

Modern datadelning med integritetsfrämjande teknik

Av Erik Janzon, Fredrik Qvist och Ann Sofie Silversved



Erik Janzon



Fredrik Qvist



Ann Sofie Silversved

Tänk om en myndighet kunde identifiera vilka personer som har rätt till ett bidrag, eller vilka personer som inte har rätt till det, utan att få tillgång till uppgifter om deras faktiska inkomster. Eller om flera vårdgivare kunde träna en gemensam AI-modell utan att patientuppgifter behövde lämna respektive organisation. Eller om det gick att på ett tillförlitligt sätt fastställa risken för att enskilda personer identifieras i en datamängd som ska tillgängliggöras som öppen data. Detta är inte längre enbart teoretiska resonemang utan faktiska möjligheter med hjälp av integritetsfrämjande teknik – *Privacy Enhancing Technologies*, PET.

I den statliga utredningen *En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning* (SOU 2026:44) analyserar vi ett antal sådana tekniker och deras rättsliga och praktiska förutsättningar. Utredningen behandlar bland annat moderna tekniker för anonymisering såsom differentiell integritet (*differential privacy*) och syntetiska data. Därutöver behandlas nya tekniker

som möjliggör analys och kunskapsdelning utan att de underliggande uppgifterna behöver delas mellan aktörerna. Exempel på sådana tekniker är federerad inläring, säker flerpartsberäkning (*secure multi-party computation*) och homomorf kryptering (*homomorphic encryption*).

I det följande redogör vi kort för utredningens slutsatser kring integritetsfrämjande tekniks nytta och potential, rättsliga förutsättningar och framtidens moderna datadelning.

Från datadelning till kunskapsdelning

Traditionell datadelning innebär ofta att en aktör lämnar över uppgifter till en annan. För offentlig förvaltning kan detta vara problematiskt när uppgifterna är känsliga, omfattas av sekretess eller medför betydande integritetsrisker. Integritetsfrämjande teknik möjliggör ett annat angreppssätt. I stället för att dela själva uppgifterna kan aktörerna dela den kunskap eller det resultat som behövs. Säker flerpartsberäkning gör det exempelvis möjligt

för flera aktörer att genomföra gemensamma beräkningar på sina respektive datamängder under kryptering, utan att datamängderna behöver delas i klartext. I det enklaste exemplet kan två aktörer jämföra listor över personer med varandra och komma fram till hur många personer som finns på båda listorna, utan att exponera vilka personer som finns på respektive lista för varandra. Vid behov kan även uppgiften om vilka personer som finns med på båda listorna delas mellan aktörerna. Ett annat exempel på integritetsfrämjande teknik som möjliggör kunskapsdelning är federerad inläring. Genom tekniken kan en AI-modell tränas gemensamt av flera aktörer, utan att det träningsdata som respektive aktör använder behöver delas med andra.

En ökad användning av integritetsfrämjande teknik kan innebära ett skifte i synen på datadelning. I stället för att utgå från att data måste överföras mellan aktörer kan uppgifterna i fler situationer lämnas kvar hos den som innehar datat och



Illustrasjon: Conolorbox

endast kunskap og insikter frå datamengden delas. Rätt utformad og använd kan integritetsfrämjande teknik göra det möjligt att tillgodogöra sig kunskap från data utan att de underliggande uppgifterna behöver exponeras. Integritetsskydd og datadelning behöver således inte vara motstående intressen utan förenas i modern datadelning.

Integritetsfrämjande teknik som teknisk skyddsåtgärd

Integritetsfrämjande teknik kan inte bara göra datadelning möjlig i situationer där det annars skulle vara svårt eller olagligt att dela uppgifter. Teknikerna kan också vara en del av de skyddsåtgärder som krävs enligt dataskyddsförordningen. Pseudonymisering og kryptering nämns uttryckligen som exempel på sådana åtgärder, og vid valet av åtgärder ska även den senaste utvecklingen (*state of the art*) beaktas. Vad som utgör den senaste utvecklingen är inte statistiskt utan behöver bedömas kontinuerligt og i förhållande till vilka tekniska möjligheter som faktiskt finns.

I utredningen har vi bedömt att integritetsfrämjande tekniker kan utgöra lämpliga tekniska skyddsåtgärder, en bedömning som stöds av uttalanden från IMY og EDPB.¹

¹ Europeiska dataskyddsstyrelsen (EDPB), Guidelines 1/2026 on processing of personal data for scientific research purposes, adopted version for public consultation, s. 65 og Integritetsskyddsmyndigheten (IMY), IMY-2025-5444, Betrodda exekveringsmiljöer för uppkopplade fordon, s. 5, 13 og 23.

Flera av de tekniker som berörs i utredningen kan dessutom anses ligga inom ramen för vad som är *state of the art*. Det gäller särskilt differentiell integritet, syntetiska data og säker flerpartsberäkning. Teknikerna har funnits inom forskning og akademi under en längre tid men är ännu inte allmänt etablerade i praktisk användning.

Det innebär att aktörer som ska dela eller bearbeta data som innehåller personuppgifter bör överväga om det är lämpligt att använda integritetsfrämjande teknik som ett ytterligare skyddslager för sin personuppgiftsbehandling. Det innebär vidare att det inte krävs någon egen rättlig grund eller något eget ändamål för att använda integritetsfrämjande teknik. Användningen av integritetsfrämjande teknik har till syfte att stärka säkerheten i samband med en personuppgiftsbehandling, på samma sätt som behörighetsstyrning, loggning og andra skyddsåtgärder.

Omfattande potential för offentlig datadelning

Betydelsen av integritetsfrämjande teknik är inte begränsad till skyddet för personuppgifter. Användningen vid datadelning kan även bidra till ökad effektivitet, säkerhet, kvalitet og service samt till bättre beslutsunderlag og ökad innovation inom den offentliga förvaltningen. Den samhällsekonomiska potentialen för användning av integritetsfrämjande teknik i samband med datadelning inom offentlig förvaltning är också betydande. En analys som RISE har

genomfört på uppdrag av utredningen uppskattar nyttan av ökad og förbättrad datadelning till mellan 30 og 80 miljarder kronor per år. Av detta bedöms mellan 10 og 40 miljarder kronor vara direkt beroende av att integritetsfrämjande teknik används.

I utredningen beskriver vi flera användningsområden för integritetsfrämjande teknik. Dessa spänner över stora delar av den offentliga förvaltningen. Ett sådant område är hälso- og sjukvård, där stora mängder känsliga personuppgifter hantearas. Det finns samtidigt ett stort behov av att dela og använda data för vård, forskning og verksamhetsutveckling. Federerad inlärning og syntetiska data kan till exempel användas för att minska behovet av att dela patientuppgifter, vilket bland annat ett svenskt projekt visar där gemensamma AI-modeller för att förutsäga vårdtider har utforskats.²

Ett annat område är brottsförebyggande og brottsbekämpande verksamhet, där stora mängder data behöver samlas in og analyseras. Integritetsfrämjande teknik kan bidra till att begränsa både vilken information som behöver behandlas og vem som får tillgång till den. I internationella pilotprojekt har det bland annat undersökts hur federerad inlärning og homomorf kryptering kan användas för att motverka penning-

² AI Sweden, Syntetiska data inom intensivvård

” En utveckling mot kryptering som regel, där data endast dekrypteras i undantagsfall, skulle kunna förena två till synes motstående intressen – ett ökat nyttjande av data och ett starkare skydd för den enskilde

Även inom andra områden av den offentliga förvaltningen finns det stor potential med användningen av integritetsfrämjande teknik. Internationellt finns det flera exempel på användning av teknikerna. Säker flerpartsberäkning och homomorf kryptering används för att identifiera pensionärer som har rätt till ett underutnyttjat bidrag i Nederländerna.⁴ Differentiell integritet och syntetiska data har använts för att offentliggöra uppgifter ur Israels födelseregister som kan användas som underlag för framtida politiska beslut.⁵ Federerad inlärning och betrodda exekveringsmiljöer (trusted execution environments) har använts för att samla in känsliga data och möjliggöra analys och träning av en gemensam AI-modell som ska ge bättre beslutsunderlag om bland annat bevattning och

skadedjursbekämpning för vinodlare i Spanien och Italien.⁶

Datadelning i framtiden

Trots potentialen används moderna integritetsfrämjande tekniker fortfarande i begränsad omfattning inom den offentliga förvaltningen. Vi har i utredningen konstaterat att många myndigheter saknar kunskap, erfarenhet och teknisk kompetens, vilket kan leda till överdriven försiktighet och att möjligheterna till datadelning inte tas till vara. Det finns inte heller någon tydlig nationell styrning av användningen av integritetsfrämjande teknik i Sverige, och det saknas även i Norge, Finland och Danmark. För att öka användningen av teknikerna vid datadelning inom den offentliga förvaltningen har vi föreslagit åtgärder som ska höja kunskapsnivån och underlätta den tekniska användningen. I korthet innebär förslagen att Myndigheten för digital förvaltning (som slås ihop med Post- och telestyrelsen 1 januari 2027) ska få i uppdrag att ge stöd och vägledning om integritetsfrämjande teknik till offentlig förvaltning. Vi har också föreslagit att Skatteverket ska tillhandahålla förvaltningsgemensamma tjänster som gör vissa tekniker lättare att använda. En förvaltningsgemensam tjänst för säker flerpartsberäkning pekas ut som en första sådan tjänst. Vi har även föreslagit uppdrag till vissa myndigheter för att stimulera användningen av teknikerna, bland annat att Socialstyrelsen ska utforska användningen av differentiell integritet inom hälso- och sjukvården.

Mot bakgrund av den tekniska utvecklingen och de ökande kraven på skydd för personuppgifter och andra känsliga uppgifter framstår det som sannolikt att kryptering på längre sikt kommer att få en alltmer cen-

tral roll i samhällets informationshantering. Utvecklingen går från att data huvudsakligen skyddas vid överföring och lagring till att skyddet även omfattar själva bearbetningen. Genom så kallad krypterad databehandling (*encrypted computation*) kan beräkningar utföras på krypterade data, bland annat genom säker flerpartsberäkning. På motsvarande sätt utvecklas inom integritetsbevarande maskininlärning (*privacy-preserving machine learning*) metoder för att träna AI-modeller på krypterade eller på annat sätt skyddade data. Att kryptering väntas få en större betydelse vid all informationshantering ligger även i linje med den moderna cybersäkerhetsmodellen Zero Trust, där säkerheten utgår från kontrollmekanismer som auktorisering och kryptering istället för systemgränser och organisatoriska avgränsningar.⁷ Sammantaget framstår det därför som sannolikt att kryptering successivt utvecklas från att utgöra en kompletterande skyddsåtgärd till att bli till regel i all datahantering.

En utveckling mot kryptering som regel, där data endast dekrypteras i undantagsfall, skulle kunna förena två till synes motstående intressen – ett ökat nyttjande av data och ett starkare skydd för den enskilde. Fler insikter kan då utvinnas och delas, vilket skapar stora nyttor samtidigt som mindre data behöver göras tillgängliga i läsbar form. Genom de förslag som utredningen har lämnat kan den offentliga förvaltningen ta de första stegen mot en modernare datadelning.

Erik Janzon var särskild utredare, Fredrik Qvist huvudsekreterare och Ann Sofie Silversved sekreterare i Utredningen om integritetsfrämjande teknik i förvaltningen.

3 Infocomm Media Development Authority, Preventing financial fraud across different jurisdictions with secure collaborations IMDA PET sandbox – Mastercard case study.

4 <https://www.tno.nl/en/newsroom/insights/2021/09/targeted-yet-privacy-friendly-approach/> (hämtad 2026-08-25).

5 S. Hod & R. Canettis, 2025, Differentially Private Release of Israel's National Registry of Live Births.

6 <https://cordis.europa.eu/project/id/101129822> (hämtad 2026-08-25) och <https://titan-cosc.eu/> (hämtad 2026-08-25).

7 Z. Adahman, A. W. Malik & Z. Anwar, 2022, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security", Computers & Security, Volume 122.