos EOS-utvalget og domstolene.

Regjeringens mandat fra 2025 avgrenser imidlertid evalueringen til å vurdere om loven «virker etter lovgivers intensjon», og utelukker eksplisitt vurderinger av behov for endringer i det rettslige rammeverket. Etter Teknas syn innebærer dette en vesentlig innsnevring av Stortingets opprinnelige bestilling. En evaluering som på forhånd avskjærer muligheten for å konkludere med at rammene bør justeres, kan vanskelig anses som uavhengig. Dersom evalueringen skal oppfylle Stortingets vedtak, må den kunne vurdere om dagens system faktisk gir reell teknisk kontrollbarhet og tilstrekkelige rettssikkerhetsgarantier, ikke bare om praksis holder seg innenfor lovens forutsetninger.

Ulovlig lagring av e-post

Den særskilte meldingen fra EOS-utvalget 12. november 2025 om ulovlig lagring av data ved E-tjenestens bruk av tilrettelagt innhenting (TI) reiser grunnleggende spørsmål om systemforståelse, internkontroll og teknisk transparens.

EOS-utvalget konstaterer at E-tjenesten over tid lagret innholdsdata i strid med lov og kjennelser, også etter at funksjonaliteten som muliggjorde lagringen var forsøkt deaktivert. Etter Teknas vurdering indikerer dette at de interne sikkerhetsmekanismene for teknisk kontroll ikke var tilstrekkelig operasjonalisert.

Saken illustrerer samtidig de praktiske utfordringene ved det formelle skillet mellom metadata og innholdsdata. Etter Teknas syn må dette skillet defineres langt tydeligere og håndheves langt strengere enn i dag. Saken, som gjaldt ulovlig lagring av e-post-emnefelt, viser at dagens forståelse og praktisering av skillet ikke er tilstrekkelig presist, og at det åpner for alvorlige brudd uten at de oppdages av interne mekanismer.

Et fungerende skille forutsetter at metadata defineres klart og operasjonelt, slik at det ikke kan være tvil om hvilke datatyper som krever særskilte rettssikkerhetsgarantier. Etter Teknas syn bør utvalget derfor vurdere om det er mulig å etablere en strammere, teknologinøytral og eksplisitt definisjon av metadata, og innføre krav om at eventuelle tekniske ambiguiteter alltid skal tolkes til fordel for borgerens rettsvern.

Som dokumentert gjennom EOS-utvalgets særskilte melding, utgjør dagens skille en betydelig rettssikkerhetsrisiko fordi data definert som metadata ofte har tilsvarende informasjonsinnhold som tradisjonelle innholdsdata, og fordi dagens arkitektur for tilrettelagt innhenting ikke synes i tilstrekkelig grad klarer å håndheve forskjellen i praksis. Selv i tilfeller der innholdsdata ikke foreligger, vil det ofte være mulig å utlede tilsvarende informasjon gjennom analyser av metadata, eller gjennom kombinasjoner av ulike typer metadata, som samlet sett kan gi et informasjonsnivå som i praksis nærmer seg innholdsdata.

Videre mener Tekna at saken viser at E-tjenestens interne kontrollmekanismer ikke fungerer tilfredsstillende. At ulovlig lagring fortsatte, selv etter at funksjonaliteten var slått av, viser en manglende evne til intern kvalitetskontroll. Oppfølgingen av bruddene har etter Teknas vurdering heller ikke stått i forhold til alvorlighetsgraden. Det er bekymringsfullt at tjenesten ikke har gjort det som må kunne anses som et absolutt minimum for å sikre etterlevelse etter at ulovlig praksis ble avdekket.

Etter Teknas syn bør utvalget i evalueringen vurdere hvordan både rettssikkerhetsgarantier, internkontroll og tilsyn kan styrkes for å forhindre gjentakelser.

Uklar nytteverdi

Da Stortinget vedtok loven, var premisset at TI skulle gi staten vesentlig bedre forutsetninger for å avdekke og motvirke trusler i cyberdomenet, herunder terror, sabotasje og spionasje.

Tekna mener det er sentralt at utvalget undersøker i hvilke typer saker TI har vært benyttet, og hvilken faktisk nytte loven har hatt. Dersom hjemlene i praksis gir liten eller uklar effekt, er det vanskelig å forsvare et så inngripende og kostbart system.

Tekna har tidligere pekt på risikoen for masseovervåkning, svak internkontroll og utilstrekkelige rettssikkerhetsgarantier. Vi har også uttrykt tvil om dagens regelverk oppfyller kravene til nødvendighet og forholdsmessighet i EU-domstolens praksis om bulkinnhenting. Det er derfor særlig viktig at evalueringsutvalget vurderer om loven faktisk leverer den sikkerhetsmessige gevinsten som ble forutsatt.

Det er vanskelig å se hvordan utvalget kan konkludere på om loven virker etter lovgivers intensjon uten å vurdere om inngrepets omfang står i forhold til den faktiske nytten. I alle andre samfunnsområder ville en slik forholdsmessighetsvurdering vært et minstekrav. Tekna mener derfor at utvalget bør gjennomføre den vurderingen som manglet da loven ble vedtatt.

Spørsmål utvalget bør belyse: For å vurdere om loven virker etter lovgivers intensjoner, anbefaler Tekna at utvalget innhenter informasjon om og vurderer:

- I hvilke typer saker TI har vært benyttet (terror, sabotasje, spionasje, cyberangrep).
- Hvilke konkrete resultater og etterretningsbidrag som kan tilskrives TI.
- Hvordan nytteverdien står i forhold til kostnader, ressursbruk og personvernulemper.
- Hvordan kontroll- og tilsynsorganene faktisk har gjennomført etterprøving.
- Hvordan teknologiutviklingen påvirker rettssikkerhet og forholdsmessighet i praksis.
- Om den brede og uspesifikke innhentingen etter § 7-3 gir en nødvendig og dokumenterbar tilleggsverdi som ikke kan oppnås gjennom målrettede tiltak?
- Hvordan E-tjenesten sikrer at algoritmene som styrer seleksjon, filtrering og analyse av TI-materiale ikke skaper utilsiktede prioriteringer, diskriminerende mønstre eller teknologiske skjevheter, gitt at databehandlingen er unntatt sivil regulering og dermed ikke følger datakvalitets- og KI-krav som ellers gjelder i Norge?

Tekna er opptatt av at våre sikkerhetsmyndigheter forvalter den tilliten de er gitt med største varsomhet. Når inngrepene er så omfattende som i dette systemet, er tillit selve bærebjelken. Vi som samfunn har ikke råd til å opprettholde et system som misbruker denne tilliten, eller som ikke kan dokumentere at den forvaltes med den presisjon og varsomhet som borgernes rettigheter krever.

Med vennlig hilsen

Sonja Lovise Berg

Sonja Lovise Berg
Konst. generalsekretær