Metaintegritet – en ny modell för framtidens dataskydd

*Daniel Akenine**

Antalet aktörer som vi interagerar med och mängden persondata har ökat exponentiellt vilket gör att det är svårt att få en meningsfull kontroll över vårt data. Finns det andra modeller för att hantera vår personliga integritet i framtiden?

Dataskydd på järnåldern

Var kommer egentligen vårt behov av integritet från? Man kanske kan tro att det är något vi diskuterat genom årtusenden men sanningen är att det en ganska modern diskussion som vi i stort är ensamma om som människor. Vi delar många saker med andra djur, vårt behov av relationer, instinkter och vår strävan efter egna val, överlevnad och frihet. Men integritet är inte en av dessa saker. En pudel har inte rätt till sina egna hunddata och har inte heller ett behov av dem. Integritet är i stort en mänsklig konstruktion.

Det är inte heller så att vi alltid haft dagens intresse av integritet. Under större delen av mänsklighetens historia har vi levt i förhållandevisa små grupper av människor som känt till det mesta om varandra och på ett fysiskt plan har vi levt nära varandra. I gamla svenska jordbrukssamhällen där man kunde leva tio personer i ett rum pratade man nog inte om sin rätt att äga sina egna data. Dels hade man en annan bild av sin egen roll som människa jämfört med andra och gud, dels hade man knappast någon data att utöva en sådan rätt på.

Historiskt har det dessutom varit kostsamt och komplicerat att lagra data, för att inte tala om att bearbeta den. Att lagra större datamängder har fått göras på papper och innan papper var tillgängligt var möjligheterna ytterst begränsade. Att försöka behandla dessa datamängder och utvinna information och kunskap från dem har varit svårt i avsaknad av

* Nationell Teknikchef för Microsoft Sverige, författare och fysiker.

datorer. Vi har helt enkelt inte levt i en värld av data tidigare och har inte behövt utveckla vår syn på området förrän den senaste tiden. Därför heter det 50 år av dataskydd och inte 5 000 år av dataskydd. Så är det förstås inte inom många andra områden som medicin, juridik, mekanik, matematik och arkitektur som funnits med oss under årtusenden.

Så vad handlar dataskydd om idag?

Dataskydd för 2000-talet

Under den första halvan av de 50 åren av svenskt dataskydd gick det ändå ganska långsamt. Skälen var i huvudsak två. För det första var det dyrt att lagra data och för det andra skapade du sällan några nya data om dig själv. Visserligen hade vi för 50 år sedan både tillgång till datorer och beräkningskapacitet men samhället var långt ifrån det vi idag kallar för ”digitalt”.

Vi hade inte något internet, vi lämnade inte några digitala spår av våra liv och den data som lagrades om oss var svåråtkomlig och tillgänglig för ett fåtal. Digitalisering skedde centraliserat, i stordatorer som exekverade beräkningar och resultat. Över tid har fokus för persondata flyttats från centraldatorer till en periferi där vi på egen hand skapar nya data om oss själva bara genom att leva. När vi handlar, reser, tittar på TV, läser en tidning, tar en semesterbild m.m… så skapar vi en digital kopia av oss själva där vi kan se vilka val vi gör, våra intressen, våra ståndpunkter, våra värdering och politiska åsikter. De första 25 åren handlade dataskydd om att skydda fragment om oss själva, medan de senaste 25 åren av dataskydd handlar om att skydda vår egen digitala kopia från att missbrukas.

Men är det viktigt? Är det värt att skydda denna digitala kopia?

För att undersöka frågan skulle man kunna föreställa sig två extrema framtidsscenarier från ett lagstiftningsperspektiv (vi kommer lite senare även titta på hur framtidsscenarier kan se ut från ett tekniskt perspektiv).

Framtidsscenario 1: Vi lever i ett samhälle där vi saknar dataskydd

I ett sådant samhälle skulle vi veta i stort allt om varandra. Våra drömmar, ambitioner och intressen. Förmodligen inte alltför olikt de små samhällen vi levt i under stora delar av vår historia, men med den skillnaden att vi skulle vara exponerade mot en mycket större publik och påverkanskrafter. I ett så pass genomdigitaliserat samhälle som vi lever i så finns det inte någon möjlighet att välja alternativet ”nej tack, jag vill inte blir registrerad” vilket innebär att i ett samhälle som saknar data-

skydd skulle vi sakna några större möjligheter att påverka om data samlas in och hur den senare används.

Varför är det inte möjligt att säga ”nej, tack”?

Man ska komma ihåg att de flesta tjänster i vårt samhälle idag har gått från att hanteras via kontanter som en anonym betalningsförmedlare till att ha en kopplad digital identitet. En resa var länge kopplad till en fysisk biljett utan anknytning till någon annan än den som höll den i handen. Idag är en resa något som är kopplat till dig genom en digital biljett eller en betaltransaktion på ett kontokort. Tidigare var en tidning du läste något anonymt, idag är din läsning registrerad i olika system. Vår konsumtion är digital och att leva utan digitala spår skulle innebära att stå utanför det moderna samhället på ett sätt som i många fall inte längre är möjligt.

Vi skulle i ett sådant samhälle leva helt exponerade för många olika intressenter av vår data, kommersiella krafter, politisk påverkan eller annan maktpåverkan av okända krafter. En möjlig moteld skulle kunna vara en modell där all användning av denna data skulle tvingas vara öppen. Där man som individ alltid ska ha rätt att få tillgång till vem som konsumerat din data, och även en total transparens kring dess syfte. Genom att utkräva fullständig transparens åt båda håll, både för den som blir övervakad och den som övervakar skulle man kunna få en bättre maktbalans.

Det skulle kunna vara en enkel lösning och i en värld där människor inte längre uppfattar att integritet har ett större värde skulle det kanske kunna vara möjlig modell.

Framtidsscenario 2: Vi lever i samhälle där all användning av persondata är förbjuden

Vi skulle även kunna tänka oss en omvänd modell där man anser att användandet av persondata är så skadlig att man inte ens skulle kunna ge sitt samtycke till användande. Det finns flera liknande exempel där man anser att man inte kan ge sitt samtycke. Det kan röra sig om prostitution eller droger där man anser att skadan är så pass stor att den överstiger rätten att ge samtycke. Man skulle i ett sådant läge inte kunna ge samtycke till en organisation att använda någon data om dig utöver det som möjligen skulle vara absolut nödvändigt för att tillhandahålla en samhällsnödvändig tjänst.

I ett sådant samhälle skulle vi förbli i hög utsträckning anonyma gentemot varandra och i stort kanske återgå till att ingå i mindre grupper av individer där vi alla känner varandra.

Förmodligen skulle världen bli mer lokal och sociala medier i stort försvinna. Kanske gå mot ett samhälle som påminner om hur våra samhällen fungerade för hundra år sedan.

Båda dessa modeller känns främmande. Då data om oss själva, som vi tidigare diskuterat, inte bara är fragment av oss själva idag utan i praktiken representerar oss själva står det klart att scenario 1, total transparens, skulle begränsa oss i ett modernt samhälle. Vi skulle tveka inför hur vi reser, vad vi handlar eller vad vi säger då det skulle få större konsekvenser än idag. Total transparens skulle paradoxalt nog förmodligen skapa ett mer begränsande liv, inte ett mer öppet.

I scenario 2, ett samhälle med för starkt dataskydd, skulle också våra liv bli begränsande, vi skulle inte kunna tillvarata internets kraft som plattform och världen skulle krympa. Vi skulle dessutom inte kunna få tillgång till flera av de innovationer som idag har skapats på internet när det gäller sociala plattformar och många av de tjänster som finns idag skulle vara mer begränsade. Vi skulle leva mindre bekväma liv som i högre utsträckning skulle fyllas med manuell administration.

Den förhandlade kontraktet mellan individer, organisationer och samhället är det som GDPR handlar om. I grunden bygger vårt existerande dataskydd på att individer har just en rätt att ge samtycke till användning.

Men fungerar samtycke idag?

Om samtycke

Samtycke är själva basen i många av de tjänster som vi har runt omkring oss idag och principen i sig är enkelt att förstå. Men fungerar det praktiskt?

Principen kring samtycke till användning av din data bygger på att du har tid, kunskap och intresse. Vi har alla mötts av sida upp och sida ner av avtalsvillkor när du börjar använda en digital tjänst. Det skulle kanske vara rimligt i en värld där du använder några få digitala tjänster. Men du använder förmodligen runt hundra. Ingen läser alla dessa villkor i detalj. Har de positiva eller negativa effekter för dig? Hur förändras dessa villkor över tid? Hur används dessa data om tio år? De flesta människor har en förhoppning att regelverk som GDPR på något sätt hantera denna balans åt dig eller att man har ett förtroende för varumärket som man ger samtycke till. Det finns en slags förhoppning att någon annan har läst villkoren och tagit ansvaret för att de är ok och man klickar på ”godkänn” med en tydlig klump i magen.

Om man frågar hundra människor frågan ”Känner du att du har en fullständig kontroll över vilken data om dig som används och vem som använder den?” så får man väldigt få händer i luften. Förmodligen inte en enda.

Däri ligger en stor brist med dagens dataskydd, även om principerna kan fungera i teorin så fungerar de inte alltid i praktiken. När mängden data om dig ökar så skalar inte människors förmåga att kontrollera sin rätt över denna data på samma sätt. Samtycke har på många sätt gått sönder i en värld av för mycket data.

Metaintegritet – framtidens dataskydd

Förenklat är dagens dataskydd skapat för tio år sedan av personer födda för sextio år sedan. Det är resultatet av den teknik som fanns vid tillfället och ett synsätt på integritet som är influerat av den för-digitala tiden utan AI eller Big Data. När generation X, Y och Z ersätts av framtida generationer så följer det med nya sätt att förhålla sig till integritet och digitalisering. Samtidigt som förhållningssätt till integritet förändras så förändras också de tekniska möjligheterna för dataskydd.

Det kan röra sig om nya möjligheter med integritetsfrämjande teknik för att anonymisera stora datamängder, unika krypteringsmöjligheter som homomorfisk kryptering som kan kombinera integritet med användning samt molnbaserade infrastrukturer som kan leverera i stort en ändlös, kostnadseffektiv lagring och snabba tillgängliga API’er.

När tekniken fortsätter utvecklas ökar både hungern efter nya data samt möjligheterna att skydda dem.

Så om vi tittar framåt mot nästa 50 år av dataskydd, hur kan framtidens digitala värld se ut och vilken typ av dataskydd skulle kunna vara möjlig att bygga?

Den överliggande trenden under tiotalet år är ett ökande digitaliserat samhälle drivet av teknikutveckling och innovationer. Mycket av det som tidigare var fysiskt och svårt att tro att det någonsin skulle kunna digitaliseras är idag digitalt, det kan röra sig om fysiska saker som pengar, bilder, musik eller ID kort. För 50 år sedan var det få som såg framför sig att vi skulle kunna betala med en teknisk pryl genom att snabbt vidröra en kassaterminal. Hur skulle det kunna gå till? Det är inte en innovation utan en kombination av många olika innovationer som mobilnät, mobiltelefoner, krypteringsfunktioner och annan infrastruktur. Saker som kan vara svåra att enkelt förutsäga sig då det är kombinationen av ett antal innovationer, inte en enstaka snilleblixt. Börjar vi

då bli färdiga med digitaliseringen och kan förvänta oss att världen ser ungefär likadan ut om 50 år som den gör idag? Självklart inte.

Man kan dock spekulera i två scenarios för hur vi väljer att anamma teknikutvecklingen och digitaliseringen i framtiden.

Tekniksc enarios 1: Ett digitalt Amish samhälle

I USA finns det över 350.000 personer som lever i ett Amish samhälle, en grupp som tar avstånd från modern teknik som digitalisering. En grupp som ökar. Det finns alltid människor som av religiösa, ideologiska eller filosofiska skäl väljer bort viss teknik och hur stor denna grupp blir i vårt framtida samhälle handlar mycket om vilka negativa effekter man får i förhållande till de positiva.

I ett digitalt Amish samhälle har vi reagerat på framtida effekter av digitalisering som varit negativa, det kan vara att vi tappar alltför mycket av vårt eget kunnande att hantera vardagen om vi automatiserar alltför mycket. Vi kanske tappar förmågan att köra bil, laga mat, läsa eller skriva om vi hela tiden har digitala hjälpmedel som gör det åt oss.

I ett sådant scenario skulle vi se ett romantiserande av det analoga och en teknikfientlighet som skulle få digitaliseringen att gå tillbaka och göra information om oss själva alltmer svårtillgänglig. Man kan idag se vissa sådana tendenser i form av en ökad digitaliseringskritik. Det kan röra sig om saker som skärmfria skolor eller generell kritik där man anser att digitalisering ger större negativa effekter än positiva. Detta är dock inte ett troligt scenario för framtiden, vi har som samhälle alltför stora utmaningar att hantera och att backa i digitalisering skulle skapa ett mer improduktivt samhälle och försämra vår välfärd.

Tekniksc enarios 2: Mot en transhumanismistisk framtid

I ett annat, mer troligare scenario, så ser vi en alltmer komplicerad sammansmältning av teknik och människor. Med hjälp av AI, kvantdatorer och mer data om oss själva kommer vi snart få en personlig läkare som diskret övervakar oss i jakt efter signaler på sjukdomar att behandla innan vi upptäcker dem själva. Kan man upptäcka cancerceller tidigt in våra kroppar så behöver inte cancer vara mycket mer besvärligt än en förkylning. Vi kommer ha avancerad generativ AI som är din närmaste kollega i nästan alla uppgifter där man behöver kommunicera, förbereda, planera eller skapa information. Vi kommer ha snabbare vägar in på internet via våra kroppar, först genom våra ögon och digitala glasögon och på längre sikt direkt inkoppling i våra hjärnor som förstärkning.

I ett sådant scenario kommer både vårt dataskydd och förmågan att upprätthålla detta dataskydd genom extremt hög IT-säkerhet inte bara ha ett integritetsmässigt intresse utan i bokstavlig mening många gånger handla om liv och död.

En ny modell för framtidens dataskydd: Metaintegritet.

Om man frågar en person om vad man är rädd att bli utsatt för när det gäller integritetsskador så handlar ofta svaren om att man är rädd för att bli manipulerad, att information blir tillgänglig som man skäms över, eller att någon använder din information för att ta över din identitet. Att stimulera användning men stävja denna typ missbruk bör prioriteras i en ny modell.

Några grundläggande principer för en ny modell.

- Det är missbruket i sig som är den huvudsakliga integritetsskadan, inte information som samlas in och lagras men inte används. Att persondata finns insamlad betyder inte att den kommer att missbrukas.
- Hur bra begreppet samtycke än låter så fungerar det inte bra i praktiken. I en värld av ”Big Data”, där du ger hundratals olika samtycken kämpar man lönlöst, likt Don Quijote, med att kontrollera berg av data om dig som finns hos olika aktörer. Man behöver mer generaliserade samtycken kring användning.

Hur skulle en ny modell för framtidens dataskydd kunna se ut?

En möjlig modell skulle vara att lämna den gamla arkitekturen där man i huvudsak ger samtycke till aktörer och i stället kopplar samtycket till data och användningstillfälle. För att få detta att fungera så behöver man tre huvudsakliga komponenter.

- Man behöver tagga all sin personliga information med en säker digital identitet.
- Man behöver tagga denna information med en integritetsprofil, dvs vilket typ av samtycke man gett till informationen.
- Man behöver en säker lagring av sin integritetsprofil.

I praktiken skulle det innebära att den data som finns om dig inte bara innehåller själva informationen utan är sammanlänkat med metadata som beskriver vad som är tillåtet och lagligt att göra med informationen. Ett exempel skulle kunna vara att man ger rätten att behandla geografiska data om sig själv för forskningsändamål men inte för kommersiella tillämpningar.

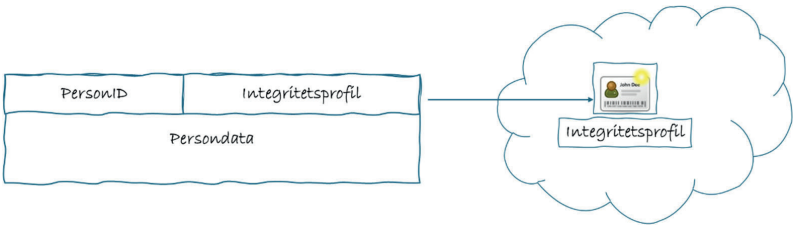

Bild: Persondata med metadata och kopplad integritetsprofil.

En sådan modell skiftar fokus från datainsamling och lagring mot tidpunkten då data används och i vilken kontext den används.

Det finns redan exempel på liknande modeller, exempelvis när det gäller Digital Right Managements. Inom musik och filmindustrin kan man kräva vissa rättigheter innan en film låses upp för att visas och inom företagsvärlden används digitala rättigheter som Information Protection för att få tillgång till säkerhetsklassade dokument baserat på din identitet och de rättigheter denna identitet ger dig. Tekniken bakom är beprövad.

Man kan tänka sig en modell där att alla applikationer som vill använda sig av din personliga data måste använda sig av liknande tekniker, det skulle innebära att all användning av din data automatiskt skulle registreras och ge transparens både kring vad som görs eller har gjorts. Missbruk av data eller denna modell skulle beivras kraftfullt.

Dina val sparas som en integritetsprofil i molnet och är tillgängligt för alla aktörer.

Samtidigt behöver man förstå vilka konsekvenser olika integritetsprofiler ger, en alltför strikt policy kanske gör att det många tjänster inte blir möjliga att använda så det gäller att skapa en profil som skapar en balans mellan sitt eget behov av integritet och vilka tjänster man behöver.

En viktig fråga är hur enkelt det är för en individ att skapa sin egen integritetsprofil? Hur får man kompetens att förstå vad din profil får för konsekvenser?

Det är inte så att man nödvändigtvis behöver skapa en sådan profil själv utan man kan tänka sig att det etableras aktörer man kan lita på och lämna över dessa beslut till. En aktör som till exempel konsumentverket skulle kunna ha färdiga integritetsprofiler man kan välja och använda.

Flera fördelar finns med en sådan modell:

- Man har bara en enda integritetsprofil som kontrollerar alla aktörer på marknaden.

- Man behöver inte ha kännedom om aktörer och bedöma vilket förtroende man bör ge dem.
- Man får en livslång och flexibel kontroll över sina egna data som är lätt att ändra över tid. Kanske är ditt behov av dataskydd annorlunda i 30-års åldern än i 130-års åldern?

Modellen ger dig en möjlighet att när som helst ändra din integritetsprofil och den skulle omedelbart slå igenom för all framtida användning. De data som samlas in idag kan ha nya användningsområden i framtiden som är svåra att utnyttja då samtycke för dessa framtida användningar kanske saknas. En dynamisk metamodell för samtycke skulle kunna adressera detta.

Att bygga en sådan ny modell på internet kräver en hel del arbete. Både kring teknisk infrastruktur, säkerhet, ändrad lagstiftning, internationell samverkan etc. men det är inte omöjligt för det land som är beredd att gå före.

Kanske en utmaning värdigt det land som 1973 införde världens första nationella datalag?