DigiTrust: Tillit i det digitala. Tvärvetenskapliga perspektiv från ett forskningsprojekt

Larsson, Stefan; Runeson, Per

2014

DigiTrust: Tillit i det digitala

Tvärvetenskapliga perspektiv från ett forskningsprojekt

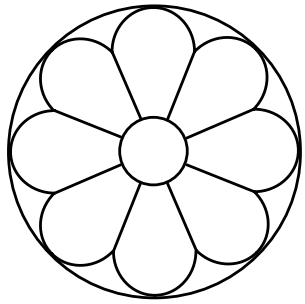
Redaktörer
Stefan Larsson
Per Runeson

PUFENDORFINSTITUTET

DigiTrust: Tillit i det digitala

Tvärvetenskapliga perspektiv från ett forskningsprojekt

The Pufendorf Institute for Advanced Studies, Lund University



Redaktörer: Stefan Larsson och Per Runeson

Omslagsbild: Pufendorfinstitutets rosettfönster, speglat i en datorskärm
Foto: Robert Willim.

Utgivare: Pufendorfinstitutet,
Lunds universitet

Layout: Bengt Pettersson
Tryckning: MediaTryck, Lund 2014
ISBN 978-91-979893-6-7

DigiTrust: Tillit i det Digitala

Del I

DIGITRUST – ETT TVÄRVETENSKAPLIGT PROJEKT

Stefan Larsson och Per Runeson

Det finns många tidens tecken som tyder på att frågor kring tillit är centrala just nu, inte minst i relation till hur digitala medier och teknologier utgör en fundamental del av vår tillvaro. På många sätt lever vi i ett väldigt tillitsfullt, eller för den som vill ange en något mer oroande ton, tillitsberoende samhälle. En fråga som är väsentlig här är i så fall på vilket sätt vi gör det, och hur detta utmanas eller förändras i en digital kontext.

Om man exempelvis ser till övervakningsdebatten, så har den nått en helt ny intensitet efter de avslöjanden som Snowden stått för gällande den amerikanska säkerhetstjänstens, NSA, massövervakning, uppbrytande av tekniska säkerhetsstandards, avlyssning av utländska statsöverhuvudens telefoner, samarbeten med företagsjättar m.m. Det har lett till frågor, ånyo, om svenska FRA och Säpos roll och gränser när det gäller signalspaning och informationsinhämtning och -bearbetning. Vilket i sin tur kan ses den ständigt närvarande frågeställningen om hur statens roll och relation gentemot medborgare, men även institutioner och organisationer, bör se ut. Man kan betrakta detta som ett spänningsfält där tillit spelar en viktig roll.

Vad krävs för att vi ska känna förtroende för att all digital data om oss hanteras på ett tillfredsställande sätt? Var går egentligen gränserna för integriteten, vem ska få ha insyn och när? Övervakning har därmed även blivit en statlig, som sagt, och överstatlig lagstiftningsfråga, där legitimitetsaspekterna kan betonas. Detta poängteras inte minst i det av EU-domstolens underkännande av det datalagringsdirektiv som nyligen implementerats av medlemsstaterna i EU. Detta underkännande lyfter upp frågan om tillit till ytan, i det här fallet i statens förhållande till medborgarna, och i vilken mån medborgarna har förtroende för sin stat, och i förlängningen även andras. Den tekniska infrastrukturen, i samklang med vårt beroende av den, gör att kampen om våra data, också blir en kamp om vem som ska få veta vad vi gör, när

vi gör det, hur vi skriver, vem vi pratar med, när vi pratar i mobiltelefoner, datorer och en rad andra uppkopplade produkter. Tilliten blir, på flera sätt, en central samhällsfråga.

Och tillitsfrågan har långt ifrån bara en övervakningsdimension kopplad till sig. Samma verktyg, samma mätbarhet som den digitalt medierade tillvaron för med sig blir även en fråga för hur vi upplever säkerhetsfrågor kontra integritet i de tjänster vi använder – för transaktioner av pengar och mötet med banker; för konsumtionsmönster och betalmedel; för en rad tjänster vi använder och i hög grad är beroende av, t.ex. medietjänster; för gränsdragningsfrågor och normer i sociala medier.

De strukturella förändringar som digitalisering medför, gör att en rad organisationer och institutioner utvecklas och förändras. Ett exempel på en sådan rör den vetenskapliga kommunikationen, som i mycket brottas med frågor om hur man värderar vilken ny kunskap som ska betraktas som vetenskaplig kunskap. De institutioner – exempelvis bibliotek – och de aktörer – exempelvis förlag – som står för mycket av det strukturella fundamentet för den vetenskapliga kommunikationen, möter en rad spännande utmaningar som ställer frågor om vilken kunskap och vilka företrädare vi känner tillit till och bedömer som trovärdiga. Hur, vem eller vad, ska definiera vad som är vetenskaplig kunskap? Notera här open access-frågan, som ett exempel på en utmaning för förlagens position i strukturerna, och wikipedia som ett annat exempel på hur tämligen decentraliserade organisationsformer kunnat ersätta mer centraliserade och expertbaserade organisationsformer för encyklopediska framställningar.

Ovanstående utgör en kort introduktion till några av de frågor som vi ägnat åt oss i den tvärvetenskapliga forskargrupp som består av 10 forskare från 5 fakulteter vid Lunds universitet. Projektet, med namnet *DigiTrust – Privacy, Identity and Legitimacy in the Digital Society*, eller snarare *DigiTrust-projektet*, har varit finansierat av Pufendorfinstitutet vid Lunds universitet, i vars inspirerande lokaler vi också befunnit oss under vårt arbete i gruppen. Projektet har löpt mellan september 2013 och juni 2014 och har letts av Per Runeson och Stefan Larsson. De forskningsfrågor som vi initialt riktade in oss mot kan sammanfattas i:

1. Säkerhet och integritet – vilka tjänster och aktörer litar vi på och varför?
2. Vilka kunskapsinstitutioner litar vi på eller litar vi inte på i en digital kontext?
3. Övervakning och datalagring som rättslig och offentlig trend, i vilken riktning går den?

Tillitsfrågan verkat som en samlande nod kring vilken vårt arbete kretsat, och ba-

lansen mellan de nämnda frågorna har skiftat, som ett resultat av vårt arbete. Arbetet inom forskargruppen har varit starkt präglad av seminariekulturen och den dynamik som följer med den, vilket är en av Pufendorfinstitutets styrkor som följer av att ställa själva huset till förfogande och ha en tydlig uppmuntran vad det gäller att arbeta tillsammans på samma plats. I arbetet med en grupp forskare med så pass skilda bakgrunder så är det troligen något av en nödvändighet att hitta former för en arbetsmetod som tillåter ifrågasättande, prestigelöst prövande och oliktänkande vad det gäller de vetenskapligt formulerade grunderna kring metod, teori och analys. Det kan vara mödosamt, men också oerhört givande.

Det är på sin plats att påpeka att i Pufendorfinstitutets syfte ligger att föra samman och bidra till att lyfta tvärvetenskapliga initiativ som är djärvare och relativt oetablerade, snarare än de som redan är färdiga till sin form och baseras på en mer homogen forskningstradition. Tanken tycks vara att det är i mötet mellan discipliner som en särdeles åtråvärd utvecklingspotential finns. Som något formativt snarare än formerat. Med detta följer också vissa tämligen påtagliga utmaningar i hur man ska jobba inom den här typen av initiativ. Vi valde exempelvis att lägga påfallande mycket tid initialt vid att presentera tillitsbegreppet utifrån de olika forskningstraditioner som är närvarande i DigiTrust-gruppen, och samtidigt uppmuntra till dialog. Det visade sig då också att mycket av det som kan tas för givet inom discipliner behöver vi lyfta upp till ytan och uttala för att kunna samarbeta. Det gemensamma förgivettagna är med andra ord inte lika mycket i en tvärvetenskaplig grupp jämfört med en grupp som har sitt ursprung inom samma disciplin, och en del av kunskapsutvecklingen och själva forskningen kan sägas bestå i – i vart fall initialt – i att enas och förenas kring en något-så-när etablerad samsyn kring perspektiv. Där någonstans finns också en potentiell lyftkraft i vår teknikrelaterade forskning av samtida kulturella, rättsliga och mediala uttryck.

Resultat

De resultat som är sprungna ur DigiTrust-projektet kan å ena sidan ses i skenet av de studier vi har gjort, varav mycket presenteras i den här framställningen, men å andra sidan också i hur vår samverkan med samhälle, media och andra forskare och deltagande i debatten har sett ut. Om vi först ser till de explicita studierna så kan man konstatera att eftersom projektet är relativt kort så har några vetenskapliga artiklar ännu inte hunnit publiceras. Några av de analyser och empiriska resultat som vi fördjupar oss mer i nedan kan likväl sammanfattas här, innan vi återkommer till samverkansformerna:

- Nära hälften av svenskarna finner det inte acceptabelt att FRA, Säpo eller polisen samlar in och bearbetar data om deras internetvanor. En majoritet anser dock att myndigheter får samla in eller bearbeta information om deras internetvanor efter domstolsprövning eller myndighetsprövning från fall till fall.
- Banker, bibliotek och traditionella medier bibehåller enligt enkäten tilliten vid övergången till det digitala. Vi ser detta som en kombination av medvetet tillitsbyggande från dessa institutioner och användarnas tillvänjning över tid.
- Säker teknik är en nödvändig men inte tillräcklig förutsättning för användarnas tillit. Användare anser sig endast i låg grad kunna bedöma hur säkra tekniska system är.
- Enkätstudien indikerar att det finns en grupp i samhället som tydligt hyser låg tillit till en rad fenomen: myndigheters insamling av data, arbetsgivares kontroll, i allmänhet gentemot sina medmänniskor. Detta är i sig intressant för vidare studier och analys.
- Rätten spelar en viktig roll i att reglera statens förhållande i datainsamlingen och databearbetning om medborgare. Lagstiftaren har dock visat på en trend mot att se nyttan av datalagring i syfte att identifiera brottslingar i efterhand.
- En tilltagande digitalisering leder bland annat till ökade möjligheter för övervakning av individer. Mycket tyder på att regler och avtal inte är tillräckliga för att skydda individers integritet (privacy by policy), och att tekniska lösningar behövs för att säkerställa detta skydd (privacy by design).
- Digitaliseringen av det vetenskapliga kommunikationssystemet medför utmaningar där de institutioner och processer som ska stå för spridande och granskning av kunskapen och de som skapar den ifrågasätts. Personliga och systemiska dimensioner av tillit omformas i mötet mellan traditionella värderingar och digitaliseringens möjligheter.
- Den digitala infrastrukturen synliggörs i regel bara när den slutar fungera. Under senare år har dock leverantörer av molntjänster lanserat suggestiva och fantasieggande bilder av annars stängda och hemliga anläggningar, vilka bidrar till att forma människors uppfattning om tillit och vilka system man egentligen kan lita på.

Med det tvärvetenskapliga tillvägagångssättet ger också att de kanaler att publicera i som forskarna från olika discipliner är vana vid inte enkelt låter sig infogas eller passas ihop. Vi valde därför tidigt att inte låta den vetenskapliga publikationen bli överordnad arbetet inom temagruppen, utan såg därför till att vara öppna för en rad andra format för dialog med omvärlden. De medel som vi kommunicerat via är:

- Hemsida i bloggformat: digitalsociety.se
- Sociala media: det som postas på bloggen tenderade att spridas i facebookflöden och via det twitterkonto som vi etablerat, @DigitalSocietyL
- Debattartikel i nyhetsmedia, SvD Brännpunkt (19/4, 2014), "Övervakning tär på medborgarnas tillit". Finns även översatt till engelska och postad på digitalsociety.se eftersom flera intressenter frågat om det.
- Filosofiska rummet, P1. Vi bjöd in redaktionen till ett av våra arbetsmöten, och två av våra forskare, Jutta Haider och Calle Rosengren, deltog sedan i söndagsprogrammet. Inslaget fick namnet "Övervakad och nöjd - om tillit i det digitala samhället." och finns att lyssna på i pod-version på Sveriges radios hemsida.
- Tillitsrelevanta panelsamtal. Eftersom temat fick en viss uppmärksamhet så kom en del förfrågningar in om att delta i olika typer av publika panelsamtal och dyl. Exv Robert Willim och Jutta Haider var så med i *Truly Digital 2014*, på MEDEA 23-24 maj, 2014.
- SR P1/Utbildningsradion. Stefan Larsson deltog i reportage om tillit i det digitala, å temats vägnar, vilket sänds efter sommarpratarna i sommar (datum ej klart).
- Robert Willim deltog i konferensen: *Beyond the Frame: The Future of the Visual in an Age of Digital Diversity,* Stockholm, april 2014, med ett paper baserat på resonemangen i kapitlet "Under molnen".
- Jutta Haider var keynote talare på konferensen *Mötesplats Open Access* i Växjö, april 2014 (Mis/trusting Open Access).
- Calle Rosengren deltog 23-27 april på konferensen *Labour Time - Life Time* vid Inter-Univercity Center (IUC) i Dubrovnic med ett paper på temat tillitsbaserade arbetstidsavtal "The Swedish Confederation for Professional Employees (TCO) and the question of trust-based working hours". Detta paper kommer senare att publiceras i fulltext i den vetenskapliga tidskriften *Management review.*
- Artikel: Jutta Haider och Fredrik Åströms kapitel nedan har sin förlaga i en post på digitalsociety.se och utvecklas till en vetenskaplig och engelskspråkig artikel.
- Minirapport: Jonas Ledendals rättsfallskommentar nedan är översatt till engelska och postad på digitalsociety.se för tillgänglighetens skull.
- Gästforskare Debora Halbert arbetar på artikel om 'privacy' ihop med DigiTrust-gruppen.

Ursprunget till DigiTrust-projektet är den så kallade Advanced Study Group om *det digitala samhället* som Per Runeson och Stefan Larsson höll i under 2012-2013. Här träffades 17 forskare från 6 fakulteter med jämna mellanrum för att i seminarieform närma sig några av de viktigaste utmaningarna som det digitala samhället står

för:[1] 1.) Metaforer och konceptuell förändring; 2.) Tillit, säkerhet och integritet; 3.) Informationssegregering / delaktighet i det digitala; 4.) Arbetsliv i förändring; 5.) Normer och lagstiftning.

Presentation av forskarna

Forskarna kommer från fem fakulteter och en rad ämnesmässiga discipliner, och dessa är Samhällsvetenskapliga (rättssociologi, arbetsvetenskap, media- och kommunikationsvetenskap), Humaniora (biblioteks- och informationsvetenskap, digitala kulturer, etnologi, kulturvetenskaper, media- och kommunikationsvetenskap), Ekonomihögskolan (handelsrätt), Universitetets särskilda verksamheter (Internetinstitutet och Arbetsmiljöhögskolan), LTH (datavetenskap, innovationsteknik, elektro- och informationsteknik) samt Universitetsbiblioteket. Utöver detta så har gruppen arbetat med en gästforskare från University of Hawaii at Manoa, political science. De forskare som ingår i digitrustprojektet är:

- Stefan Larsson, FD i rättssociologi, JK, forskare och föreståndare vid Lunds universitets internetinstitut (LUii).
- Per Runeson, professor i programvarusystem, forskar och undervisar och är prefekt vid Institutionen för datavetenskap.
- Susanna Bill, forskarstuderande i innovationsteknik, institutionen för designvetenskaper, LTH.
- Jutta Haider, FD, universitetslektor i biblioteks- och informationsvetenskap, institutionen för kulturvetenskaper.
- Jonas Ledendal, JD, forskare och lärare vid handelsrätt, Ekonomihögskolan.
- Tobias Olsson, professor och prefekt i medie- och kommunikationsvetenskap.
- Calle Rosengren, FD i industriell arbetsvetenskap, forskar och undervisar vid Arbetsmiljöhögskolan inom Centre for Work, Technology and Social Change.
- Ben Smeets, professor i elektro- och informationsteknik och expert på säkerhetssystem vid Ericsson.
- Robert Willim, docent, forskar och undervisar vid avdelningen för etnologi, Institutionen för kulturvetenskaper.
- Fredrik Åström, docent, och bibliometriker vid avdelningen för forsknings- och studieservice på Universitetsbiblioteket.

[1] Studiegruppen mynnade ut i en slutrapport, Det Digitala Samhälet, och slutsymposiet finns även filmat och har visats på UR Samtiden. Det digitala Samhället (pdf): http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3563700&fileOId=3563879

[1] UR Samtiden: http://www.ur.se/Produkter/178467-UR-Samtiden-Det-digitala-samhallet-Var-digitala-samtid-och-framtid

- Gästforskare: Debora Halbert, är docent (associate professor) och prefekt (Department chair) vid statsvetenskapliga institutionen på universitetet i Hawaii, vid Manoa.

Vi vill tacka medarbetarna på Pufendorfinstitutet för stöd, diskussioner och hjälp med stort som smått; och därmed framförallt Sune Sunesson, Sture Forssén, Eva Persson och Bengt Petersson. Vi vill även tacka för synpunkter och spännande diskussioner med en rad externa forskare, experter i näringslivet, radioprogrammakare, m.m. under projektets gång.

Disposition

Denna rapport utgår från fyra huvudsakliga delar, där den introducerande Del 1 även inkluderar en framställning kring den vetenskapliga litteraturen kring tillit. Detta är, som vi ska se, inte en helt enkel uppgift att sammanfatta, eftersom det dels beror på hur man definierar tillit men också dels på att begreppet används i en rad discipliner för en rad olika saker. Denna del innehåller också en sammanfattning av den nätbaserade enkät som vi genomförde inom ramen för projektet, om tillit i det digitala, med drygt 1100 respondenter. Vi presenterar också en översiktlig analys av enkätmaterialet.

Del 2 i rapporten samlar flera, lite kortare texter med utgångspunkt från, eller i anknytning till enkäten. Texterna har tagits fram som debattartikel, blogginlägg, eller baserat på reflektioner i seminariegruppen. Den tredje delen innehåller fyra mer omfattande, vetenskapliga texter, som avhandlar ämnen om kunskapsbyggande i det digitala, om legala aspekter, samt om fysikalisk gestalning i det digitala samhället. Del 4 innehåller frågeformuläret från enkäten, för den som är intresserad av dess detaljutformning.

Litteratur om tillitsbegreppet

Susanna Bill och Stefan Larsson

Precis som i samhället i stort spelar tillit en central roll inom forskning. Exempelvis kretsar en stor del av den säkerhetsrelaterade litteraturen i digitala frågor kring begreppet tillit. Artiklar och antologier, exempelvis "Landmark Papers on Trust vol 1-2" är värda att nämnas, likaså *Journal of Trust Research* och open accesstidskriften *Journal of Trust Management*. Som tidigare nämnts så identifierades tillit som ett centralt begrepp redan under arbetet i studiegruppen 2012-2013. I det fortsatta arbetet kändes det angeläget att inledningsvis reflektera kring tillit och dess olika definitioner och schatteringar. Ambitionen var inte att hitta en gemensam definition av begreppet tillit, utan snarare att fundera kring olika tolkningar och på så sätt skapa förståelse för hur tillit används inom olika forskningsområden.

Vad är tillit?

Tillit är ett centralt men inte exakt begrepp inom många olika forskartraditioner. Uppfattningen att tillit är ett psykologiskt tillstånd som bygger på förhoppningen att det man bidrar med i ord eller handling skall tas omhand av mottagaren på ett positivt sätt eller åtminstone neutralt sätt är dock bred (Rosseau et al, 1998; Kramer, 1999). Om tillit handlar om att våga öppna sig i förtröstan att bli väl mottagen och omhändertagen av motparten handlar brist på tillit om det motsatta, dvs känslan av att motparten kommer att vilja en illa och inte ta emot det man har att komma med på ett respektfullt och konstruktivt sätt (Govier, 1994). Tillit vittrar sönder snabbare än det skapas. Vi tenderar att ta det tillitsbyggande arbetet för givet och endast uppmärksamma bristande tillit (Kramer, 1999).

Tillit bygger i det här perspektivet på mellanmänskliga processer som i sin karaktär både kan stärka och försvaga det psykologiska tillståndet. Mer generellt kan man säga att tillit skapas mellan två *entiteter*: en människa känner tillit till en annan person, ett system, en organisation eller ett sammanhang (Ardichvilli et al, 2003; Kelton

et al, 2008). Tillit är alltså beroende av den andra entitetens karaktär. Beroende på hur motparten ”är” gentemot oss känner vi tillit eller bristande tillit gentemot denne. Tillit till systemet handlar om hur vi som individer förhåller oss till de system, såväl fysiska som digitala som vår omvärld är uppbyggda av (Kelton et al., 2008). Företag som erbjuder digitala tjänster visar inte sällan upp fysiska gestaltningar av sin verksamhet, exempelvis Google som exponerar sina serverhallar eller GPSer som visualiserar landskapet man kör igenom. Det verkar vara så att fysiska manifestationer är tillitskapande för oss människor (Willim, 2008; se kapitel 10).

Tillit kan ses ur ett rationellt perspektiv där jag väljer att lita på någon efter att ha analyserat situationen i rationella och opportunistiska termer. Vilket ger bäst utfall för mig själv, att lita på motparten eller ett inte göra det (Rousseau et al., 1998)? Vilket ger bäst utfall för mig själv, att lita på motparten eller ett inte göra det (Rousseau et al., 1998)?

”I det mer statsvetenskapliga eller nationalekonomiska perspektivet studeras och debatteras ibland korrelationen mellan välfärdsstat och tillit. Här indikerar studier på att välfärdsstaten producerar tillit och socialt kapital (exv. Kumlin och Rothstein, 2005) men kontrasteras även av studier som hävdar att kausaliteten egentligen är den omvända, att ”tillitsfulla populationer mer troligt skapar och vidmakthåller stora, universella välfärdsstater” (Bergh och Bjørnskov, 2011, s. 1). Både relationen mellan stat och individ, sedd ur ett tillitsperspektiv, och förståelsen av den ”sociala tilliten”, dvs den icke-formella, mellanmänskliga, är av otvetydigt intresse här.

Tillit kan också ses ur det sociala perspektivet; våra relationer påverkar hur vi upplever tillit. Förmågan att känna tillit menar forskningen, kan också kopplas till personlighetstyp, vilken roll man har i sammanhanget, sammanhangets sociala regelverk och individens tidigare erfarenhet av att känna tillit eller brist på tillit. På så sätt skulle tillit kunna beskrivas som en positiv lärprocess: ju större erfarenhet individen har av att tidigare ha upplevt tillit i ett visst sammanhang desto större blir förmågan att känna tillit givet sammanhanget (Kramer, 1999).

Inom organisationsforskningen pratar man om kunskapsbaserad och institutionell tillit (Ardichvilli et al., 2003). Kopplat till den positiva lärandeprocessen handlar kunskapsbaserad tillit på mängden kunskap individen har om sin motpart, som i detta fall är organisationen. Enkelt uttryck: ju mer kunskap desto större förutsägbarhet om hur inputen kommer att mottas. Den institutionella tilliten skapas genom att systemet är transparent och möjliggör insyn, samt att systemet ”agerar” tillitsfullt. Exempelvis genom att delegera befogenheter och beslutanderätt åt individerna. Genom att studera projekt konstaterar forskning att tillit byggs olika beroende på fas i projektets livscykel (Oza et al., 2006; Babar et al., 2007). I de inledande faserna

skapas är tilliten ”beräknande” eller rationell främst baserad på formella meriter som rykte, referenser och investeringar i fysiska möten. För att tilliten skall uppehållas i senare faser krävs dock ”bevis” på starka relationer, exempelvis transparens, förståelse för kultur och ett tydligt agerande åtagande till projektets aktiviteter. Tilliten blir således relationsbaserad.

Tillit i det digitala

I den digitala dimensionen kan tillit också förstås ur ett tekniskt perspektiv, dvs hur nät är konstruerade, kvaliteten på den mjukvara som används, hur den certifieras och även ur legitimitets- och lagstiftningsperspektiv som är kopplat till teknik. Begreppet trusted computing som föddes i början av 1990-talet handlar just om behovet av att stärka den tekniska tilliten i våra datasystem genom exempelvis signerad mjukvara. Problemet med trusted computing var dock balansen mellan ökad kontroll med bibehållen integritet. Synen inom tekniken är att hårdvara alltid är säkrare än mjukvara, således byggs delar av den tekniska tilliten upp kring hårdvaran genom exempelvis kryptografiska nycklar och monterbara hårdvarukretsar. Forskare har dock visat på hur dessa kan knäckas (Nohl et al., 2007).

Men skapar verkligen ett tekniskt säkert system högre tillit? Om det paras med användbarhet är svaret tveklöst ja, om inte blir det svårare. Som det kommer att visa sig i den enkät som projektet har gjort finns det en koppling mellan med vilken lätthet och frekvens vi tar oss an det digitala tjänsteutbudet och den kompetens vi upplever oss ha. Svårbegripliga och knöliga system blir svårare att dra nyttan ur oavsett den tekniska säkerhetsnivån.

Friheten och rörligheten som internet har möjliggjort gör att vi alla på olika sätt kan hitta andra med liknande intressen. Virtuella communities poppar ständigt upp där medlemmar samlas och utvecklar sina gemensamma intressen. Precis som i den fysiska världen skapas tillit i den digitala kontexten ur liknande logik kring kopplingar till den kunskap som medlemmarna har om sin kontext och dess sociala regler (van House, 2002). Genom communities, bloggar och hemsidor är internet en oändlig källa till information som vi använder till dagligdags. Vi värderar informationens trovärdighet bla utifrån den tillit som vi känner gentemot informationskällan (Ardichvilli et al., 2003), hur den presenteras och vilken typ av relation som krävs för att vi skall få tillgång till informationen. Här har kommersiella avsändare gått igenom grundläggande förändring, från att ha producerat informationen internt till att i allt större utsträckning förlita sig på externa kunskapskällor. Samtidigt måste informationen kvalitetssäkras så att trovärdigheten och således tilliten uppehålls.

Publikationer och Peer-review

Kunskap och tillit är sammanvävda (Hardwig, 1991). För att kunna lita på kunskap måste vi således lita på andra människor (Shapin, 1994, s. xxv) och i en allt högre utsträckning också på olika tekniska system. Som forskare är publicering av artiklar en central del av att sprida forskningsresultat och av meriteringssystemet. Förutom de traditionella journalerna finns numera ett stort ekosystem av open access journaler, dvs journaler som till skillnad mot de traditionella varken kräver prenumeration för tillgång eller tar betalt för nerladdning av artiklar. Peer-review, sättet på vilket akademiska artiklar utvärderas är en viktig del för att signalera att de publikationer där forskning presenteras är något att känna tillit till. Artiklarna granskas anonymt av andra forskare för att säkerställa att forskningen utförs på ett korrekt sätt med resultat som är värt att publicera.

Tillit och det rättsliga perspektivet

Även ur ett rättsligt perspektiv diskuteras tillit och behov av tillit, bla som ett kriterium för säkerhetsjuridisk analys (Magnusson Sjöberg, 2002). IT-propositionen från 1999/2000 säger att reglerna för IT-området bör vara sådana att de skapar förtroende genom att vara säkra, förutsägbara och teknikneutrala; internationella; samt skydda individens integritet. Teknikneutralitet kan låta relevant, men som Jonas Ledendals avhandling (2010) visar har det inte alltid varit fördelaktigt att upphovsrätten är teknikneutral. Tillitsteorin finns inom avtalsrätten och reglerar huruvida ett avtal skall gälla eller inte när en av partnerna har gjort fel eller skrivit fel i avtalet. Konflikten bedöms utifrån om motparten kan sägas vara i god eller ond tro, men undantar avtal som ”befordras genom telegram eller framföres muntligen genom bud” och dess analogier (Avtalslagen 32, st 2).

Om man breddar det rättsvetenskapliga perspektivet något så är det rimligt att tala om rättens legitimitet, vilket ägnats mycket forskning inte minst inom det rättssociologiska fältet. Här kan man även tala om rättsliga normer som något att jämföra med sociala normer, vilket är ett användbart synsätt när man studerar vad som växer fram och förändras i en digital kontext (Larsson, 2014; Svensson och Larsson, 2012).

Sammanfattningsvis konstaterar vi att tillit inte är ett exakt begrepp trots att det används inom ett stort antal forskartraditioner. Ur individens perspektiv finns det stora likheter med den fysiska världen kring hur tillit skapas i den digitala. Teknisk säkerhet är en möjliggörare för tillit men finns ingen användarvänlighet så räcker den inte.

Referenser

Ardichvili, A.; Page V. & Wentling, T. (2003). Motivation and barriers to participating in virtual knowledge-sharing communities of practice *Journal of Knowledge Management*, 7(1), 64-77.

Babar, M.A.; Verner. J.M.; & Nguyen, P.T. (2007). Establishing and maintaining trust in software outsourcing relationships: an empirical investigation. *Journal of Systems and Software* 80(9), 1438-1449.

Bachmann, R.; Zaheer, A. (2008). Landmark papers on trust, vol 1-2. *MPG Books Ltd, Bodmin, Cornwall*

Bergh, A. och Bjørnskov, C. (2011). Historical Trust Levels Predict the Current Size of the Welfare State, *Kyklos* 64(1): 1-19.

Hardwig, J. 1991. The role of trust in knowledge. *Journal of Philosophy,* 88(12), 693-708.

House, van N. (2002). Digital Libraries and practices of trust: networked biodiversity information. *Social Epistomology,* 16(1), 99-114.

Kolton K; Fleischmann K. R. & Wallace W. A. (2008). Trust in digital Information. *Journal of the American Society for Information Science & Technology,* 59(3)*,* 363-374.

Kramer, R. M. (1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual review of Psychology, 50*, 569-598.

Kumlin, S. och Rothstein, B. (2005). Making and Breaking Social Capital: The Impact of Welfare-State Institutions, Comparative Political Studies. 38: 339–365. Govier, T. (1994). Is it a jungle out there? Trust, distrust ad the constitution of social reality. *Dialogue,* 33(2), 237-252.

Larsson, S. (2014) Digitaliseringens Rättssociologi. Om mätbarhetens behov av teori och den digitala arkitekturens normativa relevans, *Retfærd. Nordic Journal of Law and Justice* 37(2): 78-97.

Ledendal, J. (2010). Copyright Protection of Software under the TRIPS Agreement - Software reengineering and reverse engineering in the context of international trade law. Lunds universitet. ISBN: 978-91-7473-042-5

Magnusson Sjöberg, C. (2002). Tillit i informationssamhället: Kejsarens nya kläder eller förändrade förutsättningar för rättsutvecklingen? *Anonymitet, övervakning, tillit. Nordisk årsbok i rättsinformatik*, 107-125.

Nohl K.; Evans D.; Starbug, S. & Plötz H. (2008). Reversed engineering a cryptographic RFID tag. In *USENIX Security Symposium* (28), San José CA 31, July 2008.

Oza, N., Hall, T., Rainer, A. & Grey, S. (2006). Trust in software outsourcing relationships: an empirical investigation of Indian software companies. *Information & Software Technology,* 48, 345–354.

Rousseau, D. M; Sitkin Sim B; Ronald S. & Camerer C. (1998). Not so different after all: a cross discipline view of trust. *Academy of Management Review, 23(3*), 393-404.

Shapin, S. (1994). *A social history of truth. civility and science in seventeenth-century England*. Chicago: University of Chicago Press.

Svensson, Måns and Larsson, Stefan (2012) Intellectual Property Law Compliance in Europe: Illegal File sharing and the Role of Social Norms, New Media & Society, 14(7): 1147-1163.

Willim, R. (2008). *Industrial cool: om postindustriella fabriker.* Lund: Lunds universitet, Humanistiska fakulteten.

Tillit i det digitala samhället – en kartläggning

Tobias Olsson, Calle Rosengren, Per Runeson, Susanna Bill och Stefan Larsson

Redan i planeringen av temaarbetet insåg vi att vi behövde ta reda på vad människor ute i det digitala samhället tänker och tycker. Vad känner man tillit till? Hur förhåller man sig till övervakning i det digitala? Är svaren olika beroende på ålder, kön, bostadsort, utbildning, politiska sympatier, etc? Varierar åsikterna för olika områden i det digitala? Påverkar tilliten hur man faktiskt agerar, eller tycker man en sak och gör en annan?

För att få en bred överblick över åsikter och samband valde vi en enkätundersökning. Den fördjupande förståelsen får dröja till senare studier och med andra undersökningsmetoder, till exempel djupintervjuer.

Vi bestämde oss tidigt för en internet-baserad enkät. Därmed förlorade vi den grupp i samhället som står utanför det digitala. Denna grupp adresseras i den årliga undersökningen ”Svenskarna och internet” (Findahl, 2013), och bedöms utgöra cirka 10% av befolkningen. Vi var dock främst intresserade av åsikter och beteende i det digitala samhället, och ansåg att vi får bättre kvalitet i svaren från dessa med en internet-baserad enkät, jämfört med en pappersbaserad sådan.

För enkäten identifierade vi fem huvudområden inom det digitala samhället:

- Övervakning
- Bank
- Hälsa
- Arbetsliv
- Medier

Dessa områden representerar olika aspekter i vårt vardagsliv. Övervakningsfrågorna är dagsaktuella i medierna och berör vem som ska få veta vad om vem på nätet. Bank

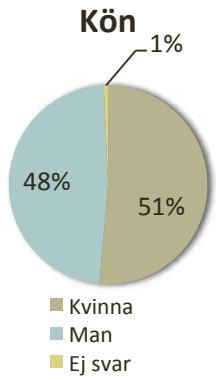
och hälsa, representerar områden där vi lämnar ut personliga data om ekonomi och sjukdomar - något som kräver tillit. Arbetslivet är också allt mer digitaliserat, och frågor väcks om hur arbetsgivaren litar på arbetstagaren, och vice versa. Medierna, såväl traditionella som sociala, har förändats radikalt med digitaliseringen och är därför relevanta att studera.

Inom varje område formulerade vi frågor om kunskap, attityd och praxis baserat på hypotesen att kunskap bygger tillit, som i sin tur har stor betydelse för praxis. Med andra ord ju mer man vet desto större tillit får man, ju större tillit desto mer praxis. Till exempel, för bankområdet lät vi respondenterna ta ställning till påståendena ”Jag har god kunskap om hur man använder Internetbaserade banktjänster” (kunskap), ”Jag känner tillit (förtroende) till de internetbaserade banktjänster som jag använder mig av” (attityd), och “Jag använder internetbaserade banktjänster för att betala räkningar” (praxis).

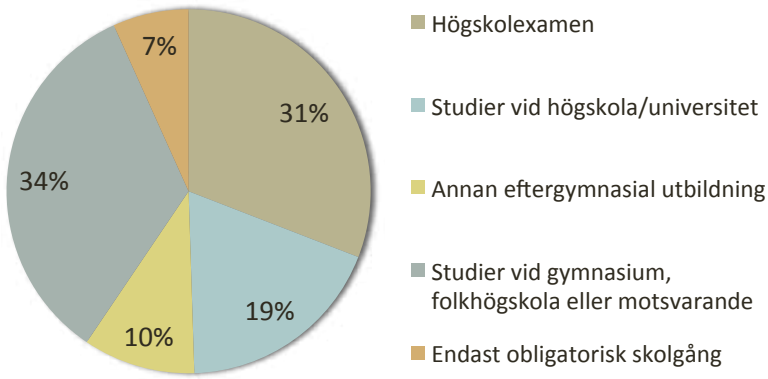
För att identifiera bakgrundsfaktorer ställde vi, förutom de traditionella demografiska frågorna, också några frågor om allmän tillit – alltså hur benägen man är att lita på folk i allmänhet, myndigheter och andra allmänna institutioner. Några av frågorna formulerades på samma sätt som motsvarigheterna i ”Svenskarna och internet” (Findahl, 2013) och SOM-institutets (http://www.som.gu.se) årliga enkäter, för att möjliggöra referenspunkter i vårt urval med resultaten från dessa regelbundna enkäter.

Enkätfakta

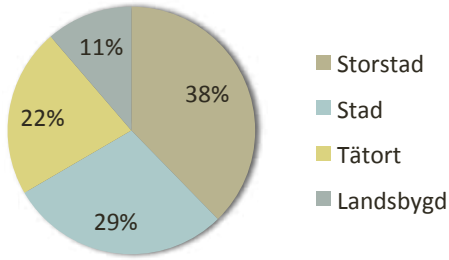
Enkäten genomfördes i samverkan med undersökningsföretaget QuestBack som administrerade den i verktyget EasyResearch. Förfrågan om att delta i enkäten sändes ut via e-mail till 1193 respondenter, varav 1118 besvarade den, vilket motsvarar en svarsfrekvens på 93,7%. Vi styrde urvalet så att vi skulle få en jämn fördelning



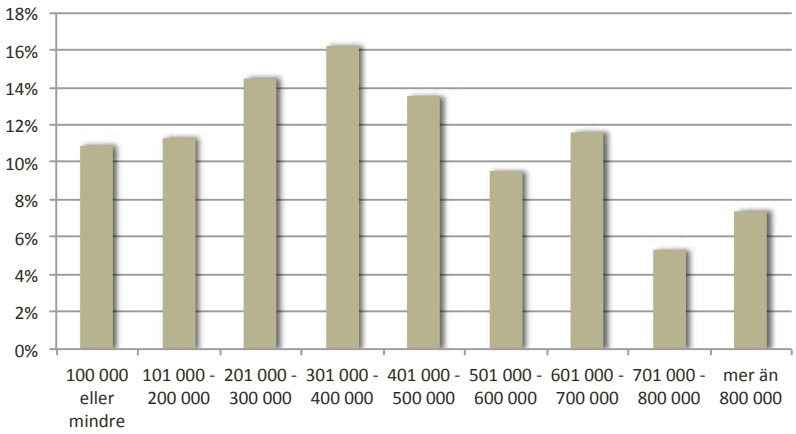
Utbildning



Bostadsort

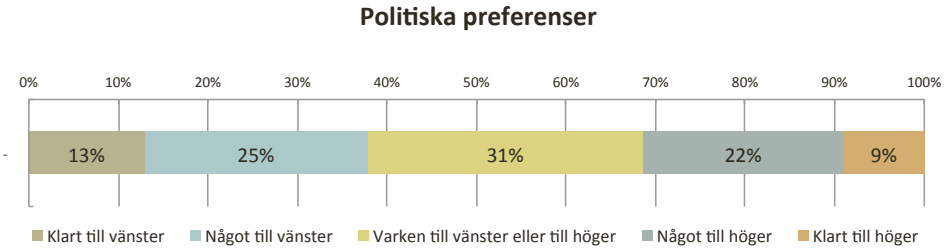


Årsinkomst



avseende kön och ålder. Urvalet drogs slumpmässigt från CINT CPX(Cint Panel eXchange) som består av omkring 400 000 individer i Sverige vilka representerar ett riksgenomsnitt av befolkningen.

Enkäten omfattade cirka 35 frågor, de flesta med fem svarsalternativ i grader av instämmande (instämmer helt, instämmer, neutral, instämmer inte, instämmer inte alls), alltså en s.k. femgradig Likert-skala. Demografin bland de svarande redovisas i graferna nedan.



De svarandes politiska preferenser ligger något förskjuten till vänster, med en tyngdpunkt i mitten, vilket sammanfaller med det aktuella opinionsläget vid tiden för undersökningen.

Allmän tillit

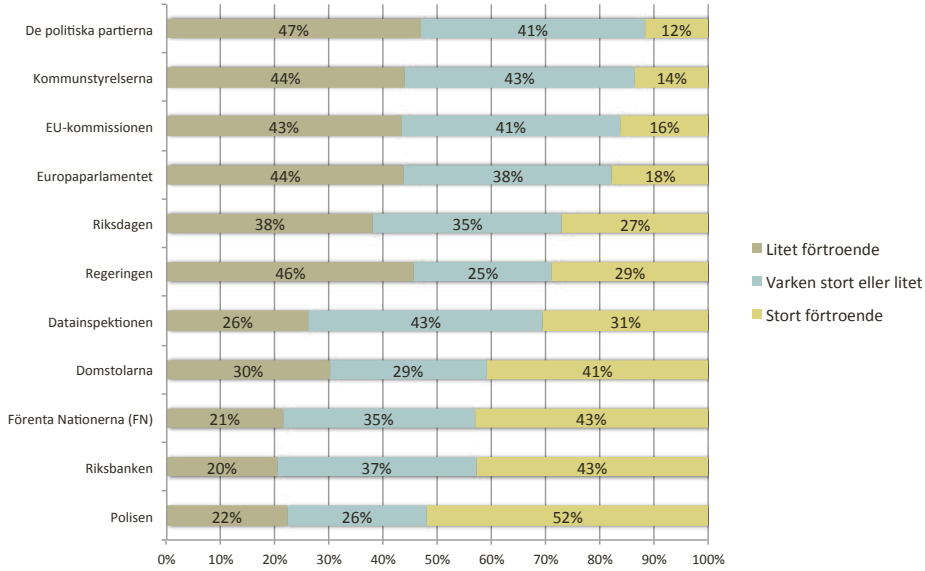
Sverige brukar beskrivas som ett ”högtillitsland”, där invånarna hyser hög tillit till varandra och till samhällets institutioner. I sin bok, ”Den svala svenska tilliten” (Trägårdh et al., 2013) som är baserad på den så kallade tillitsbarometern från 2009, bekräftar författarna denna bild. I sin diskussion av resultaten daterar de rötterna för denna tillit ända tillbaka till det sociala kontrakt som växte fram mellan bönderna på tinget för tusen år sedan. Ett led i kontextualiseringen av människors digitala tillit, är att relatera denna till i vilken grad de ger uttryck för tillit till å ena sidan andra människor och å andra sidan olika samhällsinstitutioner och -organisationer.

På den direkta frågan om i vilken utsträckning det går att lita på andra människor är respondenternas svar något svårtydda. 39 (37 plus 2) % av respondenterna anger att de anser att det går att lita på människor i allmänhet i ganska hög eller hög utsträckning, se tabell 1. Samtidigt anger en nästan lika stor del av respondenterna – 37 (31 plus 6) % av dem att det bara går att lita på människor i ”viss” eller ”låg” utsträckning. Detta ger en annan bild än den gängse uppfattningen om högtillitssamhället, åtminstone när det gäller tillit till individer. Nu är vårt syfte inte att undersöka den frågan för sig själv, utan att relatera tilliten i allmänhet till den tillit man upplever i det digitala samhället.

Tabell 1. I vilken utsträckning går det att lita på människor i allmänhet? Procent. N=1014

	Procent		Procent
I låg utsträckning	6	I ganska hög utsträckning	37
I viss utsträckning	31	I hög utsträckning	2
I varken låg eller hög utsträckning	24		

I vår studie har vi som referenspunkt för frågorna om tillit i det digitala samhället, ställt ett antal frågor om tillit i allmänhet. Bland de cirka 1060 personer som svarade på frågan, ligger förtroendet högst för polisen och de rättsvårdande myndigheterna: 52% har ganska stort eller mycket stor förtroende för polisen, 41% för domstolarna (se figur 1 nedan). Riksbanken åtnjuter också ett högt förtroende: 43% av de svarande har ganska stort eller mycket stort förtroende för riksbanken. På den internationella arenan har man förtroende för FN: 43% av de svarande har ganska stort eller mycket stort förtroende för FN.



Figur 1: Hur stort förtroende har du för det sätt på vilket följande institutioner och grupper sköter sitt arbete?

Förtroendet är påtagligt lägre för hur arbetet sköts inom mer uttalat politiska institutioner: 46 % av respondenterna anger att de har litet förtroende för hur regeringen sköter sitt arbete och för riksdagen gäller att 38 % uttrycker svagt förtroende.

Det låga förtroendet gäller också på högre nivå, då 43 procent av respondenterna anger att de har litet förtroende för EU-kommissionen.

Det låga förtroendet för politiska institutioner slår också igenom när det gäller svenska politiker. På en direkt fråga anger 54 procent av respondenterna att de har litet förtroende för svenska politiker. Bara 16 procent ger uttryck för stort förtroende, se tabell 2 nedan.

Tabell 2. Allmänt sett, hur stort förtroende har du för svenska politiker? Procent. N=1063

	Procent
Litet	54
Varken stort eller litet	30
Stort	16

Bland de bakgrundsfaktorer som vi samlat in data om, finns två som slår igenom i statistiskt signifikanta samband. Det är den ovan nämnda ”allmän tillit”, samt kön. Utbildning, bostadsort, politiska preferenser och inkomst fungerar inte i någon större grad som förklaringsmodell för de variationer vi ser i studien.

Övervakning

När man skrapar på ytan gällande övervakning ser man snart att terminologin tenderar att inbegripa en stor mängd företeelser, och i någon mån även styra tanken på ett sätt som kanske inte alltid gör fenomenen rättvisa. Det som vi i vår enkätstudie relaterar till i termer av övervakning rör respondenternas inställning till framförallt det offentligas hantering av medborgarnas internettrafik och data. Vi lyfte även fram några av de resultat vi fick i undersökning på övervakningsområdet i en debattartikel i Svenska Dagbladet (19/4, 2014), som fick titeln “Övervakning tär på medborgarnas tillit” (se kapitel 4 nedan).[2] Denna artikel finns även i engelsk översättning på digitalsociety.se och i bilaga 2 nedan.[3]

Under 1990-talet, när kameraövervakning var ett frekvent tema i den offentliga debatten, bland annat med hänvisning till införandet av det brittiska CCTV-systemet för övervakning av offentliga platser, uttrycktes inte sällan oro för vilka konsekvenser den här typen av omfattande övervakning skulle kunna få för den personliga integriteten. Den här debatten förefaller inte ha satt några djupa spår, se tabell 3

[2] http://www.svd.se/opinion/brannpunkt/overvakning-tar-pa-medborgarnas-tillit_3479682.svd

[3] http://digitalsociety.se/2014/04/26/on-surveillance-and-trust/

nedan. Endast var femte av våra respondenter menar nu att kameraövervakning riskerar att inkräkta på människors personliga integritet och 60 procent av dem hävdar till och med att den i bara låg grad är ett hot. Männen är något mer skeptiska än kvinnorna – 24 av de manliga respektive 15 procent av de kvinnliga respondenterna anser att den här övervakningen inkräktar på den personliga integriteten.

Tabell 3 I vilken grad anser du att kameraövervakning av offentliga platser riskerar att inkräkta på människors personliga integritet? Procent.

I hög grad	Varken eller	I låg grad	N
20	21	59	1066

Ur ett teknikutvecklingsperspektiv blir det intressant att jämföra inställning till kameraövervakning med inställning till nyare former av datainsamling och bearbetning. Om vi först fokuserar myndigheternas övervakning av vad som händer på internet så är inställningen något ambivalent, se tabell 4 nedan.

Tabell 4 Det är bra att myndigheterna övervakar och kontrollerar vad som händer på Internet. Procent.

Instämmer	Varken eller	Instämmer inte	N
37	31	32	1065

Figur 2 Jag anser att det är acceptabelt att följande aktörer samlar in och bearbetar

Respondenternas svar faller ut i tre näst intill jämna grupper – 37 % tycker att det är bra att myndigheter övervakar, 31 % svarar varken eller och 32 % markerar avstånd från påståendet. Den jämna fördelningen gör sammanhanget aningen svårtolkat, men svaren blir mer begripliga när vi går vidare och frågar dels om hur man ställer sig till olika aktörers övervakning dels om under vilka omständigheter som övervakning anses vara acceptabelt, se figur 2 ovan.

När det gäller synen på vilka aktörer som har legitima skäl att samla in och bearbeta data om våra internetvanor, finns det två tydliga tendenser, se figur 2. För det första är den generella acceptansen för detta att betrakta som låg. Ungefär en tredjedel av respondenterna anser att det är rimligt att SÄPO och Polisen samlar in och bearbetar data om internetanvändning. Två tredjedelar av respondenterna anser inte att det är acceptabelt. Från denna låga nivå sjunker sedan acceptansen för övriga aktörers insamling och bearbetning och bara ungefär en tiondel av de svarande tycker att det är rimligt att internationella säkerhetstjänster ägnar sig åt detta (11, 11 respektive 9 %).

När det gäller metoder för insamling, dvs. när det kan vara acceptabelt för myndigheter att samla in och bearbeta information om internetvanor, konstaterar vi att vad man framför allt vänder sig mot är rutinmässig, automatiserad insamling av användardata, se tabell 5 nedan. Dessutom är förtroendet för myndigheternas förmåga att göra rimliga bedömningar här relativt hög. Detta gäller även för domstolen, vilket även syns i de allmänna frågorna om tillit ovan där polisen, FN och domstolarna åtnjuter hög tillit. En av fem av respondenterna visar på en stark känsla för integritet, alternativt en skepsis mot myndigheternas insyn, och bedömer det som att myndigheter aldrig bör få samla in och bearbeta information om våra internetvanor.

Tabell 5 Myndigheter bör få samla in och/eller bearbeta information om mina internetvanor. Procent. N=1065.

Aldrig	18
Efter domstolsprövning	37
Efter myndighetsprövning från fall till fall	36
Rutinmässigt	7
Automatiserat	3

Bank

Banksektorn bygger i mycket hög grad på tillit mellan aktörer. Den som sätter in sina pengar i en bank måste kunna lita på att man kan få tillbaka dem. Banker och pen-

gatransaktioner måste fungera för att ett samhälles ekonomi ska fungera. Om tilliten störs kan ett helt banksystem – och en hel nation – sättas i gungning, när spararna vill ha ut sitt kapital.

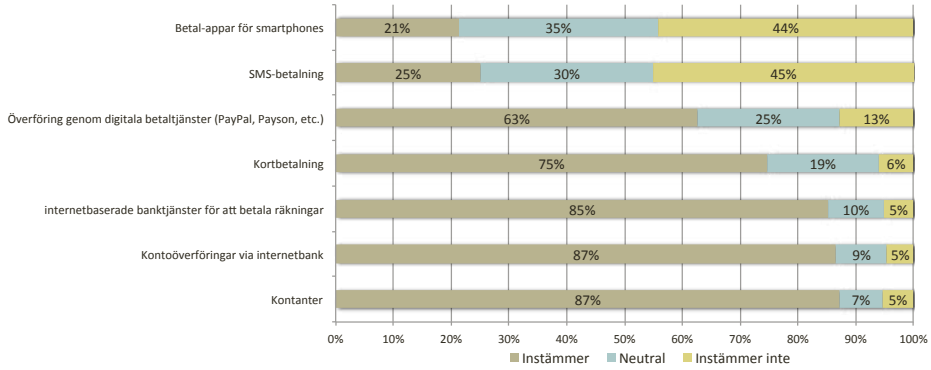
Allt sedan guldmyntfoten övergavs – i Sverige 1931 – är också riksbankernas verksamhet helt beroende på tillit. Valutans värde kan inte som förr lösas in i rent guld, utan värdet bygger på tilliten till riksbankens och landets förmåga att sköta sin ekonomi. Vidare finns statliga garantier som skydda spararna i affärs- och sparbanker, vilket ska bidra till spararnas vilja att anförtro bankerna sitt kapital. Det är alltså helt virtuella värden som skapas, och tilliten byggs upp av aktörernas agerande och utfästelser.

Inom banksektorn har man också – liksom nu i den digitala informationssektorn, se kapitel 5 – arbetat med fysisk gestaltning för att signalera tillit och förtroende. Stenfasader, marmorpelare och kassavalv motiveras delvis av ett behov av fysiskt skydd kring pengarna, men i lika hög grad utgör stenbyggnaderna symboler för det oföränderliga, det fasta, det som man kan lita på.

När det gäller digitaliseringen av banktjänsterna konstaterar vi, baserat på vår enkät, att användningen av internetbaserade banktjänster är utbredd. 84% av de svarande instämmer helt eller delvis i att de använder internetbaserade banktjänster obehindrat, 79% att de har god kunskap om hur man använder dessa tjänster, och 76% känner tillit till dessa tjänster. Däremot är det bara 39% som anser sig kunna bedöma huruvida banken har använt tillräckligt säker teknik för de digitala banktjänsterna.

När vi specifikt frågar om förtroende för olika betalningsmetoder, svarar 85% att de instämmer helt eller delvis i påståendet, att de har förtroende för internetbaserade banktjänster för att betala räkningar och 87% när det gäller kontoöverföringar, vilket är samma siffra som för kontanter. Betalningar via internetbanker åtnjuter alltså samma tillit som kontantbetalningar, se figur 3.

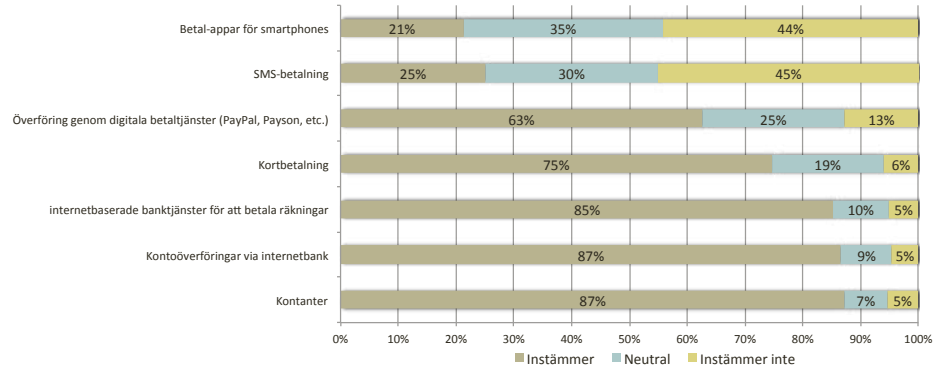
Figur 3. Andel av de svarande som har förtroende för olika betalningsmedel.



Att betala med kredit- och kontantkort är också en etablerad praxis som många har relativt stort förtroende för. Bland de svarande uppger 75% att de helt eller delvis instämmer i påståendet att de har förtroende för kortbetalningar, se figur 3. Samtidigt är det värt att notera, att när kortbetalningen sker via internet, oroar sig 44% för säkerheten i betalningen. Detta är i samma storleksordning som årets SOM-undersökning indikerar (www.som.gu.se). I denna årligen genomförda studie rapporterar cirka 42% av de svarande att de känner oro för kortbetalning på nätet, vilket motsvarar 51% av dem som faktiskt använder kortbetalning på nätet.

Däremot när det gäller nyare digitala betalningsmedel är förtroende betydligt lägre: SMS-betalning, 25%; betal-appar för smartphones, 21%. Digitala betaltjänster som PayPal och Payson ligger i mellanskiktet, med 63% av de svarande som helt eller delvis känner förtroende för betaltjänsten.

Figur 4. Andel av de svarande som använder olika betalningsmedel.



Ett annat perspektiv på de digitala betalningsmetoderna är hur ofta de används, se figur 4. Eftersom olika betalningsmetoder lämpar sig för olika köpmönster ser vi ett användningsmönster som speglar detta. Kortbetalning används någon gång i veckan eller dagligen av 74% av de svarande, medan kontanter för samma tidsperiod bara används av 52%. Banktjänster via internet för att betala räkningar används normalt mera sällan, av 26% på veckobasis eller oftare, men av 91% på månadsbasis.

Om man vänder på frågan och ser vilka som aldrig använder respektive betalningsmetod, hittar vi betal-appar och SMS-betalningar i topp, med 70% respektive 59% som aldrig använder dessa betalningsmetoder. Digitala betalningstjänster, som PayPal och Payson, används aldrig av 21% av de svarande, medan 51% använder med ”någon gång”. Endast 3% av de svarande betalar aldrig räkningar via internetbank, och endast 2% använder aldrig kortbetalning. Slutligen, 3% av de svarande lever ”kontantlöst”.

Vi kan från dessa data konstatera att ”vanans makt är stor”. De betalningstjänster man ofta använder, har man stort förtroende för. Men frågan är om detta är den enda förklaringen till förtroendet för internetbankerna. Vilken betydelse har bankernas satsningar på säkerhetsmekanismer i form av kod-dosor och annan utrustning för kryptering och lösenordshantering? Dessa är tekniskt motiverade för att öka säkerheten, men kanske bidrar också, likt bankpalatsens marmorpelare, till en känsla av säkerhet och handlingskraft för att skydda kundernas ekonomiska tillgångar?

Klart är att utformningen av systemen är viktiga för tilliten. Fallet med den norska kvinnan som skulle överföra 100 000 USD till sin dotter och knappade in fyra konsekutiva 5:or i stället för tre i ett kontonummer, illustrerar detta (Olsen, 2008). Hon skrev 715815555022 i stället för 71581555022; internetbanken klippte bara bort den sista 2:an, i stället för att kolla att 11 siffror hade knappats in, vilket råkade ge ett korrekt kontonummer. Pengarna hamnade hos en person som hävdade rätten till dem. Banken kompenserade kvinnan men först efter hot om stämning. I vilken grad utformningen påverkar tilliten återstår att studera mer i detalj och täcks inte av den här studien.

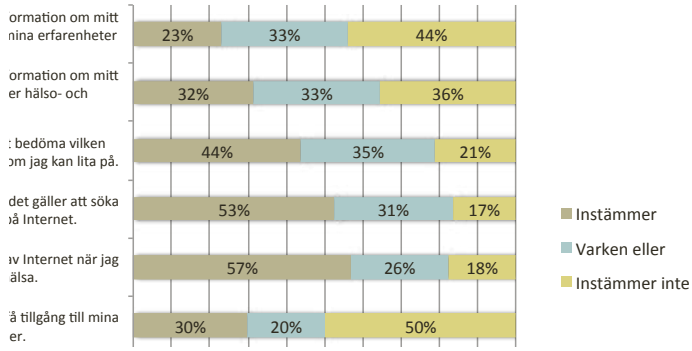
Hälsa

På ett övergripande plan tydliggör enkätsvaren tre poänger. För det första måste tilliten till vårdsinstitutionerna beskrivas som hög. Drygt 60 procent av respondenterna instämmer i att de skulle känna sig trygga med att deras medicinska journaler lagras hos dem i digitalt format, se figur 5. En nästan lika stor andel av respondenterna anger också att de litar på att sådan information inte skulle komma att hamna i orätta händer. I dessa båda fall är det bara 14 respektive 18 procent av respondenterna som inte instämmer i påståendet.

För det andra märks att det bland respondenterna finns en tämligen utbredd självtillit när det gäller att söka och värdera hälsorelaterad information på Internet. Endast runt en femtedel av respondenterna (mellan 17 och 21 procent) instämmer inte med påståendena att det ”… är naturligt för mig att använda mig av Internet när jag söker information om min hälsa”, ”Jag anser mig kunnig när det gäller att söka hälsoinformation på Internet” samt ”Jag har inga problem med att bedöma vilken hälsoinformation på Internet som jag kan lita på”.

En tredje poäng som enkäten gör tydlig, är att den tillit man upplever i relation till vårdsinstitutioner och till sin egen förmåga att navigera i och värdera hälsoinformation på Internet, inte motsvaras av en allmän känsla av trygghet ifråga om att lämna ut hälsorelaterad information på Internet. Bara strax under en tredjedel av

Figur 5 Digital tillit och hälsa. Procent.



respondenterna känner sig trygg med att lämna ut information om sitt hälsotillstånd för att söka hälso- och sjukvårdsinformation och än färre – 23 procent av respondenterna – känner sig trygga med att ”lämna ut information om mitt hälsotillstånd på Internet i syfte att dela mina erfarenheter med andra”.

Arbetsliv

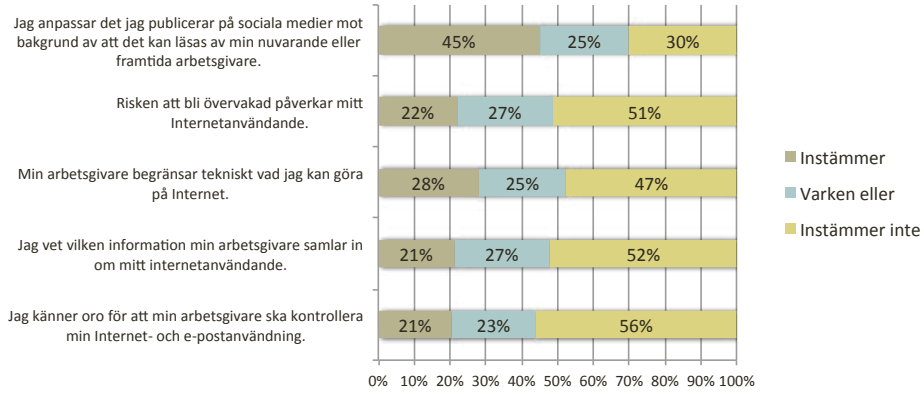
Genom hela framväxten av det moderna arbetslivet kan vi se hur olika tekniska innovationer på ett genomgripande sätt kommit att påverka, inte enbart vad som producerats utan även hur. Från slutet av 1800-talet och framåt introducerades nya tekniska innovationer som radikalt förändrade produktionsprocesserna. De första fabrikerna låg utmed floder för att kunna dra nytta av vattenkraft. Detta beroende av vattnets flöde var en hämmande faktor i produktionen, då flödet bland annat varierade med årstiderna. Ångmaskinen möjliggjorde en mer strategisk placering av produktionen och skapade samtidigt en kontinuitet i densamma. På så sätt skapades successivt ett oberoende av naturens växlingar. Över hundra år senare ser vi nu hur den digitala tekniken på ett grundläggande sätt förändrar såväl vad som produceras – i form av varor och tjänster – som var och när arbete utförs.

Ny teknik bidrar inte enbart till att övervinna rummets begränsningar, den har även i grunden kommit att påverka den sociala relationen, och mer precist tilliten mellan arbetsgivare och arbetstagare. Det är stundtals lätt att förledas till att tro att utvecklingen inom arbetslivet rör sig från en situation där arbetsgivaren, i den stinkande och rykande fabriken, övervakade och kontrollerade den alienerade arbetarens minsta rörelser – till en kunskapsekonomi där medarbetarens behov av utveckling och självförverkligande går hand i hand med organisationers mål (vilket i sig skulle medföra att behovet av övervakning försvinner, detta då medarbetaren i högre ut-

sträckning antas drivas av inre motivation). Möjligtvis ligger det någonting i detta. Men på samma sätt som fabriken möjliggjorde en form av övervakning och kontroll har den digitala teknikutvecklingen medfört andra.

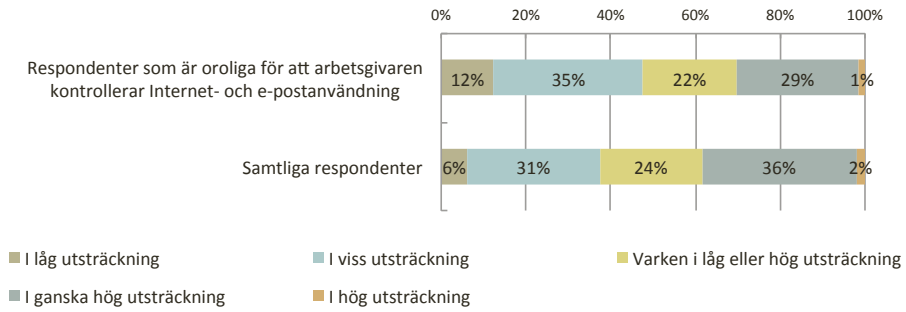
Inom ramen för projektet har det inom området arbetsliv och tillit identifierats nya former för övervakning av de anställda, samt vilka konsekvenser detta kan få för tilliten. Följaktligen fanns det även i enkäten ett frågebatteri som berörde övervakning i arbetslivet. Följande frågor fanns med:

Figur 6. Digital tillit och arbetsliv. Procent.



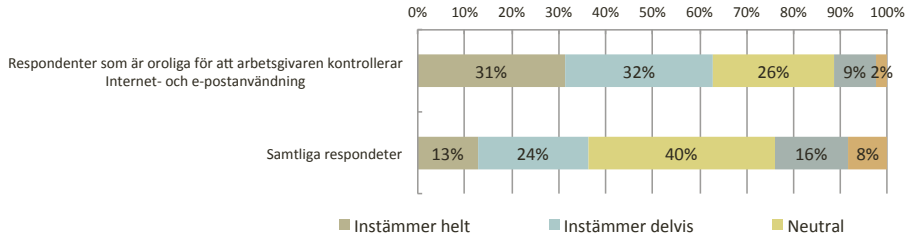
Noterbart är att lite drygt var femte respondent ger uttryck för en oro att arbetsgivaren ska kontrollera Internet och e-postanvändning, det vill säga 21 % instämmer helt eller delvis i påståendet "Jag känner oro för att min arbetsgivare ska kontrollera min Internet- och e-postanvändning", se figur 6. Bland de respondenter som uttrycker oro i detta sammanhang finner vi även en generellt en lägre tillit till andra människor. Bland gruppen som oroar sig för arbetsgivarens kontroll är det närmare hälften som uttrycker att människor i allmänhet endast går att lita på i viss eller låg utsträckning.

Enligt din mening, går det att lita på människor i allmänhet?



Vidare kan vi se att de som oroar sig för arbetsgivaren även oroar sig för vad andra aktörer på Internet samlar in för information.

Jag oroar mig för att information om min mediekonsumtion på Internet används i andra syften än de angivna.



En försiktig slutsats är att oron inte specifikt rör arbetsgivaren utan är framförallt en misstro mot andra människor samt för övervakning generellt.

Tidigare forskning har visat att när ny teknik introduceras finns ofta en eftersläpning i de sociala normer, som kringgärdar samma teknik (Beck, 2000; Rosengren & Ottosson, 2007). Som ett utslag finns det i övergångsfasen – eller om man så vill brytpunkten, många gånger en otydlighet och mångtydighet vilka riktlinjer som finns. I relation till enkäten ser vi t ex att endast var femte respondent anger att de känner till vilken information deras arbetsgivare samlar in kring deras nätanvändning, det vill säga instämmer helt eller delvis i påståendet "Jag vet vilken information min arbetsgivare samlar in om mitt internetanvändande". Mer specifikt visar tidigare studier att information som samlas in av arbetsgivaren, där syfte, omfattning och innehåll av insamlingen inte är tydligt kommunicerat riskerar att påverka tilliten negativt mellan arbetsgivare och arbetstagare, något som går att läsa mer om i blog-

ginlägget ”Tillbaka till framtiden, chefen ser dig!” publicerat på Cybernormer.se. 8 november 2013 se s. 52.[4]

Det är intressant i sammanhanget att fler respondenter uppger att arbetsgivaren begränsar tekniskt vad respondenterna kan göra på Internet. Så många som 28% instämmer helt eller delvis i påståendet “Min arbetsgivare begränsar tekniskt vad jag kan göra på Internet”, se figur 6. Rimligtvis bör insamling av arbetstagares nätanvändning samt tekniska begränsningar behandlas på ett samlat sätt.

Avslutningsvis kan vi konstatera att det blivit allmänt känt att potentiella arbetsgivare och rekryteringsföretag ”googlar” kandidater innan de kan bli aktuella för anställning. Vi kan, utifrån enkätresultaten, se att detta även kommit att påverka individers nätanvändning på det sättet att de anpassar vilken information de publicerar i sociala medier med tanke på framtida arbetsgivare. Detta då så många som 45% av respondenterna instämmer helt eller delvis i påståendet: “Jag anpassar det jag publicerar på sociala medier mot bakgrund av att det kan läsas av min nuvarande eller framtida arbetsgivare”.

Traditionella och sociala medier

Det senaste decenniet har sett en snabb framväxt av en ny typ av medier, så kallade sociala medier. Trots skillnader dem sinsemellan har de några egenskaper som förenar dem: de erbjuds användarna utan kostnad, det är användarna själva som producerar det huvudsakliga innehållet (med text, bild, film etc.) och de finansieras i huvudsak av annonsintäkter. De sociala medierna brukar också liknas vid plattformar – istället för att erbjuda användarna innehåll, ger de ramar och strukturer för användarnas skapande och delande av innehåll. Sådant innehåll brukar refereras till som användargenererat innehåll (eng. user generated content). På engelska kallas de sociala medierna ofta “social networking media”, då de både är i teknisk mening nätverksbaserade (har internet som teknisk plattform) och utgör plattformar för olika typer av nätverksskapande.

De sociala mediernas korta historia till trots har den samhällsvetenskapliga forskningen redan hunnit ägna dem en hel del uppmärksamhet. Inom den här forskningen har man bland annat analyserat de sociala medierna som affärsmodeller (Fuchs, 2013). Hur genererar de sina intäkter och vilken roll spelar användarna för affärsmodellerna? Analyserna har utmynnat i etablerandet av begrepp som prosumenter och – på engelska – “prod-users” (Bruns, 2008), vilka sätter fingret på hur plattformarna, i en och samma rörelse, positionerar sina användare som såväl producenter som konsumenter. En central komponent i de här analyserna har varit

[4] http://cybernormer.se/tillbaka-till-framtiden/

värdeskapandet: Vilka värden skapar det innehåll som användarna producerar. Och hur approprieras de?

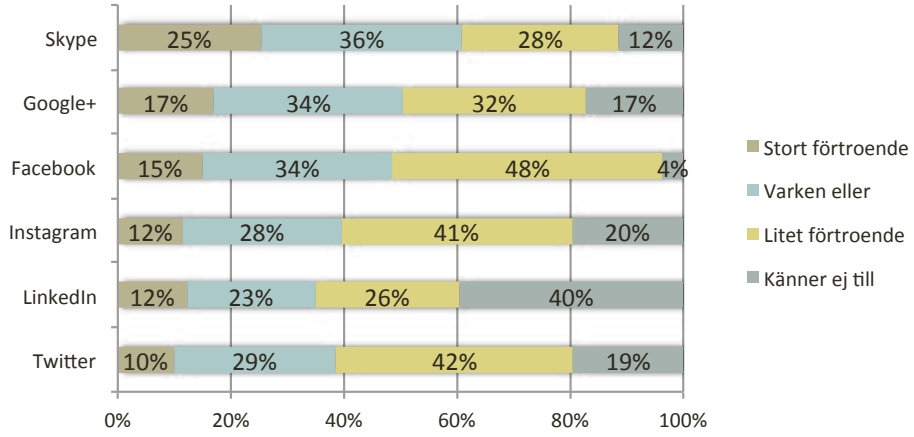
Övervakningsfrågan (surveillance) har också varit framträdande i den här forskningen. Om internet i sin tidiga historia – på 1990-talet – i första hand inspirerade till reflektioner kring risken för ett framväxande storebrorsamhälle (”storebror, staten, ser dig”), så har utvecklingen av sociala medier riktat samhällsvetenskapens uppmärksamhet mot småsyskonen. Utöver att de sociala medierna utgör plattformar på vilka användarna kan skapa och dela innehåll, så öppnar de också upp för omfattande insyn i användarnas förehavanden. Vilken information om användarna samlas in, och hur använder sig företag som tillhandahåller sociala medier av denna?

Studierna av sociala medier som affärsmodeller, och som övervakningsapparater, har huvudsakligen betraktat medierna med kritiska glasögon. Däremot har man inom andra delar av forskningen kommit att ta fasta på hur medierna också kan stärka användarna. Ett framträdande tema har varit studier av de sociala medierna som resurser för olika former av politisk aktivism. I den populära debatten har begrepp som Twitter- (i Iran 2009) och Facebookrevolution (i Egypten) figurerat, då de sociala medierna har kopplats samman med ambitionerna att skapa snabb politisk och social förändring i auktoritära samhällen.

Det är en relativt enkel analys att avfärda kopplingarna mellan de sociala medierna och politiska förändringar som ganska oreflekterade och teknikdeterministiska, men bortom mytologierna ger forskningen också viss substans till sådana sammankopplingar. Statsvetarna Lance Bennett och Alexandra Segerberg (2012) har till exempel visat hur nätverksbaserade sociala medier underbygger förändrade former för politisk aktivism, från collective till connective action och i en fallstudie av Occupy Wall Street-rörelsen exemplifierar Peter Dahlgren (2013) hur sociala medier – med sin plattforms- och nätverkskaraktär – kan fungera som resurser för omförhandling av etablerade politiska och ekonomiska (makt)strukturer.

Så här långt har således forskningen identifierat både kritiska dimensioner och möjligheter i de sociala medierna. Men oavsett vilken av dessa positioner man utgår från väcker de sociala medierna en grundläggande fråga, som forskningen på båda sidor ägnat begränsad uppmärksamhet: I vilken grad har användarna faktiskt tillit till de sociala medierna? Och hur varierar tilliten dels mellan de olika företagen som står bakom olika sociala medier dels mellan olika grupper av användare?

Figur 7 Tillit till företagen bakom sociala medier. Procent.



Givet den stora mediala uppmärksamhet som olika typer av sociala medier har genererat på senare år, tillsammans med det i många avseende utbredda användandet av dem, måste respondenternas mycket begränsade tillit till de företag som levererar tjänsterna betraktas vara något förvånande. Inte minst i ljuset av att 80% av respondenterna samtidigt anger att de faktiskt använder sig av sociala medier. Mark Zuckerbergs Facebook har till exempel existerat i snart tio år. Plattformen har miljontals svenska användare. De här användarna bidrar rutinmässigt med innehåll till plattformen och delar kontinuerligt med sig av olika typer av information om sig själva till densamma. Därför måste användarnas förtroende för företaget betraktas vara påfallande lågt: på en femgradig skala från lågt till högt anger närmare hälften av respondenterna (48%) att det har lågt förtroende för företaget bakom Facebook, se figur 7. Facebook är förvisso det mest kända företaget på området (endast fyra procent av respondenterna har svarat ”känner ej till”, vilket kan jämföras med att en så pass stor andel som 40% av respondenterna inte känner till LinkedIn), men förmår likafullt inte skapa tillit hos användarna. En av applikationerna – Skype – avviker dock något från det övergripande mönstret. Sannolikt beroende på att den tjänst företaget erbjuder skiljer sig en del från de andra, då Skypeanvändande handlar mindre om att producera och dela innehåll och mer om kommunikation personer emellan.

Våra enkätdata kan inte ge klara besked om varför tilliten till de företag som står bakom de sociala medierna är så pass låg, men de ger en del intressanta reflektioner. Bara strax under 20% av respondenterna anger att de känner sig trygga med att lämna ut personlig information via sociala medier och närmare hälften av samtliga

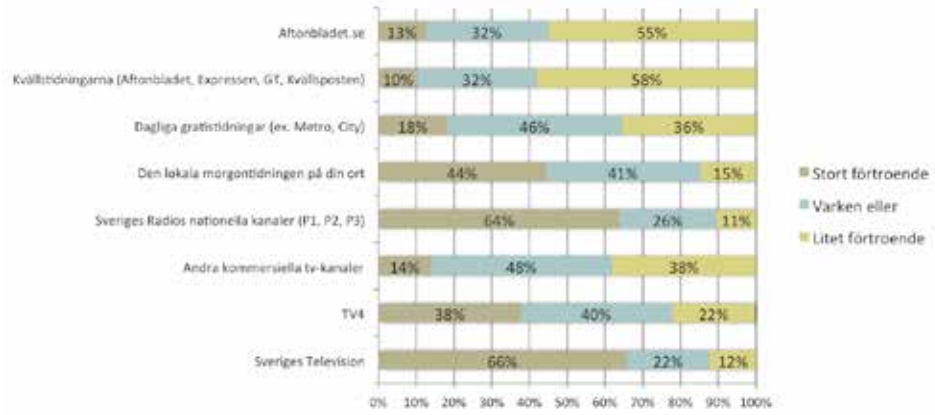
respondenter menar att sociala medier riskerar att inkräkta på människors personliga integritet.

En nedbrytning av data ger en del bakgrundskunskap ifråga om inom vilka grupper som tilliten är särskilt låg respektive något högre. För att analysera detta har vi tittat närmare på svarsmönstren när det gäller tillit till företaget bakom Facebook – den mest spridda och, inte minst, enligt våra data mest välkända applikationen. När det gäller män och kvinnor så är kvinnorna klart överrepresenterade i den grupp respondenter som anger att de har tillit till företaget bakom Facebook. Av de som uttrycker att de känner tillit till Facebook är 54% kvinnor och 46% män. Notera dock att det övergripande mönstret är att tilliten är låg i båda grupperna. En liknande skillnad finns också vad gäller ålder och här kan man konstatera att unga människor – födda i början av 1990-talet och senare (till och med 1995) – är överrepresenterade bland de respondenter som uppger att de känner tillit till företaget bakom Facebook. På motsvarande sätt finns det också skillnader i tillit till Facebook ifråga om politisk orientering. De svarande har själva fått ange sina politiska preferenser, på en femgradig skala från klart till vänster till klart till höger. Och här är mönstret tydligt: tilliten till Facebook är påtagligt lägre bland dem som anger sig stå klart eller något till vänster på den politiska skalan. Samtidigt är det värt att återigen notera att denna skillnad uppstår inom ramarna för det övergripande mönstret av genomgående låg tillit.

Vad som är särskilt väl värt att notera, är att tillit till Facebook också mycket tydligt samvarierar med vad vi skulle kunna kalla allmän tillit, vilket i det här sammanhanget innebär tillit till såväl andra människor som en rad olika samhällsinstitutioner. De respondenter som anger att de har stor eller relativt stort tillit till Facebook anser i hög grad att det går att lita på människor i allmänhet. De är också mer benägna att ha förtroende för en lång rad institutioner. Det handlar om snart sagt allt från regering och riksdag till kommunstyrelsen och domstolarna.

Dessa variationer förändrar dock inte på något sätt den generella bilden, som ger vid handen att respondenterna bara i begränsad utsträckning känner tillit till aktörerna bakom de sociala medierna. Mönstret blir ännu tydligare om enkätsvaren på frågorna om de sociala medierna kontrasteras med respondenternas syn på de etablerade medierna, se figur 8.

Figur 8 Förtroende för innehållet i medier. Procent.



För den som sedan tidigare är bekant med data kring förtroende för massmedier är det inte mycket som förvånar i tabellen – public service-medierna, Sveriges Television och Sveriges Radio, är i förtroendemässig särklass, därpå följer de lokala morgontidningarna. TV4, som är ett hybridmedium – en kommersiell public service-kanal – kommer därefter. Övriga medier – kommersiella tv-kanaler, gratistidningar, kvällspress samt tidningen Aftonbladets webupplaga – åtnjuter begränsat förtroende. Bara mellan tio och tjugo procent av respondenterna anger att de har förtroende för det innehåll som de presenterar.

Frågorna är förvisso inte ställda på helt likvärdiga sätt, eftersom det inte går att jämföra innehållet i de etablerade medierna med det innehåll som presenteras på sociala medier. Data ger ändå en användbar indikation på hur ansändarna ser på och värderar de sociala medierna. I fråga om tillit bland användarna hamnar företagen bakom de sociala medierna på ungefär samma nivå som kvällstidningar, kommersiella tv-kanaler och gratistidningar.

Referenser

Beck, U. (2000). The brave new world of work. Malden, Mass.: Polity Press.

Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: digital media and the personalization of contentious politics. *Information, Communication & Society*, *15*(5), 739-768.

Bruns, A. (2008). *Blogs, Wikipedia, Second Life, and beyond: from production to produsage*. New York: Peter Lang.

Dahlgren, P. (2013). Contingencies of online political 'produsers': discourse theory and the 'Occupy Wall Street' movement. I Olsson, T. (red.) *Producing the internet: critical perspectives of social media.* Göteborg: Nordicom, 203-220.

Fuchs, C. (2013). Social media and capitalism. I Olsson, T. (red.) *Producing the internet: critical perspectives of social media*. Göteborg: Nordicom, 25-44.

Olsen, K. A. (2008). The $100,000 keying Eerror, *IEEE Computer*, 106-108.

Rosengren, C. & Ottosson, M. (2007) From white dress to white collar – a historical perspective on the hospital ward administrator. I Aili, C. & Nilsson, L-E. (red.) In tension between organization and profession: professionals in Nordic public service. Lund: Nordic Academic Press.

Trägårdh, L.; Wallman Lundåsen, S.; D. Wollebæk D. & Svedberg L. (2013). *Den svala svenska tilliten*, Stockholm: SNS Förlag.

Del II

Debattartikel: ”Övervakning tär på medborgarnas tillit”

Medborgarnas acceptans för säkerhetsrelaterad övervakning är begränsad. Exempelvis tycker 55 procent av svenskarna inte att det är acceptabelt att FRA samlar in och bearbetar data om internetvanor, skriver forskare från Lunds universitet.

Svenska Dagbladet 19 april 2014
BRÄNNPUNKT | INTEGRITET


Svenska Dagbladet fre dag 18 april 2014

SvD
Debattredaktionen
Telefon 08-23 58 40

BRÄNNPUNKT

MER DEBATT
"S tar rygg på alliansen med försvarsanslaget"

MER DEBATT
"Större andel äldre skog innebär mer virke"

Ta debatt om dataövervakning

INTEGRITET Medborgarnas acceptans för säkerhetsrelaterad övervakning är begränsad. Exempelvis tycker 55 procent av svenskarna inte att det är acceptabelt att FRA samlar in och bearbetar data om internetvanor, skriver forskare från Lunds universitet.

Vi kunde den 8 april läsa om hur EU-domstolen gick på generaladvokatens föreslagna linje och ogiltigförklarade det datalagringsdirektiv som alla medlemsstater implementerat under de senaste åren. Direktivet handlade i stort om att ålägga internetoperatörer en massiv lagring av data kring telefonsamtal, sms, e-postmeddelanden, internetuppkopplingar och mobilpositioner i 6–24 månader, i syfte att kunna bekämpa allvarlig brottslighet.

I dagarna som följt har vi kunnat studera ett politiskt positionerande kring datalagring och integritetsfrågor, och vi välkomnar starkt att frågan lyfts i samhällsdebatten och även blir en fråga för partipolitik. För tillits- och integritetsfrågan i en digital kontext är så viktig för vårt samhälle att den måste ha en tydlig plats i det allmänna medvetandet och i politiska ställningstaganden. Integritetsfrågan kan naturligtvis läsas ihop med

FRA-frågan, och även kopplas samman med de avslöjanden som Edward Snowden gjort gällande den amerikanska säkerhetstjänsten NSA, eftersom detta är betydande pusselbitar för hur vi bygger vårt digitala samhälle.

Och vad tycker då gemene man, egentligen, om statens och myndigheters informationsinhämtning i vårt digitala samhälle? Vilken tillit och vilket förtroende känner vi för att myndigheterna, både svenska och utländska, hanterar informationen på ett passande och acceptabelt sätt? Det här har varit centrala frågor för oss som mångvetenskaplig forskargrupp vid Lunds universitet. Under samlingsnamnet Digitrust har vi under drygt ett och halvt år samlats för att studera och analysera digital tillit.

Som ett led i detta arbete har vi i januari i år frågat ett representativt urval av Sveriges befolkning, 1 100 individer, bland annat om deras upplevelse av och förhållningssätt till övervakning. Från våra enkätdata kan vi tydligt se att medborgarnas acceptans för de här typerna av säkerhetsrelaterad övervakning är begränsad. 55 procent av svenskarna tycker inte att det är acceptabelt att Försvarets radioanstalt (FRA) samlar in och bearbetar data om internetvanor.

Vad man framför allt vänder sig mot är rutinmässig, automatiserad insamling av användardata, visar enkäten. Svenskarna är något mindre kritiska när det gäller övervakning som initieras och genomförs av polisen (46 procent) eller Säpo (47 procent). Om övervakningen föregås av myndighetsbeslut, eller åtminstone övervägande av myndighetspersoner, uppfattas den också som mer legitim. Allra minst acceptabelt uppfattas det dock vara att utländska säkerhetstjänster intresserar sig för svenskarnas internettrafik. Cirka 80 procent av svenskarna tycker att det inte är acceptabelt att andra staters säkerhetstjänster (USA:s, Rysslands, Storbritanniens) samlar in och bearbetar data om enskildas internetvanor.

Undersökningssvaren väcker både frågor om demokrati och frågor om tillit. Demokratifrågorna aktualiseras av diskrepansen mellan hur övervakning på internet går till i dag och medborgarnas syn på under vilka villkor den kan betraktas vara legitim. Många svenskar anser uppenbarligen att övervakning på internet kan vara acceptabelt, men menar att sådan insamling och bearbetning av data inte bör ske rutinmässigt. Beslutsfattande kring övervakning ska i stället vara underställt myndigheter (eller allra helst ske ”efter domstolsprövning”) och – i förlängningen – vara öppet för såväl insyn som kritik.

De här medborgarsynpunkterna har onekligen haft svårt att få genomslag. Innan EU-domen föll märktes de varken i den politiska debatten på området eller i hur lagstiftningen tillämpas. Inte heller den av regeringen tillsatta Digitaliseringskommissionen har producerat något mer substantiellt än ett förslag om att barn ska utbildas i ”hur integriteten fungerar och kan skyddas på internet” (SOU 2014:13).

Ifråga om tillit noterar vi i vår undersökning att både domstolar och myndighetsväsendet i Sverige har ett relativt stort förtroendekapital. Man ska dock inte utgå från att detta är oföränderligt bestående. Tillit och förtroende kan korrumperas och förstöras. Tilliten måste ständigt värnas, och mycket i vårt samhälle beror på den. Tillit till att individens integritet respekteras är central för medborgare i relation till stat och myndigheter, och därmed även för frågor om rättens och domstolarnas roll. Även för det ekonomiska systemet är tillit central, för tjänstesektorn och för bankväsendet, liksom för mediernas och kunskapsförmedlingens roll. Detta är centrala samhällsvärden, som måste värnas, också i det digitala samhället.

Integritet handlar inte om att man som medborgare ska ha rent mjöl i påsen, och därmed inte behöver oroa sig för insyn. Det handlar om att vi inte ska behöva tolerera smutsiga fingrar i vårt mjöl. Bristande respekt för integriteten – från både offentliga och privata aktörer – skadar vårt tillitsberoende samhälle. Och frågan är viktig, eftersom den i mycket kommer att definiera morgondagens digitala värld.

Kärnfrågorna här rör att hur vi regleras och mäts i det digitala, och under vilka former, och bör vara demokratifrågor. Man skulle lite högtravande kunna säga, att tillit är fundamentet i samhällsbygget, digitaliserat eller ej. För digital övervakning är ett kraftfullt verktyg – på gott och ont. Det måste underställas politisk debatt och stå under demokratisk kontroll för att i längden kunna åtnjuta medborgarnas tillit.

STEFAN LARSSON
fil dr i rättssociologi

TOBIAS OLSSON
professor i medie- och kommunikationsvetenskap

CALLE ROSENGREN
fil dr i industriell arbetsvetenskap

PER RUNESON
professor i programvarusystem

Relevans av tekniskt skydd för tillit

Ben Smeets

En intressant fråga är i vilken utsträckning som tillit i det digitala samhället beror på säkerheten i de tekniska lösningarna. För en tekniskt kunnig person kan det kännas uppenbart att tekniken i ett digitalt system måste vara korrekt vald och utförd för att systemet ska vara tillförlitligt. I de fall där brister i säkerheten kan medföra stor skadeinverkan, är tekniken en viktig del i att begränsa riskerna att skada uppstår, eller att en viss lösning överhuvudtaget kan skapas och användas.

Det är dock oklart hur tekniken i sig leder till att användare litar på ett digitalt system. Men innan vi går vidare med denna fundering så är det relevant att undersöka hur yrkesverksamma inom IT-säkerhet ser på tillitsfrågan. Där har det blivit viktigare att produkten inte bara implementerar lämpliga säkerhetsmekanismer, men också att man kan lämna dokumentation på att dessa är realiserade på ett korrekt sätt för ändamålet.

Ett exempel hur man arbetar kring dessa frågor är tillämpningen av Common Criteria-metodiken (CC) som är standardiserad i ISO/IEC15408 standarden, se (Common Criteria). Med hjälp av CC kan en beställare och tillverkare beskriva säkerheten för sitt system och vilken nivå av grundlighet man vill ha, samt har uppnått vid tillverkning.

Även om CC har sina brister (Zhou C & Ramacciott S, 2011) – det anses vara dyrt och byråkratiskt samt att det nämligen går att avgränsa sitt system till den grad att CC inte kan ta tillräckligt med hänsyn till systemets faktiska användning – så ger användandet av CC en viss försäkran att en IT-produkt uppfyller de säkerhetskrav man förväntar sig, och följaktligen går att lita på. CC är dock enbart ett instrument som riktar sig till de som beställare, tillverkar och granskar produkter. Användare, bortsett från ev. krav på dokumentation och instruktioner, betraktas ej. Dessutom kräver CC-dokumenten att läsaren är kunnig i området, vilket medför att en användare i regel inte kan tolka CC-dokument på ett sådant sätt att det ökar dennes tillit

till produkten. Detta är dock egentligen inget fel hos CC, utan snarare en typisk brist: att det krävs mycket kunskap för att tolka det tekniska säkerhetsarbetet kring en IT-produkt.

När man då frågar en person i vilken utsträckning denne litar på ett IT-system, är det för de flesta en fråga som personen i fråga inte kan basera på egen kunskap om systemets tekniska säkerhet. Det blir en fråga där personen viktar sina olika åsikter och erfarenheter. Enkätsvaren tyder på att det är möjligt att ha IT-system i drift som människor huvudsakligen litar på. Vi såg att 85% svarar att de instämmer helt eller delvis på frågan om de har förtroende för olika betalningsmetoder och internetbaserade banktjänster för att betala räkningar och 87% när det gäller kontoöverföringar. Motsvarande siffra för kontanter är 87%. Bankernas internetbaserade tjänster för betalningar åtnjuter alltså en hög tillit som ligger på samma nivå som kontantbetalningar. Vad gör bankerna mer rätt än andra, mer tekniskt profilerade företag, som är aktiva inom sociala media? Det finns studier som behandlar frågan (Eriksson et al, 2005; Meuter et al, 2000). Utan grundligare studier om de inblandade mekanismer na om hur bilden om tillit växer fram, så kan vi inte säga mer än att det finns skillnader i hur man lyckas med att skapa tillit. Som ett första led att hitta en förklaring är det intressant att peka på några egenskaper som kan spela en roll.

Banker investerar mycket pengar i olika säkerhetssystem, såväl vid fysisk utformning (säkra serverhallar) som vid val och realisering, och drift av procedurer och IT-system. Det gör de även om tjänsten som banken säljer i sig inte är en säkerhetsprodukt (om vi bortser från att banken förvarar tillgångar). Bankerna använder mycket teknik för att skapa säkerhet, men kompletterar detta också med procedurer och image-formande aktiviteter där de vill måla upp en bild av en stark och pålitlig internetbank, ex. SEB: ”--- Internetbanken är alltid öppen och lika trygg som ett vanligt bankkontor. ---”

Bankernas verksamhet är ganska regelstyrd av olika föreskrifter och erforderliga tillstånd. Detta framgår av lagen (2004:297) samt förordningen (2004:329) om bank- finansieringsrörelse. För sparbanker finns det även regler i sparbankslagen (1987:619) och för medlemsbanker i lagen (1995:1570) om medlemsbanker. Dessutom finns det en viss tillsyn av bankverksamheten så att den uppfyller de ställda kraven för tillstånd. I Sverige hanteras detta av Finansinspektionen (FI). Det finns alltså – beroende på hur samhället i allmänhet fungerar i sin kravställning och uppföljning – mekanismer som ska ge en försäkran att banken uppför sig som allmänheten förväntar sig. Detta i sig skapar en sorts tillit, men kanske viktigare är förutsägbarheten som uppstår av ett transparent regelverk och tillsyn. Den bidrar till en bild att bankverksamheten i sin helhet går att lita på.

Slutligen finns det inte markanta skillnader vad gäller de internet-relaterade banktjänster som bankerna erbjuder sina kunder. Här ser slutkunder ofta de skillnader som finns bland de metoder bankerna använder för att realisera autentisering, dvs metoden som banken använder för att säkerställa vem som logga in, samt de behörigheter som ska gälla för den som släpps in i banktjänstsystemet. Här finns allt från manuella koder som kunderna får hemskickade, till s.k. inloggningsdosor och speciella appar till mobila enheter (ex. Mobilt BankID).

Dessa metoder upplevs av kunderna på ett sådant sätt som skulle kunna påverka helhetsbilden, men vi har inga öppna fakta för att kunna förstår hur och i vilken utsträckning som kunderna påverkas. (dock vet vi från studier att användarvänligheten spelar en roll vad gäller adoption (Lichtenstein & Williamson, 2006). Men återigen så har kunderna svårt att kunna bedöma säkerheten. Även de som är kunniga säkerhetsmässigt kan för det mesta inte skapa en komplett helhetsbild för att göra en sådan bedömning. Bankerna brukar vara medvetet sparsamma med information om sina system. Vilket man i regel inte är för att man vill dölja brister i sitt system, istället styrs detta mer av vetskapen att utsattheten ökar om personer utanför har precisa kunskaper om systemets olika delar och funktioner.

En annan faktor som kan bidra till resultatet för den höga tilliten i banktjänster kan finnas påvisad i andra studier, t.ex. Hain, (2003) där man konstaterar att banktjänstanvändare som inte använder internettjänsterna, är mer bekymrade kring säkerhet och integritet än användare som använder internettjänsterna. Många respondenter (74%) i vår studie instämmer helt eller delvis med påståendet "Jag har god kunskap om hur man använder Internet". 72% av de som svarar instämmer helt eller delvis att de hjälper gärna andra med att använda Internet. Vi har alltså en grupp som känner sig veta hur man använder bankernas internettjänster och som är positivt kring att hjälpa andra med Internetanvändning.

Bilden som framträder är att kopplingen mellan teknikval i en digital banktjänst och tillit finns, men att kundernas tillit förmodligen är ett resultat av en rad andra faktorer. En direkt följdfråga är då om bankkunderna gör rätt att lita på deras banktjänster. Eftersom man strikt taget inte kan få några garantier som kund är svaret här egentligen: nej det gör de inte. Här finns också resultaten från olika studier, t.ex. (Hole, 2008, 2011) i Norge, brister i vissa implementeringar av säkerhetsprotokollet TLS (2011, 2013, 2014) men också allvarliga driftstörningar som gör att man inte kan lita på banktjänsten. Eftersom det inte finns en bank (i Sverige) som upplevs som felfri i detta hänseende och eftersom man rent praktiskt är tvungen att använda en banktjänst är således slutsatsen att ett konstaterande att man strikt taget inte kan lita på banken är praktiskt oanvändbart. Medvetet eller omedvetet så är man tvungen

att ta risker om man vill använda digitala banktjänster. Utöver dessa överväganden så är tillitsfrågan också en fråga om bilden som banken målar upp om sig själv och de rykten kring hur man klarar av hantera brister och misstag. Faktum kvarstår att i praktiken så är den enskilde tvungen att praktisera en viss tillit till sin digitala banktjänst om han eller hon vill använda den och tilliten då inte direkt bottnar i bankens teknikval vad gäller säkerhet.

Kan man då våga dra slutsatsen att bankernas arbete med säkerhetsteknik är onödig eftersom deras kunder inte värdesätter den? Troligen inte. Förmodligen säger resultaten enbart att bankerna har inget att vinna på att synliggöra för kunderna deras val av teknik för att förbättra kundernas tillit. Arbetet med säkerhetsteknik är då mer en konsekvens av formella krav på verksamheten samt en del av arbetet med att upprätthålla ett skydd mot missbruk och attacker mot bankens digitala banktjänster. I vissa fall kan konkurrenternas agerande eller konsumentgrupper påverka val av teknik. Vidare kan rätt val av teknik minimera risken att något går fel och att proceduren att hantera eventuella fel inte blir kostsamma.

Det är frestande att tänka sig att också för andra digitala tjänster vi har en liknande situation att slutanvändarnas tillit inte alls eller bara i liten omfattning direkt påverkas av teknikval vad gäller säkerheten. I likhet med bankerna så används tekniken där av tjänsteleverantören som ett medel för att uppfylla formella och informella krav samt som ett medel att förebygga problem på grund av missbruk eller intrång. Det är få digitala tjänster där säkerhetsteknik lyfts särskild fram som en del av argumentationen att man kan lita på tjänsten. Mest känd är de så-kallade VPN tjänsterna för att skapa krypterade tunnlar för dataöverföring och molnlagring där data som läggs i molnet är krypterad och därmed oläsbart även för den som tillhandahåller lagringstjänsten. Dock, också här är argumentationen mot kunder mer byggd varför man behöver en VPN, att man har många kunder och att man eventuellt kan mer konkret peka på kända grupper eller personer som använder en specifik lösning. I regel måste kunderna som vill veta mer om de tekniska lösningarna gräva fram denna information genom egen analys eller via användarfora. I regel vet många användarna av VPN-tjänster inte ens om vilken teknik som används i den VPN tjänst man använder; t.ex. så kan du bygga på (D)TLS protokollet eller IPsec protokollet. Kunskapen om detta kan spela en roll om något fel upptäckts in en viss lösning, jmf Heartbleed-problemet i TLS implementationen Open SSL. Bortsett från enstaka kunniga och yrkesmässiga så har de flesta som använder digitala tjänster inte den förmågan att själv bedöma om man kan lita på tjänsten eller ej. De flesta användarna är beroende av vad andra säger eller vilka lösningar andra använder när man ska välja en digital tjänst eller måste bedöma om man kan lita på tjänsten.

Referenser

Common Criteria (n.d.). *Common criteria for information technology security evaluation (ISO/IEC 15408) for computer security certification.* http://www.commoncriteriaportal.org/cc/ [2014-05-19]

Duong, T. & Rizzo, J. (TLS 2011). Here Come The ⊕ Ninjas, http://www.infoworld.com/sites/infoworld.com/files/pdfe/BEAST_Duong_Rizzo.pdf [2014-05-19]

Eriksson, K.; Kerem, K. & Nilsson, D. (2005). Customer acceptance of internet banking in Estonia, *Int Journal of Bank Marketing,* 23 (2), 200-216.

Hole, K.J.; Tjøstheim, T.; Moen, V.; Netland, L.-H.; Espelid, Y. & Klingsheim, A.N. (2008). Next generation internet banking in Norway. *Teknisk Rapport 371*, Institutt for informatikk: Universitet Bergen. http://www.nowires.org/Papers-PDF/BankIDevaluation.pdf [2014-05-19]

Hole, K.J.; Klingsheim, A.N.; Netland, L.H.; Espelid, Y.; Østheim, T. & Moen, V. (2009). Risk assessment of a national security infrastructure. *IEEE Security & Privacy*, 7(1), 34-41

Jackson, W. (2007). Under attack: common criteria has loads of critics, but is it getting a bum rap. *Government Computer News, Aug.* http://gcn.com/articles/%202007/08/10/under-attack.aspx [2014-05-20]

Lichtenstein, S. & Williamson, K. (2006). Understanding consumer adoption of internet

banking: an interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, 7(2), 50-66.

Meuter,M.L.; Ostron,A.L.; Roundtree, R.I. & Bitner, M.J., (2000), Self-service

technologies: understanding customer satisfaction with technology based service encounters, *Journal of Marketing*, 64 (3), 50-64.

Sepehrdad, P; Vaudenay, S.; Vuagnoux, M. (TLS 2013). Discovery and exploitation of new biases in RC4. *Lecture Notes in Computer Science* 6544, 74–91.

Heartbleed bug (TLS 2014). Bug CVE – CVE-2014-0160". Cve.mitre.org. [2014-05-11]

Zhou, C. & Ramacciott, S. (2011). Common criteria: its limitations and advice on improvement. *Information Systems Security Association Journal,* April 2011, 24-28.

Tillit i arbetslivet – några nedslag

Av Calle Rosengren

Följande texter är tidigare publicerade som blogginlägg på Cybernormer.se samt digitalsociety.se

Tillit… kan det vara något?

Cybernormer.se, September 12, 2013

I takt med att samhälls- och arbetsliv utvecklas och förändras dyker det med jämna mellanrum upp begrepp som söker fånga, beskriva och i viss mån förutsäga förändringsprocesser. Exempel från det tidiga nollnolltalet är hur forskare

och samhällsuttolkare sökte använda begrepp såsom *kompetens* och *flexibilitet* för att fånga vad det var som drev och formade dagens och framtidens organisationer. Ser vi några år ytterligare tillbaka har vi industrisamhällets centralbegrepp ”rationell” och med det hela rationaliseringsrörelsen.

Många gånger åtföljs de av uttolkare och gurus som har/säger sig ha, insikter i hur samtiden kan förstås och tämjas utifrån just dessa begrepp. Och så är karusellen igång. Det hissnar i magen när den komplexa vardagen helt plötsligt, genom prismat på det nya perspektivet som ryms i begreppen, framträder i en ny och lite skarpare kontur. Som arbetslivsforskare har jag åkt med på flera av dessa karuseller (och t o m arbetat inom ”Programmet för kompetensutveckling”) och inte sällan har det slutat med att man står där, lite yr i huvudet, och begrundar vad det var som var så väldigt lockande med just den där karusellen… för att i nästa stund upptäcka en annan, ny, större och ännu intressantare.

Just nu är det tillits-karusellen som lyser allra klarast och dit köerna ringlar allra längst. I vart fall på det tivoli vi kallar forskarvärlden.

Som sagt har forskningen kring just tillit kommit att växa och gripa in i flera olika stora forskningsfält. Tillit eller kanske snarare bristen på tillit verkar vara ett av dagens stora samhällsproblem. Till exempel har begreppet en egen tidskrift Journal of trust research och vid Lunds universitet har begreppet fått ett eget tema vid Pufendorfinstituet – Digitrust (läs mer på http://digitalsociety.se). Som begrepp har tillit det gemensamt med kompetens och flexibilitet att det har positiva konnotationer. Vem vill till exempel vara inkompetent och irrationell?

Rent intuitivt tänker man kanske att det borde vara något bra och viktigt. Och det är väl ett rimligt antagande: att för länder och organisationer där tilliten mellan människor och till systemen är låg inte har så goda framtidsutsikter. På samma sätt har väl personliga relationer, där det saknas en grundläggande tillit gentemot den andra partens intentioner, inte de bästa chanser att utvecklas på ett positivt sätt.

Men frågan är väl dock. Varför just nu? Vad i dagens samhällsutveckling har bidragit till detta väldiga intresse för frågor som rör tillit. Har det inte alltid varit lika viktigt… frågar sig vän av ordning? Beroende på om man är dystopiskt lagd eller bär en mer positiv syn på saker och ting kan vi betrakta detta uppflammande intresse

för tillit utifrån lite olika perspektiv. Utan att på något sätt täcka hela komplexiteten i samhälls- och begreppsutveckling kan vi som exempel ta att samhället, genom globaliseringen och digitaliseringen, blivit allt mer komplext.

Företag och organisationer kan inte längre hantera risk och komplexitet genom att lite på att de byråkratiska systemen ska erbjuda tydliga och klara handlingsalternativ – utan blir tvungna att ha tillit till individers vilja och förmåga att självständigt ta ansvar för och hantera komplicerade problem och relationer. Arbete kan med andra ord inte längre (i samma utsträckning) organiseras utifrån standardiserade regler och förordningar vilka på ett enkelt sätt berättar hur vi ska bete oss. Här krävs med andra ord något annat socialt smörjmedel (ideologi?) och i ljuset av det kanske vi ska se intresset för tillit!

Om vi rör oss mot system som i större utsträckning vilar på tillit istället för regler och övervakning finner vi dock en paradox. Chris Grey och Christina Garsten har i artikeln Trust, Control and Post-Bureaucracy formulerat denna som:

> ”… bureaucratic organizations have been extremely effective in producing trust … They have been so successful in fact, that trust virtually disappeared as an explicit issue in organization theory until fairly recently, when bureaucratic structures began to come under increasing threat (Grey & Garsten 2001, p. 244-245)

Byråkratiska system, med dess enhetliga regler för beteende skapar (enligt detta sätt att se det) bättre förutsättningar för tillit än mer moderna platta diton där ansvar och befogenheter diffunderat ut i systemet. Det är kanske dystopisk insikt, men ändå värd att fundera på. Här finns med andra ord en hel del relevanta frågor som söker svar. Hur ser till exempel sambanden ut mellan system och individ vad gäller att generera tillit?

Här uppkommer dock ett problem i analogin med karusellen. Den förutspår ju nämligen att vi alltid återvänder till samma punkt – om dock lite omtumlade. Förhoppningsvis kan forskarvärldens nyligen uppkomna intresse för tillitsfrågor föra utvecklingen framåt istället för bara runt och göra oss yra.

Om inte… så är omväxling förnöjande och det är ju alltid kul att åka karusell.

/Calle Rosengen

Om risk, tillit och vansinne i relation till Internet – En teori om kognitiv dissonans

digitalsociety.se, 8 november, 2013

Människan har, om inte annat så inför sig själv, ett behov av att framstå som rationell. Att framstå som rationell innebär att hur vi upplever och tolkar världen, våra åsikter och attityder kring densamma samt vårt beteende står i samklang. När det finns en diskrepans mellan hur vi upplever och tolkar värden, våra attityder och vårt beteende, så uppstår det en form av spänning inom oss. En spänning som få av oss vill ha i våra liv. T ex om vi upplever det som livsfarligt att röka och vi ända röker så upplever vi det som Leon Festinger kallade – kognitiv dissonans. Hur kan vi då ta oss ur denna upplevda dissonans, som skapar spänningar inom oss? Beteenden är ju alltid svåra att ändra. Det ställer ju onekligen vissa krav. Det är jobbigt. Vi (eller vissa av oss i alla fall) tycker om att röka. Vi vill fortsätta röka. Då kan vi istället söka ändra vårt sätt att se på risken. Vi kan då säga (tyst i huvudet till oss själva) ”Ahh… jag känner ju någon som är gammal och tillsynes frisk men ändå röker.” Vi söker, och finner oftast, bevis på exempel som gör att vi kan vidmakthålla vårt beteende… och ändå uppleva det som rationellt. Spänningen är reducerad och vi kan fortsätta att bete oss i lugn och ro.
Igår presenterade Svt en enkätundersökning om hur svenskarna upplever risker med bland annat att vara övervakade på Internet. Förvånansvärt nog var det väldigt få som upplevde någon rädsla för övervakning i sammanhanget. Till exempel var det endast 13 % som svarade jakande på påståendet ”Ja, rädd att bli övervakad på internet”. Resultat som ligger väl i linje med andra studier på området. I den senaste upplagan av *Svenskarna och Internet* står att läsa att:

> För tolv år sedan uttryckte många (57%) en oro för de ökade möjligheter till övervakning och kontroll som internet kan erbjuda (Svenskarna och Internet 2000). Det är en oro som har minskat väsentligt idag. Endast 11 procent av internetanvändarna uttrycker en oro för att regeringen skall kolla vad de gör på internet och endast 14 procent är oroade att företag skall göra samma sak.

Trots flera stora avslöjande under senare tid om tämligen långt gående övervak-

ning och kontroll av individer på Internet, från såväl statligt håll som från stora företag verkar vår tillit till detta medium vara orubbad. Hur kan vi tolka och förstå detta? Hur skulle det se ut om vi använde Festingers begreppsliga ram på fallet – upplevelse av risk och tillit i relation till Internet.

Låt oss försöka.

De allra flesta medborgarna i Sverige använder Internet på något sätt idag. Det är väldigt svårt att interagera i samhället, såväl som privatperson som i arbetslivet, utan detta medium. Möjligheten att ändra beteendet – att använda Internet – är följaktligen låg. Vad göra då? Vi har ett beteende som är svårt, nästan omöjligt, att ändra… även om vi skulle vilja det! Skulle vi samtidigt gå runt med en upplevelse av stor risk kopplat till beteendet blir vi, enligt teorin om kognitiv dissonans vansinniga. Tokiga. Vi skulle hela tiden tvingas stå inför oss själva som varandes ytterst irrationella. Vi skulle till slut gå under.

Så vad göra?

Det finns ju inte direkt något annat Internet att välja. Internet B… eller vad man skulle kalla det. Som man enkelt kan byta till. Säga typ: ”Det här verkar ju vara helt vansinnigt! Det är ju övervakat på alla håll. Nej, det här väljer jag allt bort!” Så är det ju inte. Utan vi får ju snällt fortsätta att använda det Internet som finns. Istället kanske vi (högst omedvetet) ändrar vår upplevelse av risken av att använda Internet. Så skulle vi i alla fall kunna förstå resultaten i Svt:s undersökning utifrån teorin om kognitiv dissonans. Det vill säga. Varför upplever så många svenskar, trots alla avslöjanden, Internet som riskfritt? Jo, vi rationaliserar vårt beteende. Alternativen, fullständig isolation eller vansinne, känns ju inte särskilt lockande.

Alternativet?

//Calle

Tillbaka till framtiden, chefen ser dig!

Cybernormer.se. November 8, 2013

http://cybernormer.se/tillbaka-till-framtiden/

> "Spector Pro spelar in alla detaljer och vad de gör på datorn – deras chatt, skickade & mottagen e-post, webbsidor de besöker, vad de söker efter, vad de gör på MySpace eller Facebook, bilderna de skickar eller tittar på, tangenter de trycker, programmen de använder och mycker [sic!] mer. Tack vare SpectorPro's funktioner för övervakningsbilder, ser du inte bara VAD de gör, utan även den EXAKTA ordningen det sker i, steg för steg. Med Spector Pro, kommer du aldrig mer undra vad de gör på datorn" (utdrag från spector.se).

Det är stundtals lätt att förledas till att tro att utvecklingen inom arbetslivet rör sig från en situation där arbetsgivaren, i den stinkande och rykande fabriken, övervakade och kontrollerade den alienerade arbetarens minsta rörelser – till en kunskapsekonomi där medarbetarens behov av utveckling och självförverkligande går hand i hand med organisationers mål (vilket i sig skulle medföra att behovet av övervakning försvinner, detta då medarbetaren i högre utsträckning antas drivas av inre motivation). Möjligtvis ligger det någonting i detta. Men på samma sätt som fabriken möjliggjorde en form av övervakning och kontroll har den digitala teknikutvecklingen medfört andra. Ett exempel på denna teknik är det som på engelska benämns "employee monitoring software". Denna mjukvara, installerad på den anställdes dator, möjliggör kartläggning av bland annat följande (enligt en webbaserad review över tillgänglig mjukvara på området):

Websites visited

- Social Media Sites
- System Activities
- Search Terms
- Chat Conversations
- Keystrokes
- Microphone Conversations

I samma review står även att läsa (vilket antyder att den som gjort denna ”kartläggning” även är intresserad av att sälja utrustning) om produkten *Spector CNE Investigator* från företaget Spector soft:

> Are your employees watching YouTube videos instead of working, or sharing your client's contact information with people outside the company, or harassing another coworker using your chat protocol? Maybe you don't even know? Spector CNE Investigator captures and records everything your employees do, including what websites they visit, what documents they alter or share, full chat conversations and all keystrokes. It also records all network activity, including domain name where connections were made, ports used, number of bytes sent or received, and duration of the event. Spector CNE Investigator's Email Recorder component creates a clear record of all sent and received email exchanges, including attachments. The software records both SMTP/POP3 and Outlook type emails. It also monitors all common chat protocols, including Facebook, Skype, Google, AIM and Windows Live Manager, as well as in-house chat protocols. Once you know what your employees are doing, you can create a plan to mitigate issues.

En intressant ”feature” är att ovan nämnda mjukvara tar en screenshot på den anställdes skärm var trettionde sekund. Bilder som sedan kan sättas ihop till en film som arbetsgivaren sedan kan avnjuta:

> Spector CNE Investigator can capture everything from screenshots to ports accessed to help you know exactly what is happening on your company-owned computers. Accurate and complete records can help you with legal and policy problems should an issue arise. This employee tracking software by default collects screenshots every 30 seconds and you can play them back like a DVR player. You can also configure the software to collect data at different intervals if you desire. Screenshots can be exported individually as image files or even as an AVI video file.

Enligt Spector soft finns här pengar att tjäna. Framförallt genom att reducera ett beteende som vi skrivit om tidigare här, nämligen cyberslacking/cyberloafing. På deras svenska hemsida (spector.se) står att läsa:

> Almost every company in the world has employees who abuse the

> Internet, some of whom spend hours per day surfing news, shopping, sports, gambling and sex sites. (…) This abuse by employees is costing their companies huge amounts of money in lost productivity alone. For example, a company with just ten employees who each waste an hour a day on the Internet is **losing $50,000 per year** in lost productivity.

Att branschen växer i USA kan vi läsa om i Forbes magazine – Keep Employees Away From Cat Videos With Time Tracking Software. Här framhålls att företag även från andra länder gett sig in i kampen om marknadsandelar. En annan utveckling som pekas ut är att branschens retorik håller på att anpassa till rådande sociala normer, vilket innebär att denna typ av övervakningsutrustning snarare beskrivs i termer av produktivitets- än övervakningsverktyg… även om innehållet är detsamma. I en artikel – Snooping E-Mail by Software Is Now a Workplace Norm – i Times Magazine står det att läsa:

> With companies so clearly concerned about what employees are saying in e-mail, the market for scanning software is taking off. Forrester Research says the industry is growing at a rate of about 30% a year, **hitting $250 million to $300 million today**. Part of the growth is driven by companies' desire to weed out inappropriate content, says Mr. Penn. But increasingly, companies also are using software to make sure e-mails are compliant with corporate governance and regulatory demands, such as Sarbanes-Oxley.

I vilken utsträckning denna teknik i praktiken används av svenska företag är i dagsläget högst oklart. Enligt en rapport från Datainspektionen, som delvis bygger på inspektion av 40 slumpmässigt utvalda företag, förekommer det dock i viss utsträckning.

> I ett par fall förekom det att arbetsgivaren kontrollerade av arbetstagarens e- post- och internetanvändning utan att det vare sig fanns dokumenterade regler för användningen av IT-utrustningen, eller för i vilka fall som kontroller kunde komma att utföras.

Och ibland även utan att anställdas samtycke inhämtats. I detta sammanhang ges följande rekommendationer:

- Av PuL kan sägas följa att behandling av personuppgifter i syfte att utföra kontroller inte får genomföras på ett sätt som innebär en mycket närgången och

omfattande övervakning av arbetstagaren.

- Om behandlingen av personuppgifter för kontrolländamål bygger på samtycke ska det framgå att den är frivillig. Om behandlingen bygger på en intresseavvägning ska det framgå om arbetstagaren har rätt att motsätta sig kontrollen.

Helt klart är däremot att ABB nyligen hamnade i blåsväder för att de anställda fick installera en särskild app som möjliggör kartläggning av användning.

> ABB kan övervaka anställda via mobilen
>
> ABB om Famoc-appen – används inte för övervakning

Tekniken reser självklart ett flertal frågor om å ena sidan integritet för den anställde och å andra sidan företagens behov av övervakning och kontroll. Här finns även frågor kring hur facket ska förhålla sig till tekniken. Legala frågor kring hur den får användas samt hur information insamlad med tekniken kan användas i enskilda personalärenden som t ex grund för uppsägning. Vi (i projektet) föreställer oss dock att det finns tämligen starka normer mot denna typ av övervakning och kontroll. Följaktligen kan vi anta att, i den mån tekniken tar sig hit, kommer att lanseras som instrument för produktivitet och rationalisering – lite på samma sätt som tidsstudiemännens arbete i fabriken beskrevs på 1940-talet. På samma sätt som tidsstudiemannen sades bidra till nytta för både arbetsgivare och arbetstagare framhålls även dess elektroniske motsvarighet vara till gagn för alla – everybody wins(!):

> Spector can help you protect your computers from damage, sensitive proprietary information from compromise, and employees from harassment with the added benefit of improving production – everyone wins.

Forskning på området (Alder et al., 2006) visar dock att övervakning av anställdas internetanvändning kan påverka tilliten till arbetsgivaren negativt, vilket i sin tur även får konsekvenser för arbetstillfredsställelse, engagemang och vilja att stanna i företaget. Framförallt när det sker utan att samtycke inhämtats eller att syfte klargjorts.

Läs mer:

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006). Clarifying the effects of internet

monitoring on job attitudes: The mediating role of employee trust.*Information & Management*, *43*(7), 894-903.

Behandling av personuppgifter för kontroll av anställda. [Elektronisk resurs]. (2003). Stockholm: Datainspektionen. http://www.datainspektionen.se/Documents/rapport-personuppgifter-anstallda.pdf [2014-05-19]

Övervakning i arbetslivet [Elektronisk resurs] : kontroll av de anställdas internet- och e-postanvändning m.m.. (2005). Stockholm: Datainspektionen. http://www.datainspektionen.se/Documents/rapport-overvakning-arbetslivet.pdf [2014-05-19]

Vem i hela världen kan man lita på?

digitalsociety.se, publicerad den13 maj, 2014

Dagens inlägg behandlar frågan om utvecklingen i arbetslivet mot mer förtroendebaserade arbetstidsavtal och inleds med två centrala frågor i sammanhanget:

- Kan man verkligen lita på att de anställda – om de får mer frihet att självständigt styra över sina arbetstider – använder denna frihet till att tillgodose såväl företagets som sina egna intressen?
- Kan man verkligen lita på att företag inte använder den lägre graden av reglering av arbetstiden till att smyga in fler arbetsuppgifter och spela ut anställda mot varandra?

Vilket svar man ger på ovanstående frågor är kulturellt betingat – dvs. beroende av exempelvis institutionella faktorer och människosyn. I grunden är frågan om det är rimligt att tänka sig att arbetstiderna i större utsträckning kan styras och regleras på basis av tillit?

Nu kommer en studie från Köpenhamns universitet som behandlar förtroendebaserade arbetstidskontrakt: *Between trust and control: company-level bargaining on flexible working hours in the Danish and German metal industries*. Det är sociologen Anna Ilsøe som har genomfört en komparativ studie av Danmarks och Tysklands arbetskulturer. Utifrån respektive lands förutsättningar har fem fallstudieföretag från respektive land studerats, och resultaten ger vissa förhoppningar. Det visar sig nämligen att Danmark, som i mångt och mycket påminner om Sverige vad gäller gäller exempelvis förhållandet mellan arbetsmarknadens parter är

en god jordmån för förtroende.

> "…the Danish employers make the strategic choice of trusting their employees' working time management in contrast to the German employers, who choose to control most of the employees' working time because they find that more profitable."

En av de intervjuade tyska arbetsgivarna uttrycker denna misstro mot den anställdes vilja och förmåga att ta hänsyn till företagets intressen som:

> "every worker prioritises his own interests over the interests of the company. It is difficult to change, because in situations where the interests of the company dominate the scheduling of working hours, the workers are bothered, and this affects their future attitude towards the company. Not all workers react like this, but naturally a lot of them do [Manager, D3]."

Omvänt om de danska cheferna skriver Ilsøe att:

> "In the Danish companies the managers would tend to reason differently. They often trusted the employees to adjust their working time both to the needs of the company and to the needs of their private lives, and they were happy with the results"

Hur kan vi förstå och förklara dess skillnader då? En förklaring är att parterna på den danska arbetsmarknaden är tämligen jämnstarka:

> "high levels of trust between employers and employees can be generated if their relations are embedded in institutions that provide employees with high bargaining power (high union densities, coverage of collective agreements and presence of workers' representatives). High bargaining power for both bargaining parties enhances the trust that formal and informal agreements will be implemented in practice. The difference in employee relations could thus be explained by the fact that employees have less bargaining power in the German context …"

En annan förklaring som anges är att commitment (på svenska engagemang eller kanske snarare hängivenhet) är högre bland de danska arbetarna inför sina arbeten. Detta skulle i förlängningen innebära att arbetarna skulle bli mer självgående:

> ”…because of the high degree of commitment in the Danish cases, management allows employees to manage their own working time and thereby facilitates a close adjustment to both employee-specific and company-specific needs. This seems to enhance the scope of win–win outcomes from introducing flexible working hours, as Danish employers and employees experience additional effects with respect to their work–life balance and job satisfaction compared with their German colleagues.”

Forskning om tillit i organisationer visar att sambandet även kan vara det omvända, d v s att en hög grad av tillit till medarbetarnas vilja och förmåga att ta eget ansvar i sin tur fostrar engagemang för arbetsuppgifterna (se t ex Adler et al 2006). Man skulle därmed kunna tolka Ilsøes studie som att det det i Danmark utvecklats en ”tillitskultur”.

Avslutningsvis anges mer individbaserade förutsättningar för att hantera den ökade graden av frihet. Denna kompetens benämns i Ilsøes studie som Self-leadership alt. Self-management.

> ”The employees’ self-management, on the one hand, paved the way for further efficiency and cutback on administration because it allowed an adjustment of working hours to the exact time needed in production (less stop and go’s, reduction of unproductive working time) and a reduction of the number of lower-level managers. On the other hand, employees were able to combine their working hours and time off in lieu/holidays more adequately to adjust to the needs of modern family life. This self-management meant that the flexible working hours not only enhanced job security but also the work–life balance for employees and thereby their job satisfaction.”

Avslutningsvis kan vi säga att utvecklingen inom arbetslivet mot mer flexiblare och förtroendebaserad sociala kontrakt innebär såväl hot som möjligheter. Kontentan av ovan är att utvecklingen måste hanteras och diskuteras på olika nivåer. Arbetsmarknad, organisation och individ. Givet att detta görs ser faktiskt framtiden ganska ljus ut.

//Calle & Mikael

Läs mer:

Alder, G. S.; Noel, T. W. & Ambrose, M. L. (2006). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *Information & management*, *43*(7), 894-903.

Ilsøe, A. (2010). Between trust and control: company-level bargaining on flexible working hours in the Danish and German metal industries. *Industrial Relations Journal*, *41*(1), 34-51.

Rosengren, C. & Ottosson, M. (2014). *Ska du gå hem redan?* (blogg) skadugahemredan.se [2014-05-19]

Del III

Ett rättsligt perspektiv på övervakningstrenden: Datalagringsdirektivets underkännande

Jonas Ledendal och Stefan Larsson

Som ett av tre perspektiv i DigiTrust-projektet har vi riktat in oss mot rättens roll i relation till tillit och det digitala. Även denna fråga är bred och bjuder på en del avgränsande val som behöver göras, men samtidigt ser man snabbt poängen med att förhålla rätten till tillitsfrågor om man begrundar den mängd forskning som visar på hur legitimitet är av fundamental betydelse för att juridik och rätt ska kunna fungera som exempelvis styrmedel. Om de människor, stater eller företag som är tänkta att regleras inte på något vis "håller med om" eller känner tilltro till en lagstiftningsåtgärd så kommer den med största sannolikhet inte uppnå den effekt som var tilltänkt med den specifika lagstiftningen – med mindre att kombinationen av sanktioner, kontroll och andra efterlevnadsåtgärder är total. Och sådan total kontroll är vi i västvärlden i allmänhet inte vana vid. Man kunde rentav tänka sig att en totalitär normgivningsmakt även den skulle uppfattas som illegitim, vilket skulle i vart fall ge upphov till en rad försök till att kringgå den. Det finns en rad lagstiftningsåtgärder som är av intresse ur ett digitalt tillitsperspektiv, och vi har valt att fokusera den del som handlar om åtkomst och bearbetning av trafik- och övrig metadata, speciellt i syfte att identifiera människors identitet, vanor eller geografiska rörelsemönster. Detta relaterar bland annat till övervakningsfrågorna vi undersökt och diskuterat ovan. För att nämna några av relevans:

- FRA-lagen, som rör Försvarets radioanstalts förehavanden, som är en svensk civil myndighet som sorterar under Försvarsdepartementet. Vare sig signalspaning eller FRA är nymodigheter i svensk regi, men rättsligt sett var den anpassning av regleringen till digital kommunikation som röstades igenom under tumult i riksdagen sommaren 2008 av extra intresse här (Prop. 2006/07:63, ikraft 1 januari

2009). FRA fick då befogenheter att avlyssna trafik i kablar som passerar rikets gräns och för att välja ut intressant information används sökbegrepp.

- IPRED, eller Intellectual Property Rights Enforcement Directive, dvs. det Civilrättsliga sanktionsdirektivet. Även om IPRED berör alla så kallade immaterialrättigheter och reglerar en rad olika frågor så är den kanske mest intressanta att den stärker rättighetshavarnas möjligheter att knyta IP-nummer till identitetsuppgifter via internetoperatörerna, bl. a. som ett sätt att försöka komma åt fildelare.
- Datalagringsdirektivet är oehört aktuellt eftersom direktivet dels har implementerats i samtliga medlemsstater men framförallt - intressant nog - därefter nyligen blivit underkänt av EU-domstolen. Det betyder att staterna i hög utsträckning har nationell lagstiftning som drivits fram av ett direktiv som bedömts göra intrång i både rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Direktivet handlade i stort om att ålägga internetoperatörer en massiv lagring av data kring telefonsamtal, sms, e-postmeddelanden, internetuppkopplingar och mobilpositioner i 6–24 månader, i syfte att kunna bekämpa allvarlig brottslighet. Det vill säga, att skapa en möjlighet att efter något allvarligt har inträffat söka igenom all data som sparats om alla för att kunna finna brottslingarna. Vi utvecklar i framställningen nedan framförallt en rättsvetenskaplig kommentar gällande denna något märkliga och högst ovanliga situation.

IPRED kan nämnas som ett exempel på rättslig åtgärd av specifikt tekniskt relaterad tillitsrelevans. Regleringen berör privatlivet och balansen mellan identifikation och anonymitet i det digitala. Direktivet implementerades i Sverige 2009, något halvår efter debatten kring införandet av FRA-regleringen hade stormat som värst, och samtidigt som grundarna av The Pirate Bay dömdes i tingsrätt. Av intresse för en bedömning av just IPRED är att ett antal studier har visat på det svaga stödet hos många för upphovsrätt i en digital kontext (Feldman & Nadler, 2006; Svensson & Larsson, 2012). I ljuset av detta ligger inte minst kruxet att implementeringen av IPRED betydde att en lag med relativt låg legitimitet fick förstärkta mandat vad det gäller enforcement, dvs. åtgärder för genomdrivande och efterlevnad. Detta ledde också till att en viss ökning av användningen av krypteringstjänster som minskar risken att spåras (Larsson & Svensson, 2010; Larsson et al., 2012). Detta vittnar därmed om hur tillitsfrågan är viktig för att uppnå fungerande lagstiftning och visar på hur teknik och det digitala bjuder på dels stora utmaningar för rätten ur ett samhällsförändringsperspektiv, men även ur ett mer avgränsat enforcementperspektiv. Det finns alltid en risk att illegtim lagstiftning leder till en rad bakslag i form av mobilisering

och mot lagstiftningens själva syfte. När det gäller de mer principiella frågorna som rätten har att brottas med i det digitala samhället så finns en tydlig brottningsmatch mellan å ena sidan den nytta som polisiära och militära myndigheter har av att bygga databaser för lagring av mänskligt beteende i tid och rum och å andra sidan rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Det så kallade datalagringsdirektivet, speciellt med EU-domstolens underkännande dom i beaktande, sätter med all önskvärd tydlighet fingret på just denna brottningsmatch.

EU-domstolen ogiltigförklarar datalagringsdirektivet – vad innebär det?

Nyligen, den 8 april 2014, ogiltigförklarade EU-domstolen det s.k. datalagringsdirektivet. Det har sedan dess varit oklart vad domen egentligen betyder för telekom- och internetoperatörer, för svenska myndigheter och för vanliga användare. Vi inom DigiTrust-projektet har med stort intresse följt målet (se bl.a. debattartikel i Svenska dagbladet den 19 april 2014). I det här inlägget ska vi försöka ge svar på några av frågorna kring EU-domstolens avgörande. Det ska dock redan inledningsvis sägas att det råder en viss oklarhet om vilka rättsliga och faktiska följder som avgörandet kommer att få.

Bakgrund

Målet i EU-domstolen har sitt ursprung i två nationella rättstvister. I det första målet (C-293/12) hade Digital Rights Ireland (DRI), en organisation som arbetar för att främja och medborgerliga och mänskliga rättigheter, särskilt i det digitala samhället, väckt talan mot tre irländska myndigheter, bl.a. den irländska polisen. I det andra målet (C-594/12) väckte Kärtner Landesregierung och ett större antal privatpersoner talan enligt den österrikiska federala grundlagen. I båda dessa mål ifrågasattes förenligheten mellan de nationella åtgärder som Irland respektive Österrike vidtagit för att genomföra direktiv 2006/24 (”datalagringsdirektivet”) och EU:s stadga om de grundläggande rättigheterna (”rättighetsstadgan”). De nationella domstolarna hade därför begärt ett förhandsavgörande från EU-domstolen. Ett förhandsavgörande innebär att de nationella domstolarna ber EU-domstolen tolka en EU-rättslig bestämmelse. EUdomstolen kan också avgöra om en EU-rättsakt är giltig.

Domstolens avgörande

EU-domstolen prövade i första hand om datalagringsdirektivet var förenligt med de grundläggande rättigheterna om rätt till respekt för privatlivet i artikel 7 respektive

rätten till skydd för personuppgifter i artikel 8 i EU:s rättighetsstadga. Domstolen fann att den skyldighet för leverantörer av kommunikationstjänster att lagra trafikuppgifter samt göra dem tillgängliga för myndigheter som förskrivs i datalagringsdirektivet utgjorde ett intrång i både rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Domstolen konstaterade att lagringens omfattning gjorde att det rörde sig om ett särskilt allvarligt intrång i dessa rättigheter. Domstolen uttalade även att lagring och användning som sker utan att abonnenten eller den registrerade användaren underrättas kan leda till en känsla av att ständigt vara övervakad.

Det var därför nödvändigt att pröva om detta intrång kunde rättfärdigas enligt artikel 52(1) i stadgan. För en inskränkning av de grundläggande rättigheter som föreskrivs i stadgan krävs att inskränkningen föreskrivs i lag och är förenlig med det väsentliga innehållet i dessa rättigheter. Dessutom får begränsning ske endast med beaktande av proportionalitetsprincipen. Begränsningen måste vara nödvändig och svara mot ett mål av allmänt samhällsintresse.

Först tog domstolen ställning till frågan om begränsningen var förenlig med det väsentliga innehållet i rätten till respekt för privatlivet och rätten till skydd för personuppgifter. Domstolen konstaterade att datalagringsdirektivet endast föreskriver lagring av s.k. ”metadata” (dvs. med vem någon kommunicerat, kommunikationssättet samt tidpunkten och platsen för kommunikationen osv.). Med hänsyn till att direktivet inte tillåter lagring av kommunikationens innehåll (dvs. vad som sagts eller tagits emot av en abonnent) fann domstolen att intrånget, trots att det förvisso var särskilt allvarligt, inte var oförenligt med det väsentliga innehållet i de aktuella rättigheterna.

Domstolen tog härefter ställning till frågan om lagringen och tillgängliggörandet av uppgifterna svarade mot ett mål av allmänt samhällsintresse som erkänns av unionen. Domstolen fann att åtgärder för att bekämpa allvarlig brottslighet såsom organiserad brottslighet och terrorism var sådana mål av allmänt samhällsintresse.

Slutligen tog domstolen ställning till frågan om de åtgärder som datalagringsdirektivet föreskriver var proportionerliga i stadgans mening, dvs. om åtgärderna var lämpliga och nödvändiga för att uppnå regleringens målsättning. Domstolen fann i detta avseende att EU-lagstiftarens fria skön var starkt begränsat med hänsyn till rättigheternas art och intrångets särskilt allvarliga karaktär. Detta utrymme begränsades ytterligare av den rätt till ett förstärkt skydd för personuppgifter inom sektorn för elektronisk kommunikation som föreskrivs genom direktivet 2002/58 om integritet och elektronisk kommunikation.

Domstolen fann att lagring av sådana uppgifter i brottsbekämpande syfte kunde vara en lämplig åtgärd med hänsyn till den stora betydelse som elektronisk kommunikation har. Domstolen fann emellertid att direktivet överskred gränsen för vad som

var nödvändigt för att uppnå dessa mål. Eftersom intrånget var särskilt omfattande och särskilt allvarligt så hade direktivet inte i tillräcklig utsträckning begränsats så att intrånget rent faktiskt inskränks till vad som var strikt nödvändigt för att uppnå målet med regleringen.

För det första omfattade direktivet generellt alla personer och alla former av elektronisk kommunikation och all trafikdata utan att det gjordes någon urskiljning, begränsning eller undantag i ljuset av att målet var att bekämpa allvarlig brottslighet. För det andra saknades ett objektivt kriterium som tillförsäkrade att de behöriga nationella myndigheterna endast kunde få tillgång till uppgifterna för ändamål som kunde anses rättfärdigade i ljuset av intrångets stora omfattning och allvarlighet. Begreppet ”allvarlig brottslighet” som avgränsar direktivets tillämpningsområde saknade en enhetlig innebörd. För det tredje saknades ett objektivt kriterium för att begränsa den långa lagringstiden (minimum sex och maximalt tolv månader) till vad som var strikt nödvändigt för att uppnå målet. Dessutom konstaterade domstolen att direktivet saknade bestämmelser som tillförsäkrar att uppgifterna inte riskerar att missbrukas eller olovligen görs tillgängliga. Med hänsyn till detta fann domstolen att direktivet stred mot rättighetsstadgan och därmed var ogiltigt.

Diskussion

Justitiedepartementet har varit otydligt med vilken betydelse domen har för svensk nationell rätt. Justitiedepartementet tillsatte också den 29 april 2014 en utredning med anledning av EU-domstolens ogiltigförklarande av datalagringsdirektivet (Ju2014/3010/P). Utredningen ska dels analysera den svenska regleringen och dess förhållande till unionsrätten och internationell rätt, dels föreslå eventuella lämpliga åtgärder för att stärka skyddet för den personliga integriteten och för att leva upp till unionsrättens krav. Utredningen ska även beakta brottsbekämpande myndigheters behov av tillgång till trafikuppgifter. Sten Heckscher, före detta ordförande i Högsta förvaltningsdomstolen, har utsetts till utredare och han biträds av professorn i folkrätt Iain Cameron. Utredaren ska enligt regeringens direktiv samråda med Åklagarmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket och Post- och telestyrelsen. Det finns förutom dessa brottsbekämpande myndigheter och tillsynsmyndigheter inga direktiv om att utredningen ska samråda med andra intressenter såsom företrädare för näringslivet eller människorättsorganisationer. Förvisso kommer eventuella lagstiftningsförslag i vanlig ordning att bli föremål för remiss och inget hindrar att utredningen på eget initiativ tar kontakt med sådana andra intressenter. Utredningens direktiv ger dock intryck av att regeringen betraktar det som en rent juridisk fråga där andra aspekter såsom tilliten i det digitala samhället inte

behöver beaktas. Utredningens första del, analysen av gällande rätt, ska dessutom vara färdig redan den 12 juni 2014, vilket inte ger mycket utrymme för sådant samråd. Utredningen ska vara färdig och eventuella lagförslag slutligt presenteras den 1 oktober 2014.

Internet- och teleoperatörer, bl.a. Bahnhof och Tele2, har efter domen upphört med att lagra trafikuppgifter. Dessa har fått kritik, bl.a. av Polisen, för att de härigenom bryter mot svensk lag. Polisen har förklarat att de avser att fortsätta begära ut uppgifter med stöd i svensk lag. Post och telestyrelsen (PTS) som ansvarar för det aktuella området har emellertid uttalat att domen innebär att ingen kan lagföras för att bryta mot de svenska nationella reglerna om datalagring och att de inte avser att ingripa mot operatörer som i strid med dessa regler upphört med lagring av trafikuppgifter. Det råder således stor oenighet beträffande rättsläget.

Första frågan gäller om Sverige kan behålla sin nationella lagstiftning trots att det EU-direktiv som denna bygger på ogiltigförklarats. Ett direktiv är inte direkt tillämpligt i ett medlemsland. Det måste genomföras i nationell lagstiftning. I Sverige har de aktuella bestämmelserna implementerats genom lag (2003:389) om elektronisk kommunikation (LEK). EU-domstolen har ogiltigförklarat direktivet, men varken kan eller har upphävt de nationella bestämmelser som implementerar direktivet. Svensk lag gäller intill riksdagen upphävt den. Såtillvida är justitieministerns uttalande riktigt i formell mening. Om ett direktiv inte antagits har medlemsstaterna normalt frihet att själva utforma sin reglering. Syftet med ett direktiv är normalt att åstadkomma en tillnärmning av regleringen så att denna ser likadan ut i alla medlemsstater. Den normala effekten av att ett direktiv upphävs är alltså i första hand att medlemsstaterna åter får bestämma själva. Det finns därför normalt ingen skyldighet att upphäva eller ändra nationell lagstiftning som bygger på det ogiltigförklarade direktivet.

Det är dock mer komplicerat i fråga om datalagringsdirektivet. För det första strider direktivet mot EU:s rättighetsstadga som utgör s.k. primärrätt. Primärrätten, i motsats till datalagringsdirektivet, är direkt tillämplig i medlemsstaterna. Primärrätten behöver inte genomföras och ska följas av nationella domstolar och andra myndigheter. EU-rätten har företräde framför nationell rätt. Eftersom den svenska regleringen i princip följer direktivet måste denna i allt väsentligt också strida mot rättighetsstadgan. Om en svensk myndighet vidtar åtgärder i strid med stadgan kan Sverige göra sig skyldigt till fördragsbrott. Det spelar i detta sammanhang egentligen ingen roll om datalagringsdirektivet antagits eller inte. Svenska myndigheter ska tillämpa den svenska lagen i enlighet med stadgan och det kan vara fördragsbrott att inte ändra lagen så att den uppfyller de krav som följer av domen.

För att förstå datalagringsdirektivet är det också nödvändigt att förstå dess förhållande till två andra EU-rättsakter. Rätten till skydd för personuppgifter, som är en grundläggande rättighet enligt stadgan, regleras av direktiv 95/46 (dataskyddsdirektivet) som ska säkerställa fysiska personers rätt till privatliv i samband med behandling av personuppgifter. Denna skyddsordning kompletteras av direktiv 2002/58 (direktiv om integritet och elektronisk kommunikation), som föreskriver ett förstärkt skydd för personuppgifter inom sektorn för elektronisk kommunikation. Direktivet föreskriver bl.a. en skyldighet för leverantörer av kommunikationstjänster att utplåna eller avidentifiera trafikuppgifter som behandlas och lagras vilka rör abonnenter och användare. Datalagringsdirektivet, vars syfte det är att säkerställa att vissa sådana uppgifter finns tillgängliga för kunna bekämpa allvarliga brott, utgör ett undantag från bestämmelserna i direktivet om integritet och elektronisk kommunikation. När undantagsregeln i datalagringsdirektivet blir ogiltigt träder huvudregeln i dess ställe. Det innebär att det saknas lagstöd för att lagra trafikuppgifter. Sverige måste alltså även på denna grund upphäva eller ändra de nationella bestämmelser som implementerar datalagringsdirektivet.

Det hittills sagda gäller dock medlemsstaterna och deras myndigheter. Det innebär inte nödvändigtvis att enskilda rättssubjekt såsom internet- och teleoperatörer bryter mot lagen om de fortsätter att lagra trafikuppgifter. Internet- och teleoperatörer som följer EU-rätten kan dock knappast hållas ansvariga för det med stöd av svenska nationella bestämmelser som strider mot EU:s rättighetsstadga. Det borde åtminstone i teorin vara möjligt att ändra datalagringsdirektivet så att det uppfyller stadgans krav. EU-kommissionären Cecilia Malmström lät dock antyda att det inte finns några sådana planer. En annan fråga som det är för tidigt att besvara är vilka konsekvenser domen får för möjligheterna att fortsätta bedriva s.k. massövervakning. Det finns uttalanden i domen som kan tolkas som att sådan i sig aldrig kan vara förenlig med stadgan. Den frågan prövades dock inte av domstolen. Det återstår att se.

Referenser

Domstolens (stora avdelningen) dom av den 8 april 2014 i förenade målen C-293/12 och C-594/12, Digital Rights Ireland mot Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung (C-594/12) m.fl., (ännu inte publicerad i rättsfallssamlingen).

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, 31.

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om be-

handling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, 37.

Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter, EGT L 195, 2.6.2004, 16.

Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, EUT L 105, 13.4.2006, 54.

Feldman, Y. & Nadler, J. (2006). The Law and Norms of File Sharing. *The San Diego Law Review,* 43, 577–618.

Larsson, S. & Svensson, M. (2010). Compliance or obscurity? online anonymity as a consequence of fighting unauthorised file-sharing, *Policy & Internet* 2(4), 77-105.

Larsson, S., Svensson, M., de Kaminski, M., Rönkkö, K., & Alkan Olsson, J. (2012). Law, norms, piracy and online anonymity: practices of de-identification in the global file sharing community. *Journal of Research in Interactive Marketing,* 6(4), 260-280.

Svensson, M. & Larsson, S. (2012). Intellectual property law compliance in Europe: illegal file sharing and the role of social norms, *New Media & Society*, 14(7), 1147-1163.

Privacy, Surveillance and Digital Trust in the American Case

Debora Halbert

While generally kept out of sight, government surveillance ostensibly to ensure the security of the state from threats (both foreign and domestic) is a hallmark of the American national security state. What types of surveillance are legally allowable is constantly contested as new technologies emerge that must be tested against American constitutional principles and international law. In the wake of the Snowden revelations about the depth and scope of government spying, new concerns regarding protection of personal data have emerged and eroded trust in American government as well as private entities that have collaborated either willingly or unwillingly with the government.

In addition to the broader national security interests, other trends dominate the evolution of surveillance, privacy and trust in the United States. Among the many emerging surveillance techniques are first, predictive policing based upon metadata and surveillance systems. Using the same algorithm to predict earthquake aftershocks, Police in Santa Cruz have developed a predictive policing mechanism that helps to stop crime before it can happen.[1] The FBI has publicized this big data program as one of the next generations of crime fighting.

Second, persistent surveillance systems are being developed that offer a wide area visual surveillance to track crime in real time and offer additional information for criminal investigations. Third, while drones are primarily understood as playing a role in our national security outside the domestic territory of the United States, they have also begun to play a role in total surveillance within the United States as well. Fourth, facial recognition software can now function better than humans, suggesting new ways of capturing data in public places and documenting the movements of

[1] http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/April/predictive-policing-using-technology-to-reduce-crime

individuals (Lu & Tang, 2014). Finally, the Internet of everyday things, converging with RFID technologies that can track everything from books and clothing to passports to people brings additional layers of surveillance to play.

These technologies are built upon the assumption that crimes both cyber and real must be met with adequate scrutiny and that threats can be halted through surveillance. Furthermore, the lucrative future of the business of security continues to innovate surveillance technologies that make the Orwellian world of total surveillance closer than ever (Deibert, 2013). These technologies are sold off the shelf to democracies and dictatorships alike (Soghoian, 2013). Surveillance for profit is big business.

Privacy by Policy

In the face of persistent and extensive data surveillance, what protections exist for personal privacy?

In the United States, the predominant method for protecting privacy is for a company to issue a written privacy policy statement. Privacy by policy means that we must trust those who control data collected from us because there is a policy that says they will manage our personal information with trust. In other words, privacy by policy is premised upon a basic trust in those collecting and managing data. In the United States, for example, ISPs retain data for times ranging from six months to a year and the ways this data might be used are not clear. Data retention is of interest to the US federal government as well that wishes to have better access to this data for its own criminal and surveillance purposes. However, despite concerns about both legal and illegal uses of personal information a privacy policy is assumed to be sufficient assurance that nothing inappropriate can happen with this data.

While privacy policies may keep companies from sharing personal data unless they specifically state their intentions to do so, it cannot be assumed that data remains with the company collecting it (Cranor et al., 2014). Additionally, even without sharing, individual companies have amassed astounding amounts of personal data about their users. While surveys suggest that Americans do not want to be tracked online, even with privacy policies, most websites engage in some sort of tracking (Martin, 2013). It takes serious effort to get and/or stay off the grid (Goldstein, 2014). So much time in fact, that as Jessica Goldstein has noted, it is not worth the effort (Goldstein. 2014). Studies have shown that most users are interested in how a company uses their data but that they do not read the privacy policies in part because they are written in legal language that is too complex (Anton et al., 2010, p.24).

Is privacy by policy sufficient? We would argue that it is necessary but not sufficient. Snowden's revelations prove that policy-based privacy is not sufficient as well. In the name of national security the US federal government has ensured that any paper commitment to privacy is merely that – paper with no real force. There are backdoors, secret wiretaps, secret courts, and an entire network of surveillance for the sake of national security that occurs despite laws on the books to protect citizens against such activities. The NSA programs created and enforced in secret require big business to be complicit with government acquisition of data and the American people to be in the dark about what is collected and about whom. Verizon's privacy policy is no protection against the national security state.

Privacy by design

If privacy is to be ensured for those who do not have the technological capacity or legal comprehension to affirmatively protect their privacy, it must be done by design. Privacy by design will embed privacy at the technological level (Kleiner, 2014, pp.91–92). As privacy expert Ann Cavoukian notes, privacy by design is "the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality. Privacy must be embedded in systems, naturalized as part of the process and easy to use (Cavoukian, 2011, p.10)." Encryption is central to privacy by design. The starting assumption should be a high level of privacy with people opting out of privacy protections as they choose.

Examples of security by design include Tor, designed to protect user privacy from network surveillance and traffic analysis.[2] Other programs such as the VPN Do-Not-Track, which allows the user to opt-out of tracking websites are readily available for a monthly fee.[3] New devices taking privacy into consideration are also being innovated. The creators of PGP privacy are about to release a new encrypted telephone, the Blackphone, that is designed with security and privacy in mind (Clinch, 2014; Robarts, 2014).

Conclusion

Some might argue that without adequate security measures we face the potential failure of digital economic systems. Persistent attacks and criminal efforts to acquire personal data, data theft, and the like are becoming far more sophisticated and undermine the potential for digital commerce. While the argument is that we must

[2] https://www.torproject.org/

[3] http://donottrack.us/

give government and industry the ability to fight by keeping individual privacy settings low, others argue that the lack of privacy and the existence of US created built back doors into key security software has made the world less safe. As Snowden suggests, "if we loose the trust of SSL which was specifically targeted [by the NSA] we will live in a less safe world. We won't be able to access banks or do commerce without worrying if someone is monitoring us (Snowden, 2014)."

Based upon the fact we must place trust in e-commerce and personal communication to make the modern economy function, debates over the depth and scope of privacy are important. Both government and private actors claim that privacy by policy is sufficient to protect the individual and that technological backdoors for spying, methods of collecting data, and constant surveillance of all Internet activities about the individual is simply not a problem, as long as the policy statement discloses how things are working. This report seeks to argue otherwise. It is time to flip the default privacy settings from one where our information is shared in exchange for services and ease of communication to one where each individual affirms consciously the choice to share their private information with private industry or the state. In other words, our policy discussion must be one that implements privacy by design.

References

Anton, A.I.; Earp, J.B. & Young, J.D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security Privacy*, 8(1), 21–27.

Cavoukian, A. (2011). *Privacy by design in law, policy and practice: a white paper for regulators, decision-makers and policy-makers*. Ontario: Information and Privacy Commissioner. http://www.privacybydesign.ca [2014-05-19]

Clinch, M. (2014). Taking on BlackBerry: the mobile that promises privacy. *CNBC.com*. http://www.cnbc.com/id/101337734 [2014-05-13].

Cranor, L.F. et al. (2014). *Are they worth reading? an in-depth analysis of online advertising companies' privacy policies*. Rochester, NY: Social Science Research Network. Available at: http://papers.ssrn.com/abstract=2418590 [Accessed May 7, 2014].

Deibert, R.J. (2013). *Black code: inside the battle for Ccyberspace*. Plattsburgh, NY: Signal.

Goldstein, J. (2014). Meet the woman who did everything in her power to hide her pregnancy from big data. *Think Progress*. http://thinkprogress.org/culture/2014/04/29/3432050/can-you-hide-from-big-data/ [2014-05-04].

Kleiner, T. (2014). The future of privacy in the internet age: a European perspective. In Dartiguepeyrou, C. (ed). *Cahier de Prospective: the Futures of privacy*. France: Foundation Telecom, Institut Mines-Telecom, 83–92.

Lu, C. & Tang, X. (2014). Surpassing human-level face verification performance on LFW with GaussianFace. *arXiv:1404.3840 [cs, stat]*. http://arxiv.org/abs/1404.3840 [2014-04-24].

Martin, K. (2013). Transaction costs, privacy, and trust: the laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*, 18(12). http://pear.accc.uic.edu/ojs/index.php/fm/article/view/4838 [2014-05-06].

Robarts, S. (2014). Updated specs released for the Blackphone secure smartphone. *Gizmag*. http://www.gizmag.com/updated-sgp-technologies-blackphone-specs/31852/ [2014-05-13].

Snowden, Edward. (2014). *Here's how we take back the Internet*, TedTalks. Available at: http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet [2014-04-24].

Soghoian, Christopher, (2013). *Government surveillance — this is just the beginning*. Ted Talks. http://www.ted.com/talks/christopher_soghoian_government_surveillance_this_is_just_the_beginning [2014-04-14].

Tillit till forskningen och digitaliseringen av det vetenskapliga kommunikationssystemet: Peer review-processer och Open Access-publicering

Jutta Haider och Fredrik Åström

I en undersökning baserad på 1 000 telefonintervjuer rapporterade Vetenskap & Allmänhet i december 2013 att svenskarnas förtroende för vetenskaplig forskning är rekordhögt (Vetenskap & Allmänhet, 2013); och även i en rapport från University of Tennessee och Ciber Research konstateras att tilliten till den vetenskapliga forskningen och dess metoder är fortsatt hög samt att den vetenskapliga tidskriften fortfarande ses som det mest trovärdiga sättet att rapportera resultat av vetenskaplig forskning (University of Tennessee & Ciber Research, 2013). Men hur etableras vår tilltro till den akademiska forskningen som kunskapsskapande organisation: vad är det för mekanismer i forskningen – och inte minst i rapporteringen av forskningsresultaten – som vi lutar oss emot för att granska att forskarna är att lita på? Vilka är effekterna av att det vetenskapliga kommunikationssystemet digitaliseras? Och vad händer när institutioner och processer som ska stå för spridande och granskning av kunskapen och de som skapar den ifrågasätts?

Kunskap och tillit är sammanvävda (Hardwig, 1991). Det mesta i världen är sådant som vi inte kan uppleva och veta själva, utan ofta behöver vi förlita oss på andras bedömningar av vad som finns och sker i världen. Kunskap är alltså någonting som ägs gemensamt; och för att kunna lita på kunskap måste vi lita på andra människor (Shapin, 1994, s.xxv) och i allt högre utsträckning också på olika

tekniska system. För att skapa tillit till vår gemensamma kunskap och det vi tillsammans vet har man utvecklat en rad olika mekanismer och processer. Vetenskapen i sig kan ses som ett sådant komplex av mekanismer och processer (Porter Liebeskind & Lumerman Oliver 1998), och vidare har det inom vetenskapen också utvecklats mekanismer, institutioner och granskningsprocesser, där inte minst peer review-systemet har en viktig roll i att signalera att de publikationer där forskning presenteras är något vi ska kunna känna tillit till. Peer review-systemet är ju en process där forskarnas rapportering av sina resultat i vetenskapliga artiklar – men också t.ex. ansökningar om forskningsmedel och utvärderingar av forskningsmiljöer – granskas av andra forskare för att säkerställa att forskningen har utförts på ett korrekt sätt, att resultaten tillför något nytt till vårt gemensamma vetande och att den är värd att publicera. Tanken är att låta ämnesexperter bedöma forskningsinsatsen. Genom bland annat anonymisering av både artikelförfattare och granskare vill man säkerställa att bedömningen inte påverkas av särintressen och att vi därigenom får en granskningsprocess som endast ser till vetenskapens och forskningsfältets utveckling av vårt samlade vetande.

De vetenskapliga tidskrifterna har länge varit en av de viktigaste institutionerna för att förmedla resultat från forskning: traditionen av vetenskapliga tidskrifter går tillbaks till 1600-talet och Philosophical Transactions of the Royal Society och Journal des Sçavans; och även peer review-systemet har långa traditioner (Shapin, 1994), även om peer review-processen också är omdiskuterad, både ifråga om hur den ska definieras och under senare år också ifråga om hur mycket den egentligen tillför för att skapa tillit till vetenskapliga publikationer. Från att i början varit kopplad till en gentlemanna- och – i viss utsträckning även en – adlig kultur, där tilliten grundades i deltagarnas sociala status och ekonomiska oberoende (Shapin, 1994) och där texter granskades av andra med exakt samma status (och kön), har peer review-granskningen numera utvecklats till att innefatta ett antal processer för att säkerställa att personer, procedurer och system som ligger bakom granskningen rimligtvis kan anses som tillförlitliga (Cronin, 2005); och för att minska inflytandet av status, meriter och andra faktorer som ligger utanför det strikt vetenskapliga i bedömningen. Mycket kan sägas om huruvida det har lyckats, men poängen är att även om strategierna har ändrats och kretsen av deltagarna har utökats betydligt, så har systemets betydelse som garant för forskningens tillförlitlighet inte minskat. Graden av komplexitet i systemet har ökat betydligt, men samtidigt står peer review-systemet kvar som det, än så länge, optimala sättet att fastställa huruvida tillit till en viss forskningstext är berättigad.

Den utveckling av digitala verktyg och nätverk som vi har sett under de senaste decennierna har givetvis också påverkat forskarvärlden, den vetenskapliga kommunikationen och dess system för publicering. Det stora flertalet vetenskapliga tidskrifter publiceras idag online, många parallellt tillsammans med en tryckt upplaga, men det är också många som enbart publicerar sina artiklar i digital form. Vid sidan av tidskrifter och andra traditionella former av publikationer har också digitaliseringen av kommunikationssystemet gjort att det har uppstått allt fler alternativa former för forskare att kommunicera sina forskningsresultat. Samtidigt har dock också digitaliseringen, tillsammans med en allt mer tilltagande acceleration av forskningen utifrån ökande krav på prestationer, fortsatt att komplicera de relationer som underbygger hur vi bedömer tillit. Under de senaste decennierna har den vetenskapliga publiceringsprocessen sett stora förändringar på många plan. De vetenskapliga tidskrifterna har i allt högre grad kommit att utges av ett litet antal kommersiella förlag. Forskarna drivs i allt högre grad till att publicera snabbt och mycket för att möta prestationskrav kopplade till utvärderingssystem som mäter vetenskaplig prestanda genom att räkna antal publikationer och citeringar till dessa, system som i sin tur kan kopplas till det vi kallar 'granskningssamhället' och dess krav på prestationer och mätbarhet av prestanda i offentliga verksamheter. Publiceringsprocessen har i en ökande utsträckning kommit att bli ett tudelat system där artiklarna å ena sidan handlar om att kommunicera sina resultat, å andra sidan om att meritera sig genom att artiklarna och deras användning räknas för att mäta vetenskapliga prestationer, två processer som i tämligen hög utsträckning ställer olika – och motstridiga – krav på hur publiceringssystemet och dess processer utformas (Frohmann, 2004). Samtidigt har man också under de senaste två decennierna allt mer diskuterat frågan om hur och i vilken utsträckning offentligt finansierad forskning kan eller ska göras tillgänglig för allmänheten? Från att till en början varit en fråga som diskuterades av ett antal forskare som ville ta tillbaka den intellektuella äganderätten till innehållet i sina artiklar från förlagen, och från forskningsbibliotek med ökande problem att hantera de stigande priserna på tidskriftsprenumerationer, har vi idag kommit till en punkt där många forskningsfinansiärer – t.ex. amerikanska National Institutes of Health (en av världens största finansiärer av medicinsk och hälsorelaterad forskning), Research Councils of the United Kingdom (en sammanslutning av de sju offentliga forskningsfinansiärerna i Storbritannien) och svenska Vetenskapsrådet – kräver att de som forskat med finansiering från forskningsråden gör sin forskning öppet tillgänglig: att den publiceras 'Open Access' (OA).

Ursprunget till idéer om att göra forskningsresultat fritt tillgängliga, som de formats inom 'OA-rörelsen', kommer i hög grad från att forskare såg möjligheter att sprida sina forskningsresultat *online* i samband med att digitala tekniker för kommunikation utvecklades; och att därigenom göra processen att sprida resultat snabbare, att i högre grad undvika att skriva över den intellektuella ägnaderätten till förlagen och att kunna göra resultaten tillgängliga även för de som inte har råd med förlagens höga prenumerationsavgifter. Att göra forskningen tillgänglig genom OA-publicering motiveras som sagt i hög grad utifrån argument om att offentligt finansierad och kvalitetsgranskad forskning ska göras öppet tillgänglig och möjlig för alla att använda, utan att begränsas av förmågan att betala dyra prenumerationsavgifter, hos allt från nystartade småföretag till universitetsbibliotek i länder i tredje världen. Detta har i huvudsak kommit att organiseras på två olika sätt: antingen genom att de artiklar som publiceras i traditionella tidskrifter också parallellpubliceras i öppna arkiv – den så kallade 'gröna vägen till open access' – eller att artiklarna publiceras direkt i tidskrifter utan prenumerationsavgifter och med fri tillgång till innehållet, OA-tidskrifter – den så kallade 'gyllene vägen'. En vanlig affärsmodell för OA-tidskrifterna – publikationsverksamheten behöver ju fortfarande finansieras på något sätt – har varit *"article processing charges"* (APC), eller författaravgifter. Tanken är att finansieringen av publiceringsprocessen hanteras av dem som utför och vill kommunicera forskningen istället för dem som sedan tar del av resultaten. Och för att anknyta till inledningen av detta stycke: idag ser vi tecken på att initiativet ifråga om OA och vetenskaplig publicering åter hamnat hos de stora förlagen. Genom att erbjuda olika lösningar – i form av OA-tidskrifter och möjligheter för forskare att "köpa loss" individuella artiklar och göra dem fritt tillgängliga i tidskrifter som annars kräver prenumeration – kan förlagen möta de krav som forskarna har från de forskningsråd som finansierar deras verksamhet; och har på så sätt lyckats anpassa sig utan att i någon större utsträckning behöva oroa sig för sjunkande vinstmarginaler.

Frågan om fritt tillgänglig forskningslitteratur, om OA-tidskrifter och APC-avgifter är inte okontroversiell. Till exempel har de traditionella tidskriftsförlagen sett det fria tillgängliggörandet som ett hot mot deras vinstmarginaler och det har också funnits diskussioner kring hur pålitliga de nya OA-tidskrifterna är och i vilken utsträckning processer kring kvalitetsgranskningen av de artiklar som kommer till tidskrifterna är av tillräckligt god kvalitet. Och det har också i ökad utsträckning dykt upp förlag med en i hög grad tvivelaktig verksamhet, med spam-liknande marknadsföring, med bristande eller felaktig information om var förlaget befinner sig, bristande uppgifter om redaktörsansvar för dess tidskrifter och med löften om orim-

ligt kort behandling av insända artiklar (t.ex. peer review-granskning inom ett fåtal veckor). Vid sidan av möjligheten att göra sig en snabb vinst grundad i en ökande press på forskare att publicera sig mycket, tillsammans med krav på OA-publicering, är en starkt bidragande orsak till att marknaden för dessa förlag uppstått att dagens IT gör det både enkelt och billigt att skapa en websida där man snabbt kan ladda upp pdf-filer för att publicera forskningsartiklar.

Samtidigt har också systemet för kvalitetsgranskning genom peer review-bedömning diskuterats och kritiserats i sig. Studier har påvisat brister i granskningsprocessen, inklusive problem med t.ex. jäv och könsbaserad bias vid rangordning av forskare liksom problem med stor oenighet mellan individuella granskare i peer review-granskning av allt från vetenskapliga artiklar, via projektansökningar riktade till forskningsråd, till utvärderingar av lärosäten (t.ex. Wennerås & Wold, 1997).

I början av september publicerade Science Magazine en artikel av vetenskapsjournalisten John Bohannon (2013), där han avslöjade brister i peer review-processen i ett antal OA-tidskrifter. Artikeln baseras på en undersökning i vilken han under pseudonym och med en påhittad adress vid ett icke-existerande universitet skickat en fabricerad artikel med språkliga brister och direkta – och uppenbara – felaktigheter i de analyser och den resultatredovisning som den fabricerade artikeln byggde på. Av de drygt 300 tidskrifter som den fabricerade artikeln skickades till accepterades den i cirka hälften av fallen: ofta med tydliga spår av en mycket bristfällig eller till och med obefintlig peer review-granskning, trots att alla de tidskrifter den fabricerade artikeln skickats till hävdat att en sådan granskningsprocess ligger till grund för deras bedömning. Bohannons artikel väckte stor uppmärksamhet: i akademiska sammanhang, inom OA-rörelsen och i nyhetsmedier. Bohannons artikel väckte starka reaktioner, och bl.a. kritiserades han för att han i sin undersökning inte skickat in artikeln till t.ex. tidskrifter med prenumerationsavgifter eller OA-tidskrifter utan författaravgifter för att kontrollera hur den fingerade artikeln skulle ha tagits emot i tidskrifter med andra finansieringsmodeller. Vidare kritiserades han också för hur han valde ut de tidskrifter som han skickade den fingerade artikeln till, vid sidan av att använda *The Directory of Open Access Journals* (DOAJ), en välkänd förteckning över OA-tidskrifter, använde han också en lista över förlag som är kända för att vara mer eller mindre tvivelaktiga i deras uppsåt och med ett granskningsförfarande av tveksam kvalitet.

Bohannons artikel, och de reaktioner den väckte, är ett intressant exempel att analysera för att studera de processer som i hög grad ligger bakom hur forskningen granskas och hur dess tillförlitlighet bedöms och garanteras; och inte minst, vad som

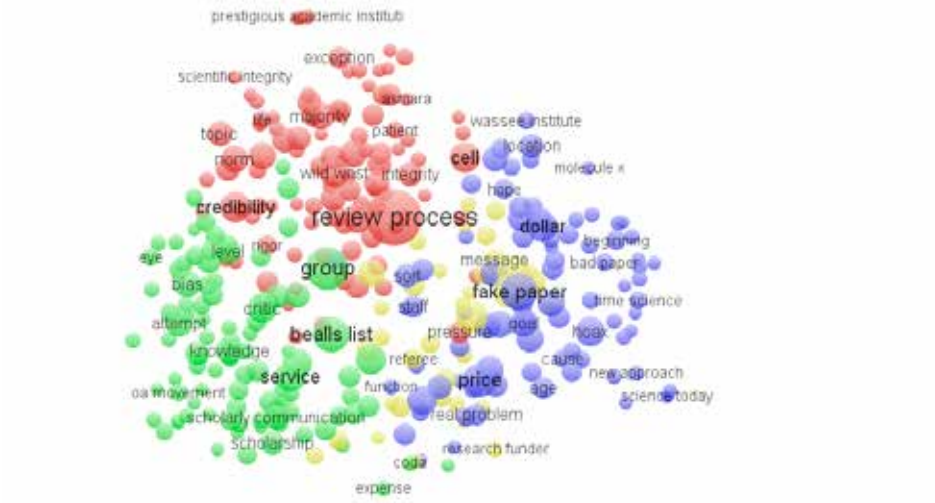
händer när dessa processer börjar ifrågasättas. För viktiga frågor i sammanhanget är i vilken utsträckning Bohannons artikel handlar om tillförlitlighet hos OA-tidskrifter med författaravgifter, eller i vilken utsträckning den handlar om peer review-processens tillförlitlighet, eller rent av om tillit till det vetenskapliga publikationssystemet och därmed också till det som vi kallar för vetenskaplig kunskap som helhet.

För att mer systematiskt kunna studera vilka teman som dyker upp i reaktionerna på Bohannons artikel använde vi en webtjänst som identifierar webpublikationer med anknytning till OA-frågor för att identifiera dokument som rapporterade om, och kommenterade, Bohannons artikel. På så sätt hittade vi ca 80 websidor med reaktioner på, eller rapportering om, Bohannons artikel. Dessa var publicerade från och med dagen då Bohannons artikel publicerades och ca två veckor framåt, i allt ifrån traditionella och webbaserade nyhetsmedier, via universitetsbibliotek och organisationer kopplade till OA-rörelsen, till individer som bloggar om OA- och vetenskaplig kommunikationsfrågor.

Den kvantitativa analysen: begreppsliga relationer

De kvantitativa analyserna av dokumenten utfördes i VOSviewer (http://www.vosviewer.com), ett program för att visualisera bibliometriska analyser. De begrepp som förekommer i de dokument vi undersöker analyseras utifrån i vilken utsträckning begreppen förekommer mer eller mindre ofta tillsammans, och baserat på detta kan man klustra begreppen för att kartlägga olika teman och få en överblick över reaktionerna på Bohannons artikel.

I centrum av kartan finner vi peer review-begreppet (Figur 1). Frågan är dock i vilken utsträckning detta handlar om kvalitetsgranskningsprocessen i allmänhet eller om det handlar om dessa processer ifråga om just OA-tidskrifter? I Bohannons artikel är det just ifråga om OA-tidskrifter som dessa processer kopplas, och inte minst, med koppling till företeelsen med APC-, eller författaravgifter som Bohannon. Samtidigt vet vi också att det finns en diskussion kring dessa processer för kvalitetsgranskning mer generellt.



Figur 1. Karta över begrepp använda i dokument med rapportering om, och kommentarer kring, Bohannons artikel.

Lite beroende på hur man tolkar kartan kan man identifiera tre eller fyra kluster, tre mer och ett något mindre framträdande. På kartans högra sida finns ett kluster med begrepp som behandlar Bohannons artikel i sig, problem med OA-tidskrifter och författaravgifter, samt – om man zoomar in i kartan – också 'Sokal's Hoax', ett välkänt exempel på tidigare användning av fingerade artiklar för att avslöja missförhållanden i den vetenskapliga publikationsprocessen. På den övre delen av kartan finner vi ett annat kluster som mer handlar om den vetenskapliga publiceringsprocessen och peer review-systemet mer generellt, och de problem som kan finnas associerade med dessa processer. På den nedre delen av kartans vänstra sida finns ett kluster av begrepp som främst relaterar till kritiken mot Bohannons artikel och hur hans undersökning är problematisk utifrån att han använt en lista över kända problematiska förlag, och att det saknas en kontroll gentemot tidskrifter med andra finansieringsmodeller än författaravgifter. I mitten av kartans nedre del finner vi också ett mindre distinkt kluster, som i hög utsträckning behandlar mer allmänna frågor med anknytning till OA-frågor och OA-rörelsen.

Den kvalitativa analysen: tre dimensioner av tillit

Den kvantitativa analysen ger oss en överblick över de teman som förekommer i reaktionerna på Bohannons artikel, men för att skapa en mer ingående förståelse

för diskussionen gjordes också en kvalitativ analys av innehållet med fokus på tillitsfrågor. Den kvalitativa analysen gjordes i ljuset av resultat från den kvantitativa analysen, dvs. begrepp som framkom som centrala i analysen utgjorde ingången till den kvalitativa, tematiska analysen. Särkilt fokus lades på synen på peer-review och kvalitetsgranskning allmänt och hur denna kopplats till föreställningar om tillit i texterna. Detta innebar att vi i den kvalitativa analysen fokuserade på begreppet *trust*, samt andra relaterade begrepp som *credibility, quality, control, ethics, conduct* eller *misconduct*; och hur dessa begrepp sattes i relation till peer review-frågor.

Reaktionerna på Bohannons artikel hittades i många olika typer av medier. Det rapporterades om Bohannons artikel i nyhetsmedier och andra medier riktade mot den bredare allmänheten, både traditionella som The Guardian och The Economist, nätbaserade som Huffington Post, och också på t.ex. National Geographics nyhetssidor. Den största andelen reaktioner och rapporter finns dock – inte överraskande – bland bloggar och på hemsidor med fokus på vetenskaplig forskning och kommunikation: vetenskapliga bibliotek är väl representerade, och bloggar av forskare och andra intresserade av publikationsfrågor utgör också en stor del av materialet. En annan betydande del av materialet kommer från bloggar med länkar till förlag och andra organisationer med stark anknytning till OA-frågor, men också från mer traditionella förlag. Som vi redan kunnat konstatera i den kvantitativa analysen finns det några övergripande teman som återkommer: problem med peer review-systemet, med författaravgifter, liksom problem med tvivelaktiga tidskriftsförlag. Ett annat återkommande tema är kritiken mot hur Bohannons studie utformats. Vilka teman som tas upp varierar, bland annat beroende på i vilken utsträckning personen eller organisationen bakom reaktionen har positionerat sig i frågan om OA-publicering - eller på vilket sätt och i vilken utsträckning forskningsresultat bör göras fritt tillgänglig: en del förespråkare för 'grön OA' tenderar t.ex. att se problem associerade med författaravgifter som en central fråga i artikeln, samtidigt som många andra med stark anknytning till OA-rörelsen fokuserar sina reaktioner på problem med hur Bohannon utformade och utförde sin studie. Det finns dock också inslag, bland annat i reaktionerna från mer traditionella nyhetsmedier, som rapporterar om Bohannons artikel utifrån ett perspektiv som mer fokuserar på hur dennes undersökning speglar en generell kris i den akademiska forskningen.

I huvudsak kan man identifiera tre dimensioner av tillit ifråga om forskning och vetenskaplig kommunikation, dvs. var tilliten till peer review-systemet – och i förlängningen trovärdigheten i vetenskapliga artiklar och i de de resultat de presenterar – lokaliseras. En dimension av detta finner vi på ett personligt plan, där vi placerar vår tilltro till våra kollegor inom forskningen när de verkar som granskare av våra

artiklar. Den andra dimensionen handlar om de kontrollmekanismer som används för att granska artiklars och tidskrifters kvalitet och genomslag. De första två dimensionerna möts i en tredje dimension, där vi talar om tilltro på ett systemiskt plan: de individer som granskar artiklarna möts inom ramen för peer review-systemet, systemet för vetenskaplig meritering genom artikelpublicering stöds av kontrollmekanismer som t.ex. indikatorer på tidskrifters genomslag mätt i citeringar, var tidskrifterna indexeras osv.

Det personliga perspektivet är den dimension som framträder i minst utsträckning, och som är begränsat till individuella forskares bloggar. Det som beskrivs här är en tilltro till de personer som vi arbetar tillsammans med. En viktig aspekt av detta är den roll våra personliga kontaktnät spelar, där vi bland annat kan se i vilken utsträckning t.ex. en tidskrift upplevs som trovärdig genom att vi känner till namnen på de som är redaktörer, på de som sitter i redaktionskommittéen eller den vetenskapliga kommittéen för en konferens. En annan aspekt av tillit på ett personligt plan speglas i beskrivningen av forskarnas tilltro till sin egen förmåga att bedöma i vilken utsträckning en tidskrift verkar trovärdig och hur trovärdiga ett e-mail som marknadsför en tidskrift eller en konferens egentligen är; men också den egna förmågan att bedöma en artikels kvalitet oberoende av om den genomgått en peer review-process eller ej. Tilliten kommer alltså i hög utsträckning från forskarnas kunskap om det fält de är verksamma inom, tillsammans med deras förmåga att granska information om olika publiceringsforum i form av t.ex. hur tidskriften marknadsför sig eller vilka som sitter i redaktionskommittéen. En tillit som baseras på personliga kontaktnät blir dock sårbar när vi börjar finna aktörer inom fältet som befinner sig utanför våra egna, eller andra etablerade, kontaktnät.

I de texter från medier som framför allt riktar sig till allmänheten framkommer kritik av hur Bohannon utförde sin studie, samtidigt som OA-publicering överlag framställs som en positiv utveckling. Här kopplas också peer review-processer samman med tillit på olika sätt, och kontrollmekanismer som underbygger de vetenskapliga artiklarnas tillförlitlighet framhävs som viktiga. Det intressanta är att det uppstår en ny dimension, där kontrollmekanismerna inte i första hand används för att granska de vetenskapliga artiklarna, utan som kriterier för att kontrollera formalia och därmed en viss form. Vetenskapliga publikationer har ett särskilt format, de använder sig av formalia som abstract, referenslistor, nyckelord och så vidare. Utan att ens behöver läsa en text ska man kunna se att den är 'vetenskaplig'. Dagens vetenskapliga tidskrifter, som i princip är genomdigitala, remedierar en form som utvecklades när tidskrifterna var tryckta (Francke, 2008). Vi kan se vissa förändringar och en viss upplösning av tidskriftsformatet som medium, men överlag är formen

oförändrad och följer i stort sett samma formella kriterier som den gjorde för 30 eller 40 år sedan; och som fortfarande signalerar textens "vetenskaplighet". Däremot har digitaliseringen gjort det möjligt att designa tidskrifter som uppfyller alla formella kriterier utan att detta behöver betyda att redaktionsprocesser eller andra garanter för kvalitet och vetenskaplig tillförlitlighet motsvarar förväntningarna på tidskriftens 'vetenskaplighet'. Detta är sällan ett problem ur ett inomvetenskapligt perspektiv, som vi var inne på tidigare, dock beskrivs det som problematiskt ifråga om i vilken utsträckning vetenskapsjournalister och 'allmänheten' kan lita på innehållet i något som formatmässigt ser ut att vara en vetenskaplig artikel. Samtidigt gör också digitaliseringen det möjligt att enkelt kontrollera en tidskrifts status, genom att konsultera kontrollinstanser som tidskriftsförteckningar och index över vetenskapliga artiklar, men också information om tidskrifternas användning och vetenskapliga renommé, är tillgängliga på nätet.

På ett systemiskt plan kan tilliten beskrivas utifrån flera olika perspektiv, där aspekter av personlig tillit och tillit till kontrollmekanismer möts. En sida av detta är att peer review-systemet i ökad utsträckning upplevs vara allt mer ur fas med resten av det vetenskapliga publikationssystemet: inte minst i förhållande till vetenskaplig meritering och kraven på att forskare inte bara publicerar sig utan att de publicerar mycket och i publiceringsforum med hög prestige. I och med att kraven på att publicera sig mycket ökar, ökar inte bara arbetsbelastningen på forskarna när de förväntas skriva mer, utan också genom att det även är de som granskar de artiklar som skickats in till tidskrifterna. Här kan man också se något av en motsättning mellan individnivån och den systemiska nivån, där vi på individbasis anser oss kunna avgöra huruvida en artikel eller en tidskrift är av god kvalitet, medan vi inom ramen för meriteringssystemet använder oss av genomslagsindikatorer – som olika sorters citeringsmått – för att avgöra i vilken utsträckning en tidskrift är av god kvalitet eller har genomslag inom ett forskningsfält. Mer generellt är peer review-systemet en av de faktorer som diskuteras mest i reaktionerna på Bohannons artikel; och även detta är en fråga som befinner sig inom ett spänningsfält mellan det individuella och det systemiska perspektivet. Av tradition litar vi på systemet i sig, och inte minst dess utformning, där vi ofta har mer än en granskare för varje artikel. Men samtidigt är frågan i vilken utsträckning vi litar på de individer som befolkar systemet. Och inte bara det: tillsammans med Bohannons artikel hittar vi också en ökande mängd studier som rapporterar om problem med peer review-processen på en systemisk nivå, med tidskrifter som i högre grad tvingas dra tillbaka redan publicerade texter och med undersökningar som visar på stora skillnader i hur olika granskare uppfattar kvaliteten i en artikel (Smith, 2006; Steen et al., 2013). Detta, tillsammans med nya

utmaningar som vetenskapssystemets exponentiella tillväxt och konstanta acceleration, har lett till diskussioner om huruvida peer review är tidsenligt och funktionellt. Numera diskuteras olika möjligheter för att förändra och öppna upp systemet, som *crowdsourcing peer review, open peer review, metareview* eller *post-publish peer review*.

Diskussion

Digitaliseringen av det vetenskapliga publiceringssystemet har inneburit grundläggande förändringar för forskarnas möjligheter att sprida sina resultat och kommunicera sin forskning till sina kollegor och till världen runt omkring. Digital publicering har medfört möjligheter till att utveckla formerna för de traditionella, tryckta artiklarna och böckerna, samtidigt som formerna för hur vetenskapliga artiklar framställs och granskas i hög grad innehåller betydande drag av konservatism: att artiklar ser ut på ett visst sätt och att de går igenom ett visst granskningsförfarande är av stor betydelse för att signalera artikelns vetenskaplighet och i vilken utsträckning den kan sägas representera tillförlitlig forskning. Digitaliseringen har också inneburit betydande möjligheter för att göra forskning mer lättillgänglig, och tillgänglig för en bredare publik, genom en spridning som inte nödvändigtvis begränsas av tillgång till prenumerationer på tryckta tidskrifter. De mer lättillgängliga möjligheterna för att sprida forskning digitalt har dock samtidigt – tillsammans med ökad press på forskare att publicera sig kombinerat med ökande krav på att göra forskningen öppet tillgänglig genom OA-publicering – öppnat upp för möjligheten för publikationer av tidskrifter som ser ut som vetenskapliga publikationer men med betydande brister i granskningen av den forskning som representeras i artiklarna.

Bohannons artikel i Science lyfter fram intressanta perspektiv att reflektera kring i anslutning till både OA-publicering och peer review-systemet, men innehåller en del problem i fråga om hur studien utformades. Detta är också något som uppmärksammats i de reaktioner och kommentarer som kommit fram efter att artikeln publicerades. Inte minst ur ett tillitsperspektiv är det också intressant att konstatera att man både kan se olika aspekter av den diskussion som uppstått utifrån å ena sidan ett individbaserat, och å andra sidan ett systemiskt baserat tillitsperspektiv; och att individ- och det systemiska perspektivet bitvis hamnar i konflikt med varandra. Men det uppstår i sammanhanget också en fråga om vad det är i den vetenskapliga publikationsprocessen vi litar på?

Ur det mest avgränsade perspektivet handlar Bohannons artikel i hög utsträckning om i vilken utsträckning OA-tidskrifter är tillförlitliga: Bohannon själv väljer ju det fokuset, och det finns också en substantiell del av de efterföljande kommentarerna som rapporterar om artikeln utifrån OA-perspektivet. Och visst finns det

problem med OA-tidskrifter med en bristfällig kvalitetsgranskningsprocess, med tidskrifter som utger sig för att vara baserade på ett ställe där de faktiskt inte är baserade och med tidskrifter som marknadsför sig med spam-utskick genom e-post; och vars främsta drivkraft verkar vara att komma åt publiceringsavgifter. Samtidigt finns också många OA-tidskrifter med en väl fungerande granskningsprocess, liksom OA-tidskrifter som finansieras genom andra affärsmodeller än författaravgifter. En central del i hur tilliten skapas i förhållande till OA-tidskrifterna finner vi i formen, i de kontrollmekanismer som säger att en vetenskaplig publikation ser ut på ett visst sätt och ingår i vissa sammanhang. Det blir påfallande när en tidskrift saknar dessa formella egenskaper, som t.ex. att inte indexeras i välkända databaser över vetenskaplig litteratur.

Även om det finns problem med vissa OA-tidskrifter, är problem med peer review-systemet generellt sett också väl kända. Tydliga tecken på detta är bluffartiklar har tagits in i tidskrifter som finansieras genom prenumerationer – ett av de senast uppmärksammade fallen var när vetenskapliga förlag som IEEE och Springer tvingades dra tillbaks ett hundratal artiklar när det visade sig att artiklarna var datorgenererade nonsens-artiklar (Retraction Watch, 2014) – och vi ser också en substantiell ökning av vetenskapliga artiklar som dras tillbaks för att de experiment de bygger på inte går att reproducera (Steen et al., 2013).

Peer review-processen innefattar både systemiska och personliga aspekter av tillit: vi litar på att de som granskar artiklarna gör ett tillförlitligt jobb och att de artiklar som de rekommenderar för publicering bygger på korrekt genomförd forskning. Samtidigt är peer review-förfarandet del av en systematisk granskning av artiklarnas kvalitet: anonymisering av både artikelförfattare och granskare, samt användandet av flera granskare, är vanliga strategier för att säkerställa att särintressen inte är inblandade i bedömningen av artiklarna. I Bohannons artikel, och i reaktionerna i kölvattnet av denna, ser vi inte bara problem identifierade med denna process, utan i dess mest extrema form ett ifrågasättande av peer review-processens nytta. Samtidigt är peer review-systemet tätt förknippad med den vetenskapliga granskningsprocessen och ofta sedd som en garant för att vetenskapliga publikationer är tillförlitliga; bedömningen av en artikels tillförlitlighet riktar sig inte bara till forskare utan handlar om att utanförstående ska kunna lita på innehållet i en artikel utan att ha ingående kunskaper om ett forskningsfält.

Utifrån det allra vidaste perspektivet handlar dessa frågor om i vilken utsträckning tillit till vetenskaplig forskning, uttryckt i publikationer, är rättfärdigat och hur det kan bedömas? Detta leder till frågor som: vad händer med forskningen när meriterings- och belöningssystem ställer ökande krav på att forskare ska publicera sig

– mycket – samtidigt som digitaliseringen förändrar villkoren för produktion, spridning och granskning av vetenskapliga publikationer? Ur ett kommunikativt perspektiv må det numera vara möjligt för forskare att publicera direkt på internet utan att gå genom ett förlag för att sedan själva bedöma kvaliteten på en redan publicerad artikel, men utifrån ett belönings- och meriteringsperspektiv – som är dagens obestridda imperativ – är peer review-processer och genomslagsindikatorer helt avgörande, samtidigt som vetenskapen som samhällets dominanta kunskapsform måste kunna läsas men också granskas av personer utanför respektive forskningsfält. Tillit och hur den skapas och upprätthålls blir därmed en del av olika system med krav på att kunna bedöma deras betydelse för produktion och distribution av vetenskaplig kunskap i en genomdigitaliserad kultur.

Referenser

Bohannon, J. (2013). Who's afraid of peer review? *Science Magazine*, 4 October 2013:342 (6154), 60-65. doi: 10.1126/science.342.6154.60

Cronin, B. (2005). *The hand of science: academic writing and its rewards.* Lanham: Scarecrow.

Francke, H. (2008). (*Re) creations of scholarly journals: document and information architecture in open access journals.* Department of Library and Information Science/Swedish School of Library and Information Science University College of Borås/Göteborg University: Valfrid.

Frohmann, B. (2004). *Deflating information: from science studies to documentation.* Toronto: University of Toronto Press.

Hardwig, J. (1991). The role of trust in knowledge. *Journal of Philosophy.* 88(12), 693-708.

Porter Liebeskind, J. & Lumerman Oliver A. (1998). From handshake to contract: intellectual property, trust and the social structure of academic research. I Lane C. & Bachman R. (red), *Trust within and between organizations: conceptual issues and empirical applications*, chapter 4, Oxford: Oxford University Press, 118-145.

Retraction Watch (2014). Springer, IEEE withdrawing more than 120 nonsense papers. http://retractionwatch.com/2014/02/24/springer-ieee-withdrawing-more-than-120-nonsense-papers [2014-05-19]

Rushforth, A. & de Rijcke, S. (2014). The Impact of indicators: the rise of performance indicators and commensuration in Dutch biomedical research. presenterad vid *EU-SPRI Early Career Research Day*, Ingenio, Valencia, Spain, 7-8 April 2014.

Shapin, S. (1994). *A social history of truth: civility and science in seventeenth-century England*. Chicago: University of Chicago Press.

Smith, R. (2006). Peer review: a flawed process at the heart of science and journals. *Journal of the Royal Society of Medicine*, 99(4), 178-182.

Steen R.G.; Casadevall A. & Fang F.C. (2013). Why has the number of scientific retractions increased? *PLoS ONE* 8(7): e68397. doi:10.1371/journal.pone.0068397

University of Tennessee & CIBER Research Ltd (2013). *Trust and authority in scholarly communications in the light of the digital transition: final report.* Knoxville & Greenhamn: University of Tennessee & CIBER Research. http://ciber-research.eu/download/20140115-Trust_Final_Report.pdf [2014-05-19]

Vetenskap & Allmänhet (2013). *VA-barometern 2013/14. VA-rapport 2013:4.* Stockholm: Vetenskap & Allmänhet. http://v-a.se/downloads/varapport2013_4.pdf [2014-05-19]

Wennerås, C. & Wold, A. (1997). Nepotism and sexism in peer review. *Nature*, 387, 341-343.

Under molnen – Synliggörandet av digital infrastruktur och hur tillit och aura skapas

Robert Willim

För femton år sedan beskrevs Internet och framväxande digitala tjänster ofta med hjälp av ord som Cyberspace och virtuella verkligheter. Under senare år har andra efemära metaforer använts. Idag talas det mer om ”molnet” och molntjänster. Sällan har konkreta fysiska anläggningar och tung infrastruktur använts i marknadsföring och i frammanandet av visioner från företag och organisationer som arbetar med Internet och digitala tjänster. 2012 skedde dock ett tydligt skifte. Nu började Google strategin att synliggöra sina verksamheter. Företaget lanserade för första gången bilder och berättelser från sina anläggningar bortom sitt berömda kontorskomplex The Google Plex i Mountain View. Nu skulle de topphemliga datacentren synliggöras via en webbplats med rubriken ”Data Centers”. (www.google.com/about/datacenters/) Genom kampanjen försökte Google frammana såväl tillit till verksamheterna som en fantasieggande aura kring anläggningarna. Frågan är vad som synliggjordes via denna kampanj?

Infrastruktur är oftast osynlig. Infrastruktur är som Nicole Starosielski (2012) påpekar i regel bara synlig och uppmärksammad när något inte fungerar eller när den ges en bredare kulturell signifikans. Den kulturella signifikansen innebär att infrastrukturen kan användas för att frammana visioner kring verksamheter. Visionerna kan handla om samhällsutveckling. De kan också etablera specifika föreställningar om varumärken och produkter. När det gäller de senaste decenniernas digitala utveckling och hur tongivande företag har agerat, är det påfallande hur lite av infrastrukturen som har använts för att synliggöra verksamheter. Ända sedan 1990-talet då det talades om behovet av nya infrastrukturella satsningar i form av bredband, eller mer metaforiskt i form av till exempel ”The Information Superhighway”, så var det inte bilder av storskalig teknik som användes i retoriken. Istället var det ofta

bilder av framtida abstrakta virtuella verkligheter eller ett flyktigt *Cyberspace* som frammanades. Drygt 15 år senare har detta alltså förändrats.

Det industriellt sublima

De bilder som 2012 presenterades i gallerier på Googles nylanserade webbplats var indelade i tre olika kategorier: platser, människor och teknik. Bilderna av människor porträtterades av anställda i olika arbetssituationer eller poserande vid företagets anläggningar. I bildtexter berättades kort om arbetsuppgifter i anläggningarna, men också om att personerna var mer än bara anställda på Google. I rubrikerna på sidan står det att de anställda är alltifrån zombie-maratonlöpare och brädspelsentusiaster till veteranbilsfanatiker.

Personporträtten var dock inte det centrala på webbplatsen, utan det som i första hand synliggjordes i Googles bilder var fantasieggande bilder av tekniken och anläggningarna. Företaget visade upp bilder av sina datacenters, med långa rader av servrar, intrikata kylsystem, mängder av kablar och lysande dioder. Här frammanades bilden av en tekniskt avancerad och välordnad organisation, men en påfallande färgrik och lekfull sådan.

Lekfullheten och de framträdande pastellfärgerna i samband med industriell verksamhet är något relativt nytt som präglar bilder av flera nya IT-företag, inte minst Google. Men suggestiva bilder av utvecklad industriell rationalitet placerar kampanjen i en längre tradition.
I flertalet av bilderna syns rader av utrustning som sträcker sig bort från betraktaren.

Google. www.google.com/about/datacenters/

Detta sätt att visualisera industriella eller tekniska anläggningar påminner om ett fenomen som teknikhistorikern David E. Nye har kallat för det tekniska och industriellt sublima (1996). Industriella miljöer kom i slutet av 1800-talet att ses som sublima scenerier, jämförbara med till exempel mäktiga bergslandskap, vattenfall och andra platser som något sekel tidigare hade blivit turistattraktioner. Fabriker och industriella anläggningar blev alltså attraktioner som ställdes mot naturens erbjudande av sublima upplevelser. Det sägs till exempel att en del besökare vid Niagarafallen imponerades mer av de stora turbinerna som fanns i vattenkraftverken än av fallen i sig. Industrilandskapen lockade med anläggningars storskalighet, maskiner och arbetande människor i långa rader. Här kunde upplevelser som var såväl frånstötande som fascinerande ta plats. Höga ljud, infernalisk hetta och imponerande moln av ånga och rök kunde betraktas. ”I de stora fabriker som byggdes fann turister och upplevelsejägare ett intresse för de närmast monstruösa utsläppen av rök, ångor och ibland eld.” (Nye, 1996, s.126 (min översättning)). Besökarna av fabrikerna kom från delar av samhället där fabriksarbete var något exotiskt eller något som inte präglade vardagen. Det var inte arbetarna i fabrikerna som jagade upplevelser och fascinerande motiv bland maskinerna, istället var det en ofta välbärgad medelklass på besök.

Betraktare kunde enligt Nye fascineras av såväl det skakande i scenerierna som det storskaligt exakta i anläggningarna. Industriella landskap visade hur människan hade lyckats framställa maskiner och anläggningar som frigjorde enorma krafter och som kunde konkurrera med naturens storslagenhet. Den dynamiska kraften tillsammans med den matematiska exaktheten, komplexiteten och den stora skalan på anläggningarna lockade.

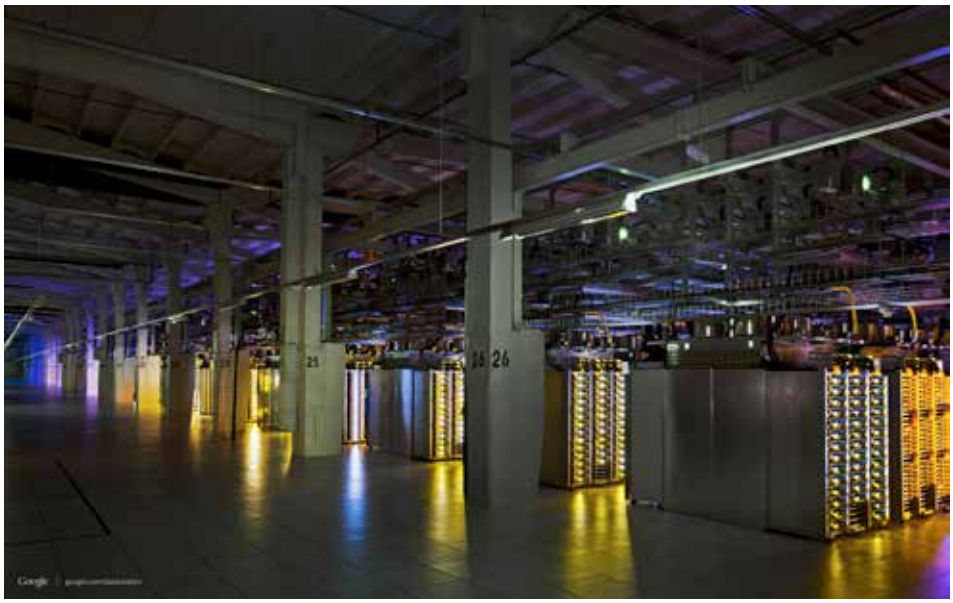
Industrier besöktes rent fysiskt, men bilder från miljöerna förmedlades även i medierad form. Med hjälp av den tidens tekniker för upplevelseproduktion, till exempel kameror och stereoskop, visades bilder tagna i fabriker. Det storslagna, det exakta och den enorma skalan betonades, och långa rader av maskiner som sträckte sig mot

Steel Works, Pittsburg, från Robert N Dennis collection of stereoscopic views. Wikimedia

Google. www.google.com/about/datacenters/

horisonten blev ett favoritmotiv. De suggestiva bilderna blev till ”visuella metaforer för den industriella produktionens ymnighetshorn” (ibid 115 (min översättning)).

Här finns likheter mellan till exempel ett tidigt stålverk i Pittsburg och Googles anläggningar idag. Bilderna inifrån datacentren skulle också kunna beskrivas som en slags visuella metaforer för den nya digitala industrins ymnighetshorn. Symmetrin, exaktheten, den underliggande matematiska komplexiteten och det storslagna kan frammana känslor av stabilitet och kan också inge förtroende. Samtidigt skapar de ibland mystiska utrymmena om visas i fotogallerierna tillsammans med suggestiv belysning och upprepningar av visuella element en gåtfull och suggestiv aura kring tekniken. Google frammanar genom bilderna såväl mystik som förtroende.



Google. www.google.com/about/datacenters/

Industrial Cool

När Google beslutade att publicera bilder av datacenters och teknisk infrastruktur på Nätet var det del i en bredare visualiseringsstrategi. Samtidigt som den webbaserade kampanjen lät man journalisten Steven Levy, som tidigare hade skrivit boken *In The Plex* om företaget, göra ett reportage inifrån några av Googles anläggningar. Både på webben och genom reportaget ville man ge en bild av transparens. Nu skulle slutligen den hemlighetsfulla verksamheten bli synlig. I en tidslinje de presenterar på webbplatsen har ordet ”transparens” skrivits vid årtalet 2012. Men ser vi på flera av

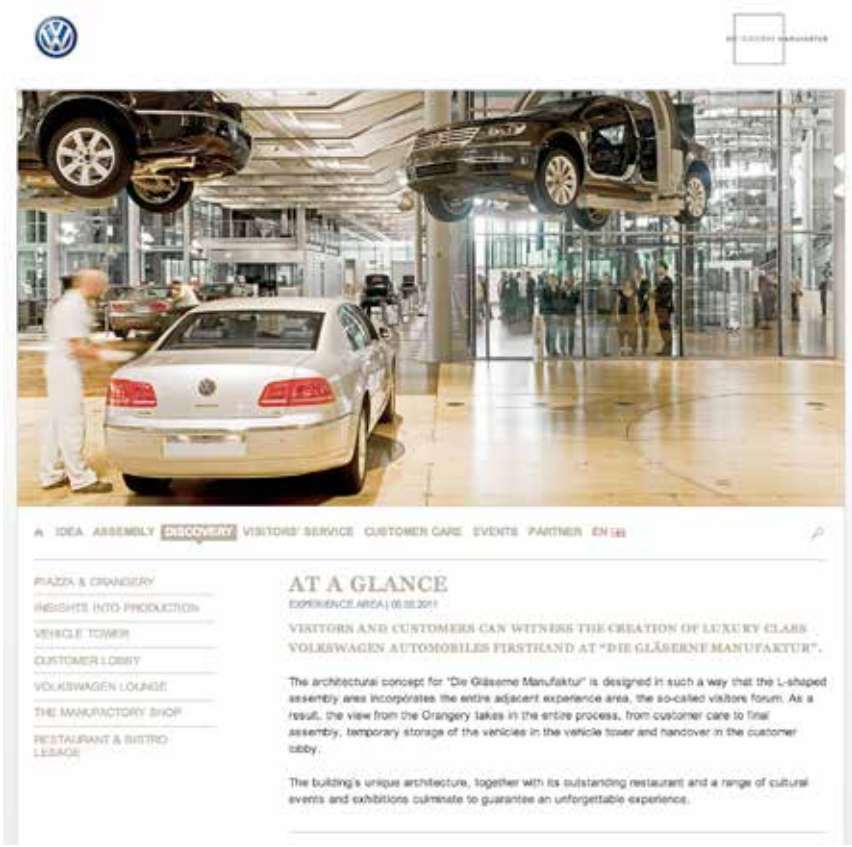
visualiseringarna så visar de som sagt ofta en mystisk aura. Flera bilder frammanar också en stillsam känsla. Här är det på sätt och vis långt till bullrig och hård industri, istället är det en påfallande harmoni som vilar över scenerierna. Anläggningarna framställs som integrerade med omgivningar, som del av den lokala ekologin med en familj hjortar som betar utanför en av datacentren. På andra bilder beskrivs dimhöljda byggnaderna som effektivt fungerande, det är nämligen när ånga från anläggningen släpps ut och bildar mindre dimmoln som kylsystemet är som allra effektivast.

Google. www.google.com/about/datacenters/

Dessa bilder och Googles presentation av det de kallar för ”The Physical Internet” är del av en affärsstrategi som ligger i linje med det jag kallar för *Industrial Cool* (2008). Det handlar om en bredare estetisering av tunga industriella verksamheter och anläggningar. En del av detta fenomen är *iscensatta fabriker*. I en studie för några år sedan pekade jag ut Volkswagens så kallade Showcase-fabrik *Die Gläserne Manufaktur* i Dresden som ett framstående exempel på Industrial Cool och iscensatta fabriker (Willim, 2005; 2008).

Die Gläserne Manufaktur är belägen i centrala Dresden. Fabriken marknadsförs som en turistattraktion bland andra, som Semper-operan, museer och barockbyggnader. Besökare välkomnas att se utvalda delar av hur lyxmodellen Phaeton produceras på andra sidan glasväggar. Bilarna transporteras sakta och värdigt av robotsystem. På parkettgolv och under spotlights monterar sedan vitklädda arbetare ihop bilarna. Hela fabriken är ett *brandscape*, en mix av noggrant designad och driven showcasefabrik och en upplevelsevärld för kunder och besökare (Klingmann, 2007). I fabriken har man låtit genomföra en rad evenemang som i regel inte förknippas med bilproduktion, såsom operaföreställningar, konserter och konstevenemang.

Läsaren kan undra vad som egentligen produceras här. Det är då värt att poängtera att en iscensatt fabrik inte handlar om någon form av låtsastillverkning. Istället



Webbsida, Volkswagen, Die Gläserne Manufaktur. www.glaesernemanufaktur.de/en/discovery

det om att visa koreograferad produktion och avsiktligt estetiserade visualiseringar av anläggningar. Iscensatta fabriker är en ny sorts mix av varumärkesbygge, kundrelationer, marknadsföring och produktionen av olika produkter och värden.

Selektiv visualisering är centralt för iscensättningen av Industrial Cool. Anläggningar är samtidigt karaktäriserade av en aura av mystisk hemlighetsfullhet och presentationen av suggestiva visualiseringar vilka framställs som transparenta. Detta ligger i linje med Googles val att visualisera infrastruktur och ”det fysiska Internet”. Materialiteten bakom digitala tjänster framställs som helt synliggjord, men i själva verket handlar det mer om iscensättning och formeringen av Internets Industrial Cool. Virtualiteten och flyktigheten hos det digitala och Internet vävs nu samman med fantasieggande bilder av den infrastruktur som dagens molntjänster baseras på.

Kan vi lita på vad vi ser?

Googles visualiseringskampanj 2012 dök inte upp av en slump. Intresset för det fysiska, det påtagliga och det materiella bakom digitala tjänster och världar verkade öka inom flera områden. Inte minst i den akademiska världen publicerades vid ungefär samma tid en rad studier som tog upp sociala och kulturella aspekter på digital materialitet. Även utanför akademin dök det upp böcker som på olika sätt handlade om Internets fysiska dimensioner. Två exempel är Andrew Blums *Tubes. A Journey to The Center of Internet* (2012) samt Douglas Algers *The Art of the Data Center: A Look Inside the World's Most Innovative and Compelling Computing Environments* (2012).

Genom sin kampanj med fascinerande bilder av sina anläggningar frammanade Google en aura av mystik och en väl iscensatt verksamhet. Genom kampanjen frammanades också tillit till det multinationella företaget. De fokuserade på transparens, men också på centrala teman i samhälleliga diskussioner vid tiden. I flera sammanhang påtalades och visades exempel på ekologisk hållbarhet. Som led i kampanjen framhölls effektiva energilösningar samt satsningar på el från förnyelsebara källor. Till exempel framhölls det hur företaget hade satsat på hållbar svensk vindkraft för att driva sin anläggning i ett nedlagt och omgjort pappersbruk i södra Finland (Jones, 2014).

Genom att peka ut konkreta platser på sina anläggningar kunde Google också relatera kampanjen till frågor om lokaliseringen av data. Under senare år har det debatterats flitigt var data egentligen huserar när det ”ligger i molnet”. Leverantörer som Dropbox, Google och Amazon tvingas visa att användares och kunders data finns lagrade på säkra platser. Ett sätt att frammana känslor av tillförlitlighet kan vara genom tilltalande bilder och lugnande samt förment transparenta beskrivningar av verksamheter. Men dessa initiativ ska ses i ljuset av en utbredd oro vad gäller Internetbaserad kommunikation. Debatter om övervakning av datatrafik och om samarbeten mellan säkerhetstjänster och diverse aktörer i IT-industrin har präglat samhällsklimatet under 2010-talets första år. Debatterna tillsammans med rapporteringar om cyberkriminalitet, om super-buggar och nya ljusskygga hacker-konstellationer gör att mörka moln vilar över dagens alltmer utbredda Internet-användande. Vem kan man egentligen lita på, och vilka viljor och motiv döljer sig bortom de lysande och färgglada skärmarna? Frågan är hur publiceringen av coola bilder kan råda bot på känslor av osäkerhet och misstro?

Google har under alla år medvetet satsat på att ge en bild av verksamheten som lekfull och innovativ, och man har ofta tonat ner kontroversiella teman. Vissa politiska markeringar, i form av till exempel kritik mot kinesisk censur, har förenats med företagets inofficiella slogan ”don't be evil”. Genom att hålla det mesta av verksam-

heten hemlig, har man låtit sin färgglada grafiska framtoning, produkterna i sig, samt väl valda visualiseringar av företaget tala.

En annan aktör inom IT-branschen, som i viss mån kan tjäna som en kontrast till Google är det svenska företaget Bahnhof. De satsar på att leverera en rad Internettjänster, och har till skillnad från flera av branschens stora aktörer tagit ställning i debatten om flera kontroversiella tjänster. Det mest uppmärksammade ställningstagandet skedde när företaget valde att lagra materialet från Wikileaks på sina servrar. På sin webbplats beskriver de sig med följande ord: ”Bahnhof erbjuder snabba, säkra och prisvärda internettjänster sedan 1994. Vårt löfte är att ge kunderna maximal säkerhet mot övervakning, företagsspionage och läckor — något som blir allt viktigare när samhället digitaliseras.”(Bahnhof.se). Mellan raderna kan kritik mot amerikanska företag som Google läsas in. Flera amerikanska företag har haft svårt att tvätta bort misstankarna om samröre med USA’s säkerhetstjänst. Som en följd av detta har initiativet *Based in Sweden* (http://basedinsweden.se/) startats för företag som levererar molntjänster och datalagring i Sverige. Det är en certifiering som garanterar att all datahantering och kommunikation från företagen aldrig lämnar landets gränser. Bakom initiativet låg företaget Bahnhof.

Logotypen för Based in Sweden.

På Bahnhofs webbplats framhålls att molntjänsterna som levereras är säkra, tar plats i Sverige och sker inom ramarna för en självständig organisation. Det framförs också att verksamheten bland annat sker i ”Sveriges coolaste serverhall”. De hänvisar till tidningen *Metro* som hade beskrivit företagets anläggning Pionen i Stockholm som ovanligt spektakulär. Pionen är en serverhall belägen i en omgjord bunker under Södermalm. Pionen hade först anlagts under kalla kriget som en civilförsvarsanläggning med kapacitet att stå emot en vätebomb. I det omgjorda bergrummet står nu

Bahnhofs servrar, som bland annat rymmer materialet från Wikileaks. Just detta material är inte särskilt omfattande när det gäller datamängd, men symboliskt är det desto större. Wikileaks passar också för att bidra till frammanandet av suggestiva bilder av Pionen.

Bahnhof Pionen.
www.bahnhof.net

Liksom Google satsade även Bahnhof på att visa upp en estetiserad bild av sin infrastruktur. På sin webbplats presenterades ett galleri med foton från Pionen, där suggestivt belysta interiörer från bergrummet sätter fart på fantasin. Det fantasieggande har också präglat några av de reportage som har gjorts om Bahnhof. När tidskriften *Wired* skrev om Pionen lyftes det fram hur företagets VD Jon Karlung tillsammans med arkitekter och designers hade inspirerats av science fiction-miljöer, bland annat filmen *Den tysta flykten* (*Silent Running*, 1972) där växter från en utplånad jord odlas i ett rymdskepp. En annan association som lyftes fram i Wired var att Pionen såg ut som högkvarteret för en skurk från en James Bond-film. Titeln på artikeln löd: ”Deep Inside the James Bond Villain Lair That Actually Exists” (2012). Även *The Daily Mail* gjorde i ett reportage kopplingen mellan Pionen och Bond-skurkar, och vävde även in Wikileaks Julian Assange i berättelsen. Detta under titeln: ”Just like out of a Bond film: Inside the astonishing subterranean WikiLeaks bunker” (2010). Fakta och fiktion vävs samman i associationerna och bidrar till en aura kring verksamheten.

Visualiseringar av digital infrastruktur karaktäriseras i dessa exempel av bländande bildvärldar och fascinerande associationer som leder åt väldigt olika håll. Infrastruktur förenas genom berättelser och visuella representationer med imaginära världar. Beroende på betraktarens perspektiv och relation till olika aktörer kan infrastrukturen få väldigt olika betydelse. Infrastrukturen kan vara integrerad och osynliggjord i vardagspraktiker, för att dyka upp i samband med brytpunkter där beslut ska fattas eller problem lösas. Men den synliggörs också, som vi har sett i PR-kampanjer,

i varumärkesstrategier och som led i framväxten av ständiga sammanflätningar mellan fantasi och verklighet.

Genom visualiseringar blir frågor om tillit och aura invävda i ett nät av associationer som sträcker sig mot så disparata ting som Bond-skurkar, förnyelsebar energi, det industriellt sublima, Industrial Cool och iscensatta fabriker. När vi ser på de senaste årens visualiseringar av anläggningar och infrastruktur från företag som Google, eller för den delen Bahnhof, är det värt att ställa frågan: varför visas just detta på detta vis just nu? Ett av världens största företag positionerar sig genom att liksom det sena 1800-talets framväxande industrier frammana det industriellt sublima. Samtidigt visar de upp coola men också i hög grad iscensatta bilder av anläggningar i Nordamerika och Europa. En betydligt mindre aktör drar en lans för maximal säkerhet och skydd mot spionage från kommersiella eller statliga aktörer, detta utifrån en omgjord svensk civilförsvarsanläggning med tydliga associationer till science-fiction. Vi bör skärskåda hur estetisering och sammanflätningar av fantasi och verklighet står i direkt relation till betydelsefulla, för att inte säga livsviktiga, strukturer och processer vad gäller dagens digitala infrastrukturer. I detta gränsland mellan fantasi och verklighet växer nämligen framtidens samhälle fram.

Referenser

Blum, A. (2012). *Tubes: a journey to the center of the internet*. New York: Ecco.

Hanlon, M. (2010, December 9). Just like out of a Bond film: inside the astonishing subterranean WikiLeaks bunker. The Daily Mail.

Jones, P. (2014). Google invests in Swedish windpower again. DatacenterDynamics 22, januari 2014.

Klingmann, A. (2007). *Brandscapes: architecture in the experience economy*. Cambridge, Massachusetts: MIT Press.

McMillan, R. (2012). Deep inside the James Bond villain lair that actually exists. Wired, November 21.

Nye, D. E. (1996). *American technological sublime*. Cambridge, Massachusetts: MIT Press.

Starosielski, N. (2012). 'Warning: do not dig': negotiating the visibility of critical infrastructures. *Journal of Visual Culture*, 11(1), 38-57.

Willim, R. (2005). It's in The Mix - Configuring Industrial Cool. In O. Löfgren, O. & R. Willim, R. (red.), *Magic, Culture and The New Economy*. Oxford: Berg.

Willim, R. (2008). *Industrial cool: om postindustriella fabriker*. Lund: Lunds universitet, Humanistiska fakulteten.

Del IV

Bilaga 1: Enkätfrågor

”DigiTrust” är ett forskningsprojekt som handlar om privatliv och identitet, säkerhet och tillit i den digitala världen. Vilken kunskap anses pålitlig, hur stark är människors medvetenhet om säkerhetsproblemen, och hur går det till när tillit och legitimitet byggs upp eller bryts ner? Undersökningen genomförs av forskare vid Lunds universitet.

A. Bakgrundsfrågor

* 1. Vilket år är du född?

* 2. Är du kvinna eller man? Kvinna/Man/Annat/Vill ej uppge

3. Vilken är den ungefärliga sammanlagda årsinkomsten i kronor för samtliga personer i ditt hushåll före skatt (pension, studiemedel etc. ska räknas in).

100 000 eller mindre / 101 000 - 200 000 /201 000 - 300 000 / 301 000 - 400 000 / 401 000 - 500 000 / 501 000 - 600 000 / 601 000 - 700 000/ 701 000 - 800 000 /mer än 800 000

* 4. Vilken skolutbildning har du?

Markera det alternativ som du anser passar bäst in på dig. Om du ännu inte avslutat din utbildning, markera den du genomgår för närvarande.

- Ej fullgjort grundskola eller motsvarande obligatorisk skola
- Grundskola eller motsvarande obligatorisk skola
- Studier vid gymnasium, folkhögskola eller motsvarande
- Examen från gymnasium, folkhögskola eller motsvarande
- Eftergymnasial utbildning, ej högskola/universitet
- Studier vid högskola/universitet
- Examen från högskola/universitet
- Examen från forskarutbildning

5. Man talar ibland om att politiska åsikter kan placeras in på en vänster– högerskala. Var någonstans skulle du placera dig själv på en sådan vänster–högerskala? Klart till vänster / Något till vönster/ Varken till vänster eller höger /Något till höger / Klart till höger

* 6. I vilken typ av område bor du?

Storstad: centralt
Storstad: ytterområde/förort Stad: centralt
Stad: ytterområde
Större tätort
Mindre tätort
Ren landsbygd

B. Frågor av generell natur kring tillit och attityder till Internet.

7. Enligt din mening, i vilken utsträckning går det att lita på människor i allmänhet?
I låg utsträckning /I viss utsträckning/Varken i låg eller hög utsträckning /I ganska hög utsträckning /I hög utsträckning
8. Hur stort förtroende har du för det sätt på vilket följande institutioner och grupper sköter sitt arbete? Inget alls/Mycket litet/Ganska litet/ Varken stort eller litet/ Ganska stort/ Mycket stort

- Regeringen
- Polisen
- Riksdagen
- Domstolarna
- Datainspektionen
- Riksbanken
- Kommunstyrelserna
- De politiska partierna
- EU-kommissionen
- Europaparlamentet
- Förenta Nationerna (FN)

9. Allmänt sett, hur stort förtroende har du för svenska politiker? Inget alls/Mycket litet/ Ganska litet/ Varken stort eller litet/ Ganska stort/ Mycket stort
10. I vilken grad anser du att kameraövervakning av offentliga platser riskerar att inkräkta på människors personliga integritet? I mycket hög grad/I hög grad/Varken i hög eller låg grad/ I liten grad/ I mycket liten grad
11. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag avstår från att säga saker via mobiltelefon i offentliga miljöer för att undvika att någon obehörig hör .
- Det är bra att myndigheterna övervakar och kontrollerar vad som händer på Internet.
- Jag känner mig orolig för att drabbas av brottslighet via Internet.
- Nuförtiden kan man aldrig vara riktigt säker på vem man kan lita på.

- Jag använder samma eller liknande lösenord i de flesta av mina Internettjänster.
- Jag använder Internet obehindrat
- Jag har god kunskap om hur man använder Internet
- Det är naturligt för mig att använda mig av Internet när jag behöver söka information
- Jag hjälper gärna andra med att använda Internet när det behövs

12. Jag anser att det är acceptabelt att följande aktörer samlar in eller bearbetar data om mina internetvanor. 5-gradig skala: Instämmer helt/Instämmer inte alls

- SÄPO
- Svenska polisen
- Försvarets radioanstalt (FRA)
- USAs säkerhetstjänst (NSA)
- Rysslands säkerhetstjänst (FSB)
- Brittiska säkerhetstjänsten (GCHQ)

13. Myndigheter bör få samla in och/eller bearbeta information om mina internetvanor. Aldrig/Efter domstolsprövning/Efter myndighetens bedömning från fall till fall/Rutinmässigt/Automatiserat

14. Hur ofta använder du Internet? Hela tiden/Några gånger om dagen/Några gånger i veckan/Någon gång då och då/Jag använder inte Internet

15. Använder du Internet i mobiltelefonen?Ja/Nej

16. Jag använder inte Internet i mobiltelefonen därför att... 5-gradig skala: Instämmer helt/Instämmer inte alls

- Det fungerar inte på min mobiltelefon
- Jag inte är intresserad, det är inte användbart
- Det är för dyrt
- Tekniken är krånglig/jag kan inte
- Det riskerar att kränka min integritet (någon kan se vad jag gör och missbruka den informationen)

17. Jag bedömer (generellt) en hemsidas trovärdighet på: 5-gradig skala: Instämmer helt/Instämmer inte alls

- Organisationen bakom
- Motiven bakom publiceringen
- Utformningen av hemsidan
- Hur uppdaterad jag upplever den
- Kvalitén på informationen Rekommendationer Tidigare erfarenhet
- Annat (vad?)

Det digitala samhället: information/tjänster

I. Ekonomi (bank, finans)

18. Nedan följer ett antal påståenden som vi vill att du tar ställning till 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag använder Internetbaserade banktjänster obehindrat
- Jag har god kunskap om hur man använder Internetbaserade banktjänster
- Det är naturligt för mig att använda mig av Internet när jag behöver utföra bankärenden
- Jag hjälper gärna andra med att använda internetbaserade banktjänster när det behövs
- Jag känner tillit (förtroende) till de internetbaserade banktjänster som jag använder mig av.
- Jag litar på att den information som jag lämnar till min bank på Internet inte används för andra syften än de angivna.
- Jag bekymrar mig för säkerheten när det gäller mitt kreditkort, om eller när jag handlar via Internet.
- Jag anser mig kunna bedöma huruvida banken har använt sig av tillräcklig säker teknik för mina banktjänster

19. Jag har förtroende för följande betalningsmetoder. 5-gradig skala: Instämmer helt/ Instämmer inte alls

- SMS-betalning
- Kontanter
- Betal-appar för smartphones
- Internetbaserade banktjänster för att betala räkningar
- Överföring genom digitala betaltjänster (PayPal, Payson, etc.)
- Kontoöverföringar via internetbank Kortbetalning

20. Hur ofta, om någonsin, använder du: Aldrig; Någon gång; Någon/några gånger i månaden; Någon/några gånger i veckan; Dagligen; Flera gånger dagligen

- SMS-betalning
- Betal-appar för smartphones
- Överföring genom digitala betaltjänster (PayPal, Payson, etc.)
- Kontoöverföringar via internetbank
- internetbaserade banktjänster för att betala räkningar
- Kortbetalning Kontanter

II. Hälsa (journalsystem, apotek)

21. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag skulle känna mig trygg med att mina medicinska journaler lagras digitalt hos min(a)

vårdgivare.

- Jag litar på att den information som lagras digitalt hos min vårdgivare inte hamnar i orätta händer.
- Jag vet hur jag går tillväga för att få tillgång till mina medicinska journaler.
- Det är naturligt för mig att använda mig av Internet när jag söker information om min hälsa.
- Jag anser mig kunnig när det gäller att söka hälsoinformation på Internet.
- Jag har inga problem med att bedöma vilken hälsoinformation på Internet som jag kan lita på.
- Jag känner mig trygg med att lämna ut information om mitt hälsotillstånd på Internet när jag söker hälso- och sjukvårdsinformation.
- Jag känner mig trygg med att lämna ut information om mitt hälsotillstånd på Internet i syfte att dela mina erfarenheter med andra.

22. När du ska utföra följande uppgifter, hur ofta använder du Internet för det: Aldrig/Någon gång/Ibland/Varje gång

- Köpa medicin genom en av Sveriges apotekskedjor.
- Köpa medicin genom någon annan leverantör. Boka tid hos din vårdgivare.

III. Privat (bildet på nätet)

23. Vilket av följande anser du är det säkraste sättet att spara bilder? Lägg säkrast överst.

- På datorn.
- Extern hårddisk/USB-minne Papperskopia
- Dvd
- Internet (webbaserad lagring av foton)

24. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag har god kunskap om hur tjänster för lagring av bilder på Internet fungerar.
- Jag litar på att de bilder som jag lagrar på Internet inte används för andra syften än de angivna.
- Jag litar på att de bilder jag delar på Internet inte kan nås av obehöriga.

Jag anser att fotografering via mobil riskerar att inkräkta på människors personliga integritet?
Jag oroar mig för att bilder på mig (och min familj) sprids på nätet mot min vilja.

25. Hur ofta, om någonsin, använder du Internet för att: Aldrig; Någon gång; Någon/några gånger i månaden; Någon/några gånger i veckan; Dagligen; Flera gånger dagligen

- Spara egna bilder/filmer
- Dela egna bilder/filmer
- Titta på personliga bilder/filmer

- Kommentera bilder/filmer

IV. Arbetsliv

26. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag känner oro för att min arbetsgivare ska kontrollera min Internet- och e-postanvändning.
- Jag vet vilken information min arbetsgivare samlar in om mitt internetanvändande.
- Min arbetsgivare begränsar tekniskt vad jag kan göra på Internet.
- Risken att bli övervakad påverkar mitt Internetanvändande.
- Jag anpassar det jag publicerar på sociala medier mot bakgrund av att det kan läsas av min nuvarande eller framtida arbetsgivare.

27. Hur ofta, om någonsin, använder du: Aldrig; Någon gång; Någon/några gånger i månaden; Någon/några gånger i veckan; Dagligen; Flera gånger dagligen

- Internet för att arbeta hemifrån (utöva ditt yrke)?
- Arbetsgivarens utrustning för att utföra privata ärenden på Internet
- Använda e- postadress från arbetet för privat kommunikation

V. Samhället

28. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag anser mig kunnig vad gäller att använda myndigheters internetbaserade tjänster
- Internet har förenklat mina myndighetskontakter
- Internet gör det enkelt att finna myndighetsinformation
- Jag rekommenderar mina bekanta att utföra sina myndighetsärenden via Internet.
- Internet underlättar att utföra mina myndighetsärenden
- Jag känner mig trygg med att lämna ut personlig information på myndigheters hemsidor
- Jag litar på att den information som jag lämnar via myndigheters hemsidor inte används för andra syften än de angivna.

29. Hur deklarerade du 2013?

- via SMS
- via Internet
- I pappersform

30. Vilket förtroende har du för innehållet i följande medier? 5-gradig skala: Litet/Stort

- Sveriges Television
- TV4
- Andra kommersiella tv-kanaler
- Sveriges Radios nationella kanaler (P1, P2, P3)

- Den lokala morgontidningen på din ort
- Stockholms morgontidningar (Dagens Nyheter, Svenska Dagbladet)
- Dagliga gratistidningar (ex. Metro, City)
- Kvällstidningarna (Aftonbladet, Expressen, GT, Kvällsposten) Aftonbladet.se
- DN.se
- Wikipedia.se
- NE.se (Nationalencyklopedin online)

VI. Media

31. Allmänt sett, har du förtroende för företagen bakom dessa sociala medietjänster? 5-gradig skala Litet förtroende/Stort förtroende - 0(kännerejtill)

- Facebook
- Twitter
- LinkedIn
- Google+
- YouTube
- Instagram
- Skype
- Vimeo
- Snapchat

32. Använder du sociala medier? (Om nej, gå vidare till fråga 33) Ja/Nej

33. Om ja, hur ofta? hela tiden/några gånger om dagen/några gånger i veckan/någon gång då och då

34. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag anser mig vara en kunnig användare av sociala medier.
- Jag känner mig trygg med att lämna personlig information till sociala medier.
- Jag oroar mig för vad som sägs/skrivs om mig i sociala medier.
- Jag anser att sociala medier riskerar att inkräkta på människors personliga integritet.

35. Läser du användarvillkoren före det att du registrerar dig som användare av sociala medier? 5-gradig skala: Alltid/Aldrig

- Jag läser användarvillkoren före det att jag registrerar mig som användare av sociala medier.

VII. Underhållning

36. Nedan följer ett antal påståenden som vi vill att du tar ställning till. 5-gradig skala: Instämmer helt/Instämmer inte alls

- Jag oroar mig för att information om min mediekonsumtion på Internet används i andra syften än de angivna.
- Många underhållningstjänster (t.ex. Spotify, Netflix) är numera kopplade till sociala medier (t.ex. Facebook). Jag känner mig bekväm med att det jag lyssnar på/läser/ser på över Internet publiceras via sociala medier.

37. Hur ofta, om någonsin, använder du: hela tiden/några gånger om dagen/några gånger i veckan/någon gång då och då

- Spotify
- Netflix
- svtplay
- tv4play
- viaplay
- youtube
- vimeo
- Pirate Bay
- Bibliotekens onlinetjänster för film och musik
- Bibliotekens utlåning av e- böcker
- Andra onlinetjänster _____

Surveillance a drain on citizens' trust

Tolerance for security related surveillance among citizens is limited. For example, 55 per cent of Swedes do not find it acceptable for FRA to gather and process data on Internet habits, researchers from Lund University conclude.

On the 8th of April, we read that the European Court had decided to follow the Advocate General's suggested route and annul the data retention directive implemented by all member states in recent years. The directive dealt largely with imposing requirements on Internet service providers to store massive amounts of data from phone conversations, text messages, e-mails, Internet connections and mobile positions for 6-24 months, with the stated intent to fight serious crime.

In the following days, one could observe political positioning in issues concerning data retention and integrity and we heartily welcome these issues being brought forth in current public debate as well as within party politics. Issues of trust and integrity in a digital context are of such importance to our society that they must be afforded a distinct place in both public awareness and in political deliberations. The issue of integrity can, of course, be observed in conjunction with the issue of the FRA and may also be linked to Edward Snowden's revelations concerning the American security agency NSA, since these are significant jigsaw pieces in how we shape our digital society.

How, then, does the average citizen feel about the state's and the authorities' gathering of information in this digital society? How much trust and confidence do we have in authorities, both Swedish and foreign, managing such information in an acceptable and appropriate manner? These questions have been central for us as a multidisciplinary research group at Lund University. Under the collective title Digitrust, we have met up for over one and a half years to study and analyze digital trust.

As a part of this project, in January we asked a representative sample of Sweden's population consisting of 1,100 respondents about their experiences and attitudes towards surveillance, among other things. Based in our survey data, we can clearly see that tolerance among citizens for these types of security related surveillance is limited. 55 per cent of Swedes do not feel it is acceptable that the National Defence Radio Establishment (FRA) should collect and process data on Internet behaviors.

As shown in the study, what people primarily object to is the perfunctory, automatized gathering of user data. Swedes are somewhat less critical of surveillance initiated and conducted by the police (46 per cent), or the Swedish Security Service (47 per cent). Furthermore, surveillance is experienced as more legitimate when preceded by decisions made by public authorities, or at least the deliberations of official persons. Foreign security services that take an interest in Swedes' Internet traffic are perceived as least acceptable.

Roughly 80 per cent of Swedes feel it is not acceptable for other states' intelligence services (USA, Russia, Great Britain) to gather and process data on Internet behaviors of individuals.

The responses to this survey prompt questions that concern both democracy and trust. The questions concerning democracy are brought to the fore by the discrepancy between how surveillance is conducted today and the citizens' perception of under which conditions it is seen as legitimate.

Many Swedes evidently feel that Internet surveillance may be tolerated, but argue that the gathering and processing of data should not be conducted routinely. Decisions on surveillance should, instead, be subject to authorities (or, even more preferably, following on "judicial review") and – in extension – be open to both transparency as well as criticism.

Such attitudes held by citizens have undeniably encountered difficulties in making an impact. Prior to the EU decision, they were neither visible in political debate on the matter, nor in the application of the legislation. Neither has the government-appointed Digital Commission produced anything more substantial than a proposal that children should be educated in "how integrity works and can be protected on the Internet" (SOU 2014:13).

As far as trust is concerned, we note in our survey that both the courts and the body of authorities in Sweden own a relatively large confidence capital. However, one should not presume that this is permanently unchangeable. Trust and confidence can be corrupted and ruined. Trust must continuously be safeguarded, and much in our society is dependent on it. Trust in the respect for the individual's integrity is central to citizens in relation to the state and authorities, and thereby also to issues concerning the role of law and the courts. Trust is also central to the economic system, to the service sector and the banks, as well as to the role of the media and the dissemination of knowledge. These are key values of society which must be safeguarded, digital society included.

Integrity is not about citizens having no skeletons in their closet and therefore nothing to fear from transparency. It is about not having to tolerate dirty fingers rummaging around in our linen. Lack of respect for integrity – both from public as well as private actors – harms our trust dependent society. And the question is important, since it largely will come to define tomorrow's digital world.

The key issues, here, concern how we are regulated and measured in the digital world, and under what conditions, and thus need to be regarded as issues of democracy. One might, somewhat loftily, claim that trust is fundamental to societal constructions, whether digital or otherwise. For digital surveillance is a powerful tool – for better or worse. It must be subject to political debate and placed under democratic control for it to deserve, in the long run, the trust of the citizens.

STEFAN LARSSON
PhD in Sociology of Law

TOBIAS OLSSON
Professor of Media and Communication Studies

CALLE ROSENGREN
PhD in Industrial Work Science

PER RUNESON
Professor in Software Engineering

Digitrust is a multidisciplinary research project funded by the Pufendorf Institute at Lund University that consists of 10 researchers from 5 faculties. Digitrust is headed by Per Runeson, professor in software engineering, and Stefan Larsson, PhD in sociology of law and head of Lund University Internet Institute (LUii): http://digitalsociety.se

Frågor kring tillit i det digitala, tycks det, ställs oftare och oftare: Hur ska vi hantera integritets- och övervakningsfrågor? Hur ska vi hantera den mätbarhet som följer av vår digitaliserade tillvaro? Vad är det som avgör vilka tjänster vi litar på och vilka vi inte litar på, i vilken mån spelar den tekniska säkerheten en roll? Liknande frågor kan ställas om vilka kunskapsinstitutioner vi litar på, eller borde lita på – hur är det med forskningens egen granskning, som också förändras och utmanas i en digital tid? Paradoxalt nog tycks bilden och den fysiska gestaltningen bli allt viktigare i den digitala världen. Därför samlar vi resultat från forskningsprojektet DigiTrust i en bok.

DigiTrust är namnet på den tvärvetenskapliga forskargrupp vid Lunds universitets Pufendorfinstitut som mellan september 2013 och juni 2014 ägnat sig åt just tillitsfrågor ur ett digitalt perspektiv. Gruppen består av 10 forskare från 5 fakulteter och har letts av Per Runeson och Stefan Larsson. Forskningen i digitrustgruppen har i korthet berört tre huvudsakliga områden: 1) Säkerhet och integritet – vilka tjänster och aktörer litar vi på och varför?; 2) Vilka kunskapsinstitutioner litar vi på eller litar vi inte på i en digital kontext? 3) Övervakning och datalagring som rättslig och offentlig trend, i vilken riktning går den?

Utöver det seminarieformsbaserade arbetet som detta tvärvetenskapliga projekt har utfört, där olika forskningstraditioner fått brottas och jämkas med varandra, har medlemmar ur gruppen deltagit i panelsamtal, radioprogram, skrivit debattartiklar, bloggat och twittrat som ett sätt att vara delaktiga i samhällsdebatten. Denna bok bjuder på en del av de analyser som gruppen har gjort, presenterar både forskningsperspektiven och forskarna, och inte minst resultat från den enkätstudie om digital tillit med 1100 svenskar som gruppen genomfört under 2014. Läs gärna mer på digitalsociety.se

LUNDS
UNIVERSITET