

Justis- og beredskapsdepartementet

Vår ref.:
MKF

Deres ref.:

Dato:
16. januar 2026

Teknas høringsinnspill til endringer i politiregisterloven og politiregisterforskriften - Bruk av kunstig intelligens (KI) til etterfølgende biometrisk fjernidentifikasjon

Tekna er fagforeningen for 117 000 naturvitere, teknologer og studenter. Våre medlemmer har høyere utdanning og representerer viktige kunnskapsmiljøer i Norge, både i offentlig og privat sektor.

Tekna viser til Justis- og beredskapsdepartementets høringsnotat om forslag til endringer i politiregisterloven og politiregisterforskriften knyttet til politiets bruk av kunstig intelligens (KI) til etterfølgende biometrisk fjernidentifikasjon.

Tekna er opptatt av at ny teknologi tas i bruk på en måte som er kunnskapsbasert, rettssikker og tillitsskapende. Tekna støtter at politiet har tilgang til effektive verktøy for kriminalitetsbekjempelse og at politiets metoder reguleres rettslig i lov og forskrift. Vi vil samtidig understreke at bruk av svært inngripende teknologi forutsetter grundige vurderinger av konsekvenser for personvern, rettssikkerhet og grunnleggende demokratiske verdier.

Etter Teknas vurdering gir høringsnotatet ikke et tilstrekkelig beslutningsgrunnlag for å åpne for bruk av etterfølgende biometrisk fjernidentifikasjon i den formen som foreslås. Tekna er særlig bekymret for mangelen på reelle personvern- og risikovurderinger slik EU-forordningen GDPR art 35 (personvernkonsekvensvurdering, DPIA) forutsetter for alle virksomheter som tar i bruk ny teknologi som behandler personopplysninger. De svært vide hjemlene for etterforskning uten klare terskler og svake kontrollmekanismer, spesielt for PSTs forebyggende virksomhet, er også problematisk etter Teknas syn.

2. Manglende personvern- og risikovurderinger

Tekna mener det er en vesentlig svakhet ved høringsnotatet at det ikke inneholder en konkret og systematisk vurdering av personvernkonsekvensene ved bruk av etterfølgende biometrisk fjernidentifikasjon.

Selv om høringsnotatet viser til Grunnloven § 102, EMK artikkel 8 og Den europeiske menneskerettsdomstolens praksis, herunder Glukhin-dommen, begrenser vurderingene seg i hovedsak til generelle rettslige utgangspunkter. Det foreligger ingen nærmere analyse av hvordan teknologien vil virke i praksis, herunder:

- omfanget av datamengder som kan analyseres
- risikoen for masseovervåkning når store mengder video- og bildemateriale blir søkbare på individnivå
- konsekvensene av feilidentifikasjoner, falske positive og hallusinasjoner
- risiko for diskriminering og skjevheter i teknologien
- mulige nedkjølingseffekter for ytringsfrihet, forsamlingsfrihet og samfunnsdeltakelse

Et sentralt problem er at teknologien som foreslås brukt i denne konteksten i praksis er svært vanskelig å avgrense på en måte som oppfyller personvernregelverket, herunder kravene etter GDPR. Bruk av KI-baserte analyseverktøy, for eksempel ved analyse av video- eller bildemateriale, innebærer uunngåelig at også andre personer enn den aktuelle målpersonen blir registrert, analysert, vurdert, logget og i mange tilfeller lagret. Disse personene er ikke mistenkt for noe, og behandlingen skjer dermed uten individuell hjemmel, uten nødvendighet og uten forholdsmessighet. Dette reiser grunnleggende spørsmål om hvordan prinsippene om dataminimering, formålsbegrensning og lovlighet faktisk kan etterleves i praksis, og om foreslått bruk derfor lar seg forene med gjeldende personvernkrav.

Tekna deler Datatilsynets vurdering av at fraværet av en reell personvern- og risikovurdering, DPIA, gir et svakt beslutningsgrunnlag både for høringsinstansene og for Stortinget. Når det gjelder ny teknologi som internasjonalt anses som høyrisiko, mener Tekna at en slik vurdering er en helt nødvendig forutsetning før regelverket endres.

3. Vide hjemler og manglende materielle skranker

Tekna er kritisk til at departementet eksplisitt velger å ikke avgrense bruken av etterfølgende biometrisk fjernidentifikasjon til bestemte formål, sakstyper eller alvorlighetsgrader. Forslaget innebærer at teknologien i praksis kan benyttes i alle tilfeller der politiet selv vurderer bruken som «strengt nødvendig», uten krav om:

- alvorlig kriminalitet
- konkret mistanke
- målrettethet tilsvarende KI-forordningen artikkel 26 nr. 10
- begrensninger i hvilke datakilder som kan benyttes

Selv om departementet fremholder at forslaget ikke utvider politiets innhentingshjemler, åpner det for biometrisk analyse av alt materiale politiet allerede har eller får lovlig tilgang til. Dette omfatter blant annet video- og bildemateriale fra offentlige og private kameraer, mobilopptak, droner, dashcams og åpent tilgjengelig materiale fra internett og sosiale medier.

Etter Teknas vurdering innebærer dette en betydelig risiko for formålsutglidning og en gradvis normalisering av svært omfattende biometrisk overvåkning, uten tilstrekkelige rettslige skranke.

4. PSTs bruk i forebyggende virksomhet

Tekna er særlig bekymret for at forslaget åpner for at PST kan benytte etterfølgende biometrisk fjernidentifikasjon i forebyggende virksomhet uten krav om forhåndsgodkjenning.

Forebyggende virksomhet kjennetegnes av uklare terskler og et vidt skjønnsrom, og er i utgangspunktet underlagt svakere rettssikkerhetsgarantier enn etterforskning. Når en så inngripende teknologi tillates brukt i dette sporet, uten forhåndskontroll og uten rapportering til Datatilsynet, mener Tekna at risikoen for uforholdsmessige personverninngrep øker betydelig.

Tekna vil også peke på at begrepet «forebygging» er uklart definert. Dette kan i ytterste konsekvens åpne for bruk av teknologien i prediktive sammenhenger, der personer risikerer å bli gjenstand for tiltak basert på antakelser om fremtidig atferd. Tekna mener dette reiser alvorlige rettssikkerhets- og menneskerettslige spørsmål.

5. Behov for sterkere kontrollmekanismer

Tekna ser positivt på at departementet foreslår en form for forhåndsgodkjenning i enkelte tilfeller, men mener at den foreslåtte ordningen er for snever og i praksis kan bli lite effektiv.

Kravet gjelder kun ved målrettet søk etter mistenkte eller dømte, og unntaket for «innledende identifikasjon» er vidt og uklart. Departementet erkjenner selv at skillet er vanskelig å praktisere, og at mye av dagens bruk vil falle utenfor godkjenningsordningen.

Tekna vil peke på at flere av Norges naboland har valgt en mer tilbakeholden og grundig tilnærming til bruk av etterfølgende biometrisk fjernidentifikasjon enn det som foreslås i høringsnotatet. Som det fremgår av høringsnotatet, har Danmark valgt å begrense politiets bruk av ansiktsgjenkjenning i ettertid til et

tidsavgrenset pilotprosjekt, med krav om evaluering før eventuell nasjonal utrulling. Den danske tilnærmingen legger dermed til rette for at erfaringer, personvernkonsekvenser og rettssikkerhetsmessige spørsmål vurderes før teknologien eventuelt tas i bredere bruk.

Videre fremgår det av høringsnotatet at Finland har foreslått en regulering der bruk av etterfølgende biometrisk fjernidentifikasjon som hovedregel skal underlegges forhåndsgodkjenning fra domstolene, med adgang til midlertidige beslutninger i hastetilfeller som i ettertid må forelegges retten. Etter Teknas vurdering representerer den finske modellen et mer hensiktsmessig og rettssikkert rammeverk for bruk av en teknologi som er særlig inngripende. Tekna støtter derfor en regulering som bygger på tilsvarende prinsipper, med uavhengig domstolskontroll som en sentral rettssikkerhetsgaranti.

6. Manglende krav til teknisk kvalitet og ikke-diskriminering

Tekna merker seg at høringsnotatet i liten grad adresserer teknologiske forhold knyttet til kvalitet, treffsikkerhet og risiko for diskriminering.

Forslaget stiller, for eksempel, ingen eksplisitte krav til:

- dokumentert treffsikkerhet
- testing for skjevheter i datagrunnlaget
- håndtering av feiltreff og falske positive
- menneskelig kontroll med og etterprøving av systemenes resultater
- åpen kildehenvisning for KI-generatorens resultater

Tekna mener det er uheldig at reguleringen av høyrisiko-KI ikke inneholder slike minimumskrav, særlig i lys av dokumenterte utfordringer knyttet til ansiktsgjenkjenningsteknologi internasjonalt.

7. Avsluttende merknader

Tekna mener samlet sett at forslaget ikke er tilstrekkelig utredet til å kunne vedtas i sin nåværende form. Etter Teknas vurdering bør departementet avvente videre fremdrift og sikre at det foreligger et mer fullstendig og kunnskapsbasert beslutningsgrunnlag. Dette forutsetter blant annet en grundig og helhetlig vurdering av personvern- og risikokonsekvenser, DPIA, ved bruk av etterfølgende biometrisk fjernidentifikasjon.

Videre mener Tekna at det er behov for å tydeligere materielle rammer for bruken av teknologien, herunder klare terskler knyttet til formål og alvorlighetsgrad, samt presise begrensninger i hvilke datakilder som kan benyttes. I tillegg må grensen mellom "innledende identifikasjon" og søk etter allerede mistenkte og dømte presiseres og eksemplifiseres i lovgivningen.

Tekna mener også at bruk av teknologien i PSTs forebyggende virksomhet må underlegges streng forhåndskontroll og klare rettssikkerhetsgarantier. Gitt tiltakets inngripende karakter vurderer Tekna det som mer hensiktsmessig at godkjenningskompetansen legges til domstolene for å sikre uavhengig kontroll.

Tekna vil videre understreke behovet for eksplisitte krav til teknisk kvalitet, herunder håndtering av feiltreff og risiko for diskriminering, samt etablering av reelle og etterprøvbare mekanismer for ekstern kontroll og transparens.

Tekna mener det er nødvendig å utvise tilbakeholdenhet i denne saken. Et regelverk av denne karakteren må være robust også over tid, og bør ikke vedtas før personvernensyn, rettssikkerhet og tillit er tilstrekkelig ivaretatt.

Med vennlig hilsen



Sonja Lovise Berg
konst. generalsekretær