

2016-11-11

Justitiedepartementet
103 33 Stockholm
samt via e-post till
sara.ahmed@regeringskansliet.se

Hur står det till med den personliga integriteten? (SOU 2016:41)

Bankföreningen välkomnar utredningens kartläggning som är en intressant genomgång av integritetsriskerna inom ett antal sektorer i samhället. I remissyttrandet kommer dock Bankföreningen i första hand att begränsa sig till avsnittet som rör Bank- och kreditmarknad.

Inledningsvis vill Bankföreningen framföra att den instämmer i utredningens ståndpunkt att det inte bör skapas en ny myndighet för integritetsfrågor utan anser i likhet med utredningen att Datainspektionen ska få en utökad roll och arbetsuppgifter.

Bankföreningen och dess medlemmar delar utredningens syn att det, i likhet med vad som är fallet inom andra områden, kan finnas risker med bankernas behandling av personuppgifter. Till skillnad mot flertalet andra sektorer i samhället har emellertid bankerna sedan mer än hundra år omfattats av regler om banksekretess enligt vilka uppgifter om enskildas förhållanden till banken inte får röjas. Detta innebär att det är djupt förankrat hos bankerna och de bankanställda att uppgifter om enskilda ska skyddas. Eftersom förtroendefrågor är av högsta vikt för en bank så finns, utöver lagkraven, starka incitament och drivkrafter för bankerna att värna sina kunders integritet. Det nya regelverket för dataskydd (GDPR) kommer också att bidra till ett ökat skydd för den personliga integriteten när det gäller användningen av personuppgifter.

Det ska också tilläggas att bland annat penningtvättsregelverket uppställer krav på att bankerna ska lämna ut personuppgifter i samband med att bankerna rapporterar transaktioner till Finanspolisen när misstanken om t.ex. penningtvätt uppstår. Kundens personuppgifter kan också behöva lämnas till Finansinspektionen inom ramen för myndighetens tillsyn av bankerna. Fler legala krav att lämna ut personuppgifter kommer också att ställas på bankerna i framtiden, vilket ökar informationssäkerhetsriskerna.

Bankföreningen ifrågasätter beskrivningen av hur personuppgifter idag används inom den svenska banksektorn. Flertalet exempel är hämtade från den amerikanska marknaden och stämmer inte alls överens med hur svenska banker hanterar kunders personuppgifter.



Bankföreningen vill även lämna särskilda kommentarer gällande några textavsnitt.

Utredningen skriver (Sid 425)

"Särskilt med tanke på att appar ofta används på offentliga platser finns en ökad risk för att någon obehörig lyckas komma åt inloggningsuppgifterna. Denne skulle därefter, genom att enkelt ladda ner bankens app till sin egen smarta telefon, kunna logga in i appen och obehörigen ta del av en stor mängd uppgifter, utan att den behörige användaren märker det".

Det är inte troligt att en bank skulle hantera kundautentisering på ett sådant sätt. Även om en person råkar se en annan persons lösenord genom att befinna sig i närheten, kan den förstnämnda personen ändå inte ladda ner en bankapp och använda det lösenordet för att komma åt saldo eller genomföra transaktioner på den andra personens konto. Beskrivningen ger felaktigt intrycket att det skulle vara ett troligt scenario vilket det, när det gäller stark autentisering t ex användande av e-legitimationer, inte är. Det är därför enligt föreningens uppfattning olyckligt att denna beskrivning finns i betänkandet.

Utredningen skriver vidare (sid 425)

"I vissa fall föregås brotten av omsorgsfull planering t.ex. på det sättet att gärningsmannen beställer ett kreditkort eller en e-legitimation i någon annans namn och därefter stjälar det kreditkort, uppgift om koder eller liknande som skickas till den förment beställarens hemadress."

Bankföreningen uppfattar den återgivna texten ovan som att det skulle finnas säkerhetsbrister i e-legitimationer. Tvärtom är det så att e-legitimationer, till skillnad mot fysiska legitimationer, möjliggör att en bra kontroll i realtid av e-legitimationens giltighet vid inloggning och signering kan genomföras. Detta är en klar säkerhetsfördel hos e-legitimationer jämfört med fysiska legitimationer. E-legitimationer gör det digitala samhället enklare och mer effektivt.

Utmaningarna för banker med att utfärda en e-legitimation (BankID) består i att säkra steget från en fysisk legitimation till en e-legitimation. Utgångspunkten för att kunna få en e-legitimation är alltid att det finns en fysisk ID-handling. Svårigheten för banken är att avgöra om den fysiska ID-handling som presenteras är äkta eller falsk, eftersom förfalskningarna ofta är skickligt gjorda och kontrollmöjligheterna av fysiska ID-handlingar begränsade.

Ytterligare ett problem är att Sverige har en bred flora av ID-handlingar och de statliga myndigheterna (Transportstyrelsen, Skatteverket och Polisen) utfärdar ID-handlingar baserat på olika krav. Transportstyrelsen, Skatteverket och Polisen



utfärdar idag 95 % av de svenska ID-handlingar som bankerna godkänner. För fysiska ID-handlingar är det utfärdarna som äger processen för ansökan, produktion, distribution och verifiering av ID-handlingen. För utfärdarna av e-legitimationer består svårigheten alltså i att säkra steget från en fysisk legitimation till en e-legitimation. För en konsument är, som nämnts, utgångspunkten för att få en e-legitimation alltid en fysisk ID-handling. Det är i utfärdande- och distributionsprocessen som svagheter finns, eftersom denna baseras på verifieringen av fysiska ID-handlingar. Robustheten i e-legitimationssystemets utfärdandeprocess är inte starkare än den fysiska ID-handlingen och utfärdarens och distributörens möjligheter att verifiera ID-handlingen.

I Sverige finns det två utfärdare av e-legitimationer: Telias e-leg och bankernas BankID. BankID är Sveriges i särklass största e-legitimation: över sju miljoner unika personer har ett BankID idag (oktober 2016) och potentialen är åtta miljoner. Antalet transaktioner med BankID uppskattas till 2 miljarder under år 2016.

För att skapa en tillförlitlig process för identifiering och utfärdande av ID-handlingar i Sverige så bör en nationell gemensam utfärdandeprocess införas. Att fastställa en persons identitet och att utfärda en fysisk ID-handling baserat på den informationen är en kärnuppgift för staten. Det är t. ex. tveksamt om ursprungsidentifiering, ansökan och utlämning av körkort uppfyller de krav som bör ställas på ID-handlingar.

En nationell gemensam utfärdandeprocess bör innehålla:

1. krav på **ansökningsprocess** genom personlig inställelse, inklusive tagande av foto under kontrollerade omständigheter
2. bakgrundskontroll av den sökande (**ursprungsidentifiering**)
3. kvalitetssäkrad tillverkningsprocess av det fysiska ID-kortet (**kvalitetssäkring**)
4. krav på **utlämning** av ID-handlingen genom personlig inställelse och,
5. en fungerande kontroll mot utfärdaren/tillverkaren (**verifiering vid användning**)

Den enskilt viktigaste åtgärden är att åstadkomma en verifiering av den fysiska ID-handlingen genom en fungerande databaskontroll mot utfärdaren eller mot en centraliserad funktion. Utfärdarna och tillverkarna kan och bör bygga in ytterligare säkerhetshöjande detaljer i kortet, men det betyder litet om det inte på ett enkelt sätt går att verifiera handlingens äkthet gentemot utfärdaren. Den kontrollen validerar en delmängd av de uppgifter som finns på den presenterade handlingen, exempelvis att ett -kort med angivet nummer tillverkats och inte är rapporterat förkommet. Utfärdare av svenska ID-handlingar har ingen skyldighet att tillhandahålla en fungerande databaskontroll av en ID-handlings giltighet. En sådan skyldighet bör införas.



Svenska
Bankföreningen
Swedish Bankers' Association

Det är alltså inte e-legitimationen i sig som är problemet utan de begränsade kontroll- och valideringsmöjligheter av fysiska ID-kortet. Motsvarande frågeställning berörs även på sidan 426. Det är en viktig integritetsfråga att svenska staten tar ett större ansvar för att skydda våra personliga identiteter bättre. En viktig del i det arbetet är att få till stånd en bättre ordning för utfärdande och kontroll av fysiska ID-handlingar.

SVENSKA BANKFÖRENINGEN

Tomas Tetzell

Agneta Brandimarti