Sveriges advokatsamfund

Stockholm den 23 oktober 2026

R-2026/1521

Till Justitiedepartementet
Ju2026/01595

Sveriges advokatsamfund har genom remiss den 23 juni 2026 beretts tillfälle att yttra sig över promemorian Ett statligt identitetskort.

Sammanfattning

Advokatsamfundets uppgift är främst att ta ställning till hur utredningens förslag påverkar den enskildes rätt till integritet och privatliv samt huruvida den eventuella kränkningen av denna rätt står i rimlig proportion till samhällets intresse av att kunna behandla personuppgifter inom de aktuella verksamhetsområdena.

Advokatsamfundet är införstått med behovet av att kunna säkerställa äktheten i våra pass och identitetskort, men detta behov får samtidigt inte leda till att intresset av att skydda enskildas integritet och tillgodose krav på rättssäkerhet åsidosätts i oproportionerlig utsträckning.

Många av de slutsatser och bedömningar som framkommer i promemorian är sådana som Advokatsamfundet kan instämma i. Advokatsamfundet har exempelvis inget att erinra mot de lagtekniska förslagen, såsom förslag om att ändra beteckningar så att hänvisningar i olika regelverk blir korrekta. Samtidigt innehåller promemorian sådana förslag som Advokatsamfundet anser sig behöva invända mot eller lämna synpunkter på i enlighet med vad som anförs nedan.

Laboratoriegatan 4, Box 27321, 102 54 Stockholm
Tfn 08-459 03 00, advokatsamfundet.se, info@advokatsamfundet.se

Sammantaget finner Advokatsamfundet att promemorians förslag till författningsåtgärder, i den utformning och med det innehåll som förslagen nu har, inte kan tillstyrkas.

Synpunkter

Osäkra identitetshandlingar missbrukas

I promemorian hänvisas till att ”enligt den myndighetsgemensamma lägesbilden om organiserad brottslighet kan de förbättrade möjligheterna att utbyta information mellan myndigheter sannolikt leda till en ökad användning av oriktiga handlingar och identiteter för att brottsupplägg som bygger på utbetalningar från välfärdssystemet ska kunna fortgå, eller för att de kriminella aktörerna ska undgå att upptäckas i myndigheternas kontroll- och tillsynsverksamhet (Polismyndigheten, 2025).[1]

Advokatsamfundet finner att det snarare borde förhålla sig tvärtom, det vill säga att förbättrade möjligheter att utbyta information mellan myndigheter borde leda till en minskad användning av oriktiga handlingar och identiteter. Om informationsutbytet i stället skulle leda till en ökad användning av sådana handlingar och identiteter, skulle detta innebära att informationsutbytet snarare främjar brottslighet, varvid det i förlängningen kunde ifrågasättas om det överhuvudtaget är en lämplig åtgärd att utöka möjligheterna till sådant utbyte.

Samtidigt ställer sig Advokatsamfundet bakom promemorians bedömning att en säker grundidentifiering där identiteten styrks på ett tillförlitligt sätt kan motverka den identitetsrelaterade brottsligheten och därmed även ha en brottsförebyggande effekt.[2] Advokatsamfundet hyser dock oro för att detta förhållande kan tas till intäkt för att låta en allt större krets av personer hos myndigheter eller andra aktörer få åtkomst till de uppgifter som inhämtas från och om enskilda och som ska utgöra underlag för den säkra identifieringen. Detta gäller särskilt om åtkomsten ska utökas genom ökade möjligheter till informationsutbyte. Promemorians förslag innebär att allt fler sådana personer kommer att få tillgång till detta slags uppgifter, även för andra ändamål än själva identifieringen. Säkerheten och tillförlitligheten i de system eller tjänster som används påverkas nämligen också av vilka som har tillgång till uppgifterna och som kan påverka deras innehåll. Risken för att sådana uppgifter hanteras obehörigen eller för

[1] Promemorian, s. 55.
[2] Promemorian, s. 55.

andra ändamål än avsett blir typiskt sett större ju fler personer hos berörda myndigheter som har åtkomst till dem. Advokatsamfundet anser att promemorian inte i tillräcklig utsträckning har beaktat denna problematik och att dessa risker därmed har underskattats. Till följd av detta saknar promemorian resonemang kring hur riskerna kan motverkas, exempelvis genom en restriktiv behörighetstilldelning eller genom kontroller och uppföljning av tillgången till och åtgärder med de tekniska system som används och informationen däri.

Det statliga identitetskortet

Promemorian framhåller betydelsen av att såväl myndigheter som företag kan lita på de identitetshandlingar som visas upp och att säkra identitetshandlingar inte kan förfalskas eller användas av någon annan än sin innehavare. I promemorian konstateras även att tilliten till identitetshandlingarna är ett centralt samhälleligt intresse, men att det samtidigt är av minst lika stor betydelse att utfärdandeprocessen är tillräckligt säker.[3] Advokatsamfundet instämmer till fullo i detta, men får även framhålla att tilliten förutsätter att uppgifterna i och om identitetshandlingarna inte obehörigen används hos myndigheterna för sådana ändamål som inte avsetts eller kan förutses.

Vem som ska få utfärda identitetskortet

Det statliga identitetskortet ska utfärdas av passmyndigheterna, det vill säga Polismyndigheten inom landet. Därtill ska ambassader och konsulat som är passmyndigheter i utlandet kunna utfärda statliga identitetskort till svenska medborgare.[4] Enligt promemorian kommer ansvaret för det statliga identitetskortet att medföra fördelar för Polismyndighetens möjligheter att bedriva en effektiv gränskontroll och brottsbekämpning.[5] Detta kan enligt Advokatsamfundets bedömning bland annat bero på att de informationssystem och tjänster som används för identitetskorten redan finns hos Polismyndigheten och står under myndighetens kontroll. Detta förhållande kan förstärka myndighetens möjligheter att hindra, upptäcka och agera mot obehörig åtkomst till eller obehörig användning av informationen i systemen. Samtidigt medför myndighetens intresse av att bedriva en effektiv gränskontroll och brottsbekämpning även en viss risk för att informationen kan

[3] Promemorian, s. 56.
[4] Promemorian, s. 63.
[5] Promemorian, s. 63.

komma att användas för andra ändamål eller i större utsträckning än vad som ska vara tillåtet. Denna risk borde ha fått större uppmärksamhet i promemorian, där det borde ha förts ett resonemang kring behovet av en restriktiv behörighetstilldelning jämte behovet av kontroll och uppföljning av hur personalen beretts tillgång till systemen och informationen däri.

Information som ska finnas på kortet

I promemorian anges att uppgift om namn, födelsetid, personnummer, kön och längd ska kunna finnas på identitetskortet men också att det ska finnas en bild på innehavaren och uppgift om kortets giltighetstid. I promemorian konstateras även att det inte behöver regleras i lag vilka uppgifter som ska ingå i kortet, utan det framhålls att det är en fördel om identitetskortets närmare utformning går att ändra relativt snabbt, utan att det krävs lagändringar, om internationella standarder skulle förändras, om säkerhetsbrister skulle uppmärksammas eller om det annars finns skäl för det.[6] Advokatsamfundet finner i detta sammanhang att promemorian tar alltför lättvindigt på riskerna för att känsliga uppgifter förs in i kortet utan att det finns någon egentlig grund för det. Promemorian lämnar nämligen öppet vilka uppgifter som kan komma att ingå genom att ytterligare uppgifter kan förekomma ”om det annars finns skäl för det”. Detta för med sig ett antal betänkligheter. Förhållandet till enskilda ska enligt grundlagen i princip regleras genom lag. Detta torde innebära att förenligheten med grundlagen kan ifrågasättas om det lämnas alltför öppet vilka uppgifter som kan komma att införas i identitetskortet.[7] Till detta kommer att det enligt promemorians resonemang inte heller finns några begränsningar vad gäller att införa känsliga personuppgifter i kortet. Detta ger i sin tur anledning att ifrågasätta promemorians förslag utifrån förhållandet till GDPR. Om det är fråga om känsliga personuppgifter ställs högre krav på tydliga ändamål och säkerheten vid behandlingen.[8] Advokatsamfundet finner att promemorian inte ägnat dessa frågeställningar tillräcklig uppmärksamhet, utan i stället har inriktat sig på effektiviteten i hanteringen av identitetskorten och myndigheternas intresse av att kunna ha åtkomst till systemen och uppgifterna.[9] Därigenom tas risken för att uppgifter i onödan införs i identitetskorten

[6] Promemorian, s. 66.
[7] Regeringsformen (1974:152), 2 kap.6, 20 och 21 §§ jämte 8 kap. 2 §.
[8] Artikel 5.1 b) och f), 24.1 och 32.1 GDPR.
[9] Se dock Promemorian, s. 76 ff., där olika bestämmelser redovisas som angår integritetsfrågor, rättigheter m.m.

inte på tillräckligt stort allvar, vilket i sin tur kan minska allmänhetens intresse av att skaffa korten och skada tilliten till myndigheternas hantering av uppgifterna.

Ansiktsbild och fingeravtryck

Enligt promemorian ska den som ansöker om ett statligt identitetskort vara skyldig att låta sig fotograferas och lämna fingeravtryck samt att fotografiet och fingeravtrycken ska sparas i ett lagringsmedium, ett chip, i själva kortet.[10] Uppgifter av detta slag är särskilt integritetskänsliga och Advokatsamfundet instämmer därför i promemorians uppmärksammande av att de regler som uppställs till skydd för den enskildes grundläggande fri- och rättigheter och GDPR måste beaktas.[11] Ansiktsbilder och fingeravtryck är sådana känsliga uppgifter för vilka särskilda och restriktiva krav på behandlingen gäller. Enligt promemorian ska dessa uppgifter lagras i själva identitetskortet, men för att uppgifternas äkthet ska kunna kontrolleras kommer de även att behöva finnas på annat håll för att en jämförelse ska kunna göras i syfte att bedöma kortets äkthet. Det betyder att bilderna och fingeravtrycken även kommer att ingå i andra informationstekniska system och vara tillgängliga för en obestämd krets personer hos myndigheterna. Denna spridning av uppgifterna för typiskt sett med sig större risker ju fler personer som kan ha åtkomst till dem. Promemorian har enligt Advokatsamfundets uppfattning inte uppmärksammat problematiken i detta förhållande i tillräcklig grad.

Vissa kontroller av identitetskortet

Enligt promemorian ska en identitetshandling kunna kontrolleras med hjälp av biometri. För detta krävs att en ny ansiktsbild eller nya fingeravtryck tas i samband med kontrollen, vilka därefter kan jämföras med den ansiktsbild och de fingeravtryck som finns sparade i identitetshandlingen.[12]

Även om detta utgör ett rimligt tekniskt förfarande för att kontrollera innehavarens identitet, finner Advokatsamfundet att promemorian inte i tillräcklig utsträckning uppmärksammar de risker som är förenade med att nya ansiktsbilder och fingeravtryck tas. Det måste enligt Advokatsamfundet säkerställas att dessa uppgifter inte sparas och behandlas för andra ändamål. Om de nya ansiktsbilderna och fingeravtrycken kommer

[10] Promemorian, s. 76.
[11] Promemorian, s- 76 ff.
[12] Promemorian, s. 90 f.

att finnas åtkomliga för ett mer eller mindre obegränsat antal medarbetare hos myndigheterna, uppstår ökade risker för obehöriga ingrepp i enskildas privatliv samt för att uppgifterna används obehörigen eller för ändamål som inte varit avsedda.

Den statliga e-legitimationen

Enligt promemorian ska Polismyndigheten utfärda även e-legitimationen, vilket enligt Advokatsamfundet är en rimlig ordning.[13] Advokatsamfundet instämmer i promemorians bedömning att den tekniska utvecklingen är så snabb att det är rimligt att regler om e-legitimationens utformning och egenskaper i övrigt meddelas i förordning eller myndigheternas föreskrifter i stället för i lag.[14] Det är även Advokatsamfundets uppfattning att sådana regler bör kunna införas och ändras förhållandevis snabbt för att kunna anpassas till den tekniska utvecklingen. Samtidigt förutsätter detta att det verkligen tas fram sådana regler. Även om hänsyn måste tas till den snabba teknikutvecklingen finner Advokatsamfundet att det är viktigt att det finns regler för e-legitimationen så att de enskilda kan förutse vad som gäller.

Krav på att godta verifiering med vissa e-legitimationer

Statliga myndigheter, kommuner, regioner och sammanslutningar av dessa samt aktörer som yrkesmässigt bedriver verksamhet inom skola, hälso- och sjukvård, tandvård, socialtjänst och vissa andra verksamheter som till någon del är offentligt finansierade (offentliga aktörer) ska enligt promemorian vara skyldiga att godta vissa medel för elektronisk identifiering i en nättjänst som verksamhetsutövaren tillhandahåller. För att en sådan skyldighet ska föreligga krävs att dessa medel motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga aktören kräver för åtkomst till nättjänsten.[15] Promemorian kan dock framstå som något svårbegriplig i detta sammanhang. Det hade enligt Advokatsamfundets uppfattning varit välkommet om promemorian hade resonerat kring och förtydligat vad som ska gälla för andra slags offentligrättsliga subjekt, såsom statliga eller kommunala bolag som inte uttryckligen omnämns bland de uppräknade offentliga aktörerna i promemorian. Det kan i och för sig antas att några ytterligare subjekt utöver de uppräknade inte ska omfattas av skyldigheterna, men detta hade kunnat klargöras tydligare. Därtill blir skyldigheten att godta vissa lösningar snarare ett minimikrav,

[13] Promemorian, s. 54.
[14] Promemorian, s. 92 f.
[15] Promemorian, s. 100 f.

eftersom det står de offentliga aktörerna fritt att tillämpa strängare krav vid åtkomst till sådana nättjänster som dessa tillhandahåller och därmed använda sig av andra lösningar för identifiering än de som promemorian hänvisar till. Aktörerna får därigenom möjlighet att vid behov anvisa särskilda tekniska lösningar för identifiering, exempelvis på grund av förhöjda säkerhetskrav. Samtidigt skulle detta kunna försvåra för allmänheten att använda de aktuella nättjänsterna, inte minst genom att det kan uppfattas som oklart, krångligt och osäkert att använda andra slags medel för identifiering än de etablerade. Advokatsamfundet finner att det hade varit önskvärt med ett resonemang även kring detta.

Passlagstiftningen

Enligt promemorian ska kontrollmöjligheterna vid utlämnandet av pass vara desamma som vid utlämnandet av statliga identitetskort. Av detta skäl föreslås att passlagen kompletteras med en bestämmelse om att sökanden på begäran ska styrka sin identitet och låta passmyndigheten ta en ansiktsbild och fingeravtryck innan passet lämnas ut. Detta ska göras för att kontrollera att den ansiktsbild och de fingeravtryck som tas vid utlämnandet motsvarar dem som finns sparade i passet.[16] Eftersom ansiktsbilder och fingeravtryck kan utgöra känsliga personuppgifter uppkommer även här frågan om hur myndigheten kommer att hantera dessa nya uppgifter. Advokatsamfundet finner det otillfredsställande att promemorian inte fört ett närmare resonemang kring denna problematik. Uppgifterna kan komma att sparas hos myndigheterna, vara åtkomliga för ett obestämt antal personer och behandlas eller lämnas ut för andra ändamål. Detta kan skapa otrygghet hos allmänheten och innebära att förtroendet för myndigheterna och deras hantering av uppgifterna påverkas negativt.

Pass- och identitetskortsdatalagen

Behandlingen av personuppgifter i verksamhet med pass och det statliga identitetskortet är såsom promemorian framhåller nödvändig för att utföra en uppgift av allmänt intresse. Detta omfattar såväl den behandling som utförs i enskilda ärenden som behandlingen i Polismyndighetens register. Handläggningen av ärendena innefattar myndighetsutövning och behandlingen är därför nödvändig även som ett led i myndighetsutövningen. I vissa fall kan behandlingen även vara nödvändig för att

[16] Promemorian, s. 104.

fullgöra en rättslig förpliktelse. Det nu sagda utgör därmed rättsliga grunder för den behandling som sker.[17]

Uppgifterna rör enskildas personliga förhållanden.[18] Samtidigt är passet i princip nödvändigt för att en svensk medborgare ska få lämna landet. Den enskilde är på detta sätt i praktiken hänvisad till att skaffa ett pass och måste därvid acceptera att myndigheterna behandlar dennes personuppgifter. Utan passet och myndigheternas behandling av personuppgifterna kommer den enskilde inte att kunna lämna landet, varvid denne i praktiken förhindras att resa utomlands. Den enskilde intar härigenom en mycket underlägsen ställning och har knappast något annat val än att underkasta sig behandlingen av personuppgifterna. Därtill kommer personuppgifterna att utgöras av ansiktsbilder och fingeravtryck, vilka även utgör känsliga personuppgifter.[19] Advokatsamfundet finner att promemorian inte i tillräcklig utsträckning har uppmärksammat dessa förhållanden.

Lagen värnar både säkerhet och integritet

Frågorna kring uppgifternas art, omfattning och känslighet förtjänar särskild uppmärksamhet och borde därför enligt Advokatsamfundet ha föranlett promemorian att ägna dem större omsorg. Exempelvis är avsnittet i promemorian som handlar om säkerhet och integritet begränsat till cirka en sida.[20] Uppgifternas art och känslighet är sådana omständigheter som särskilt aktualiserar behovet av klara och tydliga ändamål för behandlingen, begränsningar i möjligheterna att behandla uppgifterna för andra ändamål, restriktivitet vad gäller vilka myndigheter eller andra verksamhetsutövare som ska kunna få tillgång till uppgifterna och under vilka förutsättningar sådan åtkomst ska vara tillåten, en restriktiv behandling av uppgifterna i övrigt, stränga begränsningar vad gäller behörigheter för personal hos myndigheterna att få åtkomst till uppgifterna, loggning, kontroll och uppföljning av åtkomsten till och åtgärder med uppgifterna samt att uppgifter inte sparas längre än vad som är absolut nödvändigt för ändamålet med behandlingen.

[17] Promemorian, s. 108. Jfr. artikel 6.1 c) och e) GDPR.
[18] Promemorian, s. 109. Jfr. 2 kap. 6 § st. 3 regeringsformen (1974:152).
[19] Artikel 9.1 GDPR och 3 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[20] Promemorian, s. 110 f.

Det hade därför varit av stort intresse om promemorian exempelvis hade resonerat betydligt närmare kring dessa frågor och därvid framhållit behovet av behörighetsbegränsningar vad gäller åtkomst till och behandling av uppgifterna, restriktivitet i behörighetstilldelningen, tidsbegränsningar i behörigheterna samt hur det ska tillses att endast den som i utförandet av sina arbetsuppgifter behöver ha åtkomst till uppgifterna ges sådan åtkomst. Det hade även varit värdefullt med ett resonemang kring vilka fysiska, organisatoriska, administrativa och tekniska åtgärder som kan vara lämpliga för att skydda uppgifterna och de system eller tjänster som används vid behandlingen. Hit hör exempelvis frågor om lämpligheten i att låta någon extern part ombesörja behandlingen samt huruvida det ska vara tillåtet att behandla uppgifterna genom molntjänster eller i tredje land.

Om det visar sig att en mer eller mindre obegränsad krets av myndigheter, andra verksamhetsutövare eller personal hos dessa kan ha åtkomst till uppgifterna, kommer kontrollen över uppgifterna typiskt sett att vara mindre. Detta kan i sin tur föranleda att tillförlitligheten och bevisvärdet hos de uppgifter som förekommer kan ifrågasättas. Ju fler verksamheter och ju fler personer som har åtkomst till uppgifterna, desto större blir typiskt sett riskerna för att uppgifterna används av obehöriga, för obehöriga ändamål och rentav manipuleras. På detta sätt kommer tvivel om uppgifternas bevisvärde att kunna få betydelse i samband med brottsutredningar, framställandet av rättsliga anspråk och när identiteten i olika samband behöver säkerställas på ett tillförlitligt sätt. Mot bakgrund av att promemorian i så hög grad har uppehållit sig vid betydelsen av att identitetskorten och passen jämte uppgifterna däri kan anses tillförlitliga för samhället och brottsbekämpningen, borde säkerhets- och integritetsfrågorna ha ägnats ett avsevärt större utrymme.

Regler om när personuppgifter får behandlas

Såsom promemorian anger är det Polismyndigheten och utlandsmyndigheterna som behandlar personuppgifter i egenskap av passmyndigheter och även Utrikesdepartementet inom ramen för pass- och identitetskortsverksamheten.[21] Det framgår även av promemorian att andra myndigheter behandlar personuppgifter och att de i detta sammanhang ska tillämpa sina egna regelverk, såsom GDPR, brottsdatalagen (2018:1177) eller annan särskild lagstiftning om behandling av

[21] Promemorian, s. 112.

personuppgifter som gäller för respektive verksamhetsutövare jämte de kompletterande föreskrifter som kan gälla på varje område.[22]

Advokatsamfundet uppskattar att promemorian hänvisar till principen om ändamålsbegränsning och finalitetsprincipen i GDPR och att möjligheterna att behandla personuppgifterna för andra ändamål än det ursprungliga därigenom begränsas. Samtidigt framhåller promemorian att bestämmelserna inte bör utformas så snävt att de begränsar en ändamålsenlig verksamhet eller hindrar nödvändigt informationsutbyte. Promemorian utvecklar detta genom att argumentera för att kravet på att behandlingen ska vara nödvändig för handläggningen inte innebär att den måste vara oundgänglig. Innebörden i begreppet nödvändig har enligt promemorian inte denna strikta innebörd, varför en behandling enligt promemorian skulle kunna anses nödvändig och därmed tillåten om den leder till effektivitetsvinster.[23] Enligt promemorian ska uppgifter även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i en behörig myndighets verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet.[24] Advokatsamfundet konstaterar att promemorian inte föreslår någon begränsning för sådan behandling utifrån hänsyn till brottets allvarlighetsgrad, utan att behandlingen ska kunna ske vid varje slags brott eller när det på något sätt är kopplat till ordning och säkerhet. Detta kan därmed ifrågasättas utifrån proportionalitetsprincipen, särskilt när det är fråga om behandling av känsliga personuppgifter.[25]

Promemorian föreslår dessutom inte någon begränsning vad gäller behandling av ansiktsbilder eller fingeravtryck, utan även denna information kan användas för andra ändamål än pass- och identitetskortsverksamheten. I vissa fall behöver passmyndigheterna och Utrikesdepartementet behandla personuppgifter som har samlats in för handläggning av ärenden om pass eller statliga identitetskort för att lämna ut dessa till andra myndigheter eller till enskilda.[26] Uppgifterna ska rentav kunna lämnas till andra myndigheter och verksamhetsutövare även om dessa är utländska.[27] Det blir enligt Advokatsamfundets bedömning därmed i praktiken omöjligt

[22] Promemorian, s. 113.
[23] Promemorian, s. 117 ff. och prop. 2017/18:105 s. 46 f. och 189.
[24] Promemorian, s. 122.
[25] Promemorian, s. 120.
[26] Promemorian, s. 124 ff.
[27] Promemorian, s. 123.

för de enskilda att kunna förutse när, för vilka ändamål och under vilka förutsättningar deras uppgifter kommer att behandlas och även till vem uppgifterna kan komma att utlämnas. Mot denna bakgrund får Advokatsamfundet svårt att förstå hur detta kan främja allmänhetens förtroende för pass- och identitetskortsverksamheten och tilliten till de uppgifter som behandlas.

Säkerhet och tillgång till personuppgifter

Promemorian anger att tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.[28] Som promemorian själv konstaterar rör det sig till vissa delar om behandling av känsliga personuppgifter eller personuppgifter som är integritetskänsliga på andra sätt. Promemorian förefaller samtidigt även vara införstådd med vikten av att motverka att personuppgifterna sprids inom myndigheterna till någon som inte är behörig att ta del av dem. Promemorian hänvisar därutöver till GDPR vad gäller säkerheten vid behandlingen av personuppgifterna, varför man även har beaktat betydelsen av att det vidtas säkerhetsåtgärder för att skydda uppgifterna.[29] Samtidigt överlämnar promemorian till respektive personuppgiftsansvarig att närmare bestämma vilka säkerhetsåtgärder som är lämpliga och som behöver vidtas. Till detta kommer att promemorian hänvisar till att behandlingen kommer att stå under tillsyn av Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden.

En behandling för brottsbekämpande ändamål kommer alltså att omfattas av ett väl utvecklat regelverk till skydd för den enskildes personliga integritet.[30]

Promemorian går inte närmare in på vilka risker som kan föreligga vid behandlingen av uppgifterna, sannolikheten för att riskerna förverkligas eller vilken skada som potentiellt kan uppstå till följd av behandlingen. Inte heller förs något resonemang kring vilka slags säkerhetsåtgärder som skulle kunna vara lämpliga. I stället behandlar promemorian dessa frågor flyktigt och generellt på endast någon enstaka sida. Advokatsamfundets intryck är därför att promemorian inte tar säkerhets- och integritetsfrågorna på tillräckligt allvar, utan i princip uteslutande ägnar sig åt att

[28] Promemorian, s. 127 ff.
[29] Promemorian, s. 128 och artikel 9.1 GDPR.
[30] Promemorian, s. 123 och 125.

redogöra för nyttan och effektiviteten i att lämna ett stort utrymme för behandling av uppgifterna.

Som promemorian anger är det viktigt att behörigheten att få åtkomst till uppgifterna begränsas till den som behöver dem i sitt arbete. Det saknas dock ett resonemang om vilka risker som föreligger med en alltför generös behörighetstilldelning och hur behörigheterna skulle kunna begränsas. Detta borde ha föranlett promemorian att föra ett närmare resonemang kring behovet av klara och tydliga ändamål för behandlingen, begränsningar i möjligheterna att behandla uppgifterna för andra ändamål, restriktivitet vad gäller vilka myndigheter eller andra verksamhetsutövare som ska kunna få tillgång till uppgifterna och under vilka förutsättningar sådan åtkomst ska vara tillåten, en restriktiv behandling av uppgifterna i övrigt, stränga begränsningar vad gäller behörigheter för personal hos myndigheterna att få åtkomst till uppgifterna, loggning, kontroll och uppföljning av åtkomsten till och åtgärder med uppgifterna samt att uppgifter inte sparas längre än vad som är absolut nödvändigt för ändamålet med behandlingen.

Personuppgifterna kommer att utgöras av ansiktsbilder och fingeravtryck, vilka även utgör känsliga personuppgifter. Den enskilde kommer i praktiken inte att ha något annat val än att acceptera myndigheternas behandling av uppgifterna om denne vill kunna få ett pass och därmed även kunna lämna landet.[31] Detta behöver vägas in vid valet av säkerhetsåtgärder. Advokatsamfundet finner inte att promemorian ägnat dessa förhållanden tillräckligt intresse.

Promemorian borde därutöver ha fört ett resonemang kring säkerhetsåtgärderna, exempelvis avseende vilka fysiska, organisatoriska, administrativa och tekniska åtgärder som kan vara lämpliga för att skydda uppgifterna och de system eller tjänster som används vid behandlingen. Det hade även varit önskvärt att promemorian tagit upp frågor om lämpligheten i att genom utkontraktering låta någon extern part ombesörja behandlingen, huruvida det ska vara tillåtet att behandla uppgifterna genom molntjänster eller i tredje land, jämte olika slags tekniska åtgärder för att skydda uppgifterna såsom kryptering, loggning, brandväggar och backuptagning. Enligt Advokatsamfundets uppfattning kan promemorian inte anses ha ägnat dessa frågor tillräcklig uppmärksamhet, utan har utan närmare analys nöjt sig med att hänvisa till

[31] Promemorian, s. 109.

att det ankommer på de personuppgiftsansvariga att bestämma vilka säkerhetsåtgärder som ska vidtas samt till det tillsynsarbete som Integritetsskyddsmyndigheten och Säkerhets- och integritetsskyddsnämnden utför.

När känsliga personuppgifter får behandlas

När det gäller behandling av känsliga personuppgifter hänvisar promemorian bland annat till att sådana uppgifter får behandlas om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.[32] Promemorian för därefter ett detaljerat resonemang kring varför olika slags känsliga personuppgifter ska kunna behandlas.[33] Advokatsamfundet ifrågasätter i och för sig inte promemorians resonemang avseende samhällets behov och intressen, men finner det anmärkningsvärt att promemorian inte närmare berör frågan om vilka lämpliga och särskilda åtgärder som bör vidtas för att säkerställa den registrerades grundläggande rättigheter och intressen.

Biometriska uppgifter

Promemorian redogör på ett heltäckande och detaljerat sätt för vad som ska förstås med biometriska uppgifter. Advokatsamfundet har inget att erinra mot detta, men får samtidigt framhålla att även om det kan diskuteras huruvida ansiktsbilder och fingeravtryck alltid är att betrakta som biometriska uppgifter så är detta slags uppgifter typiskt sett känsliga uppgifter. Av ansiktsbilder framgår oftast sådana karaktärsdrag som gör det möjligt att identifiera den registrerades ras eller etniska ursprung, samtidigt som biometriska data i sig har definierats som känsliga personuppgifter. Detta medför enligt Advokatsamfundets uppfattning att oberoende av om ansiktsbilder anses utgöra biometriska uppgifter eller inte, ska båda dessa slags personuppgifter anses vara känsliga.[34] Detta medför i sin tur att det ska ställas särskilt höga krav på säkerheten vid behandlingen av detta slags uppgifter.

[32] Promemorian, s. 134 f. och artikel 9.2 g) GDPR.
[33] Promemorian, s. 135 ff.
[34] Promemorian, s. 139 ff. och artikel 9.1 GDPR jämte 3 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Promemorian framhåller i sammanhanget även att biometriska uppgifter ska kunna få behandlas och sparas i samband med kontroll av passets eller identitetskortets äkthet eller behöriga användande.[35] Även i denna frågeställning begränsar sig promemorian till att resonera kring behovet, nyttan och effektiviteten i att de olika verksamhetsutövarna ska kunna genomföra sådana kontroller. Några resonemang kring riskerna med en sådan behandling förs dock inte i promemorian och inte heller någon närmare diskussion kring vilka säkerhetsåtgärder dessa risker bör föranleda.

Ansiktsbilder och fingeravtryck kan rent allmänt sägas ha ett starkt bevisvärde. Om detta slags uppgifter inte hanteras på ett säkert och tillförlitligt sätt, exempelvis genom att ett stort antal personer kan ha tillgång till och kan påverka uppgifterna och att de system eller tjänster i vilka uppgifterna hanteras inte omfattas av lämpliga säkerhetsåtgärder, torde det kunna hävdas att bevisvärdet påverkas negativt. Därmed finns det också en risk för att bevisvärdet hos detta slags uppgifter överskattas med felaktiga domar eller beslut som följd.[36]

Elektroniskt utlämnande av uppgifter

Som promemorian anger kan personuppgifter lämnas ut antingen i fysisk form, exempelvis på papper, eller i elektronisk form och att man i regel skiljer mellan direktåtkomst och annat elektroniskt utlämnande vad gäller elektroniskt utlämnande.[37]

Elektroniskt utlämnande genom direktåtkomst

Med direktåtkomst avses att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan möjlighet att påverka innehållet i registret eller databasen.[38]

Promemorian konstaterar även att direktåtkomst kan innebära särskilda risker för den personliga integriteten.[39] Advokatsamfundet finner att promemorian visserligen fört resonemang kring dessa risker, särskilt utifrån att direktåtkomst möjliggör en stor spridning av uppgifterna och att den som inhämtar uppgifterna även har stora möjligheter att ändra i dem. Samtidigt saknar promemorian något egentligt

[35] Promemorian, s. 142 ff.
[36] Jfr. NJA 2015 s. 702 och 2023 s. 29 I och II.
[37] Promemorian, s. 154.
[38] Promemorian, s. 156.
[39] Promemorian s. 156 ff.

resonemang kring hur dessa risker bör hanteras. Det förs exempelvis inget resonemang kring hur det kan säkerställas att personuppgifterna inte behandlas för obehöriga ändamål hos den som inhämtar dem. Eftersom det uttalas att direktåtkomst innebär särskilda risker för den personliga integriteten, borde det anges i lag vilka som ska ha möjlighet till direktåtkomst, i stället för att det lämnas ett sådant utrymme för utökning av kretsen av berättigade subjekt som promemorians förslag innebär. De föreslagna bestämmelserna skulle medföra att det knappast går att förutse vilka subjekt som kommer att kunna få direktåtkomst till uppgifterna.

Avslutning

Advokatsamfundet kan i de flesta avseenden instämma i promemorians förslag och ställer sig till fullo bakom intresset av att olika åtgärder vidtas med olika slags identitetshandlingar för att göra identifieringen säkrare. Detta innebär också att Advokatsamfundet inte har något att erinra rent principiellt mot att myndigheterna kan få tillgång till uppgifter om identitetshandlingens innehavare när detta behövs i brottsbekämpningen.

Samtidigt finner Advokatsamfundet att promemorians förslag inte i tillräcklig grad uppmärksammat integritets- och rättssäkerhetsfrågorna. Detta tar sig särskilt uttryck i att säkerhetsfrågorna i samband med behandling av de känsliga uppgifter som förekommer, begränsningarna i myndigheternas åtkomst till uppgifterna och kontrollen jämte uppföljningen av sådan åtkomst inte ägnats tillräcklig uppmärksamhet.

Promemorian har i stället lagt tyngdpunkten på statens och samhällets behov på ett sätt som enligt Advokatsamfundet gör att utredningen fått en slagsida i förhållande till de enskildas behov av integritet och rättssäkerhet. Advokatsamfundet finner därför att denna dimension saknas i promemorian och att en mer ingående analys av säkerhets-, integritets- och rättssäkerhetsfrågorna hade gjort promemorian och utredningen mer robusta. Dessa frågor behöver därför noggrant utredas, analyseras och bedömas ytterligare i den fortsatta beredningen.

Advokatsamfundet ser med viss oro på lagstiftningsutvecklingen när det gäller frågor om personlig integritet och rättssäkerhet. Utvecklingen visar nämligen att dessa intressen i allt högre grad och på allt fler områden får stå tillbaka till förmån för samhällsnytta och effektivitet. Om den utvecklingen tillåts gå för långt finns en risk för

att sådana grundläggande värden som integritet och rättssäkerhet urholkas i en utsträckning som kan påverka de enskildas tillit till staten och samhället.

Mot bakgrund av de förhållanden som Advokatsamfundet har påtalat i detta remissyttrande får Advokatsamfundet vid en samlad bedömning avstyrka promemorians förslag.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander