Kommittén för teknologisk innovation & etik

Komet kommenterar

Differentiell integritet – korta faktablad om aktuell teknik

Komet kommenterar 2021:07, publicerad 2021-08-26

Kort om differentiell integritet (en teknik för att skydda integriteten hos de som lämnat data, t ex till myndigheter eller företag) – för beslutsfattare och andra som är nyfikna på hur aktuell teknik påverkar samhället.

Kommenterad rapport

Gandhi R. and Jayanti A. **Differential Privacy**. *Tech factsheets for policymakers*. Fall 2020 Series. Center for Science and International Affairs, Harvard Kennedy School[1]

Korta faktablad om aktuell teknik

Belfer Center vid Harvard University ger ut en serie faktablad om aktuella teknikområden. Serien är riktad till politiska beslutsfattare i USA i syfte att ge överblick och förståelse av ny teknik. Komet Kommenterar gör en svensk uppföljning av serien.

Belfer Center for Science and International Affairs är del av Harvard Kennedy School of Government. Belfer arbetar bland annat med hur ny teknik kan komma till nytta i samhället.

Komet:s kommentarer

- Differentiell integritet är en teknik för att skydda enskildas integritet vid behandling av data. Det finns flera andra tekniker i samma syfte. I sådana sammanhang brukar man skilja mellan avidentifiering (all information som kan identifiera en person tas bort helt och hållet, något som ibland kallas anonymisering) och pseudonymisering (viss information om enskilda personer finns kvar i datamängden, men den är på något vis bearbetad så att det ska bli svårare att sortera ut data från en viss specifik individ).
- Regelverket i Europa skiljer sig från det i USA. För länderna inom EU reglerar dataskyddsförordningen (GDPR, General Data Protection Regulation) hur data om enskilda personer får hanteras, bland annat avseende ansvar och krav på informationssäkerhet. En EU-förordning är bindande och gäller direkt i varje medlemsland. I Sverige kan en EU-förordning jämställas med en svensk lag.[2]
- Det amerikanska faktabladet beskriver hur företag använder differentiell integritet för att hantera platsdata, till exempel i kartfunktioner och vid pandemier. EU-kommissionen och Europeiska dataskyddsstyrelsen har gett ut en riktlinje om hur platsdata kan användas för smittspårning.[3] De menar att platsdata är nästan omöjliga att anonymisera, vilket ställer höga krav på den som trots allt använder sådana data.
- I USA görs en folkräkning vart tionde år, då en särskild myndighet samlar in uppgifter från landets invånare. År 2020 användes differentiell integritet för första gången som teknik för att skydda den personliga integriteten hos alla dem som lämnat uppgifter. Myndigheten tog fram en hel del informationsmaterial, bland annat en film som på ett lättillgängligt sätt beskriver frågeställningen, utmaningarna och tekniken.[4] I filmen beskrivs statistiken bakom metoden med ett exempel som tittar närmare på glass, grannar och gifta personer.

Länkar

1. www.belfercenter.org/sites/default/files/files/publication/diffprivacy-3.pdf
2. Rapporten Så funkar det! Om lagar och regler (Komet beskriver 2021:05) ger exempel på regler om personuppgifter
3. edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en
4. https://youtu.be/pT19VwBAqKA

Sammanfattning av originalrapporten

Författarna ser flera fördelar med differentiell integritet, särskilt att tekniken ger ett hyfsat robust skydd för personernas integritet. De menar också att tekniken främjar transparens och öppenhet, eftersom den gör det möjligt att beskriva mönster och dela sammanställningar utan att avslöja de unika data som den bakomliggande analysen bygger på. Ytterligare en fördel är att tekniken tål viss osäkerhet och felmarginal. Enligt författarna öppnar tekniken nya möjligheter för åtkomst till data som tidigare inte kunnat delas, såsom särskilt känsliga data inom medicin- respektive finanssektorn.

Men författarna ser också flera utmaningar, till exempel att det behövs stora mängder data för att uppnå tillräcklig noggrannhet. Bristen på riktlinjer för vad som är ”tillräckligt integritetssäkert” gör att företagen för närvarande tillåter ett svagare integritetsskydd än vad forskarsamhället finner acceptabelt, menar de. Ytterligare en utmaning är det finns alltför få verktyg för att arbeta med tekniken, och alltför få experter som behärskar den. Trots nackdelarna används tekniken redan av såväl stora teknikföretag som av amerikanska myndigheter.

Politiken har hamnat på efterkälken, menar författarna. Dagens regelverk bygger på att data kan kopplas till en unik person, och de begrepp som används fungerar inte riktigt för att reglera tillämpning av differentiell integritet. Enligt författarna saknas idag riktlinjer för att implementera differentiell integritet på ett säkert sätt. De ser därför ett behov av att snarast se över regelverken för såväl sekretess som integritet.

Kort om tekniken

Differentiell integritet gör det svårare att identifiera en specifik individs unika uppgifter vid publicering av resultat som bygger på sammanställning och analys av data från en mängd olika personer.

Tekniken kan beskrivas som ett sätt att få ut så mycket information som möjligt om en grupp, och samtidigt avslöja så lite som möjligt om varje enskild person som ingår i gruppen.

Tekniken bygger på en matematisk definition av integritet, där man bestämmer hur stor risk att avslöja data om en enskild individ man är beredd att ta.

Rent praktiskt går tekniken ut på att förändra data litegrann, genom att ta bort eller byta ut en liten andel data eller genom att lägga på ett matematiskt brus.

Stora företag tillämpar tekniken

Flera företag använder differentiell integritet i sina produkter, samt vid forskning och utveckling. Rapporten tar upp några exempel på applikationer:

- Microsoft använder tekniken i flera applikationer t ex Windows, LinkedIn och Office.

- Apple använder tekniken i iPhones, t ex för hälsorelaterade data.

- Google tillämpar tekniken i Maps och för maskininlärning. Snapchat har den för att träna maskininlärningsmodeller.

- Uber har skapat ett verktyg för öppen källkod, för att effektivt kunna beräkna hur känslig en fråga är.

- Facebook använder tekniken för att dela data om hur personer rör sig, t ex vid skogsbränder och pandemier.

- Amazon har testat tekniken i analyser av kunddata och LinkedIn har testat den för marknadsanalys.

Om Komet Kommenterar
Komet kommenterar aktuella internationella rapporter som rör regelverk, teknikutveckling och innovation.
Syftet är att ge ett svenskt perspektiv, sätta information i ett sammanhang och göra underlaget lätt tillgängligt.

Kommittén för teknologisk innovation och etik (Komet) arbetar för att skapa goda förutsättningar för innovation och konkurrenskraft samtidigt som utvecklingen och spridningen av ny teknik sker tryggt, säkert och med ett långsiktigt samhällsperspektiv.

Detta informationsblad är sammanställt av kommitténs sekretariat.
Läs gärna mer på vår webb: kometinfo.se
e-post: n.komet@regeringskansliet.se