Til justisdepartementet

5. januar 2022

Høringssvar: - Endringer i politiloven og politiregisterloven mv. – 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 93 000 medlemmer. Våre medlemmer har mastergrad eller mer fra tekniske og naturvitenskapelige fagområder.

Vi viser til høringsbrev av 7. oktober 2021 fra Justis- og beredskapsdepartementet. Brevet gjelder forslag om endringer i politiloven, politiregisterloven og politiregisterforskriften mv. og PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon

Tekna anerkjenner PST sitt behov for å tydeligere mandatet, samt behov for nye verktøy for å møte digitale utfordringer. Forslaget vil kunne bidra til at PST kan kartlegge trusselbildet bedre og avdekke skjulte trusselaktører mer effektivt, noe som åpenbart er positivt.

Vi er imidlertid bekymret for at forslaget slik det er utformet, vil kunne medføre at mange blir mer forsiktige med å ytre seg på nettet, den såkalte nedkjølingseffekten. Forslaget kan også bidra til å uthule noe av tankegangen i GDPR ved å samle inn info som isolert sett ikke er nødvendig for formålet. Videre er det en fare for at data (rådata eller analyser og sammenstilte data) blir misbrukt, kommer på avveie, og/eller blir misbrukt av tredjeparter. Videre er det en fare for formålsutglidning, slik at data (inkl. analyser og andre sammenstilte data) på sikt vil brukes på en annen måte enn det som er tenkt i dag.

Åpent tilgjengelig informasjon

PST skal i prinsippet kun samle inn info som ligger åpent ute på nettet, ikke info fra lukkede nettsteder eller privat kommunikasjon. Det fremgår av forslaget at det ikke skal gis generell adgang til å følge med på enkeltpersoners aktivitet, bare grupper eller grupperinger. Informasjonen som innhentes skal holdes sperret og adskilt.

Høringsnotatet viser til etterretningsloven § 6-2 hvor det fremgår av annet punktum at informasjon ikke er åpent tilgjengelig dersom tilgang krever aktiv fordekt opptreden eller forsering av passord eller lignende beskyttelsesmekanismer. Punktet med "aktiv fordekt oppførsel" er ikke inkludert i lovforslaget. Vil det innebære at PST får adgang til å registrere seg med noen annens identitet? I dette henseendet går forslaget da mye lenger enn etterretningstjenesten har adgang til.

Definisjonen av hva som anses som åpen informasjon er bredt definert. Det fremgår av høringsnotatet at informasjon må regnes som åpen selv om det kreves registrering eller abonnement, f.eks. kontoer på sosiale medier. Det mørke nettet og kryptert informasjon (f.eks. en kryptert fil som er lastet opp på et nettsted) regnes også som åpen informasjon.

Åpen informasjon vil ikke bare være informasjon man har lagt ut selv, men også informasjon andre har lagt ut uten at man selv har godkjent dette. Med lang lagringstid kan man også oppleve at

informasjon som er slettet fortsatt vil være lagret. Det vil da vært tilgjengelig for etterretningen selv om det ikke lenger er åpent tilgjengelig på nettet for en selv eller andre.

Forslaget vil også omfatte informasjon fra systemer som er hacket og delt på dark web, selv om dette er informasjon som aldri var ment å være offentlig tilgjengelig. Det oppstår da spørsmål om hvordan man har man tenkt å skille mellom informasjon som er lovlig og lovstridig lagt ut.

Lagring og sletting

I forslaget foreslås at data kan lagres i 15 år, uten at valg av frist er nærmere begrunnet. Ved langvarig lagring vil dataene kunne anses tatt ut av tidligere kontekst, være lite representative, og kan for eksempel være dårlig formulerte kommentarer på en nettside som man selv har slettet eller redigert etter kort tid. Slik langvarig lagring harmonerer ikke godt med for eksempel retten til å bli glemt og behandlingsansvarliges plikt til å sørge for at informasjonen er korrekt og oppdatert. Tidshorisonten kan fremstå uforholdsmessig lang, og dette kan oppfattes som en form for langvarig overvåking. Tekna mener på denne bakgrunn at 15 år er for lang lagringstid.

Tekna stiller også spørsmål ved hvilket tidspunkt man legger til grunn for tidsberegningen. Hva betyr det at data skal slettes etter en gitt periode? Handler det om hvor lenge det er siden dataene ble hentet, eller siden publisering? Eller hvor lenge det er siden data eventuelt ble fjernet fra nett? Ikke alle datakilder har en dato assosiert til dette. Hva med likes på Facebook og kommentarer i en Reddit-tråd? Hvordan skal dette implementeres i praksis?

Vi mener videre at mellomlagret informasjon må slettes når bruken i et etterretningsoppdrag, forebyggende sak eller etterforskning er ferdig. Slik høringsnotatet beskriver bruken er dette spesielt viktig ved etterretningsoppdrag, ettersom disse inneholder informasjon om langt flere personer

Dataene kommer til å inneholde mye personopplysninger fra mange. Det bør derfor stilles krav til lagring av data. Bør man kreve samme lagringspolicy som for PII-data? Hvilke begrensinger må gjelde for bruk av skyen? Skal det være servere i Norge? Må logger av tjenester som prosesserer dataene også være i Norge? Dette er spørsmål som vi mener bør avklares i det videre arbeidet med lovforslaget.

Analyse av data

Som påpekt av EOS-utvalget i deres høringsuttalelse, vil bruk av automatiserte analyseverktøy generere nye data om enkeltpersoner, som personen ikke har valgt å dele åpent. Vi kan ikke se at ulike problemstillinger knyttet til bruk av automatiserte analyseverktøy er utredet i forslaget. Bruken i etterretning og ved opprettelsen av en forebyggende sak er etter vårt syn mer problematisk enn bruken i forebyggende sak eller etterforskning. I siste tilfelle har man allerede en begrunnet mistanke til personene som overvåkes.

Vi savner også en klargjøring av forholdet til personopplysningsloven artikkel 22, som sikrer den enkeltes rett til å ikke være gjenstand for avgjørelser som utelukkende baserer seg på automatisert saksbehandling. Dersom PST kommer over opplysninger om en person som det er grunn til å overvåke kan det anses som profilering som er problematisk i henhold til denne bestemmelsen. Det bør avklares i loven om det gis adgang til slik profilering.

Høringsnotatet gir ikke noe klart svar på om dataene som innhentes kan bli beriket med andre data som PST allerede har. Det fremstår som uklart om dette blir dekket av begrepet «sperret». Selv om dataene ikke hentes målrettet mot enkeltindivider, er det mulig å de-anonymisere personer ved å koble alle åpne datakilder, slik at man kan lage et høy-oppløsningsbilde av mange.

Det fremgår ikke av høringsnotatet hvordan man tenker å plukke ut, filtrere, analysere og lagre relevant informasjon fra alle relevante deler av internett, med fortløpende endringer, og samtidig holde informasjonen mest mulig korrekt og representativ. PSTs formål med dataene skiller seg fra formålene som de individuelle datakildene har for dataene, og dataene vil bli gjenstand for behandling (blant annet utvalg og filtrering) før PST lagrer dem. Denne behandlingen vil kunne gjøre at informasjonen tas ut av kontekst og ikke lenger er representativ. Et system som skal gjøre utdrag fra hele internett, vil nødvendigvis bare kunne lagre utdrag og «bruddstykker» av all relevant informasjon

Anskaffelse av analyseverktøy kan i seg selv gi grunn til bekymring. Bruk av verktøy som er utviklet og driftes av aktører i andre land, åpner opp en rekke spørsmålsstillinger knyttet til GDPR, dataeierskap med mer, jf. blant annet utfordringer som New-York-politiet har opplevd med å flytte data ut fra et kommersielt system. Tekna mener derfor at det bør være åpenhet om valg av leverandør av analyseverktøy.

Rett til innsyn

Rett til innsyn og rett til å rette opp falsk informasjon er viktig. Men det er generelt ikke innsynsrett i opplysninger som behandles av PST. Videre ønsker man unntak fra kravene til at opplysningene som behandles skal være relevante, korrekte og oppdaterte, ut over at informasjonen skal være en korrekt kopi av det PST har funnet på det åpne nettet. Men «korrekt kopi» av begrenset, utvalgt informasjon kan likevel gi et feil helhetsbilde. Det vises i den forbindelse til at åpen tilgjengelig informasjon også vil omfatte uriktig informasjon som er lagt ut av andre.

Sikkerhet

Det fremgår av høringsnotatet at opplysningene skal «sperres» slik at kun personer med særskilt bemyndigelse skal få adgang. Dette omtales som en sentral sikkerhetsmekanisme. Vi savner imidlertid en nærmere vurdering av om denne sikkerhetsmekanismen er tilstrekkelig.

I høringsnotatet foreslås det en ny bestemmelse i § 21-8 om at all bruk av opplysninger skal registreres og kunne spores. Dette for å kunne kontrollere at søkene er lovlige. I det videre arbeidet med forslaget bør det avklares nærmere hva som ligger i dette. Skal man lagre alle søk og alle resultater knyttet til søk som gjennomføres?

Tilsyn og åpenhet

EOS- utvalget gis i høringsnotatet ansvar for tilsynet. Vi merker oss at tilsynet i sin høringsuttalelse finner det nødvendig å avgrense sitt ansvar ved å påpeke at deres kontroll er stikkprøvebasert og at de ikke er en garantist for at feil kan skje. Tekna mener dette ikke er tilstrekkelig, og mener det er viktig at utvalget får kapasitet og ressurser til å utføre tilsynsrollen på en god måte.

Det fremgår av høringsnotatet at investeringene i første omgang kan beløpe seg til 2 million kroner for økt lagring, men at det ikke eksisterer konkrete planer for å ytterligere investeringer.

Samtidig foreslås det en regel i § 21-8 om at all bruk av opplysninger skal registreres og kunne spores, jf. kap 5.2.7. Dette kan umulig bli oppfylt innen forventet investering på 2 million

Mekanismene som er foreslått for kontroll og etterprøving er ikke tilstrekkelige. Det fremstår også som uklart om sikringsmekanismer kommer på plass før man starter innhenting av data. Det bør derfor tydeliggjøres hvordan man skal sikre at kontrollmekanismene er på plass før datainnsamling

starter, og avklares hvordan man kan sikre en bedre kontroll enn EOS-tilsynet selv mener de har anledning til å gjennomføre.

Videre er det viktig å sikre åpenhet om bruk av leverandører og innretning av algoritmer.

Valg av verktøy og algoritmer bør gjøres med fokus på tilregnelighet og transparens. Algoritmer kan deles i to grupper: glass-box og black-box. En algoritme er glass-box hvis man kan forstå de interne mekanismer i bruk fra input til output. Ellers er algoritmen black-box. Black-box algoritmer er enkle å bygge, men vanskelig å analysere, forklare og fikse for bias, dermed blir tilsyn vanskelig.

Algoritmen som skal benyttes av PST er så viktig for samfunnet og potensielt inngripende for innbyggerne at metodikken bør være forståelig (etterprøvbar) av andre enn kun de som har produsert den. Tilgangen til informasjonen som innhentes og sammenstilles må være begrenset, men informasjon om hvordan algoritmen er satt sammen og hvilken funksjonalitet som benyttes bør være åpen. Brukere av verktøyene må også få nødvendig informasjon om innretningen av algortitmen for å kunne anvende resultatene på en riktig måte.

Åpenhet rundt tilsynets arbeid er også viktig. Vi mener derfor at det bør vurderes å gjøre tilsynsanalysene som utføres åpne tilgjengelig for allmenheten. Det er blant annet viktig å etterse at restriksjoner som finnes i produksjonsmiljøer, også gjelder øvrige miljøer (utvikling, test, stage) for å unngå misbruk fra utviklere, testere, osv. Et eksempel på en sjekkliste fra EU kommisjonen kan finnes i https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60440

Oppsummering

Tekna anerkjenner PST sitt behov for å tydeliggjøre mandatet og få nye verktøy for å møte digitale utfordringer og løse samfunnsoppdraget.

Vi savner imidlertid en grundigere redegjørelse for hvilke verktøy og metoder som skal benyttes ved innhenting, og en utredning av konsekvensene av at PST kan bruke innsamlet informasjon til både etterretning, forebygging og etterforskning. Vi håper derfor at man ser nærmere på dette i det videre arbeidet med lovforslaget.

Tekna er kritisk til den lange lagringstiden som foreslås i høringsnotatet. Videre mener vi mekanismene for etterprøving og kontroll ikke er gode nok. Andre mekanismer må på plass, EOS-utvalget må styrkes og det bør sikres åpenhet om valg av leverandører, metodikk og innretning av algoritmer, samt tilsynsanalyser. Verktøyet PST ønsker er kraftfullt, og det er derfor viktig at man gjennom tydelige avgrensninger, åpenhet og gode kontrollmekanismer reduserer risikoen for misbruk og feil.

Med vennlig hilsen
Tekna – Teknisk-naturvitenskapelig forening

Line Henriette Holten
generalsekretær