Stockholm den 22 augusti 2019

R-2019/0926

Till Justitiedepartementet

Ju2019/01281/L4

Sveriges advokatsamfund har genom remiss den 26 april 2019 beretts tillfälle att avge yttrande över betänkandet Ett säkert statligt ID-kort – med e-legitimation (SOU 2019:14).

Sammanfattning

Advokatsamfundet har i huvudsak ingen erinran mot förslagen i betänkandet såvitt avser den fysiska identitetshandlingen. Advokatsamfundet har dock vissa synpunkter i fråga om den föreslagna e-legitimationen samt vill även i övrigt särskilt framhålla följande.

Allmänt

Behovet av ett säkert statligt ID-kort är tydligt utifrån behovet av en säker grundidentifiering och ett mer strukturerat arbetssätt. Det är också av vikt att ta tillvara denna grundidentifiering för att införa en e-legitimation med en hög säkerhetsnivå. Här räcker det emellertid inte att reglera utgivningen och att införa register. Det måste också finnas infrastruktur för att använda identitetshandlingarna och regler för spärrkontroller, identitetskontroller och hantering av identitetsintygen. Den författningsreglering som föreslås tar emellertid i huvudsak endast upp frågor kring utfärdandet. Lämnas juridiska frågor kring användningen och tillhörande funktioner för spärrkontroller och identitetsintyg därhän, blir risken stor att den planerade användningen får skjutas på framtiden.

Advokatsamfundet har i olika sammanhang påtalat vikten av ett väl avvägt integritetsskydd när författningsreglering införs av tvångsmedel och andra ingrepp för att ge skydd mot brottsliga eller annars oönskade förfaranden. Här är situationen dock delvis

en annan. Föreslagna ingrepp i enskildas integritet för att ge ut identitetshandlingar syftar till att ge innehavaren ett skydd, så att andra inte enkelt kan missbruka dennes identitet. Trots att det finns ett starkt samhällsintresse är ingreppen alltså inte bara till för att skydda de förlitande aktörerna. Detta behöver beaktas vid den avvägning som måste göras beträffande vad som ska få registreras, exempelvis personnummer, vilka kontroller som ska få utföras med stöd av dessa uppgifter och vilka uppgifter om resultat från kontroller som ska få bevaras. Det måste samtidigt säkerställas att identitetshandlingar inte brukas och att identitetsintyg inte ställs ut och bevaras annat än när det krävs för en säker identifiering eller som bevis för att en behörig person har utfört en rättshandling.

Enligt Advokatsamfundet är det av största vikt att lagförslagen inte resulterar i en omfattande insamling av uppgifter genom vilka individer kan kartläggas eller övervakas. Bevis i form av exempelvis identitetsintyg bör alltså inte få samlas hos andra än förlitande parter som av juridiska skäl behöver detta. Utredningen har inte tillräckligt genomlyst dessa senare led i hanteringen, utan begränsat sina analyser och författningsförslag till utfärdandefasen. Detta är en brist som Advokatsamfundet anser måste åtgärdas under den fortsatta beredningen av lagstiftningsärendet.

Det grundläggande skyddet för identitetshandlingarna bör uppmärksammas

För att tillgodose allmänhetens behov av att kunna lita på att identitetshandlingar är äkta och att de inte används av någon annan än den som anges i handlingen, har förfalskningar och missbruk av dem kriminaliserats på ett tidigare stadium − innan identitetshandlingen har brukats. Denna koppling till det straffrättsliga skyddet för själva handlingarna och vem som brukar dem, är enligt Advokatsamfundets mening av betydelse. I betänkandet redovisas också bedrägeribrottslighetens utveckling och förekomsten av identitetsmissbruk (avsnitt 3.2-3.4). Där finns dessutom ett särskilt avsnitt om missbruk av identitetshandlingar (avsnitt 3.5). De bestämmelser i brottsbalken som ger det grundläggande skyddet mot förfalskning av såväl fysiska identitetshandlingar som e-legitimationer finns emellertid i 14 och 15 kap. BrB. Att även e-legitimationer kan vara urkunder har utvecklats i regeringens proposition 2012/13:74 Förfalsknings- och sanningsbrotten. Det nämns dock inte i betänkandet att bestämmelsen i 15 kap. 12 § BrB om missbruk av urkund visat sig vara av avgörande betydelse för att myndigheter ska kunna tillhandahålla e-tjänster utan att fel person släpps in i strid mot t.ex. röjandeförbudet i offentlighets- och sekretesslagen. Det rör sig här om en form av missbruk som inte kan hindras enbart genom tekniska skydd (se vidare Kan man lita på e-legitimationen?, JT 2017-18 NR 2, s. 517 och https://e-legitimation.se/skyddadinelegitimation/slappaldriginnagonannanpersonellerforetagmedditteleg.4.14dfc9b0163796ee3e73ee.html).

På liknande sätt lämnar utredningen den civilrättsliga ansvarsfördelningen mellan innehavare av e-legitimation och förlitande part därhän, för det fall att någon annan än den rätta innehavaren utför en rättshandling (se 17 § skuldebrevslagen, där det framgår att förfalskning och bristande behörighet kan åberopas även mot den som är i god tro). I detta

hänseende ges uttryck för en allmänrättslig princip, som tillämpas analogt även inom andra rättsområden.

Dessa frågor bör enligt Advokatsamfundet uppmärksammas under den fortsatta lagstiftningsberedningen, så att innehavare av berörda e-legitimationer och förlitande parter får en fullständig bild av vilka regler som är avgörande för användningen och skyddet av de nya identitetshandlingarna.

Två myndigheter föreslås få likartade arbetsuppgifter

Enligt 3 och 7 §§ förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning (DIGG) ges DIGG ett omfattande ansvar för tillgången till infrastruktur och tjänster för elektronisk identifiering och underskrift och ska ansvara för de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering i enlighet med eIDAS-förordningen och tillhörande rättsakter. DIGG ska dessutom uppfylla de samarbetsskyldigheter som gäller för Sverige som medlemsstat enligt eIDAS-förordningen samt företräda Sverige i övriga frågor som rör gränsöverskridande elektronisk identifiering och lämna stöd och information till myndigheter i sådana frågor. Utredningen föreslår emellertid att Polisen inte bara ska ansvara för utfärdandet av de e-legitimationer som ska finnas på föreslagna fysiska identitetshandlingar. Så som hanteringen beskrivs i det remitterade betänkandet förefaller avsikten vara att Polisen ska tillhandahålla funktioner för såväl spärrkontroll som kontroll av identiteten hos den som legitimerat sig och ska utfärda identitetsintyg (se bl.a. s. 349). E-legitimationerna ska emellertid utfärdas enligt ett tillitsramverk som DIGG svarar för.

Mot denna bakgrund uppstår frågan hur Polisens och DIGG:s uppdrag förhåller sig till varandra och vem som utreder och ansvarar för olika delar av den använda infrastrukturen. Det är knappast önskvärt att likartade rättsutredningar ska behöva göras av två myndigheter och att regelverk ska utvecklas av var och en av dem för nära nog identiska kontrollförfaranden. Båda myndigheterna behöver exempelvis analysera om funktioner utformas, så att de blir (delar av) betrodda tjänster enligt eIDAS-förordningen och hur tillitsramverket ska förstås. Ska hanteringen bygga på avtal kan det noteras att det civilrättsligt blir fråga om samma juridiska person − staten − som ska bedriva denna verksamhet. Dessa frågor borde enligt Advokatsamfundets mening ha genomlysts närmare för att uppnå samordningsvinster och undgå hinder vid införandet.

Persondataskyddet

Advokatsamfundet har i ett antal remissvar ifrågasatt dagens registerförfattningar, som blivit ett växande, svåröverblickbart och fragmenterat rättsområde som skapat osäkerhet i den praktiska hanteringen. Informationshanteringsutredningen har också i betänkandet Myndighetsdatalag (SOU 2015:39), lagt fram förslag för att komma tillrätta med detta. Förslaget har emellertid inte lett till lagstiftning. I stället har ytterligare registerförfattningar och GDPR-anpassade sådana vuxit fram, trots att 23 myndigheter och SKL, år 2016 vänt sig till Justitiedepartementet med en skrivelse om behovet av en

gemensam översyn av registerförfattningarna i enlighet med Informationshanterings-utredningens angreppssätt (Pensionsmyndighetens beteckning VER 2015:190). Registerförfattningarna utgjorde, enligt skrivelsen, ett lapptäcke av ibland otidsenliga författningar inom ett svåröverblickbart och fragmenterat rättsområde med bristande enhetlighet och struktur och normtekniska lösningar. Detta medförde enligt eSam beaktansvärda svårigheter för myndigheterna att hänga med i den explosionsartade tekniska utvecklingen, inte minst när det gäller utvecklingen av en effektiv och samverkande e-förvaltning i medborgarnas tjänst. eSams ansåg därför att mycket skulle stå att vinna om en översyn av registerförfattningarna gjordes i samband med anpassningarna till GDPR. Så blev emellertid inte fallet.

Detta upprepas nu genom förslaget till 6 kap. lagen om statliga identitetshandlingar och de regler rörande persondataskydd som föreslås i en förordning om statliga identitetshandlingar. Här kompliceras tolkningen ytterligare av att de behandlingar som inte avser registret *i huvudsak* föreslås bli omfattade av den generella regleringen i dataskyddsförordningen. Detsamma föreslås för den behandling av personuppgifter som Polismyndigheten kommer att behöva utföra med anledning av utfärdande av e-legitimation (se s. 350). Här nämns inte ens den infrastruktur som behöver tillhandahållas för spärrkontroller, identitetskontroller och tillhandahållande av intyg som resultat av kontrollerna. Erfarenheten har visat att Datainspektionen brukar hävda att ett nytt lagstiftningsärende behövs för de tillkommande behandlingarna. Utan en sådan reglering uppkommer ett antal frågor som Advokatsamfundet påtalat i tidigare remissvar. Frågan om personuppgiftsansvarets fördelning har varit och är ett återkommande problem. Till detta kommer exempelvis om angivna ändamål ska tolkas så avgränsat att författningsändringar krävs när kontrollinfrastrukturen har utvecklats och ska införas samt om regeln beträffande direktåtkomst ska förstås så att den motsatsvis hindrar utlämnande på medium, vilket numera är normalfallet för hur informationsutbytet brukar utformas när uppgifter begärs från myndigheter.

Skyddet för persondata behöver således, enligt Advokatsamfundets uppfattning, genomlysas på ett mer omfattande och till e-legitimationer och kontrollinfrastruktur anpassat sätt än i det remitterade betänkandet. Det räcker inte att reglera utfärdandeprocessen och registerföringen. Hela kedjan behöver beaktas, så att inte ett nytt lagstiftningsärende krävs innan identitetskontroller med de planerade e-legitimationerna kan tas i drift (jämför hur ID-kort tidigare försetts med chip till en extra kostnad i avsikt att införa säkra e-legitimationer, utan att någon reell användning kom till stånd). Det räcker inte att lämna dessa frågor till Polisen att analysera.

Avgiftsfrågan

Det kan ifrågasättas om full kostnadstäckning kan uppnås genom en ansökningsavgift om 400 kronor vart femte år. Så som identitetshandlingarna utformats krävs en stödjande infrastruktur för att användare ska kunna legitimera sig, för spärrkontroller, identitetskontroller och identitetsintyg samt tillhörande kanaler för säker digital kommunikation av dessa uppgifter. En ansökningsavgift om 400 kronor kan dessutom bli ett betydande belopp för många. Det finns därför enligt Advokatsamfundets mening skäl att närmare genomlysa och överväga andra former för finansiering.

SVERIGES ADVOKATSAMFUND

Anne Ramberg