

Hørings svar: - Endringer i politiloven og politiregisterloven mv. og – PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon

Tekna – Teknisk naturvitenskapelig forening er den største masterforeningen i Norge, og den største fagforeningen i Akademikerne med over 99 000 medlemmer. Våre medlemmer har mastergrad eller mer fra tekniske og naturvitenskapelige fagområder.

Vi viser til forslagene i prop. 31 L (2022-2023) fremmet i statsråd 2. desember 2022 om endringer i politiloven og politiregisterloven.

Tekna anerkjenner PSTs behov for nye verktøy i møte med digitale utfordringer og et endret trusselbilde.

Selv om departementet har drøftet og imøtekommet noen av høringsinstansene sine innvendinger, så har departementet etter Teknas syn ikke hensyntatt de største innsigelsene mot lovforslaget. Tekna savner også en grundigere vurdering av faren for nedkjølingseffekt og formålsutglidning ved innvilgning av utvidede fullmakter til PST.

Tekna etterlyser prinsipper som beskriver balansen mellom å ivareta personvern og PSTs tjenestebehov. Tekna mener at man med fordel kunne drøftet hvorvidt en mer målrettet metode ville kunne oppfylt formålene ved loven uten at inngrepet i enkeltmenneskets personvern hadde vært så stort.

Lovforslagets manglende begrensninger skaper bekymring for hvilke konsekvenser det vil få for enkeltindividers grunnleggende rettigheter, ytringsfrihet og personvern. Tekna er opptatt av å bemerke at lovforslaget må ses i sammenheng med andre overvåkningstiltak som politiet og etterretningstjenesten har fått hjemmel til, slik som tilrettelagt innhenting, lagring av IP-adresser og overvåkning av flypassasjerer. Samlet betyr disse forslagene at nærmest all vår digitale kommunikasjon kan innsamles av våre sikkerhetsmyndigheter.

Åpent tilgjengelig informasjon

Tekna uttalte seg kritisk til manglende begrensninger knyttet til PSTs innsamlingen av informasjonen under forrige høringsrunde. Flere av instansene pekte på at målretting står sentralt i praksis fra EMD og EU-domstolen.

Etter en fornyet vurdering har departementet rammet inn innhenting til «en viss grad» for å møte høringsinstansene sin bekymring for at PST kan lagre «hva som helst». Kravet om at behandlingen må «antas» å være nødvendig innebærer *ikke* at det kreves sannsynlighetsovervekt eller sikkerhet for at det vil behandle opplysningene. Videre skriver departementet at «det vil være tilstrekkelig med en rimelig og ikke helt fjern mulighet for at behandlingen er nødvendig». Etter Teknas syn innebærer denne innrammingen i praksis svært få begrensninger.

Slettefristen

Tekna er fornøyd med at lagringstiden reduseres fra 15 til 5 år, men reagerer på at sjef i PST, eller den denne bemyndiger, kan beslutte fortsatt lagring i fem år av gangen, og inntil 15 år, dersom opplysningene etter en konkret vurdering fremdeles er nødvendig for utarbeidelse av analyser og etterretningsvurderinger. Tekna mener at denne vurderingen burde blitt fattet ved en uavhengig domstolkontroll heller enn av sjef i PST. Tekna vil også påpeke at jo lenger tid som går, jo vanskeligere vil det også være å kontrollere om opplysningene er korrekte. For en registrert person vil det være vanskelig å forklare eller forsvare seg mot informasjon som er gammel, og mulig tatt ut av kontekst.

Det er etter Teknas syn fortsatt ubesvarte spørsmål knyttet til kapitelet som omhandler sletting. Tekna stiller spørsmål ved hvilket tidspunkt PST legger til grunn for tidsberegningen, hvordan slettingen skal implementeres i praksis og hvordan slettefristen skal anvendes når PST har levert informasjon til andre organer.

Tekna stiller også spørsmål ved hvordan sletteregelen skal anvendes ved, for eksempel, berikelse av data. Departementet påpeker i proposisjonen at PST kan berike innhentet data med andre data som de allerede har, selv om informasjonen ligger adskilt fra PSTs øvrige registre.

Automatiserte analyseverktøy

Tekna er fornøyd med at departementet har kommet til at adgangen til å benytte automatiserte analyseverktøy i forbindelse med utarbeidelse av analyser og etterretningsvurderinger bør inntas i lovteksten. Etter Teknas syn så burde reguleringen ikke være begrenset til *behandlingen* av opplysninger, men også hvilke verktøy som kan benyttes for behandlingen.

Etter Teknas syn bør det gis klarere føringer på hvilke typer teknologi det skal være tillatt å benytte. Videre mener Tekna at det må være transparens og åpenhet knyttet til hvilke verktøy PST benytter for å analysere den innhentede dataen. Tekna sitt ønske om åpenhet knyttet til valg og bruk av teknologi handler også om innsikt i valg av leverandør. Bruk av teknologi som er utviklet og driftet i andre land åpner opp for en rekke problemstillinger knyttet til den norske personvernforordningen og dataeierskap, for å nevne noe.

Kravet om åpenhet handler også om å opprettholde tilliten blant den norske befolkningen.

Anonymisering

Departementet skriver:

«Gitt mengden data som kan samles inn, vil det ikke være mulig å anonymisere opplysninger om enkeltpersoner for så å foreta ulike analyser.»

Tekna vil påpeke at dette er feil. Det er fullt mulig å anonymisere data om enkeltindivider før den analyserer, selv ved store datasett. Store skytjenesteleverandører som Microsoft¹, Google² og AWS³ har verktøy for å fjerne PII fra data på en massiv skala. Det finnes også

¹ <https://microsoft.github.io/presidio/>

² <https://cloud.google.com/dlp>

³ <https://docs.aws.amazon.com/glue/latest/ug/detect-PII.html>

flere andre eksempler på verktøy⁴ for å anonymisere data. Tekna anbefaler derfor at personsensitiv data fjernes fra datasettene før de analyseres for å redusere de negative effektene ved innsamlingen.

Profilering

Tekna er bekymret for at man ikke tar innover seg de potensielt negative konsekvensene ved å bli profilert på «gruppenivå». Avanserte analyser av store datasett vil samlet kunne gi et omfattende bilde av en gruppe. I et land med få innbyggere, så vil man da naturligvis fort kunne vite mye om individene i en gruppe. Det finnes ulike metoder for å fjerne personidentifiserende opplysninger som navn og adresse. En metode som ofte nevnes i denne sammenheng er «Differential Privacy». Dette er en teknikk som legger «støy» i dataene med hensikt å beskytte personvernet uten å påvirke resultatene av analysen.

Videre vil vi peke på at departementet i høringsnotatet åpner opp for at PST også kan ta automatiserte individuelle avgjørelser: Tekna vil sterkt advare mot dette.

Kontroll – og rettssikkerhetsmekanismer

Avslutningsvis vil Tekna benytte anledningen til å etterlyse bedre kontroll – og rettssikkerhetsmekanismer i lovforslaget. Verktøyet PST ønsker er kraftfullt og inngripende i enkeltmenneskets personvern, og det er derfor etter Teknas syn særlig viktig at man gjennom tydelige avgrensninger, åpenhet og gode kontrollmekanismer reduserer risikoen for misbruk og feil.

Departementet viser til at EOS-utvalget skal kontrollere det nye verktøyet til PST. Vi merker oss at EOS-utvalget i sin høringsuttalelse påpekte at deres kontroll er stikkprøvebasert og at de ikke er en garantist for at feil kan skje. Tekna mener derfor at EOS-utvalgets kontroll ikke er tilstrekkelig. Tekna vil foreslå at EOS-utvalget får myndighet til å bestille kontroll av systemet, som kan analysere og evaluere hvordan systemet har blitt implementert. Kontrollorganet vil kunne påpeke mangler og få myndighet til å kreve forbedringer⁵ innen visse tidsrammer.

Systemet vil kreve ansettelse av mange fagfolk med topp kompetanse og erfaring, både på drifts- og kontrolliden. 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 stiller seg bak NIM og Datatilsynets argumenter for ekstern kontroll, både av inngangsvilkåret for lagring, sletteplikten og adgangen til å utvide lagringen. Derre vil etter Teknas syn vil kunne dempe den nedkjølende effekten. Tekna mener at det er avgjørende forslaget må være i tråd med utgangspunkt i praksis fra EU-domstolen og EMD.

⁴ https://github.com/LeapBeyond/scrubadub_spacy eller <https://github.com/microsoft/presidio>.

⁵ Trustworthy AI: <https://arxiv.org/abs/2206.09887>