Företagens lilla katekes om INTEGRITET I EN UPPKOPPLAD VÄRLD

Termer och begrepp och vad de betyder

En produkt av tankesmedjan Digital Utmanings fjärde rådslag: *Integritet i en uppkopplad värld*. Rådslaget var i huvudsak verksamt under perioden oktober-december 2016.

I en uppkopplad värld lämnar vi spår, många spår

I Pekings kollektivtrafik har myndigheterna börjat analysera data från de digitala passerkorten för att identifiera resenärer som regelbundet uppehåller sig ovanligt länge i systemet. Syftet är att hitta ficktjuvar (The Economist 2016-08-20). Det är ett lovvärt syfte, men sådan information kan också användas i andra, mindre samhällsnyttiga, syften.

När vi handlar med betalkort i matbutiken registreras våra matvanor. Kan den informationen användas av försäkringsbolag eller sjukvård för att anmärka på vår livsstil? Alla appar vi använder i våra smarta maskiner lämnar ifrån sig data, data som samlas och används. Vi lever i ett övervakningssamhälle där de digitala spår vi lämnar ifrån oss används för olika syften, både sådana vi själva kan tycka är bra och syften som de flesta av oss troligen är skeptiska till.

Vi människor är förmodligen oftast medvetna om att vi lämnar gott om spår efter oss, men vi vet inte alltid vilka, hur de kan användas eller i vilken omfattning. Företag som samlar data bör tänka på det, och sträva efter att människor ska veta vad som händer då de lämnar ifrån sig data om sig själva.

En ”liten katekes” om integritet för företag

Nedanstående ”lilla katekes” resonerar kring ett antal begrepp kopplade till integritet, datainsamling och datahantering och hur dessa begrepp kan förstås. Skriften vänder sig till företag, stora som små, som mer eller mindre medvetet handskas med digitalt material som kan ha med integritet att göra. Vad vi som skrivit den vill uppnå är en ökad medvetenhet hos företagen om de utmaningar som uppstår då vi så enkelt kan veta alltmer om alltfler.

Vi vill kunna använda data på ett sätt som gynnar företag, användare och anställda. Men vi vill inte ”missbruka” data så att vi riskerar att få en motreaktion mot all datahantering. Att bruka men inte missbruka är katekesens budskap, samtidigt som vi är väl medvetna om att tolkningen av vad som är vad måste vara föremål för en ständig diskussion.

Rådslaget om integritet

Digital Utmanings rådslag om integritet har arbetat utifrån tanken att om problem kan identifieras tidigt så kommer de senare inte som en överraskning. Åtgärderna för att handskas med dem har då bättre förutsättningar att bli konstruktiva.

Tankesmedjan Digital Utmaning

Digital Utmaning är en tankesmedja som startats av IT&Telekomföretagen med uppdrag att belysa problem, möjligheter och utmaningar kring digitaliseringen. Tankesmedjan, som arbetar oberoende av förbundet, engagerar ett större antal experter, debattörer och opinionsbildare och arbetar problemorienterat.

Arbetet inom tankesmedjan sker i form av en strukturerad process med en serie arbetsmöten, så kallade rådslag, som leds av en person kallad Rådgivare. Ambitionen är att genomföra tre till fyra rådslag per år. Tankesmedjan Digital Utmaning leds av en styrgrupp med Lars Ilshammar som ordförande.

Personlig integritet är viktigt

Varför det?

Personlig integritet är en process med vilken vi formar oss själva som individer, inte en egenskap man har eller inte har. Personlig integritet ses tyvärr ofta som ett abstrakt begrepp, vilket är en av anledningarna till att det också är svårt att avgöra vad som egentligen är ett intrång i integriteten. Möjligheten att kunna forma sin egen personlighet, att utöva sina individuella uttryck, att forma och uttrycka egna åsikter, att undvika att uttrycka eller utöva dessa, och att kunna vara för sig själv ingår i det vi kallar personlig integritet.

Integritet är beroende av sammanhang

Vad betyder det?

Du väljer, förmodligen, att ha en viss sorts kläder på dig när du är på stranden. Skulle du plötsligt bli satt med exakt samma uppsättning kläder på ett torg eller i ett köpcentrum skulle du känna dig utsatt och uttittad. Informationen om dig, dina kläder, har inte på något sätt förändrats, men kontexten gör att du känner dig obekväm i en situation och inte i den andra. Det viktigaste för din integritet är alltså medvetenheten, anpassningsbarheten och kontrollen över vilken information om dig som är tillgänglig i vilket sammanhang.

För företag innebär detta att man måste kunna redogöra för i vilket sammanhang en användare befinner sig och hur deras data kommer att användas. Om användningen av personuppgifterna skiljer sig från vad användaren förväntar sig kommer det att kännas precis som för personen på torget – obekvämt och otryggt. Om sammanhanget däremot är tydligt och förväntningarna efterlevs, då skapas förtroende mellan användare och företag.

Metadata är personlig data

Vad betyder det?

Metadata är data om data, det vill säga informationen om transaktioner av information. Ta till exempel ett SMS. Metadata är avsändare och mottagare, tidpunkt då det skickas, textlängd och med vilken operatör det skickades. Även om man med metadata inte kan utläsa vad SMS:et innehåller så kan man dra slutsatser kring vem som pratar med vem, när och hur mycket. På samma sätt genererar våra surfmönster stora mängder metadata. Med denna information, vilka länkar någon klickat på för att komma till en sajt till exempel, kan man dra slutsatser om gruppers beteenden och med tillräckligt sofistikerade metoder kan man även i stora dataset identifiera enskilda individer baserat på deras beteenden, även utan tillgång till en personuppgift så som personnummer. Metadata är alltså inte anonymt eller integritetsvänligare än direkta personuppgifter, och man måste vara precis lika försiktig med användande och säkerhållande av sådana uppgifter.

Integritet eller integritet?

Vad är skillnaden?

I engelskan gör man skillnad på “privacy” och “integrity”, något vi inte gjort i svenskan. Svenskans integritet kan vara såväl “integrity”, med synonymerna god karaktär eller stabilitet, som “privacy”, som kan betyda ungefär privatliv eller personlig sfär. När vi talar om integritet här är det alltså privatliv eller personlig sfär vi menar, det som motsvarar engelskans ”privacy”. Man kan vara helt utan karaktär (integrity) men fortfarande ha ett behov av och rätt till privatliv (privacy).

Personuppgifter, persondata och personlig information

Vad är skillnaden?

I ordets vidaste betydelse så är all information som kan identifiera dig som person en personuppgift. Persondata är digitalt upprättade och skapade personuppgifter. Det kan vara metadata eller andra värden som är kopplade till din identitet och som används för att analysera eller registrera dig på olika sätt. Personlig information är uppgifter om dig som kan anses vara lite mer känsliga beroende på sammanhang.

I princip kan allt vara personuppgifter, så länge den kan kopplas till dig som person på något sätt. Skostorlek, hårfärg, filmsmak, konsertbesök eller bokning av tid hos frisören. Till och med frånvaron av information kan vara en personuppgift, om man ändå kan identifiera en person genom datamängden.

Personuppgifter kan avidentifieras, men inte alltid

Vad betyder det?

I stora datamängder går det ofta inte att direkt utläsa enskilda individer i datamängden. Man kan koppla isär egenskaper och beteenden från adressuppgifter eller

personnummer i databasen som används. Det kan göras genom att använda pseudonymer genom att helt enkelt inte spara några personuppgifter eller på andra sätt behandla datamängden så att identiteter inte blir relevanta för analysen. Tyvärr har många av dessa metoder också brister och med relativt enkla medel skulle man fortfarande kunna identifiera personer om man har tillgång till en databas som kan korsreferera uppgifterna i datamängden eller använder andra dataanalysmetoder. Det går nästan aldrig att göra en datamängd helt anonymiserad om den också ska vara användbar och värdefull för ett företag. Däremot kan man försöka att göra det tillräckligt bra för den uppgift som ska lösas.

”Pseudonymisering”

Vad betyder det?

För att koppla loss sambandet mellan insamlad data och enskilda individer kan informationen om individen på olika sätt ersättas av en pseudonym. Tanken är att informationen då kan göra nytta för att exempelvis se mönster och samband mellan beteenden, men utan att enskilda individer kan spåras.

Dataskydd är viktigt

Varför det?

Målet med dataskydd är att information ska hållas säker, att det inte ska förstöras och inte ska komma i orätta händer. För integritetsperspektivet handlar det om att individer ska kunna förvänta sig att deras persondata inte läcker, försvinner eller att kontrollen över informationen på andra sätt komprometteras. Det är alltså meningen att man ska kunna känna sig säker på att sammanhanget, i vilken man gått med på att dela information, inte kan förändras drastiskt. EU:s nya dataskyddsförordning, GDPR, kommer att kräva större fokus på dataskydd från ännu fler aktörer.

GDPR måste alla förhålla sig

Vad betyder det?

General Data Protection Regulation ersätter vår nuvarande personuppgiftslag (PUL) våren 2018. Kunder och konsumenter får en tydligare rätt att bestämma hur data får användas. Det kommer att behövas ett uttryckligt godkännande för att få samla in och använda data. Man kommer att kunna vända sig till den dataskyddsmyndighet i landet man är folkbokförd, i Sveriges fall Datainspektionen, istället för i det land där företaget finns. Företag kommer att behöva göra konsekvensbedömningar för informationen man samlar in och kunna visa att man skyddar dessa data. Och följer man inte reglerna kan man dömas till betydligt högre böter än med PUL.

Samtycke krävs

Vad betyder det?

Samtycke är en central del i att skydda den personliga integriteten. Genom kravet att det ska finnas ett tydligt godkännande att personuppgifter får användas, ges användaren

en möjlighet att förstå vad hen ger sig in på. Det är därför viktigt att redan i avtalen vara så tydlig som möjligt om vad data om en individ ska användas till. Man får inte lov att använda data för syften som användaren inte gett sitt godkännande för. Vill man samla in annan data från sin produkt eller tjänst, eller använda det insamlade datat på nya sätt så ska man se till att användaren ges möjlighet att godkänna en sådan förändring.

Övervakning pågår alltid

Vad betyder det?

Övervakning kan sägas vara ”den fokuserade, systematiserade och rutinmässiga uppmärksamheten på personliga detaljer för att nå inflytande, styrning, skydd eller riktning.” (David Lyon 2007). Med en sådan definition är all digital informationsbehandling övervakning, vilket också betyder att ”övervakning” ofta är en del av en tjänst, alltså ingår i den nytta som levereras, och i sig inte behöver vara negativt. ”Övervakning” kan sägas vara detsamma som digital informationsbehandling och en integrerad del av allt vi gör. För att bedöma om övervakning är god eller inte, så måste man tänka på sammanhanget och syftet. Det vill säga övervakningen ska ingå i den tjänst som den ”övervakade” köpt eller på annat sätt vill ha och vederbörande ska, direkt eller indirekt, ha gett sitt samtycke.

Övervakning måste skapa nytta och mervärde

På vilket sätt?

Genom att kartlägga hur många människor rör sig, vad de shoppar, söker på internet och berättar om sin tillvaro på sociala medier går det att se mönster och samband som tidigare inte kunde identifieras. Vi kan identifiera troliga kommersiella och politiska preferenser, sociala beteenden, riskbenägenhet och trolig brottslighet. Sådan information är värdefull för företag, politiska partier, arbetsgivare, försäkringsbolag och olika myndigheter, inte minst brottsbekämpande myndigheter. Sådana analyser kan också vara viktig för samhällsplaneringen, exempelvis för att förutse hur människor använder transportvägar och annan infrastruktur. Sådant skapar nytta för företag och för samhället.

Problem kan dock uppstå om informationen används till sådant användarna inte tänkt sig och som många människor kan tycka är att gå för långt. Var dessa gränser finns måste vara föremål för ständig diskussion. Det är oerhört viktigt att den övervakning som all databehandling på något sätt innebär, också skapar direkt nytta för användarna. Användaren som mer eller mindre medvetet släpper ifrån sig information, måste kunna tillgodogöra sig en nytta med det. Tjänsten måste helt enkelt använda informationen och genom det skapa ett mervärde.

Övervaka inte mer än som behövs

Varför inte det?

Med tillräckligt mycket information går det att få veta överraskande mycket om människor, inte minst då de grundläggande sambanden mellan olika beteenden har identifierats. Men vill vi och bör vi veta mer än vi måste? Det finns en stor risk att för mycket information och kunskap leder till att människor inte vill lämna ifrån sig någon information alls. Så fråga inte om personnummer om det inte behövs. I de flesta länder går det att klara sig utan personnummer helt och hållet, så det kan gå även här. Tänk på att ju mer information som ditt företag samlar på sig, ju mer har det också ansvar för.

Känslan av kontroll är viktig

Vad betyder det?

Ett viktigt skäl till att be om samtycke från den som lämnar ifrån sig data är det djupt mänskliga behovet av att känna att man har kontroll. Det är inte alltid det går att veta exakt vad någon godkänner, men möjligheten att inte godkänna måste finnas. Likaså är det viktigt att företag och andra så långt det är möjligt informerar användarna om hur data används.

Algoritmerna styr

Vad betyder det?

Allt större datamängder och smartare algoritmer gör att vi kan få veta alltmer om oss själva och andra. Vi är långt mer förutsägbara än vi tror. Det som hindrat oss från att förstå oss själva, är att vi tidigare inte haft förmågan att överblicka och analysera stora datamängder. Det ligger inte i den mänskliga naturen att arbeta med stora datamängder och statistik, det drar för mycket hjärnkraft. Istället arbetar våra hjärnor med exempel och vi är duktiga på att dra slutsatser och generalisera utifrån mycket små datamängder. Datorer däremot är bra på att analysera stora datamängder och statistik är naturligt för dem.

Genom att analysera mönster i stora grupper – exempelvis hur folk går, shoppar, beter sig på internet och förskönar sin tillvaro på sociala medier - går det att kartlägga trolig personlighet, troliga åsikter och troliga riskbeteenden. Vi får veta enormt mycket om hur vi är och vad vi förväntas göra, kunskap vi aldrig tidigare haft. Men ska vi använda algoritmerna till att skaffa sådan kunskap och kan vi undvika att använda kunskapen när vi har den? Vi kan göra gott genom att upptäcka den statistiska sannolikheten för olika risker, men på individnivå blir allt mycket svårare. Algoritmerna styr, men det är bra om fler vet hur algoritmerna styrs.

”Samhällskontraktet” bygger på informationsbalans

Vad betyder det?

Regering, riksdag, det oberoende rättsväsendet och vi medborgare har ett sorts kontrakt mellan oss. Institutionerna gör sitt, företag sitt och medborgarna sitt. När det nu går att få alltmer kunskap om var och en, kunskap vi inte ens har om oss själva, så kan det påverka maktbalansen i samhällskontraktet. Artificiell intelligens, AI, och algoritmer ger rättsväsendet och myndigheter verktyg som är långt effektivare än vad som tidigare varit möjligt. Digitaliseringen gör det möjligt att öka makten hos företag eller myndigheter på bekostnad av medborgares valfrihet, autonomi eller inflytande. Men man kan också stärka medborgarna med hjälp av transparens och valmöjligheter. Den balansen måste vi ha i åtanke när det digitala samhället fortsätter att byggas.

Värdedelning är viktigare när det handlar om data

Varför det?

I tjänster och produkter som bygger på användares data måste även användaren uppleva att de får tillbaka ett värde i transaktionen. Nyttan av tjänsten för användaren bör alltså överstiga eller motsvara värdet av datat de ger ifrån sig, på samma sätt som företaget ska få ut en större vinst än vad det kostar att tillhandahålla produkten eller tjänsten. Att skapa värdedelning blir viktigare när det är data istället för pengar som utgör det verkliga värdet.

Värdet av att inte veta

Vad betyder det?

Ett ideal är att individen äger sina data, men vad är syftet med det? Vad ska man göra med dessa data? Och frågan är om vi inte bör sträva efter att begränsa insamlingen av data. Samhällskontraktet kan bli svårt att hålla om institutionerna har för mycket kunskap, försäkringsbranschens affärsidé krackelerar om alla risker går att förutse och vi som individer mår möjligen inte bättre om vi vet väldigt mycket mer om oss än vi redan vet.

Det brukar sägas att livskvaliteten kan bli lidande av att man vet exakt när man ska dö. Men det finns mer vi inte vill veta. Låt oss vara försiktiga och begränsa insamling av data till precis det som behövs för att utföra de uppdrag eller tjänster som vi lovat anställda, kunder och användare. Låt oss se till så att vi även i oträngt läge alltid kan förklara och försvara varför vi samlar in uppgifter och vad som är nyttan med insamlandet. Nyttan av att allt blir uppkopplat och att vi med hjälp av mer data och smartare analyser kan öka vår kunskap måste vara tydlig för att på sikt kunna försvara bruk utan missbruk.

Efterord

Hur man i slutändan hanterar integritetsfrågor finns det ingen färdig formel för. Det finns saker man måste göra och saker man måste låta bli att göra. Men i mångt och mycket handlar det om att vara medveten om vilka val man gör, att resonera kring vilka konsekvenser det kan få att hantera data på olika sätt, att vara medveten om sina kunders och användares preferenser så att de fortsätter vilja använda tjänsten så att alla får ut ett värde av det.

I denna lilla katekes har vi samlat resonemang kring vanliga frågor och dilemman som rör den personliga integriteten och konsekvenserna av att leva i ett uppkopplat samhälle. Det är resonemang och inte tvärsäkra svar eftersom ett företag själva måste göra de val som passar deras egen verksamhet och sammanhang.

Digitaliseringens möjligheter är enorma, men det kräver också att vi visar en ödmjukhet inför dessa möjligheter och strävar efter att hitta en balans mellan de effekter vi önskar uppnå och sådana effekter som det är klokt att avstå från. Denna balans är resultatet av en ständig anpassning till omvärldens och företagens förändringar och vårt eget lärande.

Medlemmar i Rådslaget om integritet

Digital Utmanings fjärde rådslag, *Integritet i en uppkopplad värld*, var i huvudsak verksamt under perioden oktober-december 2016 och bestod av:

Jacob Dexe, som är forskare på RISE SICS och projektledare för initiativet Engaging Privacy. Jacob är statsvetare och arbetar med hur beslut och avvägningar kring hantering av personuppgifter görs.

Daniel Akenine, som är fysiker, föreläsare, författare och tidigare hjärnforskare på Karolinska Institutet. Han arbetar som teknik och säkerhetschef på Microsoft och är även IASA Fellow.

Rebecka Cedering Ångström, som är Senior Advisor på Ericsson Consumer Lab och har arbetat med konsumentinsikter inom ICT och digitalisering i snart 10 år. I sitt arbete har hon genomfört flera internationella studier i ämnena privacy och digital säkerhet.

Christer Norström, som är arbetande styrelseordförande och grundare för WeMeMove. WeMeMove utvecklar en världsledande tjänst för digital personlig coach för sport baserat på rörelse data. Lösningen baseras på maskininlärning och analys av stora datamängder där frågor kring integritet är av mycket stor vikt. Christer är också adjungerad professor på KTH och medlem av IVA-avdelning 12.

Cristina Portnoff, som arbetar som Privacy Officer på Telia Company, region Sverige. Cristina har arbetat med privacyfrågor de senaste 3 åren och ha en bakgrund inom försäljning och kundtjänst

Carl Rudbeck, som har doktorerat i litteraturhistoria, har varit verksam som journalist i bland annat Svenska Dagbladet och arbetat vid den liberala tankesmedjan Timbro. Carl är också en välbekant skribent och krönikör.

Stockholm 2017-01-23