



Justitiedepartementet
Enheten för lagstiftning om allmän
ordning och säkerhet

Remissvar över betänkandet Säkerhetspolisens behandling av personuppgifter (SOU 2025:49)

Ju2025/00954

Institutet för mänskliga rättigheter (institutet) yttrar sig över betänkandet **Säkerhetspolisens behandling av personuppgifter (SOU 2025:49)**. Yttrandet sker inom ramen för institutets uppgift att främja säkerställandet av de mänskliga rättigheterna i Sverige, med utgångspunkt i våra grundlagar och för Sverige folkrättsligt bindande förpliktelser inom området mänskliga rättigheter. Institutet har även en särskild roll som oberoende nationell mekanism enligt artikel 33.2 i FN:s konvention om rättigheter för personer med funktionsnedsättning.

Sammanfattning

Mot bakgrund av det säkerhetsläge och de säkerhetshot som Sverige står inför delar institutet bedömningen i betänkandet att den nuvarande lagstiftningen kring Säkerhetspolisens behandling av personuppgifter behöver uppdateras och anpassas till dagens läge. Genom förslagen i betänkandet innebär detta en ökad personuppgiftsbehandling som får konsekvenser för mänskliga rättigheter, särskilt skyddet för den personliga integriteten och rätten till privat- och familjeliv.

Institutet **tillstyrker** att det införs en proportionalitetsprincip i den föreslagna lagen om Säkerhetspolisens behandling av personuppgifter. För att tillförsäkra att proportionalitetsbedömningen även inkluderar en bedömning om behandlingen är nödvändig föreslår vi att paragrafen förtydligas på följande sätt: ”All behandling av personuppgifter ska vara **nödvändig och proportionerlig**.”

Institutet **tillstyrker** att det i den föreslagna lagen om Säkerhetspolisens behandling av personuppgifter särskilt regleras kring förutsättningarna för Säkerhetspolisens användning av personuppgifter för tekniska utvecklingsändamål. Vi **ser dock med oro** på risken att sådan teknisk utveckling

som beskrivs kan leda till användande av typer av AI-modeller som innefattar social poängsättning och motsvarande. Vi vill därför **betona** vikten av att den föreslagna proportionalitetsbedömningen ska genomföras inför varje tänkt nytt behandlingsområde.

Institutet **tillstyrker** även att det i den föreslagna lagen om Säkerhetspolisens behandling av personuppgifter införs en bestämmelse om att automatiserade beslut utan mänsklig inverkan ska vara förbjuden.

Gällande den föreslagna lagen om Säkerhetspolisens behandling av personuppgifter i särskilda uppgiftssamlingar **föreslår** vi att ett säkerhetsklassat ombud ska vara del av tillståndprocessen, snarare än Säkerhets- och integritetsskyddsnämnden.

Övergripande synpunkter

Sverige befinner sig i ett alltmer komplext säkerhetsläge med den hotbild det medför genom till exempel påverkansoperationer och cyberattacker samt extremistiska budskap som sprids via digitala plattformar. Dagens ökade informationsmängder och tekniska utveckling kräver effektiva verktyg. Institutet delar därför bedömningen i betänkandet att den nuvarande lagstiftningen kring Säkerhetspolisens behandling av personuppgifter behöver uppdateras och anpassas till dagens läge.

Med detta följer dock en ökad personuppgiftsbehandling, vilket får konsekvenser för mänskliga rättigheter såsom skyddet för den personliga integriteten och rätten till privat- och familjeliv såsom de skyddas i regeringsformen, europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och FN:s konvention om medborgerliga och politiska rättigheter.¹ Utredningens förslag innebär att en betydligt större mängd av integritetskänsliga uppgifter kan komma att behandlas, vilket i sin tur medför en ökad risk för kränkningar och inskränkningar i enskildas personliga integritet.

¹ 2 kap. 6 § 2 p regeringsformen, 2 kap. 20 § regeringsformen, artikel 8 Europakonventionen, artikel 17 FN:s konvention om medborgerliga och politiska rättigheter.

Skyddet av den personliga integriteten och rätten till privat- och familjeliv är rättigheter som får inskränkas enligt de kriterier som regeringsformen och konventionerna ställer upp. Åtgärderna måste vara nödvändiga, ha stöd i lag och vara proportionerliga. En grundlig analys behöver därför alltid göras över hur förslagen förhåller sig till de mänskliga rättigheterna enligt dessa kriterier.

Institutet välkomnar att det i betänkandet genomgående gjorts en grundlig analys av hur förslagen förhåller sig till relevanta rättigheter samt de resonemang som förs om behövda rättssäkerhetsgarantier. Vi välkomnar även hur det i betänkandet resoneras kring hur förslagen indirekt påverkar yttrandefriheten och andra opinionsfriheter genom den så kallade avkylningseffekten.

I betänkandet lyfts Europadomstolens praxis fram, framför allt i förhållande till signalspaning och målet Centrum för Rättvisa mot Sverige² och dess relevans för Säkerhetspolisens behandling av stora informationsmängder. Institutet delar bedömningen i betänkandet om att denna praxis är vägledande, och vill särskilt lyfta fram vikten av att de rättssäkerhetsgarantier som Europadomstolen anger behöver finnas på plats och fortsatt finns med i tillämpningen av lagstiftningen.

Proportionalitetsprincipen i säpodatalagen

Ett av de kriterier som behöver vara uppfyllda för att inskränka skyddet för den personliga integriteten och rätten till privat- och familjeliv är att åtgärden som föreslås ska stå i proportion till de rättighetskränkningar som riskeras. I detta ligger även en bedömning av om åtgärden är nödvändig för att uppnå syftet och att det inte finns några andra mindre ingripande åtgärder som kan genomföras i stället.

Mot bakgrund av bestämmelserna i artikel 5.1 i Europarådets dataskyddskonvention 108+ (Convention for the protection of individuals with regard to the processing of personal data 108+) om att all personuppgiftsbehandling ska vara proportionerlig, föreslås det i betänkandet att en uttrycklig proportionalitetsprincip införs i säpodatalagen. Institutet **tillstyrker** detta förslag eftersom det också i lagstiftningen förtydligar de

² Centrum för Rättvisa mot Sverige, no 35252/08, 25 maj 2021.

intresseavvägningar som krävs för att genomföra en åtgärd som annars kan riskera att kränka mänskliga rättigheter. Det är också i linje med andra bestämmelser som lyfter proportionalitetsprincipen såsom 2 kap. 21 § regeringsformen och 1 kap. 5 § förvaltningslagen.

Det som däremot saknas i förslaget om proportionalitetsprincipen i den föreslagna 2 kap. 1 § lagen om Säkerhetspolisens behandling av personuppgifter (säpodatalagen) är tydligheten att en proportionalitetsbedömning också inkluderar en bedömning om åtgärden är nödvändig och att mindre ingripande åtgärder inte är tillräckliga. Detta syns till exempel i 2 kap. 21 § regeringsformen där det står att en begränsning aldrig får ”gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den”. Vikten av att bedöma om en åtgärd också är nödvändig framgår inte av författningskommentaren i betänkandet.

För att tydligt visa att en bedömning av om en behandling är nödvändig också måste göras i proportionalitetsbedömningen föreslår vi att skrivningen i 2 kap. 1 § säpodatalagen skrivs: ”All behandling av personuppgifter ska vara **nödvändig och proportionerlig**.”

Synpunkter på specifika förslag

8.1.2 Lagens tillämpningsområde

Personuppgiftsbehandling för teknisk utveckling bör ske med stöd av säpodatalagen

Det framhålls i betänkandet att Säkerhetspolisen har ett stort behov av att kunna utveckla och testa olika IT-system och tekniska förmågor för informationshantering, där framtagande av AI-modeller utgör en särskild gren. Nuvarande lagstiftning ger inte Säkerhetspolisen någon möjlighet att samla in uppgifter enbart för teknikutveckling. Den innebär även att användandet av autentiskt material för detta syfte är begränsat eftersom det är en tidskrävande process.

Utredningen bedömer att det finns skäl för Säkerhetspolisen att kunna inhämta och behandla personuppgifter för att säkerställa en god teknisk förmåga, men att detta måste ske transparent och inom lagens ram. Det bedöms därför finnas skäl att uttryckligen reglera teknisk utveckling som en verksamhet där Säkerhetspolisen får behandla personuppgifter. Genom denna reglering tydliggörs att personuppgifter kan komma att behandlas i verksamheten utanför det uttryckliga syftet om brottsbekämpning.

Institutet är **positiva** till att användandet av personuppgifter för teknisk utveckling regleras uttryckligen då det skapar tydlighet och transparens. Vidare ser vi det som positivt att det tydliggörs och avgränsas att personuppgifter som används enbart för teknikutveckling inte får användas för något annat ändamål och att behandlingen som regel ska upphöra i samband med att ändamålet uppnåtts.

8.4.6 Övrig brottsbekämpande verksamhet som rör nationell säkerhet

Användning för teknikutveckling – risker i användandet

I betänkandet föreslås att behandling av personuppgifter som initialt skett för andra ändamål även ska få ske för tekniska utvecklingsändamål. I dessa fall föreslås att samma proportionalitetsprincip som ska vara vägledande för övrig behandling ska tillämpas även på behandling för detta ändamål. Föreslagen proportionalitetsprincip begränsar bland annat vilket slag och hur många uppgifter som får behandlas, hur länge och på vilket sätt. Att intrånget i enskilda och allmänna intressen måste vägas mot ändamålet med behandlingen påverkar bland annat valet av uppgifter och hur många som får tillgång till dem. Institutet **vill understryka vikten** av att sådan proportionalitetsbedömning görs vid varje tillfälle då syftet med behandlingen ändras. Behandling av känsliga personuppgifter och ett intrång i en enskilds intressen kan vara motiverat i en proportionalitetsbedömning utifrån ett brottsbekämpande syfte. Vid motsvarande proportionalitetsbedömning där syftet med behandlingen är utvecklingsändamål måste intrånget i enskildas och allmänna intressen ges en större tyngd.

Institutet **ser med viss oro** på att användandet av personuppgifter för tekniska utvecklingsändamål även innebär en ökad risk för utveckling av tekniska/AI-modeller som kan leda till indirekt social poängsättning och liknande mönster. Som har konstaterats i utredningen är Europaparlamentets förordning (EU) 2024/1689 om artificiell intelligens (den s.k. AI-förordningen eller AI-act) inte direkt tillämplig på Säkerhetspolisens verksamhet.³ Vi vill dock peka på att det är lämpligt att ta vägledning av de principer som ges till uttryck i sagda förordning. Det framgår bland annat av art. 5 c) att användning av AI-system för ”utvärdering eller klassificering av fysiska personer eller grupper av personer under en viss tidsperiod på grundval av deras sociala beteende eller kända, uttydda eller förutsedda personliga eller personlighetsrelaterade egenskaper, med en social poängsättning” utgör förbjuden användning om den leder till skadlig eller ogynnsam behandling av vissa fysiska personer eller grupper:

- i sociala sammanhang som saknar koppling till de sammanhang i vilka berörda data ursprungligen genererades eller samlades in.
- som är omotiverad eller oproportionerlig i förhållande till personernas sociala beteende eller till hur allvarligt beteendet är.

Vidare framgår av art. 5 d) att användning av AI-system för riskbedömningar av fysiska personer i syfte att bedöma eller förutse risken för att en fysisk person begår ett brott, uteslutande grundat på profileringen av en fysisk person eller på en bedömning av deras personlighetsdrag och egenskaper, utgör förbjuden användning.

Då Säkerhetspolisen genom sitt uppdrag har ett intresse av att kunna identifiera egenskaper och mönster som kan ge en indikation för riskbedömningar understryker vi risken för ändamålsglidning i utveckling av tekniska verktyg/modeller och att detta inte får leda till den typen av generaliserande och kategoriserande bedömningar som det ges uttryck för i ovan exempel.

³ Art. 2.3 Europaparlamentets förordning (EU) 2024/1689 om artificiell intelligens; ”Denna förordning är inte tillämplig på områden som inte omfattas av unionsrättens tillämpningsområde och ska under alla omständigheter inte påverka medlemsstaternas befogenheter när det gäller nationell säkerhet, oavsett vilken typ av enhet som av medlemsstaterna har anförtrots uppgiften i fråga om dessa befogenheter”.

Institutet vill även betona vikten av att säkerställa att informationen som eventuella AI-modeller ”tränas” på avser alla typer av människor så att utfallet inte leder till diskriminering.⁴ I frågan om användning av ansiktsgenkänningsteknik har FN:s rasdiskrimineringskommitté särskilt framhållit att stater noggrant ska utvärdera potentiella konsekvenser för de mänskliga rättigheterna innan de använder ansiktsgenkänningsteknik som kan leda till felidentifieringar på grund av bristande representation i insamlade data. Tekniken som ska användas bör vidare testas i en pilotfas och under övervakning av ett oberoende tillsynsorgan innan den börjar användas. De anger också att stater bör säkerställa att algoritmerna inom brottsbekämpning utformas med transparens och att forskare och civilsamhälle ges möjlighet att granska koden. Vi menar att samma typ av överväganden och säkerställande bör tillämpas i detta fall.⁵

Tillsyn och lagringstid

Mot bakgrund av vad som anförts ovan och de risker institutet ser i att teknikutveckling kan innebära att personuppgifter används på ett sätt som kan riskera att skapa system som grundar en form av social poängsättning eller ogynnsam behandling av vissa personer/grupper, så ser institutet positivt på att utredningen betonar att för att lagens syfte ska uppnås är det av vikt att den tillsyn som ska ske av Säkerhetspolisens användning av personuppgifter blir tillräcklig. Institutet välkomnar därmed utredningens förslag om både stärkta befogenheter för tillsynsmyndigheten, samt att Säkerhetspolisen blir skyldiga att vidta de tekniska åtgärder som krävs för att tillsyn ska kunna bedrivas effektivt. Institutet vill betona att de föreslagna skyldigheterna för Säkerhetspolisen avseende just AI-system och modeller är en förutsättning för att tillsynsmyndigheten ska kunna säkerställa att teknikutvecklingen enbart sker inom ramen för en proportionerlig och rättssäker personuppgiftsbehandling som är förenlig med grundläggande fri- och rättigheter.

⁴ Webbälla Integritetsskyddsmyndigheten [Vägledning: Ansiktsgenkänning och GDPR | IMY](#)

⁵ FN:s rasdiskrimineringskommitté, General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials, UN Doc. CERD/C/GC/36, 17 december 2020, p. 59-60.

Vi ställer oss vidare positiva till att utredningen föreslår en tydlig avgränsning i en markant kortare längsta behandlingstid när syftet med behandlingen är utvecklingsändamål.

8.19.1 Det bör vara förbjudet med automatiserat beslutsfattande som påtagligt påverkar den enskilde

Institutet delar utredningens bedömning att personuppgifter inte ska få användas för att fatta automatiserade beslut som har en betydande påverkan på en person. Det är viktigt att automatiska processer inte är ensamt utslagsgivande för ett beslut utan att den mänskliga beslutsfattaren ska göra egna bedömningar och avvägningar utifrån materialet. Institutet **tillstyrker** den föreslagna bestämmelsen.

9. En ny lag för Säkerhetspolisens behandling av stora informationsmängder

Utredningen föreslår en ny lag som reglerar Säkerhetspolisens behandling av stora informationsmängder som ofta inledningsvis är ostrukturerade och där granskning enligt såpotalagen inte är möjlig. Jämförelserna som görs med signalspaning är här relevanta, tillsammans med praxis från Europadomstolen, särskilt domen Centrum för Rättvisa mot Sverige. Där betonas att rättighetskränkningen ökar ju längre in i processen man kommer och det är därför avgörande att så kallade ”end to end safeguards” finns på plats för att garantera rättssäkerhet för den enskilde och motverka godtycklighet. Genom den föreslagna lagen föreslås flera sådana rättssäkerhetsgarantier, såsom krav på tillstånd och tillsyn. Däremot föreslås i betänkandet att Säkerhets- och integritetsskyddsnämnden som tillsynsmyndighet ska delta i tillståndsbedömningen för att behandla uppgifter ur uppgiftssamlingen. Institutet **delar inte** denna bedömning. Vi anser i stället att ett säkerhetsklassat ombud kan fylla en bättre funktion för att tillvarata skyddet för individers personliga integritet och rätt till privat- och familjeliv. Institutet förde även ett sådan resonemang i remissvaret över delbetänkandet Signalspaning i försvarsunderrättelseverksamhet - frågor med anledning av Europadomstolens

dom (SOU 2023:51). Ett sådant ombud kan även bidra till att öka allmänhetens tilltro till systemet, något som också Europadomstolen nämner som viktigt i sin dom.

Ärendets handläggning

Detta remissvar har beslutats av direktör Fredrik Malmberg och föredragits av utredaren/juristen Amelie Sällfors och förvaltningsjuristen Christina Håkansson Modin. I den slutliga beredningen har även enhetschefen Eva Glückman, utredaren/juristen Anna Rosenmüller Nordlander och ställföreträdande direktör Charlotte Palmstierna deltagit.

Fredrik Malmberg, direktör