kirei

Yttrande

2024-01-31

Finansdepartementet
Dnr. Fi2023/02704

Yttrande över Utredningen om säker och tillgänglig digital identitets delbetänkande (SOU 2023:61)

Kirei AB önskar lämna följande yttrande över Utredningen om säker och tillgänglig digital identitets delbetänkande (SOU 2023:61). I vårt yttrande har vi valt att endast kommentera några övergripande frågor som vi anser kräver ytterligare utredning.

Om användningen av biometriteknik

Utredningen föreslår att fingeravtryck och ansiktsbild ska registreras i samband med utgivningen av den statliga e-legitimationen, i huvudsak i syfte att senare användas för identifiering av innehavaren på distans. Vi avstyrker utredningens förslag i dessa delar.

Vad beträffar fingeravtryck har den idag tillgängliga biometritekniken inte de efterfrågade egenskaperna. Fingeravtryck kan inte användas för tillförlitlig identifiering på distans. Denna fråga har belysts i andra sammanhang, och behöver inte utvecklas ytterligare här. Det framstår därför som något märkligt att utredningen först konstaterar att förutsättningarna för fingeravtrycksavläsning på distans saknas (s. 138), och i nästa led gör gällande att behandlingen av fingeravtryck är nödvändig av säkerhetskäl (s. 230). Med denna logik skulle det inte vara möjligt att införa en statlig e-legitimation.

Såvitt gäller behandling av biometriska uppgifter som framställts ur ansiktsbilder är förutsättningarna något annorlunda. Moderna smarttelefoner har kameror som kan användas för att ta upp bildsekvenser av den som använder telefonen, och överföra dessa till en motpart. Inledningsvis kan det konstateras att detta skulle kräva tillgång till utrustning som begränsar den statliga e-legitimationens tillgänglighet. Jämfört med en vanlig elektronisk identifiering är det är också fråga om förhållandevis komplicerande förfaranden att genomgå för innehavaren. Detta får oundvikligen negativ påverkan på användbarheten och tillgängligheten, särskilt för de grupper som idag riskerar ett digitalt utanförskap. Målet att den statliga e-legitimationen ska vara tillgänglig för alla skulle därför inte kunna uppnås om något liknande det utredningen föreslår skulle göras tvingande.

Det kan påpekas att de föreslagna åtgärderna skulle ha begränsad inverkan på möjligheterna att skydda innehavaren av e-legitimationen från att utsättas för olika former av bedrägerier. Detta då bedragare idag i huvudsak inriktar sig på att vilseleda innehavaren av e-legitimationen att bruka den på ett sådant sätt att gärningspersonen gagnas. I dessa situationer är det således inte fråga om obehörig användning av e-legitimationen.

Utredningen synes istället ha haft för ögonen den problematik som aktualiseras genom att så kallade målvakter överlämnar sina e-legitimationer och personliga koder till en huvudman, som i sin tur använder dessa för att begå brott i olika former. Kännetecknande för denna problematik är att den rättmätige innehavaren av e-legitimationen medverkar i brottsupplägget. Här önskar man således införa en kontroll att den som erhållit en e-legitimation också är den som brukar densamma. Det kan vid första anblicken framstå som en lysande idé, men i själva verket finns betydande svårigheter att åstadkomma detta på ett effektivt sätt. Dessa svårigheter har inte berörts i delbetänkandet på något relevant sätt. Några av de mer uppenbara frågorna är:

- Sverige har idag ett väl utbyggt och fungerande e-legitimationssystem där uppåt 90% av befolkningen använder e-legitimationer dagligen. Denna spridning och detta genom-

slag är större än i någon annat land i världen. Samtidigt är e-legitimationssystemet idag en infrastruktur där flera olika typer av e-legitimationer är gångbara, såväl nationella som utländska. Alla typer av e-legitimationer kommer inte att ha stöd för att förmedla ansiktsbilder för biometrisk jämförelse, av olika skäl. E-legitimationer ska också vara tillgängliga och kunna användas av alla. Vilka alternativ ska erbjudas den som av olika anledningar inte kan eller inte vill genomgå en biometrisk identitetskontroll?

- Om svaret på den föregående frågan är att personen ifråga får genomföra sitt ärende på traditionellt vis, på pappersblankett till exempel, vilka kontroller utför förlitande aktör vid ärendehandläggningen då? Vid traditionell handläggning sker vanligen inga identitetskontroller alls. Hur ska denna asymmetri hanteras? Myndigheter kan till exempel knappast vägra att handlägga ett ärende för att den enskilde inte har rätt teknisk utrustning eller att andra förutsättningar att genomgå den biometriska identifieringen saknas.

- Även om förutsättningarna skulle finnas att genomföra en biometrisk identitetskontroll baserad på ansiktsbilder, kommer denna kontroll oundvikligen att fallera i en viss andel av fallen. I ett väl avstämt system för biometrisk identitetskontroll kan det förväntas att cirka 5-6% av alla kontroller misslyckas (så kallade *falska negativa utslag*). Hur ska dessa situationer hanteras? Det är knappast acceptabelt att en sådan stor andel av alla ärenden där biometrisk identitetskontroll är påkallad inte kan genomföras elektroniskt. Den börda en manuell hantering skulle medföra kan komma att bli ohanterlig. Det måste alltså finnas andra automatiserade rutiner som tar vid då de biometriska jämförelserna misslyckas. Hur ska dessa se ut?

- Om biometriska identitetskontroller baserade på ansiktsbilder ska genomföras, vem ska då utföra dem? Ska varje förlitande aktör inrätta egna system och behandla biometriska uppgifter i den egna verksamheten? Förutom att det skulle leda till avsevärda kostnader att inrätta alla dessa system skulle det även medföra en omfattande spridning av känsliga personuppgifter. Vore det ett bättre alternativ att i så fall låta utfärdaren av e-legitimationen göra kontrollerna i samband med autentiseringsprocessen och utställandet av identitetsintyget? När och i så fall för vilka syften ska då den biometriska kontrollen kunna utföras?

- Ytterligare en fråga av avgörande betydelse är hur de kriminella aktörerna kan tänkas svara på införandet av biometriska kontroller. Risken är betydande att problemet endast flyttas från ett led till ett annat. Medger till exempel undantagshanteringen enligt ovan att ärendena kan utföras ändå? Kommer de kriminella att välja e-legitimationer som inte har stöd för biometriska kontroller? Är kontrollerna ens effektiva, kan det till exempel säkerställas att den som kontrollerar e-legitimationen är samma person som avbildas i videoströmmen? Här kan man tänka sig såväl mer som mindre raffinerade sätt att kringgå kontrollerna. Till de mer triviala exemplen hör att låta målvakten i fråga, mot en mindre ersättning, också medverka i kontrollerna. Det skulle också kunna ske från en helt annan plats än där den verkliga gärningsmannen befinner sig. Mer raffinerade sätt, men som kan omsättas i större skala, kan innefatta att låta datorgenerera bildströmmar som avbildar innehavarna (s.k. *deep fakes*) för att lura funktionerna för biometrijämförelserna. Riskerna är uppenbara att de kriminella aktörerna anpassar sina modus och finner vägar runt biometrikontrollerna, med resultatet att avsevärda tröskeleffekter införts i e-legitimationssystemet, med betydande kostnader för både produktivitet och tillgänglighet, utan att de efterfrågade nyttorna uppstår.

Det är aktningsvärt att utredningen försökt finna möjligheter att utveckla e-legitimationstekniken bortom det som växt fram genom de senaste decenniernas arbete i Sverige och internationellt, inom såväl privat som offentlig sektor. Utredningen har emellertid inte gjort de analyser och överväganden som krävs för att erhålla en komplett bild av utmaningarna med biometritekniken. Dessa är av såväl teknisk som säkerhetsmässig natur. De berör tillgänglighet, användbarhet, effektivitet och har den vägen materiell påverkan på e-förvaltningen och de kostnader och nyttor som är knutna till denna. Inte minst har man också att utreda de juridiska förutsättningarna och skyddet av enskildas grundläggande rättigheter och friheter.

Åtgärder av detta slag kan inte göras lättvindigt eller bygga på önsketänkanden. Det är på det hela taget svårt att se att användning av biometriteknik i samband med elektronisk identifiering på distans med dagens teknik skulle kunna leda till någon betydande positiv inverkan på säkerheten i identifieringsprocesserna. Målvaktsproblematiken får i det övergripande perspektivet betraktas som en tämligen begränsad företeelse, även om följderna av den kan vara nog så allvarliga i de enskilda fallen. Likväl, det skulle krävas ett paradigmskifte i tillgänglig teknik för att biometrijämförande kontroller på distans ska kunna införas på ett säkert, tillgängligt och användbart sätt, något som inte kan förväntas ske inom en överskådlig framtid.

Om regeringen överväger att införa biometrisk identitetskontroll som del av e-legitimationssystemet behöver bland annat de frågor vi lyft fram här grundligt utredas vidare. Till dess kvarstår att de mest betydelsefulla åtgärderna som kan vidtas idag sker i förlitande aktörers verksamheter. Genom införande av bättre kontroller i ärendehandläggningen kan det stora flertalet bedrägerimönster identifieras, motverkas och i många fall förhindras. Ökad möjlighet till informationutbyte har även lyfts fram för att kunna komma åt den kriminella ekonomin[1].

Författningsreglering av användningen av e-legitimationer

Sverige är ett av få länder inom EU som inte författningsreglerat användningen av e-legitimationer. Vid ett införande av en statlig e-legitimation kan därför behovet av särskilda bestämmelser om till exempel ansvarsbegränsningar och aktsamhetskrav i samband med användning av e-legitimationer behöva ses över. Det kan övervägas om en reglering som är anpassad till den utveckling som ägt rum bör omfatta all användning av e-legitimationer, och inte endast den tänkta statliga e-legitimationen.

Utredningen lyfter bland annat fram att det är hur en e-legitimation används som avgör vilken reglering som blir tillämplig. Bland annat gäller skilda regler för om e-legitimationen används för identifiering eller om den används för underskrift. Men i själva verket är det inte möjligt att bruka en e-legitimation för underskrift, utan att den i samma åtgärd också används för

[1] Stärkta åtgärder mot penningtvätt och finansiering av terrorism (SOU 2021:42).

identifiering[2]. Ändå bedöms de två åtgärderna på helt skilda sätt i rättspraxis[3].

I vissa fall är en e-legitimation även ett betalningsinstrument enligt lagen (2010:751) om betaltjänster. Utredningen gör tolkningen (s. 195) att om en e-legitimation används för att genomföra en betalning anses den utgöra ett betalningsinstrument.

Denna tolkning är dock felaktig, och utgör en lucka i det juridiska skyddet för innehavaren i förhållande till en betaltjänstleverantör. Ett betalningsinstrument är en personlig anordning och/eller rutiner som *betaltjänstanvändaren och betaltjänstleverantören har träffat avtal om och som används för att initiera en betalningsorder*.[4] Endast då en e-legitimation används i relationen mellan *betaltjänstanvändaren och betaltjänstleverantören* gäller de regler om ansvar och aktsamhet som återfinns i 5 a kap. lagen om betaltjänster[5].

Detta har bland annat till följd att om en statlig e-legitimation skulle användas för att genomföra betalningar av något slag, så gäller inte de ansvarsbegränsningar och aktsamhetskrav som följer av betaltjänstlagen. För att sådana regler ska bli gällande krävs särskild reglering. Vi anser att det är angeläget att se över behovet av reglering av användning av e-legitimationer generellt och föreslår att en utredning tillsätts i detta syfte.

Fredrik Ljunggren, Kirei AB

[2]Jfr. hur undertecknaren ska kunna identifieras genom en elektronisk underskrift enl. förordning (EU) 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen), artikel 26(b).

[3]Jfr. Högsta Domstolens dom den 9 december 2021 i mål T 930-21.

[4]Prop. 2017/18:77 s. 118.

[5]Hovrätten för Västra Sveriges domar den 18 juni 2018 i mål nr T 3583-17 och den 29 november 2018 i mål nr T 2473-18.