

Dnr Ju2025/00676
Justitiedepartementet

YTTRANDE ÖVER BETÄNKANDET POLISENS ANVÄNDNING AV AI FÖR ANSIKTSIGENKÄNNING I REALTID (DS 2025:7)

SAMMANFATTNING

Civil Rights Defenders har i sitt tidigare remissvar angående *Ds 2024:11 om förbättrade möjligheter för polisen att använda kamerabevakning* avstyrkt förslaget om att Polismyndigheten och Säkerhetspolisen ges möjlighet att i vissa fall få tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål. Vi välkomnar att regeringen har öppnat upp för en mer omfattande och djupgående analys av hur förslaget påverkar mänskliga rättigheter men anser inte att proportionalitetsbedömningen som har gjorts är riktig. Med anledning av detta är Civil Rights Defenders inställning till utredningens förslag följande:

- Civil Rights Defenders **avstyrker** utredningens förslag om att Polismyndigheten och Säkerhetspolisen ges möjlighet att i vissa fall få tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål.

ALLMÄNNA SYNPUNKTER

Civil Rights Defenders har granskat utredningens förslag och bakomliggande resonemang utifrån Sveriges internationella åtaganden att respektera och garantera mänskliga fri- och rättigheter.

Under de senaste åren har vi sett en rad straffskärpningar och flera nya tvångsmedel, vilka sammantaget har lett till en mer omfattande övervakning under förundersökningar och i brottsförebyggande syfte. Det är inledningsvis viktigt att understryka att de genomgripande förändringar som genomförts på området under mycket kort tid har gjort det svårt att överblicka regelverket och dess konsekvenser.¹ Kameraövervakning utan föregående tillstånd, hemlig dataavläsning och preventiv avlyssning är numera möjligt. För närvarande bereds dessutom förslag om utökad tillgång till elektroniska kommunikationstjänster (SOU 2023:22), fler preventiva tvångsmedel (prop. 2023/24:117) och utökad kamerabevakning av polisen (Ds 2024:11) samt minskad sekretess inom polisen (Ju 2025/00814). Generellt sett möjliggör dessa reformer en storskalig insamling, delning och analys av data.²

¹ MR-institutet, Remissvar Utökade möjligheter att använda hemliga tvångsmedel Ju2022/01563 (2022), s. 4.

² Marie Eneman, Vad betyder den ökade övervakningen för vårt samhälle? (Göteborgs universitet, 2023).

Lagrådet har konstaterat att det samlade regelverket blivit mycket komplicerat, vilket skapar tillämpningssvårigheter och riskerar att underminera rättssäkerheten.³ När så många reformer genomförs i snabb takt blir det särskilt angeläget att granska hur detta påverkar de mänskliga rättigheterna och den personliga integriteten.⁴ Civil Rights Defenders välkomnar att regeringen tillsatt en utredning som ska ge en samlad översyn av reglerna om hemliga och preventiva tvångsmedel, men ser med oro på att förevarande utredning ändå tillsatts.⁵

Även om det finns stora förväntningar på att övervakning ska öka tryggheten i samhället, kan det också få konsekvenser för utövandet av fri- och rättigheter och det demokratiska samhället i stort.⁶ Enligt MR-institutets enkätundersökning *Kunskap, attityder och uppfattningar om mänskliga rättigheter i Skandinavien*, genomförd under 2024, har ökad statlig övervakning en kylande effekt på yttrande- och åsiktsfriheten.⁷ Den kan dessutom avskräcka från användning av offentliga rum för mötesfrihet, demonstrationsfrihet och åsiktsbildning på ett sätt som i längden förändrar deras karaktär.⁸

Den ökade övervakningen motiveras inte sällan politiskt av en brottsutveckling som sägs skapa otrygghet långt utanför den kriminella miljön. Det är dock viktigt att notera att användningen av hemliga tvångsmedel och övervakning inom brottsbekämpning ofta bygger på en föreställning om ett "vi" och "dem". Samhället tenderar att acceptera oproportionerliga inskränkningar av grundläggande rättigheter när det upplevs som att de endast drabbar "dem" och inte "oss". Detta förklarar varför många i Sverige inte tycks oroa sig för integritetsrisker kopplade till brottsbekämpande myndigheters användning av övervakning.⁹ När detta resonemang tillåts prägla kriminalpolitiken finns en risk för att inskränkningar normaliseras och därefter eskalerar. Därför har staten ett särskilt ansvar att värna om mänskliga rättigheter för samtliga invånare, också i kampen mot brottslighet.¹⁰

Att ytterligare komplicera regelverket genom att tillåta användning av AI-ansiktsgenkänningsystem i realtid, trots Lagrådets varningar¹¹ och de allvarliga riskerna för grundläggande rättigheter, är ett steg i fel riktning. Det är inte förenligt med rättsstatens principer att införa lagstiftning som inskränker individens rättigheter utan en analys av den samlade påverkan på den personliga integriteten. Därtill är det mycket svårt att föreställa sig ett samhälle där biometrisk ansiktsgenkänning med hjälp av AI skulle bidra till ökad trygghet.

Civil Rights Defenders har kommenterat de delar av förslaget där vi har synpunkter.

³ Lagrådet, Utdrag ur protokoll vid sammanträde 18 oktober 2024, Hemlig dataavläsning mot allvarliga brott, s. 2–3.

⁴ MR-institutet, *Årsrapport 2025*, s. 15.

⁵ William Eriksson, *Samlad översyn av hemliga tvångsmedel ska göras* (Dagens Juridik, 2025).

⁶ Marie Eneman, *Vad betyder den ökade övervakningen för vårt samhälle?* (Göteborgs universitet, 2023).

⁷ MR-institutet, *Årsrapport 2025*, s. 11.

⁸ Hille Koskela, *The gaze without eyes': video-surveillance and the changing nature of urban space* (2000).

⁹ Marie Eneman och Jan Ljungberg, **Välkommen till det digitala övervakningssamhället*.

¹⁰ Dennis Martinsson, *Trender och tendenser i den samtida straffrättsanvändningen – sett genom åtgärder mot terroristrelaterad och gängrelaterad brottslighet* i *Teori och politik – straffrätt i omvandling* (2022), s. 264.

¹¹ Lagrådet, Utdrag ur protokoll vid sammanträde 18 oktober 2024, Hemlig dataavläsning mot allvarliga brott, s. 2–3.

NÄRMARE OM UTREDNINGENS FÖRSLAG

5 Polisen ska ges möjlighet att använda AI-system för ansiktsgenkänning i realtid

- Civil Rights Defenders avstyrker utredningens förslag om att Polismyndigheten och Säkerhetspolisen ges möjlighet att i vissa fall få tillstånd att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål.

En ny FN-rapport uttrycker oro över den växande övervakningen av offentliga platser.¹² Tidigare praktiska begränsningar av övervakningens omfattning har undanröjts genom storskalig automatiserad datainsamling och -analys, nya digitaliserade identitetssystem samt omfattande biometrisk databaser.¹³ AI-baserade analysfunktioner ökar kapaciteten för ansiktsgenkänning och möjliggör även identifiering av beteenden som kan tolkas som misstänkta, vilket FN:s människorättsråd pekar ut som bland de mest problematiska funktionerna i moderna videoövervakningssystem.¹⁴ Integritet och privatliv är rättigheter som påverkar vår möjlighet att utöva nästan alla andra rättigheter, som yttrandefrihet, föreningsfrihet, religionsfrihet, politiska val, tillgång till sjukvård, utbildning och ett familjeliv. De är det skydd inom vilket vi formar våra tankar och vår identitet.

I *Integritetsskyddskommitténs* utredning från 2007 om kartläggning och analys av skyddet för personlig integritet underströks vikten av ett gediget lagstiftningsarbete.¹⁵ En högkvalitativ lagstiftning kännetecknas av välgrundade behovsanalyser, noggranna intresseavvägningar och utförliga konsekvensbeskrivningar. Utan detta riskerar viktiga skyddsbehov att förbises eller underskattas.¹⁶

Ur ett effektivitetsperspektiv kan tvångsmedel ha ett värde i att "föra utredningen framåt". Det är lätt att identifiera sådana fördelar i enskilda fall, och därigenom formulera ett upplevt behov. Just därför krävs en rimlig avvägning mellan effektiv brottsbekämpning och skyddet för rättssäkerhet och personlig integritet.¹⁷ Det är lagstiftaren som har ansvaret att göra denna avvägning, att sätta riktningen för samhället och att säkerställa att mänskliga rättigheter efterlevs i Sverige. Brottsbekämpningen beskrivs ofta, som Advokatsamfundets tidigare generalsekreterare påpekat, i termer av ett krig.¹⁸ Det gör att vad som är tekniskt möjligt blir styrande för politiken. Nu när AI är tekniskt möjligt, tycks slutsatsen vara att det också ska användas, trots de allvarliga problem det medför i fråga om rättssäkerhet, transparens och likabehandling. Även om regeringen identifierar ett syfte med att använda AI, måste det göras en proportionalitetsbedömning i relation till skyddet för mänskliga rättigheter.

Utredningen framhåller att det i balansen mellan effektiv brottsbekämpning och personlig integritet också måste beaktas hur brottsligheten ser ut i samhället, att brottsutvecklingen skapar otrygghet även utanför den kriminella miljön.¹⁹ Civil Rights Defenders anser att

¹² Human Rights Council Fifty-first session 12 September–7 October 2022, The right to privacy in the digital age.

¹³ Ibid, punkt 29.

¹⁴ Submissions of the International Network of Civil Liberties Organizations (INCLO), The right to privacy in the digital age Human Rights Council adopted resolution 48/4 4 June 2022, s. 9.

¹⁵ SOU 2007:22 s. 445.

¹⁶ Ibid.

¹⁷ Anne Ramberg, Tvångsmedel, rättssäkerhet och integritet — går det att förena? (SvJT, 2007).

¹⁸ Ibid.

¹⁹ Ds 2025:7, s. 58.

trygghetsbegreppet i detta sammanhang måste problematiseras. Att vistas i det offentliga rummet utan att utsättas för brott är en demokratisk rättighet, men trygghet får inte reduceras till en fråga enbart om brottslighet. Studier kring kamerabevakning i socioekonomiskt utsatta områden visar att kameror sällan bidrar till ökad upplevd trygghet. I stället uppger intervjupersoner att andra insatser, som ökad polisiär närvaro, bättre renhållning eller trygghetsvandringar, haft större påverkan på deras trygghetskänsla.²⁰ Trygghet präglas alltså av att engagera medborgare och bygga lokala samhällen som präglas av omsorg och tillit.

Liksom vid andra hemliga tvångsmedel lär sig kriminella snabbt att anpassa sig.²¹ Det är mer sannolikt att fler integritetskränkande system kommer att införas för att kompensera för teknikens brister, när den kriminella aktiviteten flyttar till trappuppgångar, källare och innergårdar, snarare än att ansiktsigenkänning i sig visar sig vara en effektiv metod att bekämpa brott.²² Även om det går att identifiera ett behov av ansiktsigenkänningsteknik, finns det inget som tyder på att den skulle vara effektiv för att uppnå sitt syfte. Fjärrbiometrisk ansiktsigenkänningsteknik lider dessutom av betydande tekniska brister. Ansiktsigenkänningssystem tenderar att vara mindre träffsäkra för personer med mörkare hudtoner samt för kvinnor.²³

Mot bakgrund av de risker som övervakning innebär för personlig integritet och rättssäkerhet krävs mycket tungt vägande skäl för att motivera användningen av ansiktsigenkänning. Det behov som utredningen beskriver är inte tillräckligt välmotiverat för att berättiga en så långtgående inskränkning. Civil Rights Defenders avstyrker därför förslaget att möjliggöra användning av biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål.

6 Förutsättningar för att använda AI-system för ansiktsigenkänning i realtid

- Civil Rights Defenders **avstyrker** att AI-system för ansiktsigenkänning i realtid ska få användas om det är av synnerlig vikt för att lokalisera eller identifiera en person, om skälen för användningen uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Det är inte en polisiär utredningsmetod

Utredningen beskriver ansiktsigenkänning som en polisiär utredningsmetod.²⁴ Detta är rättsligt felaktigt. Ansiktsigenkänning i realtid på offentlig plats innebär insamling och behandling av personuppgifter om individer i rörelse. Myndigheter samlar in, bearbetar och analyserar personliga data genom att matcha bilder som tidigare inhämtats utifrån biometriska data som identifieras i rörlig bild i realtid och upptar information om personens geolokalisering. Datan bearbetas i realtid och kringuppgifter om personen samlas in, som var och när en person befinner sig på en viss plats. Enligt utredningen innebär en polisiär utredningsmetod en bearbetning av redan tillgängligt material.²⁵ Biometrisk ansiktsigenkänning av

²⁰ Karl Kronkvist, Sara Nordqvist och Anna-Karin Ivert, Kamerabevakning i ett särskilt utsatt bostadsområde (Malmö Universitet, 2019) s. 81.

²¹ Ina Hennen och Manne Gerell, Hot Spot 'Knarkrondellen' (Nordisk politiforskning, 2019) s. 132; Brå, Kameraövervakning på Stureplan och Medborgarplatsen (2015) s. 20.

²² Karl Kronkvist, Sara Nordqvist och Anna-Karin Ivert, Kamerabevakning i ett särskilt utsatt bostadsområde (Malmö Universitet, 2019) s. 79.

²³ Kade Crockford, How is Face Recognition Surveillance Technology Racist? (American Civil Liberties Union, 2020).

²⁴ Ds 2025:7, s. 50.

²⁵ Ibid, s. 90.

brottsbekämpande verksamhet skiljer sig från detta då det innebär en insamling av ny information, och inte bara ett jakande eller nekande svar om huruvida det sker en matchning eller inte.

När en sådan åtgärd vidtas som ett led i myndighetsutövning och får antas äga rum mot den drabbades vilja, men inte utgör en regelrätt sanktion, är detta ett tvångsmedel.²⁶ Biometrisk ansiktsigenkänning i realtid uppfyller således kriterierna för ett straffprocessuellt tvångsmedel. Eftersom detta dessutom, i likhet med dataavläsning och avlyssning, görs utan att personen i fråga känner till det, utgör det ett hemligt tvångsmedel.²⁷ Användning av ansiktsigenkänning är inte endast i paritet med hemlig dataavläsning och rumsavlyssning, det är juridiskt sett ett hemligt tvångsmedel och är inte att betrakta som en polisiär utredningsmetod.

Det är för låga trösklar och inte tillräckliga rättssäkerhetsgarantier

Enligt Europadomstolens praxis måste hemliga tvångsmedel vara tydligt lagreglerade, tidsbegränsade och förenade med rättssäkerhetsgarantier, däribland möjlighet till rättslig prövning. Sådan prövning ska antingen kunna ske efter underrättelse till den enskilde, eller genom att den som misstänker att hen varit föremål för tvångsmedel ges tillgång till domstol oberoende av underrättelse.²⁸

Trots detta föreslår utredningen inga bortre gränser för hur länge ett tillstånd om ansiktsigenkänning får förlängas.²⁹ Att ett tillstånd endast gäller en månad i taget är otillräckligt, utan en faktisk bortre tidsgräns riskerar användningen att glida över i en form av löpande och generell kartläggning. Särskilt när det används i förebyggande syfte. Vidare anser Civil Rights Defenders att kravet på att användningen ska vara av "synnerlig vikt" och bidra till att ärendet förs framåt inte uppfyller det krav på absolut nödvändighet som bör gälla vid användning av så ingripande åtgärder.³⁰ För att åtgärden endast ska användas när behovet är kvalificerat och för att undvika regelmässig användning, som utredaren anger som målsättning, måste rekvisiten spegla detta.

Civil Rights Defenders anser att det är positivt att beslut om användning av ansiktsigenkänning främst ska fattas av domstol, men avstyrker att åklagare ska kunna besluta om detta i förebyggande syfte. Vi konstaterar dessutom att det saknas tillräcklig vägledning kring hur proportionalitetsbedömningen ska utföras. Det är otillräckligt att enbart ställa upp en allmän intresseavvägning. Det krävs att lagstiftningen preciserar vilka intressen som ska beaktas, hur dessa ska vägas mot varandra och hur tungt varje aspekt ska väga. Det gäller inte bara det intrång som uppstår för den enskilde, utan också det kollektiva intrånget för alla personer som övervakas i realtid, samt risken för felidentifieringar som kan få allvarliga rättsliga och sociala konsekvenser för oskyldiga.

Vid användning av tekniken i närheten av platser där personer kan ge uttryck för sina politiska, religiösa eller filosofiska övertygelser, exempelvis demonstrationsytor, religiösa byggnader eller föreningslokaler, tillkommer ytterligare skyddsvärda intressen. Sådana faktorer måste väga tungt mot tillståndsgivning i en proportionalitetsbedömning och det är därför angeläget att lagstiftaren i förarbetena tydligt anger hur sådana avvägningar ska göras i praktiken.

Slutligen bör det framhållas att Polismyndigheten tidigare kritiserats internt för att prioritera brottsofferperspektivet framför objektivitet och rättssäkerhet i utredningsverksamheten.³¹ Det väcker frågan om myndigheten har tillräckliga interna kontrollmekanismer för att hantera så

²⁶ Prop. 2013/14:237, s. 43.

²⁷ Ibid, s. 43.

²⁸ Roman Zakharov v. Russia Grand Chamber (2015), §§ 231, 238–301 och 233–234.

²⁹ Ds 2025:7, s. 94.

³⁰ Ibid, s. 79.

³¹ Polisen, Systemgranskning av polisens utredningsverksamhet (2020), s. 7.

känsliga tvångsmedel med den försiktighet som krävs. Att ge polisen tillgång till en teknik med så djupgående konsekvenser för den personliga integriteten, utan att samtidigt att föreskriva tydliga och bindande rättssäkerhetsgarantier, är inte försvarligt i en rättsstat.

8 Tillståndsprövningen

- Civil Rights Defenders **tillstyrker** utredningens förslag om att det ska krävas tillstånd för att använda system för biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpningsändamål.
- Civil Rights Defenders **föreslår** att det i tillståndsprövningen hålls ett sammanträde, utses ett integritetskyddsombud, att besluten är överklagbara för båda parter samt att besluten innehåller en dokumenterad konsekvensbedömning som så långt som möjligt är offentlig.

Som tidigare konstaterats utgör användningen av ansiktsgenkänning i realtid inte en ordinär polisiär utredningsmetod, utan ett hemligt tvångsmedel. Detta medför att särskilda rättssäkerhetsgarantier måste gälla. Civil Rights Defenders ser positivt på att utredningen föreslår att det ska krävas tillstånd för användningen av ansiktsgenkänning men anser att prövning bör förenas med ytterligare rättssäkerhetsgarantier, i likhet med vad som gäller för andra hemliga tvångsmedel.

Prövningen bör innehålla ett sammanträde i domstol samt att det utses ett särskilt integritetsombud vars uppgift är att bevaka de enskildas rättigheter, men också integritetsintresset i stort. Utredningen har begränsat sin behovsanalys av ett eventuellt sammanträdesbehov till att enbart omfatta önskemålet om en snabb och mindre formbunden handläggning.³² Någon egentlig prövning av sammanträdesbehovet ur ett integritetsperspektiv har inte gjorts. Ett integritetsombud är särskilt motiverat när övervakningen riskerar att träffa ett stort antal personer som inte är föremål för någon misstanke. Syftet med ett integritetsombud är att åstadkomma en mer kontradiktorisk process, där inte endast den beslutande myndigheten får komma till tals. Genom att föra in en motpart i tillståndsprövsprocessen stärks skyddet för den personliga integriteten och rättssäkerheten förbättras.³³ I tidigare förarbeten har detta motiverats av att det är ett särskilt integritetskänsligt tvångsmedel och att det finns utrymme för stora variationer, till exempel vem tvångsmedlet kan tänkas påverka utöver den som är föremål för beslutet men också vilken typ av platser, och därmed aktiviteter, som blir föremål för åtgärden.³⁴ Dessa frågor aktualiseras vid användningen av biometrisk ansiktsgenkänning i realtid. Nämnvärt är att i utredningen om huruvida det fanns ett behov av ombud vid övervakning av elektronisk kommunikation tillfrågades åklagare, domare och offentliga ombud. Det har inte skett i förevarande utredning.³⁵

Det är vidare en betydande rättssäkerhetsbrist att beslut om tillstånd till ansiktsgenkänning i realtid inte alltid är överklagbara. Om ett beslut kan överklagas endast när åklagare är part, men inte i andra fall, uppstår en obalans mellan den enskildes intresse av skydd mot övervakning och statens intresse av brottsbekämpning. Denna brist på symmetri i rättsmedelsskyddet framstår som rättsosäker och är inte tillräckligt motiverad i utredningen.

Utan en möjlighet till överklagan och utan att ett integritetsombud företräder den enskildes intressen, är tillståndsförfarandet den enda befintliga rättssäkerhetsgarantin under den tid

³² Ds 2025:7, s. 90.

³³ Prop. 2002/03:74 s. 23.

³⁴ Prop. 2013/14:237, s. 120.

³⁵ Ibid.

ansiktsgenkänningen pågår. Det innebär att en person som utsätts för felaktigt, oproportionerligt eller annars rättsstridig övervakning inte har någon faktisk möjlighet att tillvarata sina rättigheter utan dröjsmål. Rätten till ett effektivt rättsmedel, som följer både av artiklar 52 och 53 Law Enforcement Directive (LED) och artikel 47 i EU-stadgan, kräver att den enskilde ges möjlighet till oberoende prövning av intrång i den personliga integriteten. Ett rättsmedel som endast består i en tillsynsmyndighets generella efterhandskontroll av myndighetsbeslut, som Integritetsskyddsmyndigheten, uppfyller inte detta krav. För att IMY ska genomföra en laglighetsprövning krävs det dessutom att vissa krav uppnås. Det måste finnas en faktisk möjlighet för enskilda att få sin sak prövad och ett felaktigt beslut undanröjt, även medan behandlingen pågår.³⁶

11 Det ska finnas krav på underrättelse till enskild

- Civil Rights Defenders **avstyrker** utredningens förslag om att den som har varit föremål för ansiktsgenkänning endast ska underrättas i vissa situationer.
- Civil Rights Defenders **föreslår** att det bör införas bättre garantier för att tillgodose kraven på transparens och underrättelse till enskild, bland annat genom att göra det publikt vilka kameror som använder ansiktsgenkänning i realtid, tydligare krav som ställs på utvecklingen av programvaran samt garantier för att säkerställa transparens kring AI-verktyget.

Användningen av AI väcker särskilda frågor om korrekthet och öppenhet, två centrala principer i LED. När denna teknik används i myndighetsutövning innebär det i praktiken en omfattande insamling, delning och lagring av känsliga personuppgifter, ofta i realtid och baserat på bedömningar från ett AI-system tillhandahållet av en extern leverantör.

Den enskildes rätt till information

Enligt artikel 14 i LED har varje individ som omfattas av personuppgiftsbehandling rätt att underrättas om denna behandling. Vid traditionell kamerabevakning sker detta genom tydlig skyltning som informerar om övervakningen, vad syftet är och anger vem som är personuppgiftsansvarig. Undantag från skyldigheten kan göras enligt artikel 15 LED men endast för att undvika att hindra förundersökningar eller förebyggande av brott i den utsträckning det är försvarligt i ett demokratiskt samhälle. Utredningen menar att det inte är praktiskt möjligt att underrätta varje individ som fångas av ett ansiktsgenkänningssystem, men detta resonemang är svårförsvarligt. Eftersom användningen enligt utredningens egna förslag ska vara begränsad i tid och rum, borde det vara fullt möjligt att informera om sådan användning genom skyltar på plats. I andra fall, hade en digital tjänst för underrättelse kunna användas. Till exempel skulle en central plattform kunna tillhandahålla information om var ansiktsgenkänning tillämpas i realtid, på motsvarande sätt som i San Francisco, där staden är skyldig att publicera information om kameraövervakning på sin hemsida.³⁷ En sådan tjänst skulle inte bara tillgodose kraven i LED, utan även bidra till allmänhetens upplevelse av transparens i ett samhälle där ansiktsgenkänning annars kan tillämpas utan att invånarna känner till det.

Underrättelse om användning av ansiktsgenkänning är avgörande för att tillvarata sina rättigheter och till exempel begära rättelse eller få personuppgiftsbehandlingen prövad.

³⁶ An EU Artificial Intelligence Act for Fundamental Right (2021); Anna Langseth, Därför kritiserar förslaget om ansiktsgenkänning (Syre, 2024).

³⁷ San Francisco Police, CHAPTER 19: PUBLIC SAFETY CAMERA ORDINANCE.

Transparens

Transparens är en grundläggande rättssäkerhetsgaranti vid användning av AI inom offentlig verksamhet.³⁸ En central fråga är därför om myndigheters konsekvensbedömningar för mänskliga rättigheter, som ska göras enligt artikel 27 i AI-förordningen, kommer att vara offentligt tillgängliga. För närvarande undantas brottsbekämpande myndigheter från vissa transparenskrav i förordningen, men det finns starka skäl för Sverige att säkerställa offentlig insyn i konsekvensbedömningarna, särskilt eftersom detta är mycket viktigt för att se till att Sverige inte kränker mänskliga rättigheter. Dessa bedömningar bör göras tillgängliga för allmänheten.

Ett stort problem är att polisen i stor utsträckning kommer att behöva samarbeta med privata aktörer vid utveckling och inköp av AI-system. Detta innebär att kontrollen över hur systemen utformas, tränas och används delvis ligger hos externa företag, vilket begränsar insynen både för myndigheten själv och för allmänheten. Utredningen behandlar inte vilka krav som bör ställas vid upphandling av sådana system, exempelvis avseende transparens, datakvalitet och likabehandling. Eftersom förprogrammeringen av systemen, innan de större kvantiteterna av data matas in för att träna verktyget, ofta skyddas som företagshemlighet kan det bli omöjligt att granska hur systemet fungerar i praktiken. Det finns alltså en dubbel problematik: dels att myndigheten inte har full kontroll över tekniken, dels att själva testdatan och implementeringen av systemen är oåtkomliga för insyn av allmänheten.

Denna brist på transparens innebär att rättigheter riskerar att kränkas utan att det upptäcks, än mindre åtgärdas. För att säkerställa att sådana överträdelser inte sker i det fördolda måste all relevant information göras tillgänglig för offentlig granskning. Informationen som omfattas av sekretess måste åtminstone delas med oberoende tillsynsmyndigheter. Dessutom behöver det tydliggöras vilka rättsliga vägar som står till buds för enskilda som anser att deras rättigheter har kränkts genom användning av AI, inklusive situationer där en privat aktör varit inblandad i utformningen eller användningen av tekniken.

14 Förslagets förenlighet med grundläggande fri- och rättigheter

- Civil Rights Defenders **gör bedömningen** att utredningens bedömning om att förslaget är förenligt med grundläggande fri- och rättigheter är oriktig.

Civil Rights Defenders välkomnar att utredningen prövar om det nya verktyget är proportionerligt och nödvändigt, men vi delar inte alltid dess slutsatser. Att hävda att en lag är proportionerlig endast för att myndigheterna förväntas tillämpa den på ett proportionerligt sätt är otillräckligt. Det innebär att regeringen skjuter över lagstiftningsansvaret på myndigheter, vilket strider mot 2 kap. 22 § regeringsformen.³⁹ Ett starkare beredningsunderlag krävs för att rätt skyddsbehov ska uppmärksammas.

Personlig integritet och rättssäkerhet

Förslaget strider enligt Civil Rights Defenders mot grundläggande rättigheter, inklusive rätten till privatliv och personlig integritet. Tekniken möjliggör en mer detaljerad kartläggning av våra liv och ökar statens informationsmakt. Algoritmiserade verktyg i brottsbekämpning hotar rättssäkerheten, inte minst genom risken för fel och brist på insyn.

³⁸ Statskontoret, Myndigheterna och AI - En studie om möjligheter och risker med att använda AI i statsförvaltningen (2024) s. 35.

³⁹ Ds 2025:7, s. 132.

Särskild hänsyn bör tas till riskerna för dataläckor. Ansiktsgigenkänningsdata är biometrisk och därmed oersättlig, till skillnad från lösenord kan dessa inte ändras om de röjs. Det används dessutom i nära anslutning till information om var människor befinner sig och när. Under perioden 2018–2024 anmälades 514 misstänkta dataintrång hos polisen, vilket understryker allvaret.⁴⁰ LED:s krav på datasäkerhet och rapportering av intrång blir här särskilt viktiga.

Fria åsiktsbildningen

Utredningen medger att ansiktsgigenkänning i offentliga miljöer kan ha en avskräckande effekt på yttrande- och mötesfriheten.⁴¹ Civil Rights Defenders delar denna bedömning, men menar att de föreslagna begränsningarna i syfte och användning inte erbjuder ett tillräckligt skydd.

Internationella rapporter, inklusive från FN:s människorättsråd, har varnat för den så kallade "chilling effect" som övervakning kan ha, det vill säga att människor självcensurerar eller avstår från att utöva sina grundläggande fri- och rättigheter av rädsla för övervakning.⁴² En studie visar till exempel att mellan 34–61 procent av journalister och författare undviker eller åtminstone övervägt att undvika att skriva om vissa ämnen på grund av rädsla för statlig övervakning, och en annan att 39 procent av svaranden undviker ord som övervakas av polisen.⁴³ Amnesty International har bedömt att inga skyddsåtgärder är tillräckliga för att förhindra de negativa effekterna på mänskliga rättigheter som ansiktsgigenkänning orsakar och att tekniken bör förbjudas helt.⁴⁴

AI-övervakning kan teoretiskt sett öka deltagandet i sociala och politiska sammanhang genom att minska brottsligheten i utrymmen där övervakning sker, men forskning visar att dessa system tenderar att hämma sociala interaktioner och bidra till exkludering genom att utsatta områden ghettoiseras genom kamerabevakning.⁴⁵ Även om utredningen inte föreslår generell övervakning, kommer realtidsigenkänning främst att användas i områden med hög brottslighet, vilket innebär att invånare i dessa områden, ofta socioekonomiskt utsatta, påverkas oproportionerligt. Med det sagt kan det likväl användas mer allmänt i större städer eftersom det ofta är högre risk för att brottslighet sker där.⁴⁶ Övervakning med hjälp av ansiktsgigenkänning kan skapa en känsla av osynlig kontroll och leda till att vissa individer inte känner sig trygga i det offentliga rummet särskilt när de vill uttrycka sina åsikter eller delta i offentliga sammankomster.⁴⁷ Hur mycket ens integritet inskränks, och hur stor mötesfrihet man har, kan

⁴⁰ Åsa Erlandsson och Kristoffer Örstadius, Polisläckorna: Gängen värvar poliser – med sexuella relationer - DN.se (DN, 2024).

⁴¹ Ds 2025:7, s. 137.

⁴² Human Rights Council Fifty-first session 12 September–7 October 2022, The right to privacy in the digital age, punkt 47.

⁴³ Pew Research Center, Americans' Privacy Strategies Post-Snowden (2015); Ibid; Global Chilling: The Impact of Mass Surveillance on International Writer (PEN America, 2015).

⁴⁴ Amnesty International, Under Protected and Over Restricted the State of the Right to Protest in 21 European Countries (2024), s. 197-198.

⁴⁵ Clive Norris, Mike McCahill och David Wood, The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space, s. 396-414; Statskontoret, Myndigheterna och AI - En studie om möjligheter och risker med att använda AI i statsförvaltningen (2024) s. 34.

⁴⁶ Kommuner mot brott, SOU 2021:49, s. 56-58.

⁴⁷ Mariko Hirose, Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology 49 Connecticut Law Review 2016-2017; Hille Koskela, The gaze without eyes': video-surveillance and the changing nature of urban space (2000).

därför påverkas av var man bor. Detta måste adresseras i en utredning om AI-baserad ansiktsgenkänning i syfte att öka trygghet.

Att vi har yttrande-, mötes- och demonstrationsfrihet innebär inte bara att alla har rätt att yttra sig, mötas eller demonstrera. Det förutsätter också att människor känner sig trygga med att utnyttja dessa rättigheter i praktiken, utan risk för repressalier. Om individer drar sig för att visa sina politiska åsikter på grund av en upplevd rädsla för repressalier utgör detta ett allvarligt hot mot opinionsfriheterna, då rättigheterna, trots att de finns kvar i teorin, inte kan utnyttjas i praktiken. Detta gäller oavsett om det finns saklig grund för en sådan rädsla eller om den endast är upplevd.

Diskriminering

Vi ser en stor risk för att användning av ansiktsgenkänningsteknologi får en diskriminerande verkan. Enligt artikel 21 i EU-stadgan är diskriminering förbjuden. Men AI-system reproducerar ofta fördomar snarare än att eliminera dem.⁴⁸ AI-verktyg har generellt sämre förmåga att korrekt identifiera kvinnor än män.⁴⁹ När polisen i London använde sig av ansiktsgenkänning år 2018–2019 pekade AI:n ut fel person i 81 procent av fallen, visar en studie gjord av bland annat University of Essex.⁵⁰ Användningen av AI förstärker rasistisk och diskriminerande brottsbekämpning.⁵¹

Detta strider också mot artikel 4 i LED:s krav på riktighet och likabehandling, eftersom AI är känd för att göra fel när de försöker identifiera ett förvalt ansikte i realtid i en rörlig bild där mycket händer. Felaktig identifiering kan dessutom få allvarliga konsekvenser för den enskilde individen. Att bli felaktigt identifierad som misstänkt för brott kan leda till flertalet allvarliga konsekvenser, som exempelvis felaktiga frihetsberövanden, olaglig lagring av deras personuppgifter eller användning av ytterligare hemliga tvångsmedel och övervakning.

Vi vet att icke-vita individer redan idag löper högre risk för att bli godtyckligt stannade och misstänkta för brott än andra.⁵² FN särskilda rapportör på rasdiskriminering har också varnat för att övervakning generellt används på ett sätt som ökar utsattheten för icke-vita individer, samt att användningen av AI-teknologi riskerar att förvärra denna situation.⁵³ För den som ansöker om medborgarskap kan bara misstanken om brott dessutom fördröja processen.

Utredningen förklarar inte hur risken för diskriminering ska hanteras. Diskrimineringslagen i Sverige omfattar inte polisens verksamhet. Regeringen har som svar på en skriftlig fråga från riksdagen dessutom angett att det inte finns någon tidsplan för när detta kommer ändras.⁵⁴ Kan det inte garanteras att enskilda inte utsätts för diskriminering, och inte har möjlighet att få

⁴⁸ Srabonty Das Gupta, [The EU AI Act and Its Adherence to the European Convention on Human Rights](#) (EmildAI, 2025).

⁴⁹ [Privacy International's submission for the UNSR on racism's thematic report on artificial intelligence \(AI\) and racial discrimination](#) (2024); UN Women, [Artificial Intelligence and gender equality](#) (2024).

⁵⁰ [New report raises concerns over Met Police trials of live facial recognition technology](#) (University of Essex, 2019)

⁵¹ Amnesty International, [EU: AI Act at risk as European Parliament may legitimize abusive technologies](#) (2023).

⁵² Brå, [Polisens arbete med profilering och likabehandling](#) (2023), s. 54.

⁵³ Human Rights Council Fifty-sixth session 18 June–14 July 2024, [Contemporary forms of racism, racial discrimination, xenophobia and related intolerance A/HRC/56/68](#), s. 4.

⁵⁴ [Ett utökat skydd mot diskriminering \(Skriftlig fråga 2024/25:1003 av Ulrika Westerlund \(MP\)\)](#) | Sveriges riksdag.

upprättelse om det skulle ske, ska inte en åtgärd som riskerar att förstärka diskriminering vidtas. Hur ett sådant ansvarsutkrävande skulle se ut i nuläget tydliggörs inte heller i utredningen.

ÖVRIGA SYNPUNKTER

Utredningen menar att användningen av ansiktsgenkänning kan motiveras med hänvisning till att AI-förordningen utformats med beaktande av mänskliga rättigheter och Kommissionens bedömning om att den är i enlighet med EU-rätt och Europarådets AI-konvention.⁵⁵ Men detta är långt ifrån oomstritt.⁵⁶

Europaparlamentet röstade 2023 för ett totalförbud mot biometrisk ansiktsgenkänning.⁵⁷ Även oberoende institutioner inom EU som European Data Protection Board och European Data Protection Supervisor har förespråkat ett generellt förbud mot ansiktsgenkänning i offentliga miljöer med hänvisning till integritetsintrånget och rätten till anonymitet.⁵⁸ Människorättsorganisationer som *Ligue des droits humains* och *Liga voor Mensenrechten* i Belgien varnar för att vagt formulerade undantag i förordningen kan möjliggöra godtycklig användning.⁵⁹ Att Sverige modellerat sin lagstiftning efter denna förordning utan en mer gedigen proportionalitetsbedömning är därför problematiskt.⁶⁰

Att EU öppnar för denna teknik innebär inte att Sverige bör följa efter.

Remissvaret har beretts av Alma Bergqvist.

Stockholm som ovan,

Martin Nyman
Senior jurist

⁵⁵ Ds 2025:7 s. 59 och 137.

⁵⁶ Natacha López, Slutversion av AI-lag väcker kritik – tillåter mer ansiktsgenkänning (Altinget, 2024).

⁵⁷ Luca Bertuzzi, AI Act enters final phase of EU legislative process (Euractive, 2023).

⁵⁸ EDPB-EDPS, Joint Opinion 5/2021.

⁵⁹ Masha Borak, EU ban on 'unacceptable' AI comes into force with crucial details unresolved (Biometric Update, 2025); 'Unacceptable risk': Human rights groups call for ban on real-time facial recognition (Brussel Times, 2025).

⁶⁰ Masha Borak, Biometric surveillance will be debated until the final stages of AI Act (Biometric Update, 2023); Gian Volpicelli, EU set to allow draconian use of facial recognition tech, say lawmakers (Politico, 2024); Pieter Haeck, The EU's AI bans come with big loopholes for police (Politico, 2025).