

Styrelsen för
PSYKOLOGISKT FÖRSVAR

24-timmarshotet

Michael Nydén

RAPPORT 189

24-timmarshotet

– Om förvaltningens förvandling och hotet mot
den personliga integriteten

Michael Nydén

RAPPORT 189

Utgiven av Styrelsen för psykologiskt försvar

ISSN 1401-2383

Stockholm 2002

Omslagsbild: Photonica/Bulls Fotograf: John Still

INNEHÅLLSFÖRTECKNING

SPFs förord	4
Författarens förord	5
Sammanfattning	6
The 24-hour threat – A Summary	8
Förvaltning i förvandling	10
Konflikten	11
Integritet	11
Effektivitet	12
Byråkrati	12
Konfliktens sammantagna dimensioner	14
Förväntningarna på myndigheterna	15
Serviceförväntningar	15
"Utbudet av ärenderelaterad information"	16
Utbudet av allmäninformation på webbplatsen	17
Övergripande informationspresentation	17
Tjänstesamverkan	18
Samverkansförväntningar	19
Samhällets grundläggande information	20
Byråkratiska förväntningar	23
Myndigheternas supermarket?	26
Har individen någon rätt till informationen om sig själv?	29
Myndigheternas relation till service och integritet	35
Genomförande	36
Resultat	36
Servicefunktioner	38
Navigering	39
Direkta tjänster	39
Öppenhet	40
Den sammantagna bilden av servicen på nätet	40
Integritetshot	40
Det svaga hotet	42
Det starkare hotet	43
Det starkaste hotet	43
Den sammanvägda bilden	44
Är bilden av myndigheterna konsistent?	45
Slutsatser	47
Komplexitetens konsekvens	48
Den i grunden förändrade relationen	49
Myndigheter är också människor	50
Rätt data till fel ändamål	52
Kan man prata med en agent?	53
Försvarsperspektiv	56
Integritet eller offentlighet?	61
Bilaga	63
Referenser	74
SPFs senaste rapporter och meddelanden	79

SPFs FÖRORD

Styrelsen för psykologiskt försvar (SPF) har under en följd av år ägnat ett stort forskningsintresse åt frågor som rör samhällets informativa och kommunikativa förmåga främst under störda men också under ostörda förhållanden. Forskningsarbetet inriktas då på sådana företeelser och förlopp som kan påverka människors inställning till och förtroende för samhället och dess institutioner.

Den snabba utvecklingen inom kommunikationsområdet under senare år – främst ITs och Internets accelererande betydelse på allt fler områden inom samhället – har kommit att förändra delar av samhällskommunikationen. Detta har av självklara skäl lett till att SPF vidgat sitt forskningsintresse till att också innefatta dessa inslag i samhällsmiljön.

SPF har genomfört en rad studier som ur olika aspekter avsett att belysa hur IT- och Internetutvecklingen kan påverka samhällskommunikationen. Hotet från IT (1993) och Myndigheter, Internet och integritet (2000) är två studier av den nu aktuella författaren. Andra studier är Från löpsedel till webb (1999), Källkritik för Internet (2000) och Vilseledning på Internet (2002). Krisinformation på Internet (1999) och Nya vägar för nyheter (2000) är andra publikationer från SPF på temat IT/Internet.

Utgångspunkten för föreliggande studie är att tidigare relations- och kommunikationsmönster mellan medborgare och myndigheter förändrats på senare tid. Regering och departement lägger allt större vikt vid myndigheternas IT-utveckling och framhåller i sin styrning av dessa kontakter med och information till medborgarna via IT som en önskvärd färdriktning. Men den ambitionen är långt ifrån oproblematiserad. Vad blir konsekvenserna när skilda krav och intressen möts i en punkt nämligen i relationen mellan medborgare-myndighet? Frågan om den personliga integriteten i relation till den svenska offentlighetsprincipen har knappast utretts tillräckligt. En brist som i förlängningen menligt skulle kunna påverka medborgarnas förtroende för samhället och dess institutioner.

Det är om detta denna studie handlar. Jag vill tacka författaren, fil dr Michael Nydén, för en mycket intressant och tankeväckande studie. Erhållna resultat och hans diskussioner och reflektioner kring dessa bidrar till att ge en breddad och fördjupad insikt om samhällets kommunikativa förmåga i en kommunikationsmiljö som kan vara verklighet inom en mycket snar framtid. De värden som ingår i den miljön och som kan komma att påverkas på ett oönskat sätt är bl.a. grundläggande demokratiska funktioner som trovärdighet, förtroende och tillit.

Stockholm i juni 2002

Göran Stütz
Forskningschef, SPF

FÖRFATTARENS FÖRORD

Detta är den tredje studien jag genomfört om relationen IT och samhälle och som publicerats i Styrelsen för psykologiskt försvars serie. I denna studie liksom i de tidigare hämtas mycket av materialet från en empirisk studie – i detta fall en studie av utbudet på 94 myndigheters hemsidor.

I studien kopplas myndigheternas faktiska hantering av IT ihop med de ambitioner som staten givit uttryck för i såväl handlingsprogrammet *En förvaltning i demokratins tjänst* som i Statskontorets arbete med *24-timmarsmyndigheten*. Resultatet är för mig oroväckande. Vi ser nu en ny förvaltningsstruktur födas med ett omfattande informationsnätverk mellan myndigheter och en mycket svag kontrollmakt när det gäller vilka uppgifter som kan samlas in. Den debatt om personlig integritet och rätten till information om sig själv som förts i samband med diskussionen om personuppgiftslagen (PuL) och andra utredningar har uppenbarligen förts helt vid sidan av denna förvaltningsförändring.

För mig innebär denna utveckling i mångt och mycket ett hot. Den ”storebror” som vi tidigare lite skämtsamt pratat om har nu kanske faktiskt fötts – även om det just nu enbart skett i princip. Men med den tekniska utvecklingens hastighet är det inte orimligt att anta att vi om tio år inte längre har många myndigheter med självständiga handläggare utan i stället en gemensam myndighetsstruktur med många olika ansikten där samma information om medborgarna delas av alla myndighetsfunktioner. Det är inte en särskilt tilltalande tanke.

Denna studie hade inte kunnat genomföras utan stöd från Styrelsen för psykologiskt försvar. Mitt tack går till styrelsen och i synnerhet till Göran Stütz som på sedvanligt sätt har utgjort en kritisk betraktare och ställt rätt frågor med fingret på de ömma punkterna.

Linköping i juni 2002

Michael Nydén

SAMMANFATTNING

Utgångspunkten för denna studie är en konflikt med förvaltning, medborgare och grundläggande intressen som parter – alla med rättmätiga krav. Konflikten kan illustreras som en triangel i respektive hörn, integritet, effektivitet och byråkrati.

Det första perspektivet på konflikten gäller *integriteten*. I grunden gäller frågan om integritet vem som har rätt att utan mitt medgivande använda information om mig eller mitt liv? I takt med att möjligheterna att lagra och samla information från olika håll blir allt bättre (och billigare) och vi samtidigt i vårt dagliga liv lämnar ifrån oss allt fler och tätare spår, blir också frågan om vem som har rätten att hantera denna information allt mer aktuell.

Det andra perspektivet i konflikten gäller *effektiviteten* hos myndigheter vad avser informationshantering. Trenden går här mot en allt mer centraliserad hantering av uppgifter, där den gyllene regeln är att information bara skall lagras *en gång på ett ställe av en ansvarig*. Motivet för detta är enkelt – om samma information lagras på två eller fler ställen innebär detta uppenbara risker för felaktighet och dessutom oklarheter vad gäller ansvaret för informationen samt kostnaderna för dubbelarbete.

Det tredje perspektivet i konflikten gäller rättssäkerheten inom förvaltningen (*byråkrati*) i relation till informationstekniken. Där byråkratin bygger på hierarki bygger IT-system på subsidiaritetsprincipen (närhetsprincipen), dvs. att det är "den som möter kunden" som skall handlägga kundens ärende.

Förväntningarna på myndigheternas effektivisering med hjälp av IT-verktyg har varit mycket stora under senare år. Det tydligaste exemplet på detta är regeringens förvaltningspolitiska program *En förvaltning i demokratins tjänst* och arbetet med *24-timmarsmyndigheten*. Grundprincipen bakom dessa insatser är dels att medborgaren, d.v.s. den person som söker upp myndigheten, i allt väsentligt skall betraktas som kund och att förvaltningen skall använda samma kvalitetsmätningssystem som t.ex. den privata industrin, dels att all information och alla tjänster som *kan* tillhandahållas elektroniskt också *skall* göra det. Myndigheterna förväntas förädla och utveckla sina tjänster för att slutligen samverka med alla andra myndigheter i ett omfattande nätverk.

Detta innebär bl.a. att information om den enskilda individen kommer att kunna nås och bearbetas av alla myndigheter, även om informationen inte primärt samlats in för deras arbete. Detta underlättas genom att riksdagen antagit ett antal propositioner där frågan om vad som är grundläggande information (och därmed skall vara ett offentligt åtagande) i praktiken har luckrats upp och utvidgats, samt att frågan om vem som skall tolka vad som är grundläggande information har flyttats från riksdagen till regeringen och myndigheterna.

I sammanhanget bör hanteringen av personuppgiftslagen (PuL) noteras, där det EU-direktiv som antagits och som tillkommit för att skydda den personliga integriteten i

Sverige har kommit att ge ett betydligt svagare skydd genom undantag i lagen som införts på grund av myndigheternas informationsbehov och en förmodad konflikt med den svenska offentlighetsprincipen.

I studien redovisas en empirisk undersökning av de Internettjänster som 94 svenska myndigheter erbjuder användaren/"kunden". Myndigheternas hemsidor har granskats med avseende på servicefunktioner och hot mot den personliga integriteten.

Undersökningen pekar på att det är mycket stor olikhet mellan myndigheternas sätt att hantera mediet Internet. Servicegraden är ofta låg – 16 procent av myndigheterna kommer upp i hälften eller mer av de undersökta typerna av service. Det råder också en till synes stor omedvetenhet hos myndigheterna vad gäller integritetsfrågor i allmänhet och personliga uppgifter i synnerhet. Det visar sig också att det inte finns något samband mellan graden av service och graden av integritetshot – det går utmärkt att erbjuda hög service på nätet utan att för den skull begära information om den som söker service.

Det problematiska med denna utveckling är att den bygger på en rationalistisk teori om hur förvaltningar skall fungera. Denna teori saknar i huvudsak empiriskt stöd – medan stödet för en motsatt teori är stark. Myndigheter fungerar på sätt som organisationer i allmänhet fungerar. Detta innebär att de hanterar informationsverktyg och ny teknik utifrån ett nyttoperspektiv, dvs. teknik implementeras när den behövs för att myndigheten skall kunna fullgöra sina uppgifter. Detta stärks också av den empiriska studien där spridningen av myndigheters användning av IT är mycket stor.

Man kan inte generellt förvänta sig att myndigheterna kommer att klara av att hantera information om medborgarna, d.v.s. användarna/"kunderna" på ett förtroendeingivande sätt. Empiriskt stöd för detta saknas inte. Myndigheternas hantering av bl.a. virusattacker och datahaverier stödjer uppfattningen att denna typ av teknik ofta är dåligt förankrad i myndighetens organisation även om konsekvenserna av avbrott i tekniken får allvarliga konsekvenser.

Konsekvensen av den utveckling som granskas i studien är att informationen om enskilda personer snabbt riskerar att spridas på många fler händer än vad som idag är fallet och att detta skapar nya risker för såväl individer som samhälle. Detta är olyckligt ur ett försvarsperspektiv. Ur detta perspektiv är det ett grundläggande krav att känslig myndighetsinformation om medborgare inte kan nås, störas eller förändras av någon annan – vare sig "den andra" är en främmande makt, en kriminell organisation eller "bara" en hacker. Studier av myndigheters hantering av data tyder inte på att detta krav kan uppnås – snarare ökar risken snabbt vid skapandet av nätverk där många myndigheter delar på samma grundinformation.

Den yttersta konsekvensen av den här redovisade konflikten kan bli att medborgarna tappar förtroendet för förvaltning och rättssäkerhet och känner sin personliga integritet än mer hotad än vad som är fallet idag, samtidigt som samhällets sårbarhet ökar på grund av att man utgår från en i grunden felaktig teori om myndigheters och andra organisationers beteende.

THE 24-HOUR THREAT

– The transformation of government administration and the threat against the citizens personal integrity.

A SUMMARY

By Michael Nydén, Ph.D in Political Science

This study's point of departure is a conflict between three sides with legitimate interests – the government administration, citizens and basic human rights. The conflict could be characterized as a triangle with the corners integrity, efficiency and bureaucracy.

The first perspective on the conflict deals with *integrity*. The question is, basically, who has the right to use information about me or my life without my consent? As it becomes cheaper and easier to collect and store information, and as we simultaneously leave increasing numbers of electronic traces of our daily lives, this question becomes more and more pertinent.

The second perspective deals with *efficiency* within government agencies as regards information technology. The trend here is towards increasing centralization. The golden rule of information is that it should be stored only *once*, in *one* place and by *one* responsible agency. The motive for this is simple – if the same piece of information is stored in two or more places, the risk is imminent that there will be errors, and also ambiguities with regard to responsibility. There will also be increased costs.

The third perspective deals with the concept of due process in government agencies in relation to information technology. The basic problem here is that while *bureaucracy* is based on the principle of hierarchy, information technology is based on the principle of subsidiary,

which implies that whoever meets the "customer", should also make the pertinent decision. In recent years, the expectations of more efficient government information technology have been very high. The most obvious example in Sweden has been the government's program *An administration in the service of Democracy*, and also the work with e-government (*The 24-hour agency*). The basic principles behind these programs have been that citizens should be treated as customers and that the administration should use the same tools of quality assurance used by private organizations. It is further stated that all information and services that *can* be delivered by electronic means also *should* be delivered in this manner. The government agencies are expected to refine and redevelop their services, and the final goal is that all agencies should be part of a central administrative network.

This means, among other things, that information regarding a private individual can be reached and processed by a large number of agencies – and that this would also hold for information not primarily collected for use by these agencies. This process has been accelerated by the fact that the Swedish Parliament has passed a bill defining the basic information of society. This decision has also resulted in a transfer of competence, such that it is now the government and not the parliament that

determines what constitutes basic information. This competence can also be further transferred to government agencies.

In this context, the Swedish handling of the European Union's directive regarding personal integrity and information should be noted. The Swedish legislation resulting from the directive is considerably weaker than the directive itself, insofar as an exception to the principle of consent has been granted if the intended user of information is a government agency that requires the information in order to carry out its administrative duties.

This study contains an empirical investigation of the web-sites of 94 Swedish government agencies and the services they offer the citizenry. The agencies' web-sites have been examined with regard to services and with regard to threats to personal integrity.

The investigation shows a great difference between different agencies' ways of handling the Internet media. The degree of service offered the visitor is often low – 16 percent of the agencies investigated fulfil half or more of the criteria set for service. There is also a high degree of unawareness with respect to personal integrity. Only two of the agencies have some sort of statement concerning personal integrity and use of information obtained through Internet browsing. Furthermore, there is no evident relationship between a high degree of service and threats to personal integrity. It is quite possible to offer a high degree of service without collecting personal information from the visitor.

The problem with this development is that it is based on a rationalistic theory of how administrations work – a theory lacking empirical evidence. Moreover, there is substantial evidence supporting the opposite stance, i.e., – that government agencies function in the same way as most organisations. This also means that they tend to utilise information tools and new technology from a utilitarian

standpoint – not on the basis of policy. Thus, new technology is implemented when it is needed in order for the agency to complete its tasks. This is also supported by the empirical study that shows large diversity as regards agencies' use of Internet tools.

Further, it is not expected that agencies can handle citizen's personal information in a secure manner. Empirical support for this position is not lacking. The way several agencies have handled virus attacks and computer breakdowns confirms the position that this kind of technology is often poorly supported by management and the organisation. This seems to be true even if the consequences of technical breakdowns are serious.

The consequence of the development discussed in this study is that personal information on private citizens is at risk for being dispersed to a considerably larger number of users than at present, and that this will constitute new risks for private citizens as well as society as a whole. From this point of view, it is a basic demand that sensitive information regarding private citizens must not be reached, disturbed or changed by any person other than the intended user – regardless of whether this "Other" is a foreign power, a criminal organization or "just" a hacker. This study of government agencies' handling of information technology implies that this demand cannot be met at present. It is quite likely that the risk will increase sharply if a large number of agencies are connected in a network and share the same basic information.

The final consequence of the conflict presented here might well be that citizens will lose trust in society's administrative structures and also feel their personal integrity more threatened than what is the case today. This will occur at the same time as society's vulnerability increases due to implementation of an erroneous theory of rational behaviour in governmental and other organisations.

FÖRVALTNING I FÖRVANDLING

Ambitionerna för svenska myndigheter i fråga om delaktighet i samhällslivet är höga. Regeringen anger uppdraget:

Den statliga förvaltningspolitiken syftar till att skapa organisations-, styr- och ledningsformer som ger förutsättningar för att de tre grundläggande värdena demokrati, rättssäkerhet och effektivitet skall få genomslag i hela förvaltningen.¹

Detta mål innebär att förvaltningen skall uppfylla en rad krav – den skall vara öppen för medborgarna och Internet skall tas till hjälp för att ge ökat informationsutbud och ökade tjänster. Förvaltningen skall vidare ha en hög kvalitet – för att behålla ett medborgerligt förtroende, för att åstadkomma tillväxtförutsättningar och för att fungera föredömligt i det internationella samarbetet. Enligt regeringen skall förvaltningen också fungera som en föredömlig IT-användare med bl.a. följande mål:

Statliga myndigheter bör ha en webbplats på Internet med en hemsida av hög kvalitet som är kopplad till Sverige Direkt. Hemsidan bör snabbt leda till grundläggande fakta om myndigheten och annan för medborgarna intressant sakinformation. Den bör också möjliggöra för medborgarna att till myndigheten sända in uppgifter och initiera ärenden elektroniskt etc.²

Än starkare framstår regeringens krav på myndigheterna i samband med förverkligandet av den s.k. 24-timmarsmyndigheten:

Regeringen har också slagit fast att målet för myndigheternas utvecklingsarbete är: att all information och alla tjänster som kan tillhandahållas elektroniskt skall göra det. Två villkor är knutna till detta mål. För det första skall övergången till e-tjänster leda till bibehållen eller ökad kostnadseffektivitet. För det andra skall tjänsterna utformas och tillhandahållas på ett sådant sätt att de kan användas av alla och inte utestänga grupper av medborgare.³

När regeringen anger vilka åtgärder som förvaltningen skall vidta för att nå dessa mål är det flera punkter som har en direkt koppling till IT-utveckling:

- 24-timmarsmyndigheten
- en elektronisk ingång till offentlig information
- ett Internetbaserat informationssystem för företagare
- säker elektronisk överföring av dokument och meddelanden
- användningen av elektroniska signaturer.

Även andra punkter på åtgärdslistan, t.ex. "samhällets grundläggande information" eller

1) Regeringskansliet, 1998: En förvaltning i demokratins tjänst, 7

2) Ibid, 13

3) Statskontoret, 2001: Utveckling av 24-timmarsmyndigheter – lägesrapport december 2001, 2

”samverkan mellan statliga och kommunala myndigheter” har en koppling till IT-frågor. Det är mot bakgrund av detta inte en överdrift att påstå, att regeringen förväntar sig att den statliga (och kommunala) förvaltningen skall fungera som föredömen och spjutspetsar i användningen av avancerad informationsteknologi.

Samtidigt som detta konstateras måste man ställa sig frågan – ur vilket eller vems perspektiv sett är denna utveckling önskvärd? Det är inte givet att en effektiv förvaltning är det enda önskvärda eller att en effektiv förvaltning automatiskt leder till en effektiv demokrati. Det kanske till och med kan vara tvärtom?

Uppenbarligen finns det tre tydliga krav som delvis står i konflikt och som alla påverkar förvaltningens roll i samhället i allmänhet och förvaltningens förhållande till informationsteknik i synnerhet. Dessa tre krav är kravet på *integritet*, kravet på *effektiv datahantering* och kravet på en *rättvis och känd process* i byråkratin. Låt oss se hur dessa tre kan förhålla sig till varandra.

Konflikten

Konflikten kan beskrivas som hur olika rättmätiga intressen från olika aktörer hamnar på kollisionkurs.

Integritet

Ur medborgarens perspektiv är integriteten en hörnsten i samhällslivet. Integritet definieras här som rätten att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligt störande ingrepp.⁴ I det politiska perspektivet innebär detta att staten och ”samhället” inte har rätt att störa den enskilda personens göranden och låtanden i andra fall än där detta är klart motiverat av samhällets regelverk.

I ett djupare perspektiv kan man utvidga diskussionen till att gälla frågan om vem som äger rätten till information om personen. För tjugo eller trettio år sedan hade denna diskussion måhända känts ovan och konstlad, men i takt med att frågor rörande upphovsrätt och t.ex. rätten till patent på levande material blivit allt vanligare har även denna dimension av integritet blivit allt mer aktuell. I USA, som ofta är föregångsland i frågor av denna karaktär, har bl.a. frågan om vem som äger telefonnummer, namn m.fl. personligt unika identifikatorer väckts med varierande slutsatser.⁵

I grunden gäller frågan om integritet vem som har rätt att utan mitt medgivande använda information om mig eller mitt liv. I takt med att möjligheterna att lagra och samla information från olika håll blir allt bättre (och billigare) och vi samtidigt i vårt dagliga liv lämnar ifrån oss allt fler och tätare spår, blir också frågan om vem som har rätten att hantera denna information allt mer aktuell.

I regeringsformen står att ”den offentliga makten skall utövas med respekt för ... den enskilda människans frihet och värdighet”, medan de lagar som styr hälso- och sjukvården, socialtjänsten och omsorgerna om psykiskt utvecklingsstörda med smärre variationer använder formuleringarna ”respekt för självbestämmande och integritet”. Personlig integritet har därför nära samband med människans *värdighet*.

Nyligen har en utredning, *Integritetsutredningen*, lagt fram ett förslag om Lag om skydd för personlig integritet i arbetslivet (LIA), där det bl.a. föreslås att arbetsgivare inte skall ha rätt att utan särskilda skäl ta del av arbetstagares e-post, genomföra tester eller prov av integritetskränkande karaktär på arbetsplatsen.⁶

4) Nationalencyklopedin, nätupplagan 2001-11-06

5) Wells Branscomb, A., 1994: Who owns information?

6) SOU 2002: 18: Personlig integritet i arbetslivet

Effektivitet

Statens krav på att myndigheterna skall vara effektiva är tydliga och klart formulerade. "Kravet på effektivitet innebär att förvaltningen skall åstadkomma avsedda resultat och uppnå de mål som fastställts av statsmakterna och att detta skall ske kostnadseffektivt."⁷ I detta krav som det är formulerat i verksförordningen framgår bl.a. att myndigheterna skall "verka för att myndigheten genom samarbete med andra myndigheter och på annat sätt tar till vara de fördelar som kan vinnas för staten som helhet".⁸

Sett ur perspektivet informationsteknik/IT kan detta krav få stora konsekvenser om det ställs till sin spets. Eftersom alla myndigheter i någon del av sin verksamhet har en enskild som föremål för sina aktiviteter – vare sig det är i form av föremål för beslut eller i form av kunskapskälla eller på annat sätt – innebär detta att det alltid kommer att finnas stora fördelar med samordning av information om vederbörande. Det går ganska enkelt att konstatera att den maximala effektiviteten när det gäller information om denne eller denna uppnås när informationen om medborgaren finns lagrad på ett, och enbart ett, ställe, där samtliga myndigheter hämtar denna information. Så är ju också fallet idag när det gäller en del register – folkbokföringsregistret kan anföras som exempel. Andra exempel är passregister och skatteförvaltningsregistret.

Det finns ingen anledning att tro att trenden mot allt mer centraliserade register skall ändras – tvärtom. All erfarenhet från datalager och databashantering framhåller en gyllene regel – information skall bara lagras *en* gång på *ett* ställe av *en* ansvarig. Motivet för detta är enkelt – om samma information lagras

på två eller fler ställen innebär detta uppenbara risker för felaktighet och dessutom oklarheter vad gäller ansvaret för informationen samt kostnaderna för dubbelarbete.

En annan infallsvinkel på effektivitetsproblemet är att man inom den politiska sfären nu allt mer lånar verktyg och begrepp – ja hela paradigmet – från den kommersiella sfären. Regeringen framhåller t.ex. i arbetsprogrammet för en bättre förvaltning att "(r)egeringen kommer därför att genomföra åtgärder för att bl.a. stimulera förvaltningen till att mer systematiskt arbeta med att utveckla den totala kvaliteten i sin verksamhet. Därmed avses ett systematiskt kvalitetsarbete som baseras på de kriterier som i dag anses känneteckna framgångsrika organisationer, såsom kundorientering, engagerat ledarskap, personalens delaktighet, kompetensutveckling, långsiktighet, ständiga förbättringar, lära av varandra, samverkan m.m."⁹

Problemet är bara här att medborgaren inte är kund! En kund är en aktör som återfinns på en marknad med fritt in- och utträde och där det dessutom ofta förutsätts perfekt information om marknadens tillvägagångssätt. En medborgare har inte som kunden möjligheten att lämna marknaden (om man inte röstar med fötterna) och kan så gott som aldrig ha samma informationsmängd om verksamheten som politiker eller tjänstemän.

Byråkrati

Byråkrati används oftast i dagligt tal som en lätt nedsättande beskrivning på ett stelt och opersonligt förhållningssätt. I grund och botten kanske detta är korrekt, men utgångspunkten för resonemanget är egentligen rätts-säkerhet och skydd för den enskilda. "Modern

7) Regeringskansliet, 1998, 6

8) Verksförordning (1995:1322), § 6:2

9) Regeringskansliet, 1998, 5

byråkrati” förknippas ofta med en av sociologins förgrundsgestalter, Max Weber, som formulerade ett antal grundsatser om byråkratiens egenskaper.

Weber karakteriserade byråkratiens funktioner med hjälp av ett antal särdrag, som översiktligt kan beskrivas enligt följande:

- 1) *Specialisering i olika områden genom fastställda kompetensregler.*
- 2) *Tjänstehierarki och instansordning där det råder ett subordinationsförhållande.*
- 3) *Ämbetsutövning baserad på skrivna dokument.*
- 4) *Specialutbildning som förutsättning för ämbetsutövning.*
- 5) *Ämbetsutövning som en heltidssyssla.*
- 6) *Regelstyrd verksamhet.*¹⁰

Vi kan till dels känna igen en del av Webers särdrag med dagens debatt om processorientering av verksamhet och koncentration till kärnverksamheter, men det viktigaste i Webers krav är ändå *förutsägbarheten*. En förvaltning som har sin utgångspunkt i särdrag av den typ som beskrivits ovan är transparent (“genomskinlig”) i den meningen att det är relativt lätt för en utomstående att se vilka kompetensområden som gäller och att ta reda på vilka regler som styr verksamheten. I byråkrati i denna mening ingår också *dokumentationen* som en viktig faktor – händelser skall dokumenteras (tjänsteanteckningar, korrespondens, protokoll) och dokumenten skall i sig ordnas (diarieföras, registreras). Vidare skall dessa dokument och arkiv med vissa klart angivna undantag vara *allmänt tillgängliga*.¹¹ Eftersom verksamheten dessutom är regelstyrd är den ställd under regelskaparens

kontroll, vilket är ytterligare ett sätt att förhindra godtycke i hanteringen av medborgaren.

Just frånvaron av godtycke har varit ett framstående drag i försvaret för den regelstyrda förvaltningen – även om resultatet har kunnat bli brist på effektivitet.

Det är lätt att se att ett tilltagande bruk av informationsteknologiska verktyg går på tvärs emot de karakteristika som kännetecknar en byråkrati enligt ovan. Där byråkratin bygger på hierarki bygger IT-system på subsidiaritetsprincipen (närhetsprincipen), dvs. att det är “den som möter kunden” som skall handlägga kundens ärende. Detta innebär också att ett stort ansvar läggs på den enskilda tjänstemannen – och också en förväntan om generalisering. Cecilia Magnusson-Sjöberg har i sin avhandling framhållit de konfliktlinjer som finns mellan IT och offentlighetsprincipen:

*Vad gäller datoranpassningen av offentlighetsprincipen är det aktuellt att göra avvägningar mellan främst följande: offentlighet och sekretess, offentlighet och effektivitet, offentlighet och integritet samt offentlighet och gallring: I ett snävare perspektiv – med anknytning till myndigheternas utnyttjande av IT – finns vidare intressekonflikter i form av en god offentlighetsstruktur (med krav på organiserad informationshantering) å ena sidan och användaranpassade system som möjliggör (t.o.m. understödjer) för handläggarna att t.ex. utväxla personliga meddelanden med varandra å andra sidan.*¹²

En mer allvarlig konfliktlinje mellan IT och byråkrati går emellertid mellan ämbetsutövning baserad på skrivna dokument å ena sidan och specialistutbildning för att sköta ett ämbe-

10) Magnusson-Sjöberg, C., 1992: Rättsautomation – särskilt om statsförvaltningens datorisering, 85

11) Detta har historiskt främst gällt svenska förhållanden med vår betoning på offentlighetsprincip och allmän handling.

12) Magnusson-Sjöberg, C., 1992, 410–411

te å den andra. Det finns idag en trend inom statsförvaltningen att mer och mer komplicerade IT-stöd tas i bruk där programmen/stödet självt i någon mening fattar beslut. Formellt fattas beslutet fortfarande av tjänstemän, men idag torde det finns ett flertal exempel från försäkringsärenden, studiestöd eller skattefrågor, ersättningsfrågor och pensioner där de enskilda tjänstemännen inte själva kan förklara de resultat som IT-systemet ger dem att besluta om. Det grundläggande problemet här är att insynen i det kritiska skedet i framtagandet av IT-stöden – systemutvecklingen – förefaller svagt och överlämnat åt tekniker.¹³

Konfliktens sammantagna dimensioner

Utifrån de ovan skisserade förväntningarna på förvaltningen kan man konstatera att relationen mellan IT och myndigheter är långt ifrån oproblematiske:

- integritetsaspekterna i samhället blir fler och fler i takt med att volymen personlig information som är teoretiskt tillgänglig för många ökar;

- förvaltningen utsätts för ett allt hårdare tryck för att uppnå effektivitet och därmed samordna informationsinhämtning och lagring;
- informationsteknologiska verktyg har en tendens att hamna i konflikt med den traditionella synen på vilka värden som skall styra förvaltningen.

Vad innebär då detta för myndigheter och medborgare? Vilka blir konsekvenserna när de olika intressena och kraven möts i en punkt – mötet mellan medborgare och myndighet? Detta är centrala frågor i ett civilt samhälle och belyser också en typ av fredskris som baseras på förändrat förtroende mellan medborgare och statsmakt. Styrelsen för psykologiskt försvar (SPF) har i en serie av analyser studerat just hur olika påfrestningar i samhället påverkar medborgares förtroende för myndigheter och myndigheters arbete, och denna studie anknyter till denna tradition även om den påfrestning som här analyseras ännu inte har känts av fullt ut.

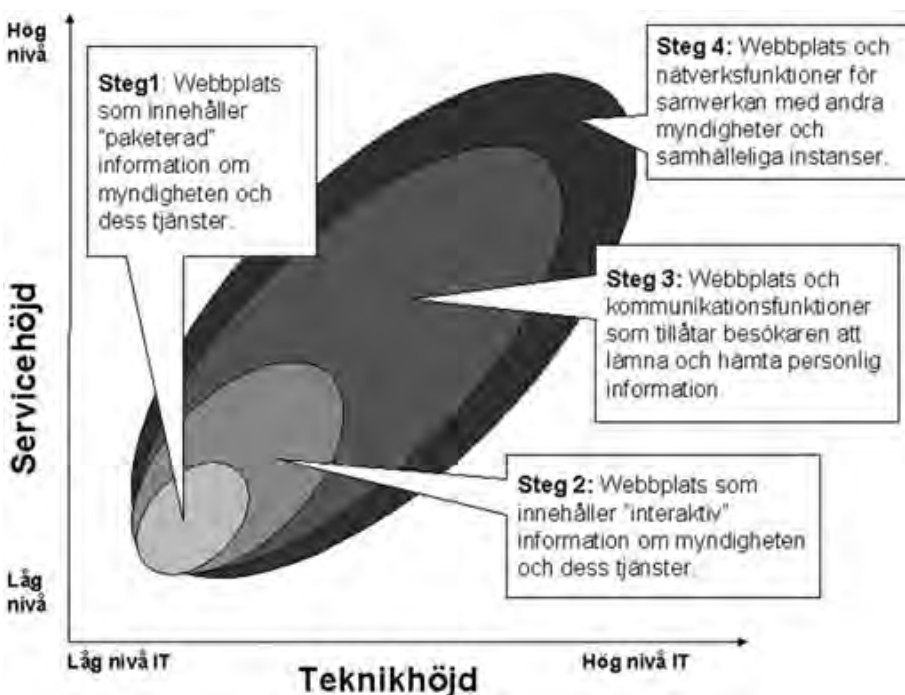
13) Ibid, 510

FÖRVÄNTNINGARNA PÅ MYNDIGHETERNA

Serviceförväntningar

Det politiska systemets förväntningar på svenska myndigheter är höga. Verksamheten skall gå fort, vara kvalitetsfylld och helst utföras med hjälp av IT. Men vad innebär detta i praktiken? Det tydligaste exemplet på praktiska konsekvenser kan vi se om man ser till hur Statskontoret har valt att operationalisera begreppet *24-timmarsmyndighet*.¹⁴

I det första steget förutses webbplatser som i stort sett enbart är statiska, dvs. innehåller information om myndigheten som myndigheten själv valt att lägga ut. Normalt kan man på denna teknisknivå när man söker upp myndigheten inte göra annat än hämta information för att sedan agera/interagera med myndigheten på traditionellt sätt. Här handlar det egentligen mest om metatjänster, dvs. de



Figur 1. Beskrivning av 24-timmarsmyndighetens utveckling (Statskontoret).

14) Denna operationalisering är inte oomstridd. Riksrevisionsverket har i sitt remissvar på Statskontorets förslag på kriterier på 24-timmarsmyndighet bl.a. konstaterat att man anser att Statskontoret misstolkat de ursprungligen australiensiska kriterierna. Huvudkritiken här gick ut på att det som Statskontoret betraktade som en trappa i stället kunde ses som nivåer som myndigheterna kunde välja att lägga sig på.

tjänster som erbjuds användarna är information om andra tjänster som man måste kontakta myndigheten för att ta del av.

I det andra läget ligger tyngdpunkten på interaktiv information. Här skall den enskilde kunna precisera sitt önskemål och få en mer personlig information utan att för den skull genomföra ärendet via myndighetens hemsida. Här handlar det om stödsystem för sökning, falldatabaser, information som tas fram efter angivande av relevanta parametrar om användaren m.m. Exempel kan vara system som räknar ut pensionen om man anger de uppgifter som man tidigare fått sig hemsänt i t.ex. ett orange kuvert.

I det tredje steget inträffar den verkliga förändringen för användaren ur integritetsperspektiv. Nu blir webbplatsen ett myndighetskontor där jag kan anhängiggöra mina ärenden, följa dem, kontrollera arbetsprocessen och få slutresultatet av interaktionen redovisad. I detta läge är webben en kommunikationsform mellan myndigheten och mig som identifierad person. Exempel skulle kunna vara möjligheten att söka bygglov direkt över Internet och därvid få reda på vem handläggaren är och vilka uppgifter jag måste skicka in m.m.

Det fjärde steget inriktar sig egentligen inte så mycket på relationen medborgare-myndighet som på relationen myndighet-myndighet. Avsikten är här att medborgaren inte skall behöva fundera på vilka myndigheter som eventuellt ytterligare blir involverade i ärendet – detta skall systemet klara av genom att all relevant information om medborgaren finns lagrad på identifierade platser som är sammanlänkade. Detta innebär inte att all information finns i en databas – men väl att en viss information enbart finns i en databas.

Statskontoret skiljer i sitt arbete mellan tre olika typer av information som blir aktuell för utveckling för att alla myndigheter skall nå det fjärde steget i kedjan. Dessa framgår nedan:¹⁵

”Utbudet av ärederelaterad information”

Graden av interaktivitet kring ärenden kan åskådliggöras med följande fingerade utvecklingsnivåer för ärederelaterad information involverande exempelvis tillämpning av informationsutbyte medelst ärendeblanketter:

”titta” Aktuell information lämnas om exempelvis ärendegången, tillämpliga regelverk och svar på vanliga frågor.

”beställa” Möjlighet att beställa blanketter, informationsmaterial m.m. Distribution med reguljär post.

”hämta” Möjlighet att hämta hem blanketter och informationsmaterial som nedladdningsbara filer för lokal utskrift. Blanketter fylls i manuellt. Distribution till myndigheten med reguljär post.

”utföra” Möjlighet att fylla i t.ex. blanketten på skärmen före lokal utskrift. Distribution till myndigheten med reguljär post.

”interagera” Möjlighet att fylla i t.ex. blanketten på skärmen före lokal utskrift. Online beräknings- och kontrollprogram som stöd vid ifyllandet. Distribution till myndigheten med reguljär post.

”inlämna” Möjlighet att fylla i t.ex. blanketten på skärmen. Online beräknings- och kontrollprogram som stöd vid ifyllandet. Sändfunktion som online ärendeinitiering.

15) Statskontoret, 2000:21: 24-timmarsmyndigheten – förslag till kriterier för statlig elektronisk förvaltning i medborgarnas tjänst.

"kontrollera" Möjlighet att följa ingivet ärende i handläggningsprocessen. Möjlighet till online komplettering och handläggardialog vid behov.

"slutföra" Möjlighet att online ta del av ärendebeslut. Vägledning för ev. besvär/överklagan i form av t.ex. online kontakt med högre instans.

Utbudet av allmäninformation på webbplatsen

Bredden i utbudet av allmän information är avgörande för hur långt en 24-timmarsmyndighet kommit i utvecklingstrappan. Ordningföljden i följande insatsområden är inte kritisk.

Myndighetens instruktion, regleringsbrev och regeringsbeslut som rör verksamheten, årsredovisning, budgetunderlag och verksamhetsplaner samt styrelseprotokoll och viktigare beslut av myndigheten.

Organisationsöversikt med kontaktinformation till chefer, samt personallistor med telefonnummer, e-postadresser m.m. (Utläggningen av listor måste lämplighetsbedömas.)

Översikt och kontaktinformation rörande pågående projekt, utredningar m.m., som syftar till att öka tjänsteutveckling och servicetillgänglighet.

Myndighetens remissvar i sökbar form.

En elektronisk version av utgivna publikationer (rapporter, utredningar m.m.) samt möjlighet för online-beställning av tryckta publikationer.

Redovisning av vilka register som myndigheten för och regler för tillgång till dem.

Redovisning av myndighetens olika former av deltagande i EU-arbetet.

Möjlighet för omvärlden att ta del av och söka i diariet.

Proaktivt förhållningssätt inkluderande möjlighet att prenumerera på såväl allmäninformation (pressmeddelanden, nya rapporter etc.) som specifik serviceinformation (sista ansökningstiden för bidrag etc.).

Övergripande informationspresentation

I takt med myndigheternas inträde i nätverksamhället växer kraven på informationens synliga layout och bakomliggande struktur. Ordningföljden i följande insatsområden är inte kritisk.

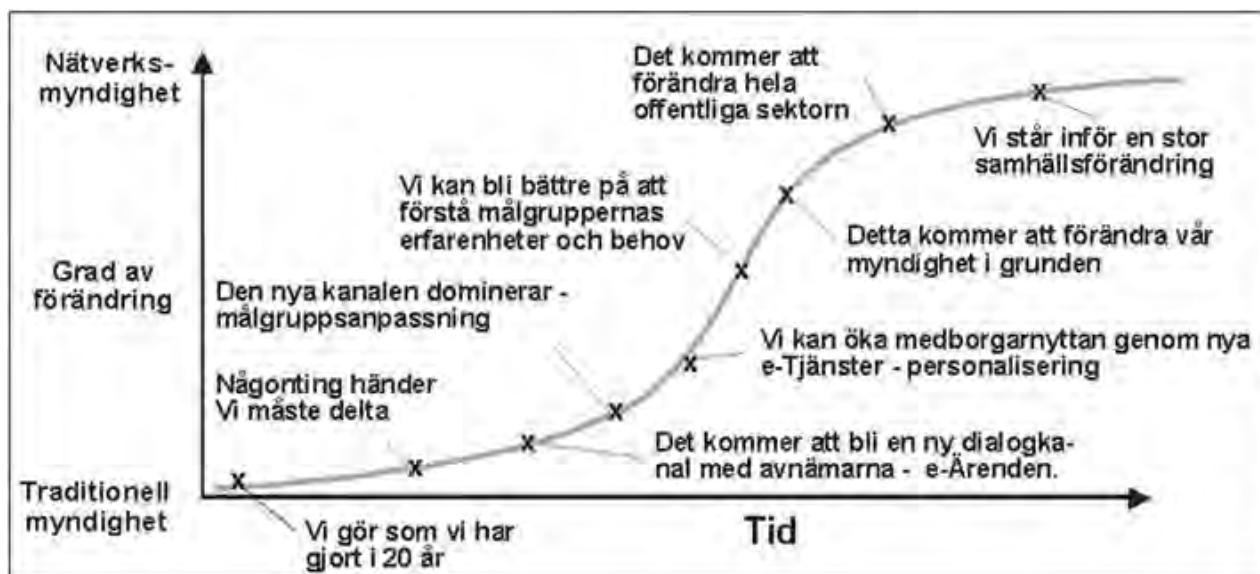
Det totala informationsutbudet är organiserat efter användarens behov snarare än efter myndighetens verksamhetsorganisation. Relevanta länkningsar till andra myndigheter och samhällsinstanser.

Alla myndighetens dokument är sökbara via sökmotor tillhandahållen på webbplatsen.

Webbplatsen är producerad med standardiserade fältkoder (W3C), speciellt beträffande märkning för tillgänglighet. Vid behov tillhandahålls en ren textversion för bl.a. användare med röstsyntesbrowser.

För att underlätta för bl.a. användare med "smalbands"-uppkoppling är användningen av bilder och animeringsteknik minimal. Stora filer i formatet PDF finns också uppdelad i portionsförpackningar (t.ex. kapitelvis). "

Som framgår av uppräkningsen är det knappast fel att prata om virtuella myndigheter när alla myndigheter kan sägas uppfylla dessa krav. Det torde tvärtom vara så att de myndigheter vi har idag inte kommer att vara desamma som morgondagens när den ovan beskrivna förvandlingen är genomförd. Detta är också en del i Statskontorets vision



Figur 2. Förvaltningens förvandling (Statskontoret.)

som den redovisas i en bild av förändringsarbetet (figur 2).¹⁶

Det kan vara värt att notera att i visionen så kommer den stora samhällsförändringen efter den tekniska förändringen. Man kan förstås också tänka sig en annan ordning.

Just det fjärde steget i utvecklingen är kanske det allra viktigaste – det är här de idag åtskilda myndigheterna knyts ihop till ett stort myndighetsnätverk. Statskontoret självt sammanfattar tanken under begreppet "Tjänstesamverkan":¹⁷

Tjänstesamverkan

I många ärenden, t ex ansökningar om bidrag och tillstånd, måste den ansvariga myndigheten ha information som finns registrerad hos andra myndigheter eller privata aktörer. Det finns t ex ett 50-tal olika ärendetyper för vilka det krävs personbevis. Idag måste den sökande själv i de flesta fall hämta sådan kompletterande information och bifoga sin ansökan. För att kunna ge bättre service, förenkla handläggningen och förkorta tiden till beslut måste varje myndighet se till att hämta den infor-

mation som behövs för ett ärende som redan finns lagrad hos andra aktörer genom direkt överföring från befintliga register hos andra myndigheter, banker etc.

Samtidigt ser Statskontoret också hinder för denna utveckling, framförallt i fråga om kompetenser och utvecklingskostnader:¹⁸

Kostnaderna för enskilda myndigheter att själva etablera e-tjänster är höga och ställer stora krav på kompetens. En gemensam infrastrukturtjänst blir därför särskilt viktig för förvaltningens mindre aktörer, dvs. mindre myndigheter, landsting och de flesta kommuner. Dessa befinner sig ofta i en situation, där de inte har råd eller egen kompetens att på egen hand utveckla e-tjänster. För denna grupp är det därför av särskilt stor vikt att en gemensam infrastrukturtjänst kommer fram. Men tjänsten är även viktigt för de stora aktörerna genom att de kan dra nytta av de ekonomiska skalfördelar som en gemensam infrastrukturtjänst innebär i jämförelse med att utveckla egna lösningar.

16) Ibid, avsnitt 2.2.1

17) Statskontoret, 2002

18) Ibid, 15–16

Det måste i detta läge ställas frågan om det i servicevisionen ryms självständiga myndigheter, eller om det egentligen handlar om en jättelik myndighetsstruktur där olika specialiteter möter en enskilds olika behov genom olika "fronter", men där den bakomliggande informationen är densamma.

Samverkansförväntningar

Förväntningarna på myndigheterna när det gäller samverkan är inte mindre än förväntningarna när det gäller service. Detta kan inte minst märkas i de utredningar som till slut resulterade i propositionen *Ett informationssamhälle* för alla.¹⁹ Grundläggande för denna serie av offentliga utredningar och dokument var att förvaltningen, IT och medborgaren står i fokus. I propositionen konstaterar regeringen bl.a. att argumenten som talar för en samordning av samhällets informationsresurser är starka.²⁰

Utvecklingen av informationstekniken innebär att praktiskt taget all offentlig information kommer att vara elektroniskt producerad, lagrad och distribuerad för att effektivisera den offentliga verksamheten. Särkostnader för att ta fram och leverera information till medborgare och företag blir i det läget små.

I övrigt lutar sig regeringen mot Statskontoret när det gäller utvecklingen av myndigheters interna informationsutbyte. Statskontoret får i och med propositionen ansvaret för att ta fram kriterier för 24-timmarsmyndigheten, där det bl.a. ingår frågor som samverkan mellan myndigheter.

Statskontoret är ovanligt tydligt när det gäller visionen om hur det framtida myndighets-Sverige skall se ut ur den enskildes perspektiv.²¹

Enligt Statskontorets bedömning är just nätverksaspekten en avgörande dimension för definition av elektroniska självservicejänster och därmed för begreppet 24-timmarsmyndighet.

I den första skriften läggs ingen större tonvikt vid det fjärde steget annat än den allmänna formuleringen.²²

Steg 4 *Webbplats och nätverksfunktioner för samverkan med andra myndigheter och samhällsliga instanser.*

I stället läggs stark tonvikt vid kontaktfrågorna med medborgarna. Däremot återkommer Statskontoret till integrationsfrågorna i statusrapporten i december 2001, där man preciserar vilka krav behovet av integration ställer på myndigheterna:

Tjänstesamverkan *I många ärenden, t ex ansökningar om bidrag och tillstånd, måste den ansvariga myndigheten ha information som finns registrerad hos andra myndigheter eller privata aktörer. Det finns t ex ett 50-tal olika ärendetyper för vilka det krävs personbevis. Idag måste den sökande själv i de flesta fall hämta sådan kompletterande information och bifoga sin ansökan. För att kunna ge bättre service, förenkla handläggningen och förkorta tiden till beslut måste varje myndighet se till att hämta den information som behövs för ett ärende som redan finns lagrad hos andra aktörer genom*

19) Propositionen, som föregicks av departementspromemorian SOU 1997:46 Grunddata – i samhällets tjänst, ledde till propositionen 1997/98:136 Statlig förvaltning i medborgarens tjänst. Denna ledde till ytterligare en utredning, Ds 2000:34, Samhällets grundläggande information, som i sin tur ledde till propositionen 1999/2000:86, Ett informationssamhälle för alla.

20) Proposition 1999/2000:86: Ett informationssamhälle för alla, 94

21) Statskontoret, 2000:21

22) Ibid

direkt överföring från befintliga register hos andra myndigheter, banker etc.

Statskontoret är också mycket tydligt vad gäller målen för förändringsarbetet:

Ledning och styrning Regeringen bör lägga fast ett långsiktigt operationellt mål innebärande att vid utgången av år 2005 medborgare och företag i ett enskilt ärende bara skall behöva ha egen kontakt med en myndighet.

Infrastruktur för informationsförsörjning Det är angeläget att etablera en för offentlig förvaltning gemensam infrastrukturtjänst med ett utbud av grundläggande funktioner, som stödjer utvecklingen av 24-timmarsmyndigheter, genom att erbjuda myndigheterna kostnadseffektiva, gemensamma lösningar som behövs vid utvecklingen av e-tjänster. Kostnaderna för den enskilda myndigheten att själv etablera e-tjänster är höga och ställer stora krav på kompetens. En gemensam infrastrukturtjänst blir därför särskilt viktig för förvaltningens mindre aktörer, dvs. mindre myndigheter, landsting och de flesta kommuner. Dessa befinner sig ofta i en situation, där de inte har råd eller egen kompetens att på egen hand utveckla e-tjänster. För denna grupp är det därför av särskilt stor vikt att en gemensam infrastrukturtjänst kommer fram. Men tjänsten är även viktig för de stora aktörerna genom att de kan dra nytta av de ekonomiska skalfördelar som en gemensam infrastrukturtjänst innebär i jämförelse med att utveckla egna lösningar. Exempel på funktioner som på kort sikt kan ingå i den gemensamma infrastrukturtjänsten är grundfunktioner för att t.ex.:

- kontrollera identitet, kontrollera behörighet, kontrollera signatur
- ta emot ärenden/dokument, tidsstämpla, skicka kvittens

- postrum, dvs. lagra, diarieföra, arkivera ärenden/dokument
- hämta, fördela, skicka ärenden/dokument
- söka information, söka e-tjänst
- hantera blanketter
- hantera e-betalning

I ett längre perspektiv är även mer avancerade funktioner tänkbara, t.ex.:

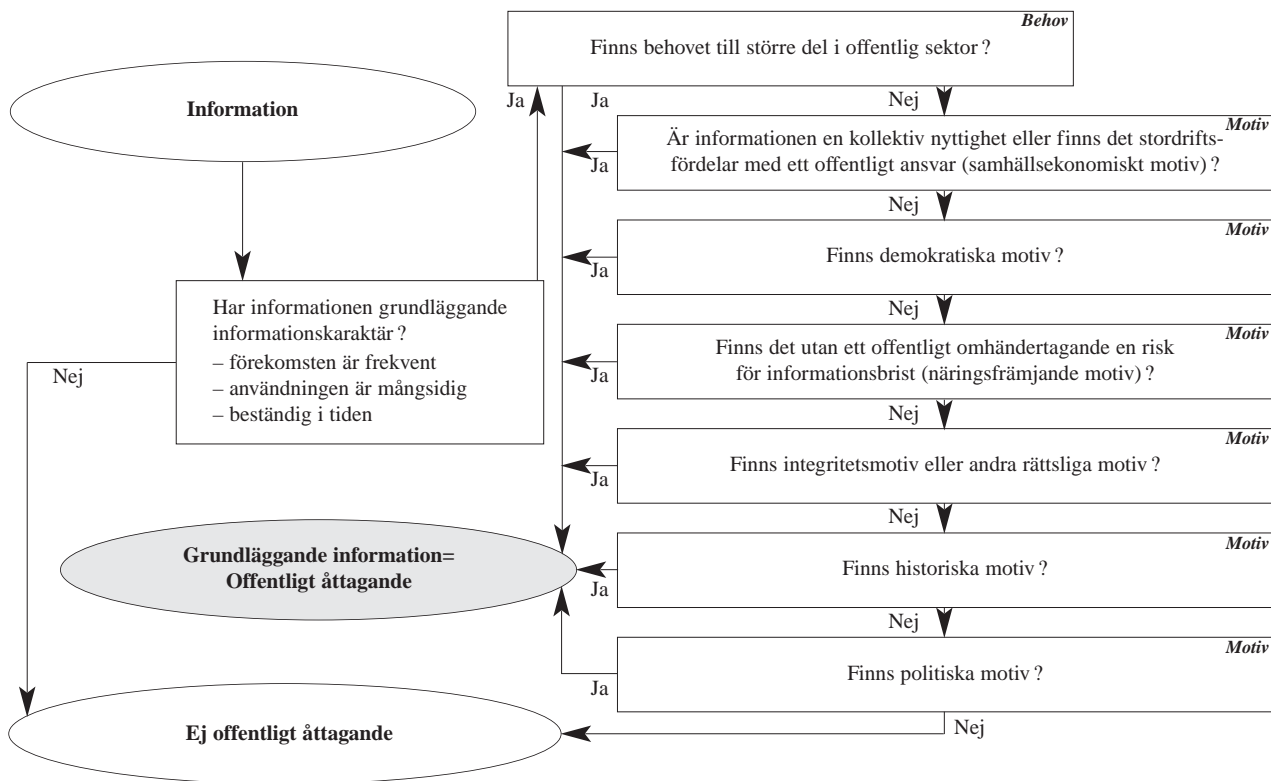
- myndighetsövergripande ärendehantering
- gemensamma processer för t.ex. hantering av olika typer av tillstånd
- förmedling/tillhandahållande av gemensamma vokabulärer för att möjliggöra en gemensam begreppsapparat och standardiserade meddelanden, vilket är en förutsättning för automatiserat informationsutbyte över myndighetsgränserna.

Det kan vara värt att dröja något vid denna precisering av steg fyra i 24-timmarstrappan.

Samhällets grundläggande information

Frågan om myndigheternas samverkan inom dataområdet har diskuterats i stort sett sedan ADB gjorde sitt intrång i samhällets verksamhet. Dock vore det fel att påstå att frågan har stått särskilt högt på dagordningen, åtminstone inte förrän under slutet av 1990-talet. Departementspromemorian *Grunddata i samhällets tjänst* från 1997 kan sägas utgöra ett startskott i denna ännu så länge ganska myndighetsinterna diskussion. I promemorian konkretiseras ett antal tankegångar som tidigare förts fram i olika sammanhang till en helhetssyn på när, hur och varför samhället och samhällets institutioner skall ta ett ansvar för insamling av grunddata. Figur 3 som hämtats ur *Samhällets grundläggande information* visar hur utredningen resonerar:²³

23) Ds 2000:34: Samhällets grundläggande information, 44



Figur 3. Vad är grundläggande information? (DS 2002:34, 44.)

Som framgår resonerar utredningen på följande sätt: "Om förekomsten av data är frekvent *eller* om användningen av informationen är mångsidig *eller* informationen är beständig i tiden och något av följande motiv är uppfyllda:

- är informationen en kollektiv nytthet *eller*
- finns stordriftsfördelar med ett offentligt ansvar *eller*
- finns demokratiska motiv *eller*
- finns risk för informationsbrist utan offentligt omhändertagande *eller*
- finns integritetsmotiv *eller*
- finns andra rättsliga motiv *eller*
- finns historiska motiv *eller*
- finns politiska motiv,

då är informationen av grundläggande karaktär och skall vara ett offentligt åttagande."

Man kan självklart fråga sig vilken typ av information som inte skulle falla inom någon av dessa kategorier, men det är att övertolka promemorian. Utredningen framhåller explicit tre prioriterade områden där modellen skall tillämpas – befolkningsinformation, näringsinformation och fastighetsinformation och geografisk information. Andra områden som tas upp är rättsinformation, Sveriges statistiska databaser, nationell vägdata, miljödata och kulturdata.²⁴

Även med denna begränsning är det dock lätt att konstatera att en stor mängd information om människor, företag och olika aktiviteter med detta synsätt skulle komma att falla inom ramen för vad som skall betraktas som sådan information som samhället skall ha ansvar för.

Utredningen föreslår också att ett samverkansorgan mellan myndigheterna – en sam-

24) Ibid, 39–31

verkansnämnd – skall etableras för att information inte skall dubbellagras eller lagras på ett sådant sätt att den inte kan användas av andra myndigheter. Även en gemensam begreppsapparat föreslås för att underlätta för myndigheter att använda varandras insamlade och lagrade information.

Regeringen har (ännu) inte agerat fullt ut på förslagen i promemorian, men det går att se mycket tydliga paralleller till hanteringen av 24-timmarsmyndigheten. Ett exempel på detta är när statssekreteraren i Justitiedepartementet redovisar regeringens vision med arbetet kring förändringen av förvaltningen:²⁵

Målet är en ärendehandläggning som tar hänsyn till enskilda medborgares och olika gruppers olika behov och livssituation och inte begränsas av traditionella myndighets- och ansvarsgränser. Om flera myndigheter och andra organ behöver medverka i ett ärende, så skall detta vara ett gemensamt ansvar för alla berörda, inte ett byråkratiskt problem för medborgaren eller företaget.

Vi talar alltså snarare om offentliga tjänster än om myndigheter. Vi talar kanske inte ens om 24-timmarsmyndigheter, utan om offentlig förvaltning som en 24-timmarsmyndighet.

Statskontoret konstaterar ett stort behov av samverkan mellan myndigheter och mellan myndigheter och andra aktörer:²⁶

Vi avser att i det fortsatta arbetet pröva i vad mån det finns skäl att vidareutveckla nuvarande myndighetsorienterade modell för kapitalförsörjning av utvecklingsinsatser. Det är två förhållanden som gör en sådan prövning motiverad. Ett är att livssituationsbaserade tjänster i många fall

förutsätter att myndigheter samverkar med kommuner och/eller landsting i gemensamma utvecklingsprojekt som är av den storleksordningen att de kan behöva lånefinansieras eller behöver göras genom att några få aktörer utvecklar prototyper som ett första steg och att tjänsten därefter ges mer allmän spridning. Livssituationsbaserade tjänster kan också komma att kräva samverkan i utvecklingskedet mellan flera myndigheter och att kostnader och effektiviseringsmöjligheterna fördelas olika mellan de deltagande myndigheterna. Det andra förhållandet rör utvecklingen av gemensam infrastruktur och då i första hand den infrastruktur-tjänst som beskrivs i kapitel 3.2 kan kräva någon form av gemensam finansiering.

Statskontoret för här in begreppet "livssituationsbaserad tjänster", med vilket skall förstås att medborgaren inte skall behöva bry sig om att hitta rätt myndighet för att hantera frågor som ansvarsmässigt berör flera myndigheter:²⁷

Den nya informations- och kommunikationstekniken skapar nya förutsättningar för att åstadkomma ett gemensamt uppträdande i mötet med medborgare och företag utan att förändra de grundläggande ansvarsgränserna mellan olika myndigheter och mellan stat och kommun. Genom en systematisk uppdelning av verksamhetsprocesserna i 'front-office' och 'back-office-funktioner' och olika former av standardisering kan medborgaren kan få tillgång till en samlad tjänst. Därmed behöver han/hon inte längre anstränga sig för att hitta "rätt instans", utan kan ange önskemål och behov med utgångspunkt från livssituationer och problemområden. Genom en digital samverkan både i kontaktfunktionen och i ärendehanteringens kan vi efterhand närma oss visionen om en 24-timmarsmyndighet.

25) En medborgaranpassad statsförvaltning – anförande av statssekreterare Hans-Eric Holmqvist vid konferensen "24-timmarsmyndigheten" den 6 juni 2001.

26) Statskontoret, 24-timmarsmyndigheten, 16

27) Ibid, 11

Tankegodset är här i grunden detsamma som i departementspromemorian om grunddata – myndigheterna skall organisera data så att de kan användas av alla andra myndigheter och frågan om vem som skall samla in och lagra vilka data avgörs av myndigheterna i samverkan. Principen om att data lagras vid källan och endast där är tydlig – information skall enbart hämtas en gång och lagras en gång och ansvaret för hämtning, lagring och uppdatering skall vara tydligt. Tillgången till data från andra aktörer avgörs utifrån kundens (medborgarens) behov och myndighetens behov av information för att tillmötesgå kunden. Eller, som Statskontoret konstaterar:²⁸

För att kunna ge bättre service, förenkla handläggningen och förkorta tiden till beslut måste varje myndighet se till att hämta den information som behövs för ett ärende som redan finns lagrad hos andra aktörer genom direkt överföring från befintliga register hos andra myndigheter, banker etc. I takt med att nya samverkande tjänster utvecklas kommer behovet av informationsutbyte mellan olika offentliga organ att drastiskt öka.

Det är värt att se att Statskontoret lägger ambitionsnivån ännu högre än utredningen. I statskontorets framtid förekommer även överföring av information från icke-offentliga aktörer, t.ex. banker, kommuner och landsting.

Byråkratiska förväntningar

Inledningsvis redovisades regeringens programskrift *En förvaltning i demokratins tjänst* och hur man där hämtat inspiration från det privata näringslivet när det gäller kvalitetsutveckling m.m. Just i fråga om kopplingen IT-förvaltning finns anledning att stanna till. Här

formulerar regeringen såväl höga som tydliga krav på "sin" förvaltning:²⁹

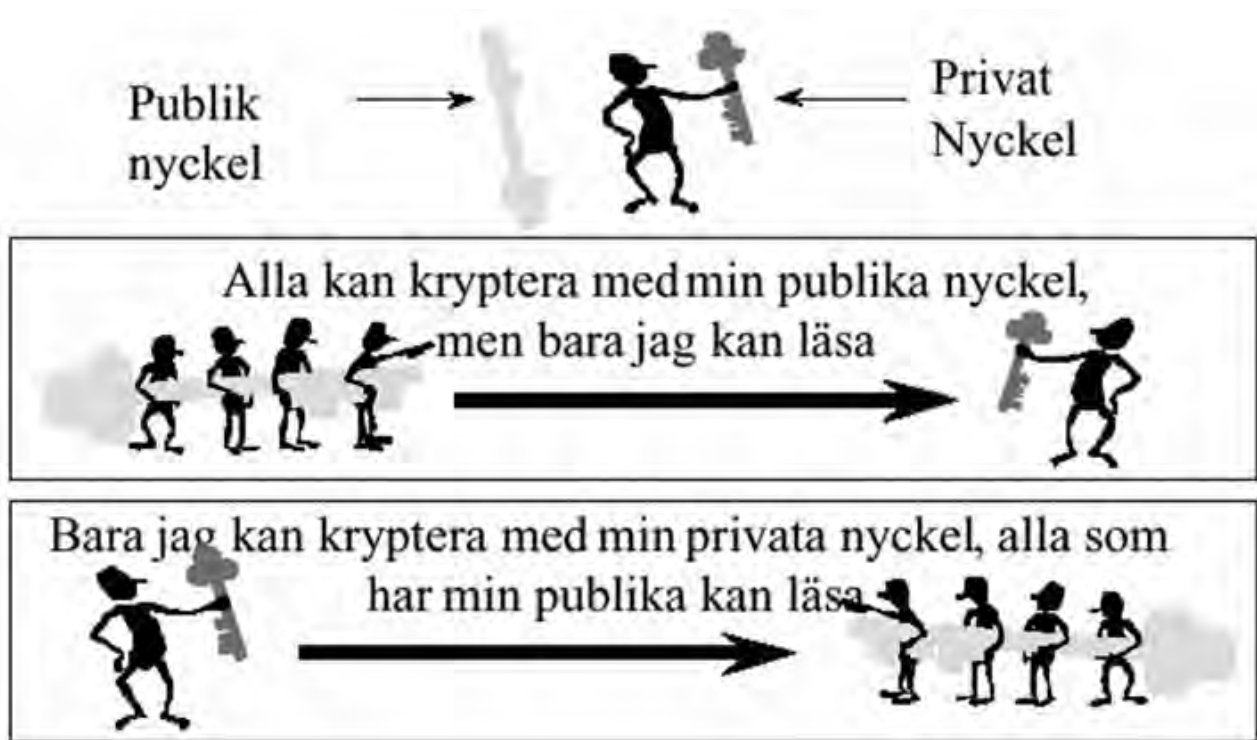
Det främsta redskapet för att utveckla servicen i förvaltningen är informationstekniken. Tjänster som riktar sig till individer och företag skall också erbjudas via Internet. Statliga myndigheter måste samverka såväl med varandra som med kommuner, landsting och näringsliv för att skapa rationella servicelösningar för alla parter. Enskilda individer och företag bör – så långt som det är möjligt – enkelt kunna hämta och lämna den information som är relevant i varje enskild situation oavsett hur informationsansvaret är fördelat mellan myndigheter eller mellan stat, kommun och landsting. Informationstekniken är ett utmärkt instrument också för att underlätta insyn och kontroll samt för att i större utsträckning informera och hämta in synpunkter från medborgare och företag. En gemensam öppen och säker IT-infrastruktur baserad på Internet skall ligga till grund för de elektroniska kontakterna med enskilda individer och företag. Särskilt bör små och medelstora företags kontakter med myndigheter elektroniskt underlättas.

Regeringen radar i programmet upp en mängd åtgärder vilka alla syftar till att göra förvaltningen mer öppen, mer genomsynlig och mer samverkande. Samtidigt framhåller man kraven på säkerhet i systemen och redovisar att lösningen på säkerhetsproblemen är kryptering och verifiering med elektronisk signatur. Statskontoret använder följande bild (figur 4) för att visa baselementet i den säkerhetslösningen man ser framför sig som ett krav med en elektronisk förvaltning.

Alla som vill utföra transaktioner med förvaltningen måste ha en asymmetrisk krypteringsfunktion med en publik nyckel och en privat nyckel. Nycklarna är kopplade till

28) Ibid, 16

29) Regeringskansliet, 1998, 12–13



Figur 4. Kryptering med publik nyckel (Statskontoret föredrag 2001-11-06).

varandra på det sätt som redovisas i figuren.

Detta är också den kritiska framgångsfaktorn som kan identifieras för att visionen om 24-timmarsmyndigheten skall lyckas. Om man inte hittar en teknik för elektroniska signaturer som är säkra och som fungerar för samtliga myndigheter så kommer projektet inte att lyckas i sitt fjärde steg. De effektivitetsvinster och servicevinster som såväl utredningar, regering som Statskontoret har identifierat med 24-timmarsmyndigheten kommer inte att kunna realiseras om inte en enhetlig standard för elektroniska signaturer etableras. Detta i sin tur kräver någon form av centraliserad hantering av publika nycklar m.m.

Statskontoret har rekommenderat regeringen att ge ett uppdrag till Riksrevisionsverket att hantera denna fråga:

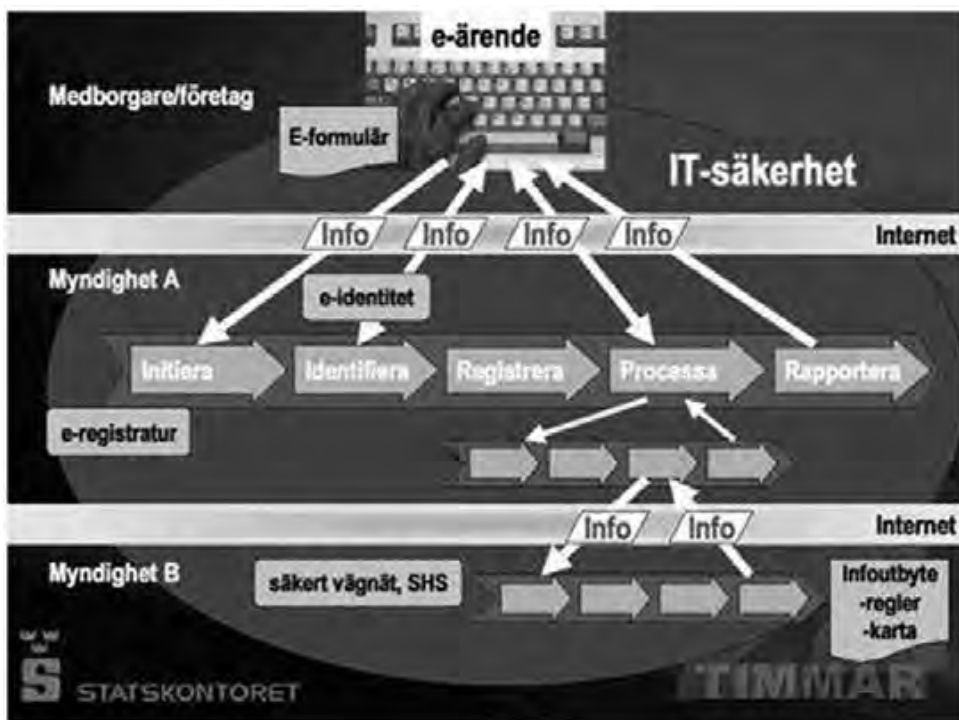
Regeringen uppdrar åt Riksskatteverket (RSV) att under ett inledningsskede ha ett sammanhållande ansvar för administrationen av certifikat för elektronisk identifiering och elektroniska signaturer inom statsförvaltningen.

En utvärdering av verksamheten skall redovisas till regeringen senast den 1 mars 2003.

- utarbeta allmänna riktlinjer och gemensamma rutiner för certifikathanteringen inom statsförvaltningen
- samordna statsförvaltningens krav och behov inför upphandling och avrop av certifikat och tillhörande tjänster för elektronisk identifiering och elektroniska signaturer
- samordna de myndighetsgemensamma tjänster som krävs för en väl fungerande infrastruktur för användningen av statlig verksamhet
- svara för information och vägledning till myndigheterna i dessa frågor.

Med de elektroniska signaturerna öppnar sig alla möjligheter för två centrala funktioner i 24-timmarsmyndigheten – "elektronisk ärendehantering" och "data på en plats".

Den elektroniska ärendehantering innebär i korthet att det nu blir möjligt för såväl enskilda som myndighet att på ett säkert sätt kommunicera med varandra via krypterad trafik där legitimeringen är garanterad och



Figur 5. E-medborgare och e-myndighet (Statskontoret).

där säkerheten gentemot obehöriga är hög. Tekniken öppnar också vägen för att lagra data enbart på ett enda ställe i förvaltningen – lagring vid källan – eftersom behörigheter och hantering av data kan kontrolleras via personalens elektroniska nycklar som är kopplade till tjänsten inom organisationen. Statskontorets vision om det framtida tillståndet har konkretiserats i en bild som återges i figur 5.

I bilden syns tydligt de eftersökta sambanden – den enskilde agerar gentemot myndigheten via e-formulär och en säker e-identitet. Myndigheten registrerar elektroniskt ärendet och samverkar i processen med andra myndigheter för att få tag på relevanta data. För att göra transaktionerna säkra har man ett säkert vägnät och tydliga regler och kartor för informationsutbytet.

För att testa 24-timmarsmyndigheten i större skala har regeringen föreslagit riksdagen att ge klartecken för försöksverksamhet inom socialförsäkringens område.³⁰

Avsikten är här att testa om de tänkta effekterna verkligen uppstår:³¹

I begreppet 24-timmarsmyndighet ligger enligt Statskontoret även ett antal andra funktioner, såsom lämnande av information om myndigheten och de ansvarsområden den administrerar. Dessa typer av tjänster tillhandahålls av såväl Riksförsäkringsverket som försäkringskassorna redan i dag genom de hemsidor som är tillgängliga via Internet. Den centrala funktionen inom begreppet 24-timmarsmyndighet är dock möjligheten till interaktiva tjänster som inbegriper såväl lämning och hämtning av individorienterad information som inledande och annan hantering av ärenden. Ett samlingsbegrepp för den sistnämnda funktionen kan sägas vara självetjäningstjänster. Självetjäningstjänsten inom föräldraförsäkringen skall omfatta möjligheter för de försäkrade att via en hemsida få tillgång till allmän information om de olika förmånerna. Det skall därvid finnas möjligheter till interaktiv simulering av olika uttag

30) Proposition 2001/02:9: Vissa socialförsäkringsfrågor

31) Ibid, 28

etc., utifrån förutsättningar angivna av den försäkrade. De försäkrade skall ha tillgång till individorienterad information om tillgängligt antal dagar att ta ut, anmäld årsinkomst etc., som hämtas från socialförsäkringsregister. Även den individorienterade informationen kommer att kunna användas av den försäkrade i olika simuleringsprogram. Dessa kommer bl.a. att innebära förbättrade möjligheter för individen att exempelvis överblicka och planera ett uttag av föräldradighet. Dessutom kommer den individorienterade informationen att kunna användas på så sätt att registrerade uppgifter automatiskt läggs in i elektroniska blanketter för försäkraren m.m. En försäkrad skall således också kunna göra anmälan om uttag av förmåner och lämna in s.k. försäkraren för föräldrapenning respektive tillfällig föräldrapenning direkt via Internet och därvid använda sig av olika hjälpfunktioner som underlättar detta.

Denna passus i propositionstexten ger en bra beskrivning av hur medborgare och myndighet är tänkta att samspela; individorienterad information skall kunna tas fram över Internet, simuleringar av effekter av val av tjänster skall kunna göras, och – får man förmoda – skall kompletterande information kunna hämtas direkt till myndigheten, t.ex. bankkontonummer eller motsvarande. Samtidigt kan man fundera på hur mycket försöksverksamhet det här egentligen rör sig om eftersom den fullskaliga verksamheten är tänkt att starta vid årsskiftet 2002/03.³²

Trycket på myndigheterna i detta sammanhang är mycket stort – inte minst av kostnads-skäl. Detta framkommer t.ex. tydligt när det gäller hanteringen av personuppgifter:³³

”I höst ska RSVs nya folkbokföringssystem vara klart. Då blir det möjligt för medborgarna att ta del av egna handlingar och göra flyttan-

mälningar via Internet. Riksskatteverkets helt nya folkbokföringssystem beräknas vara klart i oktober.

– Allt från födelse och flytt till giftermål, barn, skilsmässa och död ska vara möjliga att anmäla digitalt till folkbokföringssystemet, säger Christer Lindström, IT-projektledare på RSV. [...]

- Vårt mål är att alla massärenden ska gå digitalt. Endast ärenden som inte är standard, exempelvis partnerskap mellan homosexuella, ska hanteras manuellt, säger Christer Lindström. [...]

- Enligt förstudien ska projektet spara närmare 25 miljoner kronor per år till RSV. Men enligt Christin Ulfskans, som ansvarar för projektet, bygger förstudien på lite andra beräkningar än det system som nu utvecklas. [...]

- Folkbokföringen har hand om så otroligt mycket information, och om det går att automatisera registreringen av fastighets- och lägenhetsbyten, kommunala uppgifter och utslag från domstolar och Migrationsverket så sparar det mycket pengar och resurser, säger Christer Lindström.”

Man kan således konstatera att förväntningarna är höga på att myndigheterna och byråkratin skall finna nya former för sitt arbete, men också på att medborgarna – användarna, ”kunderna” – i allt högre grad skall ägna sig åt självbetjäning – ”åt var och en byråkrati efter sin egen förmåga”.

Myndigheternas supermarket?

Ett genomgående drag i myndigheternas beskrivningar av vad framtiden skall innehålla är att medborgaren medelst självbetjäning skall kunna sköta många olika ärenden. Genom regelstyrd interaktiv kommunikation skall man själv kunna lämna uppgifter till myndighetens datasystem och få besked om

32) Proposition 2001/02:9, 30

33) *Computer Sweden*, 2002-01-28

INNEHÅLL	SENASTE NYTT	TJÄNSTER
<ul style="list-style-type: none"> Startsidan Lokala nyheter Inrikes Utrikes Opinioner Sport & fritid Arbete & pengar Kultur & nöje Familj Vardags Lördag C ung Bilagor Radionyheter Recensioner Diskussioner TEMA Var dags rum Bostad 	2002-03-21 <ul style="list-style-type: none"> Maten på universitetet ska bli bättre [11:25] Bilexpllosion i Jemen dödade minst fyra [11:13] Dömd för hets mot folkgrupp [11:10] Trevande börsöppning [11:05] Dagsböter för bussolycka i Köpenhamn [10:55] 	Skriv ut <p>[02:00] Premiär i år för den elektroniska blanketten</p> <h2>Deklarera på nätet</h2> <p>STOCKHOLM (TT SPEKTRA) Deklarationsångest? Glöm det! I år kan du skippa blanketterna och deklarerera på Internet. -- Över 3 miljoner svenskar kan använda den nya tjänsten, säger Ulf Kjellin som är projektledare för den elektronisk deklarationen på Riksskatteverket.</p> <p>Den 2 april är det dags. Då slår Riksskatteverket upp portarna till ett helt nytt sätt att deklarerat. I stället för att lämna in deklarationsblanketten på vanligt sätt går det att deklarerat på Internet.</p>
		Sök på Corren.se: <input type="text"/> <input type="button" value="Sök!"/> <ul style="list-style-type: none"> Köp & Salj Fyndet Bilar & Fordon Båtar Nättjänster Lunchguiden Evenemang Reseguiden Länkguide Fonder Till din mobil Platsannonser Östergötland Hela landet

Figur 6. År 2003 skall vi alla kunna deklarerat över nätet.

pension eller bostadsbidrag, lämna sjukbesked eller deklarerat eller ansöka om tillstånd av olika slag. Systemet påminner inte så lite om e-handel – med den skillnaden att kunden i stället för att köpa skall utföra medborgerliga handlingar.

Samtidigt är det viktigt att se skillnaderna mellan denna typ av hantering och den hantering som genomförs av en tjänsteman. I det fall att en tjänsteman bedömer ett ärende kan man utgå från att många uppgifter förutom de uppgifter som finns i ärendet och i det relevanta regelverket – samtal med kollegor, tidigare erfarenhet, kunskap om avsikten med regelverket m.m. I en automatiserad rättsprocess finns inte dessa kringfaktorer utan regelverket är överfört till matematiska regler av någon som oftast inte har någon kännedom om själva sakfrågan. Dessutom är det sällan så att de som är experter inom området har varit med i framtagandet av det elektroniska regelverket. Cecilia Magnusson-Sjöberg har framhållit att de datorprogram som idag används

inom förvaltningen har en oklar offentligrettslig status.³⁴ Detta bekräftas också av det resonemang som Erik Woodcock för i rapporten från *Det IT-rättsliga observatoriet*:³⁵

Karakteristiskt för agenttekniken är automation. Det handlar om försök att datorisera verksamhet som traditionellt tagit sig uttryck i mänsklig analys, eftertanke och slutledning. Begrepp som agent och agentteknik kan sägas innefatta en rad företeelser som på mer eller mindre avancerat sätt ersätter eller avser ersätta sådana mänskliga aktiviteter. Genom att mobila agents operationer liknas vid människors handlande uppkommer frågan om det kan hävdas att program kan utföra rättsligt relevanta handlingar såsom rättshandlingar o.dyl. Juristen står inför det faktum att rättsliga frågeställningar med anknytning till en långt driven automation blir allt vanligare ju mer utbredd användningen av agentteknik blir. De frågeställningar som därvid aktualiseras har redan i viss mån aktualiserats då teknik såsom Electronic Data Interchange (EDI) tagits i bruk.

34) Magnusson-Sjöberg, C., 1992, 410–411; 508–510

35) IT-kommissionen, 1998: Mobila agenter, 4

Om en agent är ett objekt som har egenskaper som kan uttryckas med ord som självständighet, social förmåga liksom reaktionsförmåga kan juristen komma att ställas inför frågan om agenterna ingår avtal liksom utför andra rättshandlingar. Kan då en agent vara något mer än ett meddelandesystem? Kan agenten självständigt utföra rättshandlingar? Frågan kan möjligtvis inledningsvis begränsas till en fråga om det är möjligt att göra gällande att en agent kan ingå avtal?

Genom agenter överlåter människan till datorprogram och maskiner moment vari ingår att fatta "beslut" som har rättslig betydelse. Agenten kan ses som ytterligare ett steg i riktning mot en ökad grad av automation i samhället. Det kan konstateras att datorns operationer vid utväxling av agenter innebär att tekniken används till något mer än enbart att förmedla ett meddelande mellan människor då datorprogram i dessa fall på olika sätt tolkar och bearbetar meddelanden.

Av detta kan man sluta sig till att även om det tekniskt går att ersätta handläggning av regelstyrda situationer med automatiserade system är inte frågan entydigt enkel. Samtidigt finns självfallet mycket starka krafter som skyndar på en utveckling där jag som enskild skall använda mig av agenter i olika form när jag skall genomföra rutinmässiga interaktioner med myndigheter. De rent ekonomiska fördelarna för staten är uppenbara, men också de hanteringsmässiga fördelarna i form av att alla ärenden får en likartad bedömning – ovidkommande hänsyn tas inte med. För mig som medborgare är fördelarna också tydliga – systemet går snabbt och jag kan själv välja när jag skall genomföra interaktionen.

Det går alltså att konstatera att krafterna som verkar för en snabbt ökad grad av automation i förhållandet mellan medborgare och myndighet är starka.

HAR INDIVIDEN NÅGON RÄTT TILL INFORMATIONEN OM SIG SJÄLV?

Ur ett strikt individperspektiv – vad har jag rätt till för information om mig själv? Svaret på en till synes enkel fråga är långt ifrån självklar. Dock får man en tydlig uppfattning om betydelsen av integritetsbegreppet när man läser utredningen *Konsumenter och IT*.³⁶

Rätten till privatlivet är en av de grundläggande fri- och rättigheterna. Den svenska regeringsformen reglerar skyddet för personlig integritet gentemot myndigheter. I Europakonventionen föreskrivs att envar har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.

Man kan utifrån detta konstatera att rätt till privatliv, och därmed skydd för personlig integritet, står mycket högt upp på värdeskalan. Grunden för resonemanget hämtar sin kraft i synen att alla människor har ett lika värde som grundar sig i just det faktum att man är människa, och att detta värde således inte är kopplat till egenskaper av typen kunskaper, inkomst, härkomst eller annat. Samtidigt som man således kan finna någon form av konsensus kring principen om var människas rätt till en privat sfär, så blir frågan hur denna skall skyddas desto svårare. Två saker förefaller emellertid gemensamma; dels är den personliga integriteten kopplad till den privata sfären, dels uppfattas intrång i den privata sfären

som en kränkning. *Integritetsutredningen konstaterar*.³⁷

Det har emellertid visat sig att begreppet personlig integritet inte är så lättfångat. Stora ansträngningar har gjorts för att definiera det men någon kortfattad generell konkretisering av begreppets språkliga innebörd har utredningen inte kunnat finna. Men som en klar gemensam nämnare framstår i vart fall uppfattningen att begreppet personlig integritet innebär att alla människor har rätt till en personlig sfär där ett önskat intrång, såväl fysiskt som psykiskt, kan avvisas. De flesta människor har också en bestämd uppfattning om vad personlig integritet innebär för deras egen del och de uttrycker detta mestadels på motsvarande sätt som nyss nämnts. Men uppfattningen om storleken av den privata sfären kan variera kraftigt mellan olika människor beroende framför allt på deras kulturella, etniska, religiösa och sociala bakgrund. Omfånget av den personliga sfären uppfattas inte heller som statistiskt, inte ens för den egna individen, utan kan förändras med hänsyn till bl.a. vunna erfarenheter och den aktuella situationen.

Poängen med resonemanget är att den personliga integriteten – och den sfär som bestämmer den – är personligt definierad. Det går inte att med objektiva mått konstatera hur stor den privata sfären skall vara för varje

36) SOU 1999:106: Konsumenter och IT, 134

37) SOU 2002:18: Personlig integritet i arbetslivet, 53

individ för att denna inte skall uppfatta den personliga integriteten som kränkt. Det är sannolikt också så, att det inte heller går att säga att den privata sfären är lika stor från tid till annan. Det kanske inte är alltför vågat att anta att en student som bor i korridor med kollektivt kök uppfattar den personliga sfären annorlunda än en medelålders person som bor i villa.

Ur ett samhällsligt perspektiv blir hanteringen av personlig integritet självfallet besvärlig. Dels har vi här att göra med ett politiskt honnörsord av format som skyddas av i stort sett all nationell och internationell lagstiftning. Dels har vi här att göra med ett subjektivt definierat värde som inte låter sig fångas på samma sätt som t.ex. en hastighetsgräns eller ett förbud.

Saken blir inte lättare av att den personliga integriteten kan kränkas på en rad olika sätt. Den fysiska kränkningen – att bli nedslagen, rånad eller motsvarande – är ett uppenbart brott mot den privata sfären, vilket också är tydligt hanterat i strafflag. Den icke-fysiska kränkningen är däremot betydligt svårare att konstatera och därmed också att förutse. Just denna problematik har EU försökt att hantera i direktivet om skydd för personuppgifter³⁸ vilket i sin tur har lett till den svenska personuppgiftslagen (PuL). Man kan säga att utgångspunkten bakom direktiv och lag är att all användning av uppgifter om personer skall vara förbjuden om den inte är explicit tillåten av personen i fråga. I utredningen *Konsumenter och IT* sammanfattas synsättet bakom personuppgiftslagen:³⁹

Lagens definition av begreppet personuppgift är "all slags information som direkt eller indirekt kan

hänföras till en fysisk person som är i livet". Härmed avses uppgifter om en enskild person som t.ex. upplysningar om namn, personnummer, födelse-datum, nationalitet, utbildning, familj och anställningsförhållanden. Även andra uppgifter av mindre personlig karaktär räknas som personuppgifter. Enligt regeringen avses även uppgifter om en persons bostadsförhållanden, banktillgodohavanden, fastighets- eller bilinnehav och upplysningar i övrigt om en persons ekonomiska ställning. En person kan vara identifierbar även genom en kombination av särskiljande kriterier (ålder, yrke, bostadsort etc.), vilka gör att personen kan kännas igen genom att den grupp han eller hon tillhör omfattar färre och färre personer. Krypterade uppgifter omfattas av lagen så länge någon kan göra uppgifterna läsbara och därmed identifiera individer. Också sådana i sig anonyma uppgifter som gör det möjligt med s.k. bakvägsidentifikation av en fysisk person omfattas. Det är tillräckligt att en fysisk person kan identifieras med hjälp av uppgifterna, inte att den personuppgiftsansvarige själv kan förfoga över samtliga uppgifter som gör identifieringen möjlig. Frågan om en person är identifierbar är oberoende av kostnaden för att fastställa personens identitet. Definitionen omfattar även uppgifter om utseende, röst, fingeravtryck och genetiska karakteristika.

Men nu går det inte att utan vidare tvärbromsa samhällets hantering av uppgifter på det sätt som en strikt tolkning av direktivet och PuL skulle leda till. Detta insåg också regeringen och konstaterar redan i förordet till propositionen om personuppgiftslagen att den personliga integriteten i fråga om uppgifter måste balanseras:⁴⁰

Det behövs därför en ny, modern lagstiftning om personuppgifter som tillförsäkrar den enskilde ett

38) EU, 1999, COM(1999) 337 final 99/0153 (COD)

39) SOU 1999:106, 139–140

40) Proposition 1997/98:44: Personuppgiftslag, 29

fullgott integritetsskydd i IT-samhället och som inte hämmar samhällsutvecklingen eller försvårar förverkligandet av andra viktiga mål. Samtidigt har Sverige att – i enlighet med skyldigheterna som medlem i Europeiska unionen – i svensk lagstiftning genomföra 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, se bilaga 1.

Vad som sedan hänt med PuL skall inte avhandlas här, men det kan konstateras att lagen, tolkningen och konflikten med offentlighetsprincipen har lett till en omfattande samhällelig debatt och ett antal domar i såväl lägre som högre instans.

Det som är av intresse här är att EU-direktivet och PuL har lyft upp debatten om personlig integritet i förhållande till andra samhälls värden till hittills oanade höjder. Bland annat har vi nu för första gången fått en konkret debatt om arbetstagares rätt till personlig integritet inom arbetslivet, manifesterat i Integritetsutredningens betänkande.

Grunden till debatten kan förmodligen i många fall spåras till förhållandet mellan den svenska offentlighetsprincipen och synen på allmän handling å ena sidan och, å den andra, den europeiska synen på rätten till privatliv och sekretess som standard. Den svenska offentlighetsprincipen med sina krav på allmän handling, utlämnande av handling till personer som inte behöver identifiera sig och krav på specificerad hänvisning till sekretesslagstiftning för att inte lämna ut hela eller delar av handling, står i förhållandevis bjärt kontrast till det allmänna förhållandet i EU. Grunden där har varit att all information är sekretessbelagd till dess man fattar ett aktivt beslut om att offentliggöra den. I ljuset av

denna kulturkonflikt är det knappast konstigt att införandet av ett i vissa avseenden extremt skydd för individens rätt till sina egna data har förorsakat debatt.

Det är mot bakgrund av detta ganska väntat att PuL innehåller en rad undantag från kravet på tillstånd från den enskilda att lagra uppgifter om honom eller henne:⁴¹

Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att

- (a) ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,*
- (b) den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet,*
- (c) vitala intressen för den registrerade skall kunna skyddas,*
- (d) en arbetsuppgift av allmänt intresse skall kunna utföras,*
- (e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller*
- (f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilka personuppgifterna lämnas ut skall kunna tillgodoses om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.*

Personuppgifter får inte behandlas för ändamål som rör direkt marknadsföring, om den registrerade hos den personuppgiftsansvarige skriftligen har anmält att han eller hon motsätter sig sådan behandling.

När en behandling bara är tillåten med samtycke, får ytterligare person-uppgifter inte behandlas sedan den registrerade har återkallat sitt sam-

41) Proposition 1997/98:44, 64

tycke. I övrigt har den registrerade inte rätt att motsätta sig behandling av personuppgifter som är tillåten enligt den nya lagen.

Mest uppseendeväckande ur logisk synvinkel är kanske att regeringen hävdar att det är av nationellt intresse att bryta mot EU-direktivet vilket gör att man kan acceptera detsamma.⁴²

Med tiden har grundtanken i direktiv och personuppgiftslag allt mer kommit att urholkas under trycket från fackliga företrädare, journalister och andra samhällsdebattörer.⁴³ Effekten har bl.a. blivit att den omdebatterade paragrafen 7:16 i sekretesslagen omarbetats och att hemsidor på Internet som kan bedömas vara journalistiska nu kan publicera personuppgifter utan tillstånd.

Och hur gick det då med kopplingen mellan direktiv, personuppgiftslag och myndigheternas hantering av uppgifter? Ja det som debatten handlat om har nästan uteslutande varit myndigheternas utlämnande av uppgifter – inte inhämtandet och inte regleringen av vem som får avgöra undantag från direktivet. Ur perspektivet medborgare–myndighet är detta av betydligt större intresse. I propositionen om personuppgiftslagen framhåller regeringen att undantag från direktivet och personuppgiftslagen skall få beslutas av regeringen och de myndigheter regeringen delegerar rätten till. Detta innebär i praktiken att grundtanken bakom direktivet urholkas. I propositionen redovisas också debatten kring detta och att Lagrådet ställt sig tveksamt till denna tolkning av personuppgiftslagens relation till regeringsformen.⁴⁴

Regeringen väljer dock en mer offentlighetsliberal linje och förordar ett stort antal undantag från direktivets grundtanke.⁴⁵

Vårt förslag innebär att regeringen eller den myndighet som regeringen bestämmer skall få meddela föreskrifter om

- undantag från ett förbud mot behandling av känsliga personuppgifter, om det behövs med hänsyn till ett viktigt allmänt intresse,
- undantag från ett förbud för andra än myndigheter att behandla personuppgifter om lagöverträdelse som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden,
- undantag från ett förbud mot överföring av personuppgifter till tredje land, dvs. en stat utanför EES, om det behövs med hänsyn till ett viktigt allmänt intresse eller om det finns tillräckliga garantier till skydd för de registrerades rättigheter,
- undantag från skyldighet att anmäla automatiserade behandlingar till tillsynsmyndigheten för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten, och
- inom den ram som den nya lagen ställer upp meddela närmare föreskrifter om
 - a. i vilka fall behandling av personuppgifter är tillåten,
 - b. vilka krav som ställs på den personuppgiftsansvarige vid behandling av personuppgifter,
 - c. i vilka fall användning av personnummer är tillåten,
 - d. innehållet i en anmälan eller ansökan till en personuppgiftsansvarig,

42) När det gäller konflikten mellan offentlighetsprincipen och direktivet konstaterar regeringen att det är av vitalt svenskt intresse att offentlighetsprincipen bibehålls – vilket alltså faller under undantaget i punkt (d). Eftersom man på detta sätt kan leva upp till bokstaven om än kanske inte till andemeningen så anser man att man kan implementera direktivet.

43) Se t.ex. *Statstjänstemannaförbundets debattbok 7:16* eller den journalistiska debattsidan <http://www.pul.nu>.

44) Proposition 1997/98:44: kap. 10 Normgivningsdelegation

45) *Ibid*, 57

- e. vilken information som skall lämnas till registrerade och hur lämnandet av information skall gå till, och
- f. anmälan till tillsynsmyndigheten och förfarandet när anmälda uppgifter har ändrats.

Regeringen skall vidare – utan möjlighet till vidare delegation – enligt vårt förslag få meddela föreskrifter om

- undantag från förbudet mot överföring av personuppgifter till tredje land för överföring till vissa stater eller om överföringen regleras av ett avtal som ger tillräckliga garantier till skydd för de registrerades rättigheter, och
- att vissa behandlingar av personuppgifter som kan innebära särskilda risker för otillbörligt intrång i den personliga integriteten skall för förhandskontroll anmälas till tillsynsmyndigheten tre veckor i förväg.

Trots att flera remissinstanser ansåg att regeringens förslag att flytta makten från riksdagen

till regeringen och dess organ gick för långt vidhöll regeringen sin uppfattning om behovet av att kunna flytta rätten att tolka och förordna från den lagstiftande församlingen till den verkställande makten.

Den praktiska konsekvensen av detta återstår att se. Inom det område som har diskuterats mest – myndigheternas möjligheter att neka utlämnande av personuppgifter samt privatpersoners möjligheter att publicera namn – har ett antal rättsfall givit ledning till hur personuppgiftslagen skall ses. Inom området normgivningsdelegation och rätten att besluta om undantag från PuL har ännu ingen debatt eller något domslut aktualiserat frågan. Samtidigt är det kanske detta område som kommer att få den största betydelsen för de enskilda individerna på lång sikt.

Det går redan nu att se att den svenska regeringen uppfattar EUs direktiv och den därpå följande personuppgiftslagen som en hämsko. Regeringen har under januari 2002 dels tillsatt en utredning med uppgift att

The screenshot shows a news article from Dagens IT. The main headline is "Ny utredning om ändringar i personuppgiftslagen". The sub-headline reads: "På torsdagen tillsatte regeringen en ny utredning för att se över den omdiskuterade personuppgiftslagen (PuL). Syftet med utredningen är att underlätta hanteringen av personuppgifter och i stället försöka komma åt missbruk av uppgifter om privatpersoner. Sören Oman, chefsjurist på justitiedepartementet, ska under drygt ett år utreda vilka ändringar i PuL som kan bli aktuella." The article is dated "Onsdag 20 mar" and includes a sidebar with other news items and an advertisement for "Det Trådlösa Kontoret".

Figur 7. Personuppgiftslagen (PuL) är ständigt aktuell.

lämna förslag till översyn av PuL, dels tagit fram en egen modell för revidering av direktivet. Där direktivet avser att skydda individen från *processer* där integriteten kan hotas vill regeringen dels inrikta ett nytt direktiv på *effekterna* av integritetskränkningen, dels väga denna effekt mot andra samhälleliga insatser.⁴⁶

Sådan behandling är förbjuden bara om spridning av personuppgifterna är till skada för den registrerade. Spridningen skall dock alltid vara tillåten, om den som sprider uppgifterna är skyldig att uttala sig eller det annars med hänsyn till ett allmänt intresse är försvarligt att personuppgifterna sprids.

Resultatet av hanteringen blir till slut dock den att regeringen genom hanteringen av dels

offentlighetsprincipens ställning i relation till EU-direktivet och dels den potentiella kraften i normgivningsdelegationen har bäddat för att den syn på personlig integritet och rätten till uppgifter om sig själv som EU har fattat beslut om får ett betydligt svagare stöd i Sverige än i andra EU-länder. Och resultatet för den enskilda individen i Sverige är att skyddet för den personliga integriteten och rätten till informationen om sig själv är och blir betydligt svagare än för andra medborgare inom EU. Men resultatet blir samtidigt att man öppnar vägen för en sammanhängande förvaltningsstruktur där personuppgifter delas mellan myndigheterna och där skyddet mot att personuppgifter insamlade hos en myndighet (också) används av en annan, i praktiken blir obefintligt.

46) Regeringen, 2002

MYNDIGHETERNAS RELATION TILL SERVICE OCH INTEGRITET

Ett antal mätningar har genomförts utomlands vad gäller myndigheters och företags förhållande till service och integritet när det gäller webbkontakter. En mycket omfattande mätning har gjorts i Danmark, där regeringen har startat projektet *Danmark paa Nettet*, där även kvalitetsmätningen *Bedst paa Nettet* ingår. Kvalitetsmätningen innebär att man under tre år följer, värderar och poängsätter samtliga offentliga danska webbsajter på Internet och delar ut pris till dem som på bästa sätt ger brukarvänlighet, nytta samt öppen-


het.⁴⁷ Ett exempel på hur värderingen ser ut för användaren redovisas här.

Svenska Konsumentverket har deltagit i en internationell undersökning där man främst studerat hur olika myndigheter och företag förhåller sig till integritetsinformation, dvs. information om vilka personliga uppgifter webbplatsen samlar upp och vad som sedan händer med dessa.⁴⁸ En generell observation från den undersökningen är att de flesta webbplatser samlar in information om användaren, dock utan att vare sig tala om detta för

Styrelser og direktorater

Klik på en institution for at se kvalitetsvurderingen af dens hjemmeside. Du kan ændre rækkefølgen i listen ved at klikke på overskrifterne.

Screening 2002	Screening 2001			
▼ Samlet vurdering	▶ Institution	▶ Brugervenlighed	▶ Nytteværdi	▶ Åbenhed
●●●●○	IT- og Telestyrelsen, Informationsportalen	74%	54%	46%


Printervenlig

Figur 8. Danskt exempel på utvärdering av myndighetsinformation.

47) Se <http://www.bedstpaanettet.dk/ombodst.asp?page=document&objno=5102>, Bedst paa Nettet, 2001-01-07, för en komplett beskrivning av kriterier m.m.

48) Se <http://www.consumersinternational.org/news/pressreleases/privacy250101.html>, Consumers International, 2001-01-07, för en kort redovisning av resultaten. Se även Konsumentverkets pressmeddelande från den 25 januari 2001.

vederbörande eller än mindre fråga om lov att göra detta (något som strider emot EUs direktiv om personuppgifter).

I ett tidigare arbete har redovisats hur svenska myndigheter hanterar olika aspekter av Internetanvändning under två perioder.⁴⁹ I den studien fanns dock ingen faktisk mätning av innehållet på myndigheternas webbsidor, främst beroende på att många myndigheter inte hade webbsidor då studien påbörjades. En sådan mätning redovisas emellertid här.

En utgångspunkt för den nu aktuella undersökningen är att den skall omfatta samma myndigheter som studerades vid årsskiftena 1997/98 och 1998/99 för att ge möjlighet till jämförelser och för en koppling mellan myndighetens uppfattning inom ett antal viktiga områden (som de redovisas i enkätsvaren i de tidigare studierna) och myndighetens genomförande av mötet med användaren via webbsidorna.

Genomförande

De ursprungliga 103 myndigheterna – indelade i de tre kategorierna kunskapsorganisationer, statliga bolag/affärsdrivande verk samt traditionella myndigheter – har minskat i antal sedan den första undersökningen vid årsskiftet 1997/98. När den nu aktuella studien genomfördes (juli/augusti 2001) fanns 94 myndigheter kvar. De nio som saknas har antingen upphört eller slagits samman med andra till nya och större enheter. Sedan augusti 2001 har ytterligare förändringar skett. Så har t.ex. Överstyrelsen för civilberedskap (ÖCB) lagts ner.

De olika myndigheternas webbplatser har besökts och granskats. I likhet med de ovan refererade undersökningarna av danska myndigheters hemsidor och Konsumentverkets internationella studie har fokus i frågeställ-

ningen varit dels sajtens användbarhet, dels aspekter på integritetsfrågor. Samtidigt har också frågan om myndighetens hantering av myndighetsuppgifter studerats.

För varje myndighet har ett antal nyckelfunktioner från webben identifierats och värderats (se tabell 1 i bilagan).

Förutom de enskilda variablerna har två index skapats. Det ena måttet redovisar den samlade poängen för aspekter som har integritetspåverkan, medan det andra redovisar det samlade värdet för service. Sammansättningen av respektive index visas i tabell 2 i bilagan.

Dessa två index avser att lämna information om *graden av integritetshot* på webbsajten respektive *graden av service* som webbplatsen ger användaren. Att aspekterna "integritetsdeklaration" respektive "vidarebefordran" återfinns under samlingsvariabeln "servicepoäng" beror på att såväl integritetsdeklaration som information om vidarebefordran i sig inte har någon integritetspåverkan, men väl innebär en förhöjd service till användaren.

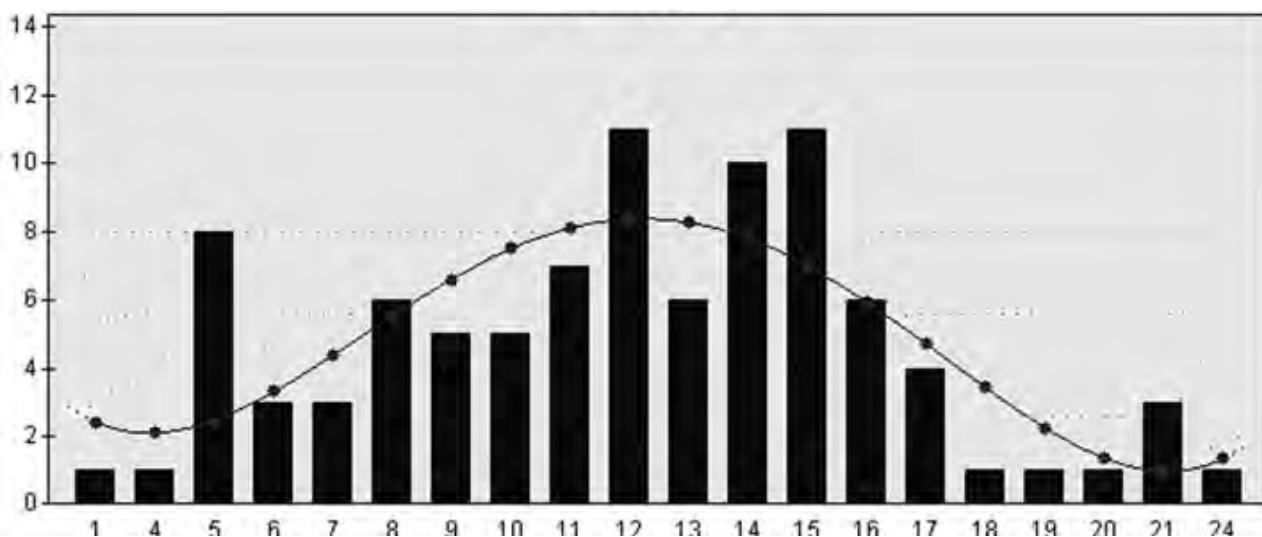
Högsta möjliga värde på den sammantagna servicemåttet är 36, medan högsta möjliga värde på integritetshotmålet är 27.

Resultaten skall sålunda läsas så att höga poäng på serviceindex är önskvärt från användarsynpunkt, medan hög poäng på integritetshotindex innebär att användare kan eller måste lämna mycket personlig information på webbplatsen.

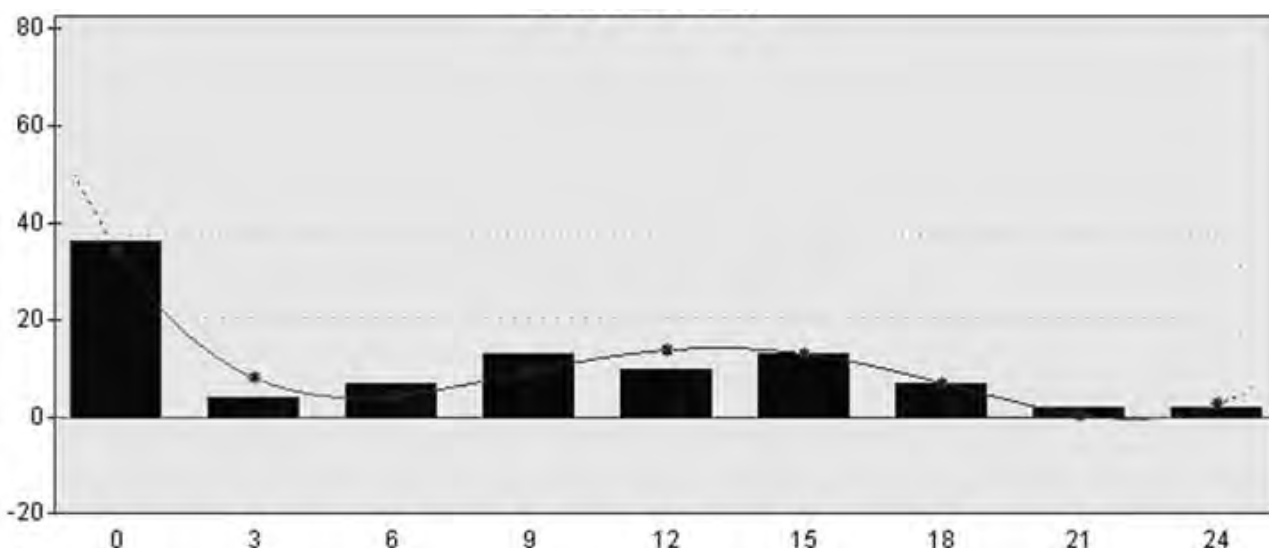
Resultat

Om man ser till den service som användaren får via myndigheternas webbsidor så uppvisar detta stora skillnader mellan myndigheterna. Fördelningen av servicepoäng är i det närmaste normalfördelad, vilket framgår av figur 9. Detta innebär att ett mindre antal

49) Nydén, M., 2000: Myndigheter, Internet och integritet



Figur 9. Servicepoängen bland de undersökta myndigheterna.



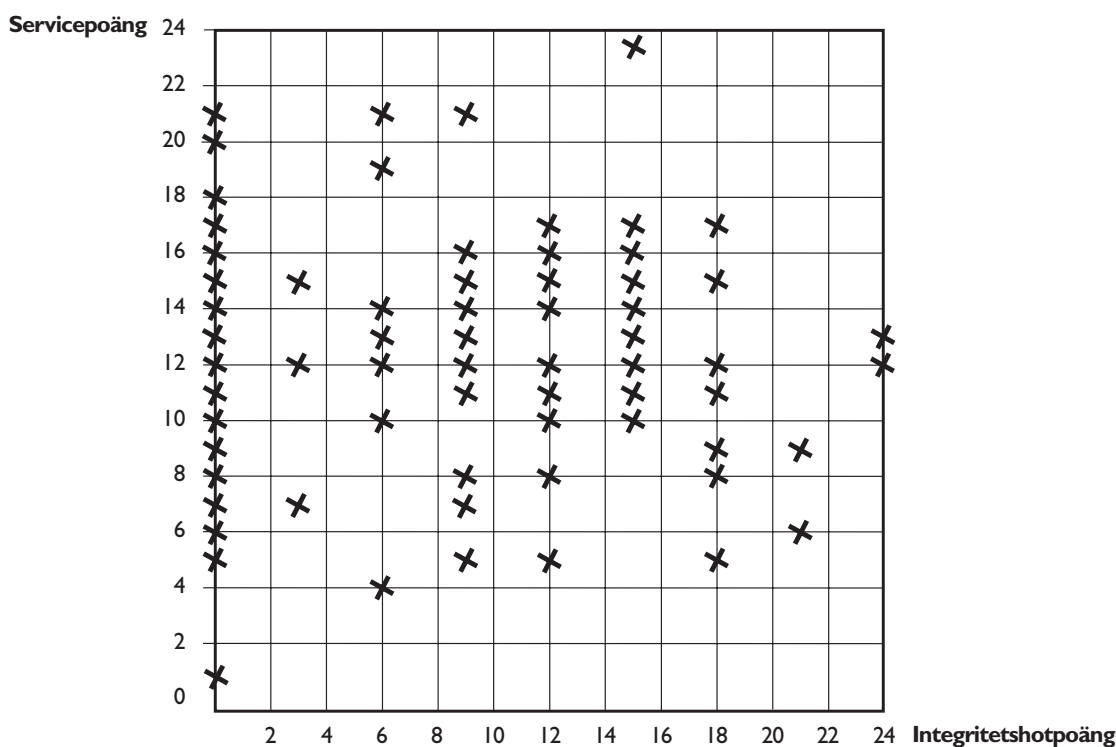
Figur 10. Integritetshotpoängen bland de undersökta myndigheterna.

myndigheter har mycket låg servicegrad, likaså ett mindre antal myndigheter har en mycket hög servicegrad. Spridningen av värden på samlingsvariabeln "servicepoäng" ger klart besked om detta. Huvuddelen av myndigheterna befinner sig i mitten av skalan.

Om vi vänder blicken mot integritetshotfrågan så skiljer sig resultatet här ganska markant från serviceresultatet. Som ses i figur 10 återfinns ett mindre antal myndigheter med hög integritetshotpoäng för sin webbplats,

medan många av myndigheterna får noll poäng på denna variabel, vilket skall tolkas så att i dessa fall så finns inget utbyte av integritetskänslig information mellan myndigheten och användaren på myndighetens webbplats.

På det sätt som index har konstruerats här har 47 myndigheter (50 procent) fått 9 poäng eller mer på integritetshotindex. Detta kan också tolkas som att hälften av myndigheterna i studien har öppnat för möjligheten att ta emot integritetskänslig information via Inter-



Figur 11. Sambandet mellan servicegrad och integritetshot.

net. Givet att trafiken på Internet i dessa fall är okrypterad innebär det att användaren i dessa fall riskerar att information om transaktion med myndigheten lätt kan avlyssnas, loggas eller på annat sätt hanteras av obehöriga för eventuellt egna syften.

En fråga man ställer sig när man ser indexfördelningarna är huruvida det är samma myndigheter som har hög servicepoäng som också hanterar hög grad av integritetshotande information? Som framgår av figur 11 finns det i stort sett inget samband alls mellan index. De myndigheter som har god service återfinns ofta till vänster i diagrammet, dvs. utgör låga hot mot integriteten.

En reflektion kring detta kan vara följande: hög service innebär oftast att användaren av webbplatsen har stora möjligheter att få information och har lätt att hitta den. Detta behöver

inte nödvändigtvis innebära att utbytet är synkront, dvs. att användaren också behöver lämna mycket information om sig själv. Som resultatet visar går det att ha hög grad av service utan att kräva mycket information från användaren i gengäld. Exempel på sådana myndigheter är Finansinspektionen⁵⁰, Statens pensionsverk⁵¹ och Vägverket⁵².

Servicefunktioner

När man ser till servicefunktioner på en webbplats är det i första hand tre funktioner som är viktiga – *navigering, direkta tjänster* samt *öppenhet*.⁵³ Nielsen konstaterar att användbarheten är det som skiljer webben från andra former av marknadsplatser mellan leverantörer och kunder eftersom användbarheten här kommer till uttryck innan köpet. Även om analogin mellan marknad och myn-

50) <http://www.fi.se>, kodad 2001-08-15 för denna undersökning

51) <http://www.spv.se>, kodad 2001-08-15 för denna undersökning

52) <http://www.vv.se>, kodad 2001-08-15 för denna undersökning

53) Nielsen, J., 1999: Designing web usability, 10

digheter inte är enkel och relationen medborgare och kund inte är självklar kan man konstatera att om de demokratiska ambitionerna bakom den statliga webbsatsningen skall lyckas, så är användbarheten av lika stor vikt här som på marknaden. Möjligheten att utföra direkta tjänster på webben torde vara en av de främsta orsakerna till att användaren över huvud taget vänder sig till myndigheten. Kravet på öppenhet har varit ett av den statliga huvudmannens främsta motiv för att uppmantra myndigheter att använda webben som kommunikationsform med medborgarna.

Navigering

Kravet på navigering innebär att det skall vara lätt för användaren att snabbt hitta de väsentliga funktionerna – helst utan att behöva hoppa runt på webbplatsen. Webbplatsen skall också vara överskådlig, dvs. det skall vara lätt för användaren att få en snabb uppfattning om webbplatsens hela innehåll. Kravet på direkta tjänster, slutligen, innebär att användaren skall kunna utföra tjänster direkt via webben, dvs. inte bli hänvisad att ta kontakt med myndigheten på ett annat sätt för att få tjänsten utförd.

Bland de undersökta myndigheterna har 11 stycken (12 procent) såväl sökfunktion som webbkarta. Dessa elva framgår av tabell 3 i bilagan.⁵⁴

Betydligt fler myndigheter erbjuder inte användaren de möjligheter som behövs för att kunna navigera på ett enkelt sätt. 29 myndigheter i undersökningen (31 procent) har varken söksystem eller webbkarta, och kan därmed sägas göra det maximalt svårt för användaren att hitta det man söker. Dessa 29 framgår av tabell 4 i bilagan.

Kanske kan man särskilt notera att ett antal myndigheter med till synes stort behov av kontakter med medborgarna – t.ex. Integrationsverket och Premiepensionsmyndigheten – hamnar i denna kategori.

Direkta tjänster

Den som går in på en myndighets webbsida förväntar sig nog, om inte besöket är av rent unik natur, i de flesta fall att kunna få en del uppgifter avklarade – antingen i form av information om någon del av myndighetens verksamhetsområde eller i form av handläggning av ett ärende. Det torde vara ett mindre antal fall där användaren går till en webbplats i akt och mening att bli hänvisad till ett annat sätt att kontakta myndigheten.⁵⁵ De varianter på direkta tjänster som mäts här är möjligheten att ladda hem dokument, möjligheten att ha en interaktiv dialog med myndigheten via webben samt möjligheten att utföra myndighetsfunktioner direkt på webben.

Två myndigheter – Glesbygdverket och Statens institut för särskilt studiestöd – klarar av att möta användare i alla tre formerna av direkta tjänster (tabell 5).

Däremot är det betydligt fler myndigheter, 12 stycken, som inte klarar av någon form av kommunikation med användare på detta sätt vilket framgår av tabell 6 i bilagan. Här återfinns bl.a. Statistiska centralbyrån, Folkhälsoinstitutet och Konsumentverket, och möjligheterna för användaren av webben hos dessa dussinet myndigheter får anses vara synnerligen begränsad. Detta skall inte tolkas som att respektive myndighets webb inte innehåller information – de flesta myndighetswebbplatser innehåller mycket information – utan snarare så att användaren inte kan använda denna kanal för att uträtta myndighetsärenden.

54) Sidorna kontrollerade 2001-08-15 för denna undersökning.

55) Ett undantag är det fall där man går till myndigheten för att hitta telefonnummer vilket torde vara vanligt – och ställer stora krav på myndighetens webbsajt.

Öppenhet

När det gäller öppenhet har fyra aspekter beaktats för att ge en uppfattning om detta – tillgång till diarium via webben, tillgång till personalförteckning på webben, möjlighet att ta del av årsredovisning samt möjlighet att ta del av regleringsbrev. Här är det endast en myndighet – Konkurrensverket – som klarar av samtliga fyra öppenheitskriterier.

Ingen myndighet får noll poäng på denna variabel, men tre myndigheter har tre poäng – Jordbruksverket, Domstolsväsendet samt Fastighetsmäklarenämnden – vilket i deras fall representerar att regleringsbrevet finns att tillgå via webben (se tabell 7).

I själva verket finns enbart tre myndigheter bland de undersökta som på något sätt låter sitt diarium redovisas på webben för användaren – Skolverket, Socialstyrelsen och Konkurrensverket. Även bland dessa myndigheter varierar hanteringen av diariet starkt – från löpande lista till full sökbarhet.

Den sammantagna bilden av servicen på nätet

Som man gjort i Danmark i undersökningen Bedst paa Nettet kan man lägga samman värdena på de tre serviceslagen navigering, direkta tjänster och öppenhet. Om man gör detta och standardiserar mätvärdena så att en myndighet som uppfyller alla krav som ställs för att få högsta värdet på respektive mätvariabel blir det maximala värdet 100. Ingen myndighet når upp till detta värde i undersökningen. Ett fåtal myndigheter kommer upp i värden högre än 50 (13 procent) vilket framgår av tabell 8 i bilagan.

Studien visar att 79 av de 94 undersökta myndigheterna (84 procent) har sammantagna servicevärden som ligger på som mest hal-

va maximala värdet. Mest iögonenfallande är att 29 av myndigheterna (31 procent) får värdet noll på tjänsten navigering, vilket i praktiken innebär att det torde vara mycket svårt för en användare att hitta det man söker på myndighetens webbplats.

Integritetshot

Studien visar att det inte finns något starkare samband mellan service på webbplatsen och hot mot användarens integritet. Om man tittar närmare på integritetshoten – hur ser dessa ut?

Frågan om vad som utgör integritetshot kan självfallet göras mycket komplicerad. Samtidigt kan den göras mycket enkel. I utredningen rörande konsumenterna och IT anslöt sig utredaren till en juridisk definition av begreppet integritet enligt följande:

Begreppet personlig integritet definieras ofta utifrån vad som anses utgöra en kränkning av den. Enligt en inom skadeståndsrätten ofta citerad katalog av Stig Strömholm kan integritetskränkningarna delas in i tre huvudgrupper; (i) intrång i fysisk eller annan mening i en persons privata sfär, (ii) insamlande av uppgifter om en persons privata förhållanden och (iii) offentliggörande eller annan användning (t.ex. som bevisning i rättegång) av material om en persons privata förhållanden. Integriteten kan således kränkas på många olika sätt. Kränkningar kan komma från en annan person eller från det allmänna. Gemensamt för alla kränkningar är att de innebär intrång i en skyddad zon som den enskilde är tillförsäkrad. Det anses vara en av grundpelarna i vårt rättssystem att integritetsskydd i denna vida bemärkelse skall upprätthållas.⁵⁶

Utifrån denna definition kan man konstatera att individen i vårt samhälle är tillförsäkrad

56) SOU 1999:106, 136

ett skydd för uppgifter om sin person och för att andra skall samla in och/eller hantera dessa uppgifter på ett för individen okontrollerbart sätt. Samma resonemang genomsyrar också personuppgiftslagen och det underliggande EU-direktivet, där grundstenen är att individen har rätt till information om sig själv och har rätt att ta ställning till hur denna information skall lagras och/eller förändras.

Samtidigt som detta sägs kan man också konstatera att uppgifter om individen konstituerar hot mot den personliga integriteten i olika hög grad. De flesta är nog fullt tillfreds med att vissa uppgifter om dem lämnas ut till allmänheten – t.ex. det fåtal som avstår från deltagande i telefonkatalog eller motsvarande. Det är säkert fler som idag gärna avstår från att uppge sitt personnummer utan tydlig orsak.

När det gäller myndigheter finns ytterligare en dimension i integritetsfrågan att ta hänsyn till. Offentlighetsprincipen innebär bl.a. att man inte skall behöva uppge sitt namn eller visa legitimation för att få ut en allmän handling. Denna princip gäller även för nyare medier – riksdagen har så sent som 1998 t.ex. givit regeringen sin uppfattning tillkänna att offentliga myndigheter inte skall få använda nummerpresentatörer vid telefonsamtal, just därför att anonymiteten skall skyddas.

I webbsammanhang blir detta mer problematiskt. Om man skall följa offentlighetsprincipens anda skulle detta innebära att myndigheten inte får spara någon elektronisk spårinformation över huvud taget kring de besök som användare gör på webbplatsen. Som har visats i en tidigare utredning är praxis här mycket varierande.⁵⁷ En del myndigheter i studien sparar ingen spårinformation över huvud taget, medan andra sparar alla transaktionsuppgifter i femton år.

Samtidigt som myndigheten sålunda inte bör samla spårinformation om personer som önskar ta del av allmän handling, så har myndigheten en lika självklar rätt att registrera uppgifter om den eller de som anhängiggör ett ärende i myndigheten. I samma ögonblick som individen som användare slutar att efterfråga allmän handling och i stället efterfrågar tjänster eller myndighetsutövning så kan individen inte längre ställa krav på anonymitet.

Här finns uppenbart utrymme för gränsdragning och tolkning. Är en kostnadsfri broschyr kring en myndighetsuppgift att anse som en allmän handling – och därmed täckt av anonymitetsskyddet? Hur är det i så fall med en produkt som användaren/"kunden" får betala för? Det torde vara orimligt att kräva att myndigheten helt skall avstå från att samla in uppgifter om den mottagare man skall ta betalt från.

I denna studie har åtskillnad gjorts mellan tre olika grader av integritetshot, sett ur perspektivet användare respektive materialets natur. Själva hotet består i att individen lämnar ifrån sig information som kan möjliggöra intrång i dennas privata sfär och/eller som gör det möjligt att koppla individen till vissa handlingar, som denna, om han eller hon hade fått välja, skulle ha avstått från att göra offentliga. Det är således fullt möjligt att det som upplevs som ett integritetshot i samband med ett visst material inte uppfattas som sådant i samband med annat material.

Den lägsta graden av hot uppstår när användaren av en myndighetswebb måste uppge sin e-postadress för att erhålla något i gengäld. E-postadressen behöver inte säga mycket alls om den person som har den – det behöver t.ex. inte finnas någon koppling mellan e-postadress och namn. Det finns idag goda möjligheter för den som så önskar att

57) Nydén M., 2000

använda anonyma e-postservrar, t.ex. hotmail. Samtidigt är det dock så att e-postadressen i de allra flesta fall utgör en länk till användaren som är möjlig att spåra. Ofta är det också så att e-postadressen i relativ klartext talar om vem som sänt dokumentet – antingen genom namn eller telefonnummersystem. För den som vill veta vem som skickat sin e-post till en viss myndighet och kanske begärt viss information eller vissa dokument denna väg är det fullt möjligt att med litet arbete koppla en e-postadress till en person. Därför kan en lämnad e-postadress sägas utgöra ett svagt integritetshot.

Nästa nivå på integritetshot, fortfarande sett ur användarens synvinkel, är när man ombeds lämna ifrån sig information som direkt talar om *vem* som begär information eller tjänst. Information av detta slag är namn, telefonnummer, adress och faxnummer. Denna information länkar direkt och i klartext användaren till transaktionen med myndigheten och därmed också användarens fysiska identitet och lokalisering. Samtidigt kan man utgå från att den information som transaktionen berör är av förhållandevis opersonlig natur – framförallt myndighetsinformation och offentligt material som inte är direkt avsett för användaren. I de fall som har noterats i denna undersökning rör det sig nästan undantagslöst om publikationer som tagits fram av myndigheten och som antingen inte finns för webbpublicering eller också kostar pengar för användaren att komma över.

Den tredje nivån på integritetshot är den där myndigheten interagerar med användaren i vad som närmast kan beskrivas som handläggning. Det kan till exempel röra sig om svar på frågor – antingen avgivna via en handläggare eller via ett FAQ-system. Det kan också röra sig om system för olika typer av beräkningar där den enskilde via Internet lämnar ifrån sig olika typer av uppgifter –

inkomst, levnadsförhållanden, bostadsförhållanden m.m. för att få kunskap om t.ex. pension, bostadsbidrag eller skatteeffekter. Här är transaktionen av direkt personlig natur och innebär sannolikt överlämnande av information från till myndigheten som är av ett sådant slag att individen helt säkert skulle avstå från transaktionen om det fanns ett tydligt hot att informationen skulle hamna hos tredje part.

Det svaga hotet

39 av de 94 myndigheterna (42 procent) har på sin webbplats funktioner som låter användaren skicka e-brev till myndigheten. Detta är då e-brevsfunktioner som är kopplade till tjänster hos myndigheten – t.ex. beställning av blanketter, dokumentation eller motsvarande. Alla myndigheter har möjligheter till e-postkontakt, men det är inte denna funktion som avses här. Här handlar det om att myndigheten – via formulär eller e-postkoppling – uppmanar användaren att kontakta myndigheten för att erhålla en tjänst av något slag. Myndigheten har alltså valt att låta användaren identifiera sig för att få information. Ett alternativ hade ju varit att lägga ut blanketter och dokument i PDF-format eller på annat sätt, men det valda sättet ger myndigheten en direkt tillgång och kanal till de medborgare som önskar information om verksamheten.

Ur integritetsperspektiv innebär detta ett flertal hot för den enskilda; dels finns hotet från någon som övervakar kommunikationen på Internet. Detta hot är förhållandevis reellt – för den som vill följa kommunikationen mot en e-postserver på en myndighet erbjuder inte tekniken några större hinder. Dels finns hotet från myndigheten. I det ena fallet kan myndigheten själv sägas utgöra hotet om man bygger upp någon form av "kunddatabas" där de som närmar sig myndigheten med begäran om information läggs upp för att vid senare tillfällen kunna nås med ny information. Myn-

digheten kan på detta sätt utnyttja *pull*-tekniken (att låta användaren skicka e-post för att få information) för att i ett senare skede själv kunna utnyttja *push*-teknik (att skicka ut information till dem man tror är intresserad eller har behov av en viss typ av information). Dels, och slutligen, finns hotet att myndigheten säljer information om vem som närmat sig myndigheten. Som har visats ovan är det mycket ovanligt att myndigheter har någon form av integritetsdeklaration, och i och med att personuppgiftslagen trätt i kraft är det tidigare förbudet för myndigheter att sälja information i praktiken upphävt. PuL innebär i detta sammanhang en avsevärd försämring jämfört med den tidigare datalagstiftningen.

Samtidigt skall det åter poängteras att en e-postadress inte innebär någon helt automatisk identifiering. Även om det alltid går att spåra en e-postadress till en person kan det innebära mer eller mindre stort arbete att koppla adress till person.

Det starkare hotet

I det starkare hotet finns en direkt koppling mellan person och uppgift. Här handlar det om att via myndighetens webb lämna uppgifter om namn, adress, telefon, fax, m.m. Ett betydligt större antal myndigheter använder denna form av kontaktväg än de som utnyttjar e-posten – hälften (47 av 94) myndigheter tar in denna typ av information. 15 av dessa myndigheter tar emot alla fyra typerna av personlig information och får därmed högst poäng i sammanhanget, vilket framgår av tabell 9 i bilagan.

Det är värt att notera att flera av de myndigheter som samlar in personlig information på detta sätt också är myndigheter som kan ha en direkt relation till individuella användare, antingen i form av att tillhandahålla medel för ansökan (forskningsråd t.ex.) eller som hjälper personer i utsatta situationer (ombudsmän,

arbetsförmedling) eller som har tillsynsansvar över lokala funktioner (Skolverket, Socialstyrelsen). Exempel på detta är Vetenskapsrådet, AMS och Forskningsrådet för miljö, areella näringar och samhällsbyggande.

Två saker är värda att notera. Dels kan man konstatera att de 15 nämnda myndigheterna samlar in precis den information som brukar ingå i en sedvanlig kontaktdatabas. Med tillgång till denna information finns inga tveksamheter om *vem* som kontaktat myndigheten – och eftersom uppgifterna allt som oftast samlas in i samband med begäran om information så finns där också kopplingen till *varför* man kontaktar myndigheten. Dels att det inte på någon webbplats av de 15 här utpekade finns någon myndighet som lämnar information till besökaren om hur informationen används eller kan komma att användas. Det finns således heller inte någon möjlighet för en enskild att ta ställning till om utlämnandet av personlig information kan utgöra något hot mot den egna personen.

Det starkaste hotet

Man kan tycka att de två ovan beskrivna situationerna kan vara ganska harmlösa – de flesta personer känner inget större integritetshot vid en förfrågan att lämna ut namn och adress. Däremot skulle nog de flesta fundera en eller två gånger innan man lämnar ut t.ex. personnummer eller annan typ av personlig identifikation som kan medföra rättsligt ansvar om de missbrukas. På samma sätt förhåller det sig nog med s.k. inloggningssidor. Här har ju användaren ansökt om att få interagera med myndigheten bakom "stängda dörrar", och har i gengäld antingen betalat för detta eller lämnat annan information som motiverar den särskilda behandlingen eller rätten att ta del av informationen.

Ett särskilt fall utgör det där myndigheten utför ekonomiska transaktioner över Internet

och låter användaren betala via sitt kreditkort. Mycket har sagts och skrivits om denna funktion (att betala med kreditkort) men det går ändå att konstatera att i det fall transaktionen inte sker via en krypterad sida så finns risker förknippade med denna hantering. Och även om svensk lagstiftning gör det sannolikt att en bankkund som blir bestulen på sitt kreditkortsnummer som senare används utan ägarens medgivande, inte blir skyldig att stå för kostnaderna så är rättsläget här inte helt klart. Risken för att kreditkortsnummer skall stjälas och därefter utnyttjas olovligen skall inte vare sig underskattas eller överskattas, men eftersom den enskilde per definition står i underläge i förhållande till myndigheten är det tveklöst så att integritetshotet är tydligt om myndigheten erbjuder möjlighet att lämna denna information.

Sammantaget är sex myndigheter identifierade i studien med funktioner som ger ett starkt integritetshot (tabell 10 i bilagan). Noteras kan att såväl Vetenskapsrådet som Arbetsförmedlingen återfinns även i denna kategori av integritetshot.

Alla dessa sex myndigheter har möjligheter till interaktion med medborgaren som inne-

håller de moment som klassats som starkt integritetshotande.

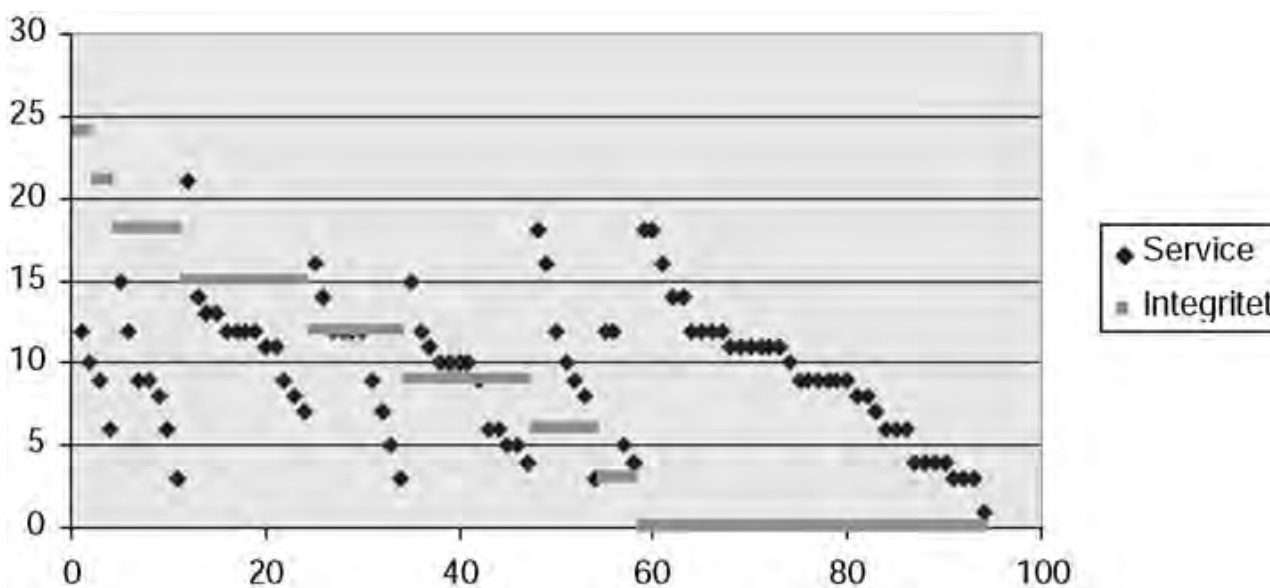
Samtidigt skall konstateras att det fortfarande hör till ovanligheten att en myndighet har denna typ av tjänster – 62 av de 94 undersökta myndigheterna (65 procent) uppvisar inte några starka integritetshot.

Den sammanvägda bilden

Även när det gäller hotet mot integriteten kan en samlad redovisning göras där de olika faktorerna normerats så att en myndighet som får högsta poäng på alla faktorer får värdet 100. Redovisningen återfinns i tabell 11 i bilagan.

Listan är så konstruerad att förekomsten av t.ex. e-postbegäran om material ger värdet 100 i denna kolumn, men i den sammantagna kolumnen "integritet" enbart bidrar med en niondel av den totala summan (eftersom det finns nio olika delfaktorer i begreppet "integritetshot"). På motsvarande sätt hantearas kolumnerna "svagt hot" respektive "starkt hot". Detta innebär bl.a. att Vetenskapsrådet och arbetsförmedlingen med 89 poäng av 100 möjliga har alla i undersökningen förekommande integritetshot förutom ett.

Lika intressant är emellertid också att note-



Figur 12. Servicepoäng inom olika nivåer av integritetshot.

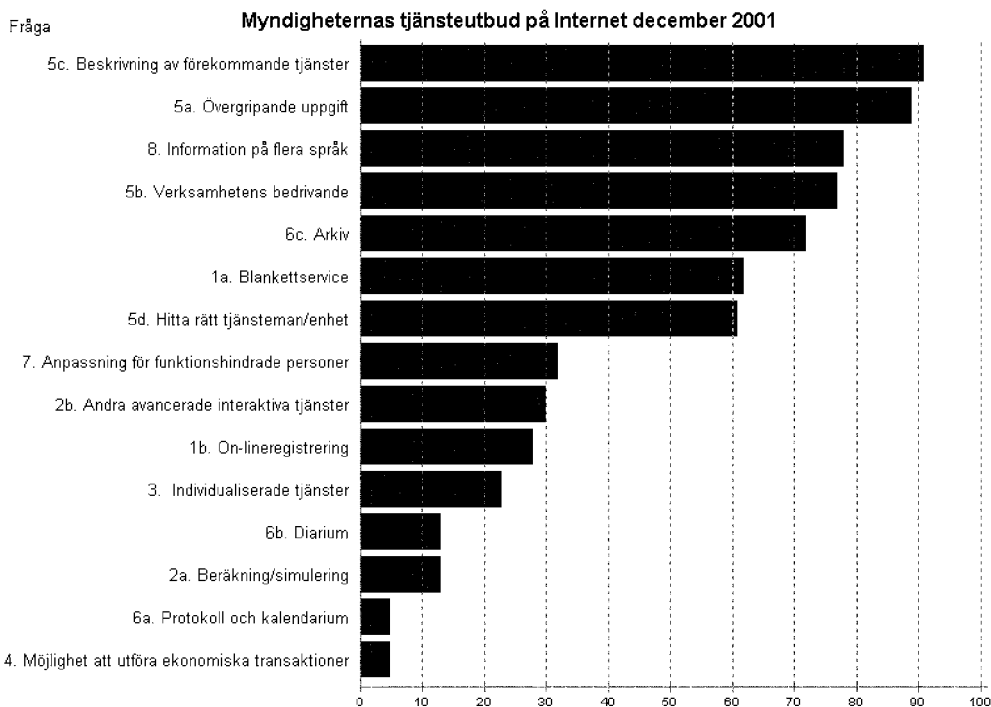
ra att 36 av de 94 myndigheterna (38 procent) inte har någon poäng alls på integritetshotvariabeln – man saknar helt de integritetshot som definierats i denna undersökning. På samma sätt som i fråga om servicepoängen kan man här konstatera att spridningen är mycket stor. Det finns en grupp myndigheter där användaren kan utträta kvalificera de ärenden i utbyte mot integritetskänsliga uppgifter och det finns myndigheter som lämnar hög service till webbanvändare. Det är dock inte samma myndighet, vilket visats i figur 11. I figur 13 visas detta på ett annat sätt, där spridningen av servicepoäng inom de olika nivåerna för integritetshot syns tydligt.

Som framgår av figuren finns en mycket stor spridning av servicepoäng inom respektive nivå av integritetshot. Sålunda finner vi bland de myndigheter som inte har något integritetshot allt från 18 till 1 poäng. På sam-

ma sätt finner vi för värdet 15 på integritetshotsskalan servicepoäng mellan 21 och 7. Det går alltså utifrån detta inte att dra slutsatsen att en ökad service till medborgaren automatisk innebär ett ökat integritetshot.

Är bilden av myndigheterna konsistent?

Statskontoret har i december 2001 genomfört en undersökning av hur långt myndigheterna har kommit i arbetet med 24-timmarsmyndighetsarbetet.⁵⁸ En intressant fråga i sammanhanget är då huruvida den bild som Statskontoret kommer fram till är konsistent med den bild som har redovisats här? Svaret är inte alldeles lätt att ge eftersom dels urvalet av myndigheter är olika, dels frågorna är olika. Statskontoret har i sin undersökning explicit frågat hur myndigheternas webbplatser förhåller sig till tjänsterna i 24-timmarsmyndighetskon-



Figur 13. Myndigheternas tjänsteutbud på Internet (Statskontorets decemberundersökning 2001).

58) Statskontoret, 2002

ceptet, medan den här studien fokuserat på service- och integritetsaspekter. Någon direkt jämförelse går därför inte att göra.

Däremot kan man se till det allmänna resultatet från de två undersökningarna. Följande bild sammanfattar Statskontorets resultat.

Som framgår av figur 13 är bilden från Statskontorets undersökning i stort samstämmig med resultatet av föreliggande studie. Myndigheterna använder i stort sett webben som en anslagstavla och som ett offentligt blankettarkiv. Det är presentationen av förekommande tjänster och övergripande information om myndigheten som dominerar. Det går också i denna undersökning en relativt tydlig gräns när man lämnar de allmänna informationstjänsterna och kommer in på mer specialiserade eller individbaserade tjänster. 30 procent av myndigheterna i Statskontorets studie har avancerade interaktiva tjänster och on-line-registrering m.m., vilket stämmer förhållandevis väl med observationen tidigare i

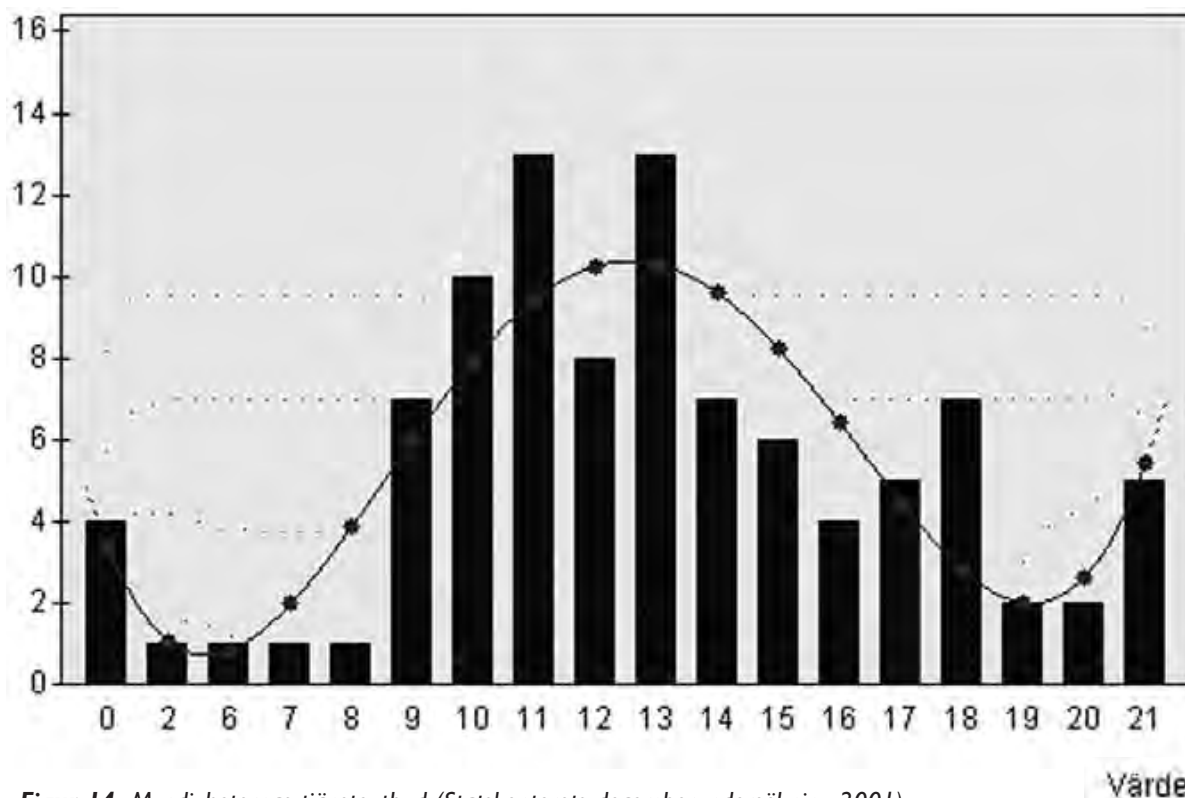
föreliggande studie att drygt 30 procent av myndigheterna har kontaktmöjligheter som har klassats som "starkt integritetshot", vilket oftast sammanfaller med avancerade individbaserade tjänster.

Även den sammantagna bilden av hur poängen fördelar sig inom myndighetskollektivet är likartad den undersökning som redovisats ovan.

Skillnaden mellan figur 9 och figur 14 är i första hand att fler myndigheter finns högre upp i skalan hos Statskontoret än i föreliggande studie, men detta kan sannolikt förklaras av dels skillnader i frågor, dels skillnaden i urval och att det dessutom sannolikt skett förändringar på myndigheternas webbplatser under perioden augusti – december 2001.

Slutsatser

Om man jämför de studerade 94 svenska myndigheternas användning av Internet som kommunikationsmedel visavi medborgarna i



Figur 14. Myndigheternas tjänsteutbud (Statskontorets decemberundersökning 2001).

augusti 2001 är det vissa saker man speciellt lägger märke till.

En första reflektion är den stora *olikheten* mellan myndigheternas sätt att hantera mediet Internet. Denna observation har gjorts tidigare men befasts åter i denna studie.

En andra reflektion gäller att många myndigheter har en *svag servicegrad* på nätet: endast 15 av de 94 undersökta myndigheterna (16 procent) får hälften eller mer av servicepoängen, vilket bör innebära att det är svårt för många användare att få stöd och/eller få tag på rätt material.

En tredje reflektion är att *navigering* förefaller vara ett obekant begrepp för myndigheternas webbkonstruktörer – i de allra flesta fall får användaren famla eller söka – s.k. navigeringskartor finns i de allra flesta fall inte.

En fjärde reflektion avser en till synes stor omedvetenhet om *integritetsfrågor* i allmänhet och personliga uppgifter i synnerhet. Detta är sannolikt ett resultat av bristande genomtänkthet snarare än ett medvetet val. För denna tolkning talar det faktum att nästan inga myndigheter har någon form av integritetsdeklaration eller motsvarande upplysningar.

När man ser till i vilka sammanhang integritetshoten visar sig kan man snarare dra

slutsatsen att dessa uppkommer på grund av önskan att ge användaren service och tillgång till material, men att man när man skapat denna tjänst inte funderat särskilt mycket på de eventuella negativa konsekvenserna av denna hantering.

Mot denna tolkning talar att många myndigheter i onödan begär uppgifter, t.ex. e-postadress för att sända information som skulle ha kunnat finnas på myndighetens webbplats för nedladdning. Att så är fallet visar också det faktum att det inte finns något samband mellan servicepoäng och integritetshotpoäng – *det går utmärkt att erbjuda hög service utan att för den skull begära information om den som söker service.*

Bilden av myndigheternas hantering av uppgifter befasts vid en jämförelse med Statskontorets undersökning i december 2001. Även i den studien framkommer bilden av myndighetswebben som i första hand en informationskanal. Samtidigt verifieras också uppfattningen att cirka en tredjedel av myndigheterna har individanpassade eller andra kvalificerade tjänster – tjänster som genom sin konstruktion och sin relation till den person som använder dem i sig konstituerar ett potentiellt hot mot integriteten.

KOMPLEXITETENS KONSEKVENNS

Det sägs att när man läser avtalsförslag så skall man hela tiden utgå från det värsta som kan hända. Avtal skall skrivas för den situation där parterna är oense om allt. Detta kan vara en förnuftig inställning – om parterna vore överens hela tiden behövdes inget avtal till att börja med.

I grunden gäller samma resonemang när man ser på den enskildes relation till myndigheter, Internet och integritet – utgå från det värsta! I ett läge där allt fungerar som det är tänkt och där alla uppträder på ett sätt som inte stör någon annan finns ingen anledning att reglera skyldigheter och rättigheter – men så är som bekant inte alltid fallet.

En invändning emot en misstänksam syn på relationen medborgare–myndighet är att "den som inte har gjort något har inget att frukta", eller varianten att "den som inte är skyldig har inget att dölja". Denna invändning innehåller ett antal felaktiga argument, men det viktigaste är att den helt bortser från effekten av den dramatiskt ökade informationsmängden och hastigheten i hanteringen av informationen. Som har diskuterats i andra sammanhang lämnar vi nu så många elektroniska spår efter oss att den som har intresse, förmåga och kunskap om hur dessa skall samlas upp kan skapa en "fantombild" av oss som innehåller så pass mycket information som många nog skulle anse som integritetskrän-

kande.⁵⁹ En fara i detta ligger i att den som så önskar och har tillgång till tekniken kan välja vilka fakta man skall presentera och ändra sammanhanget dem emellan så att bilden av personen som fakta rör blir helt fel – även om data i sig är helt korrekta.⁶⁰

Nu är emellertid detta försvar emot invändningen tämligen meningslöst – argumentet mot tesen om de oskyldigas rättvisa behandling skall inte bemötas med tekniska argument utan med moraliska och etiska. Det grundläggande argumentet är i stället att informationen om mig som individ är min egendom och användningen skall bestämmas av mig. I de fall andra skall samla in, lagra eller använda information om mig skall detta baseras på ett avtal eller en affärstransaktion eller på mina skyldigheter som medborgare. Detta argument är knappast särskilt kontroversiellt – det är i själva verket just den argumentationen som ligger bakom EUs direktiv om skydd för personuppgifter. I den tidigare redovisade utredningen om integritet i arbetslivet visade också genomgången av integritetsdebatten att rätten till personlig integritet och rätten till en privat sfär i de allra flesta fall ses som en mänsklig rättighet, och som sådana inte behöver någon positiv argumentation – det är tvärtom så att den som avser att minska den personliga integriteten eller minska den privata sfären har ansvaret för argumentationen på sin sida.

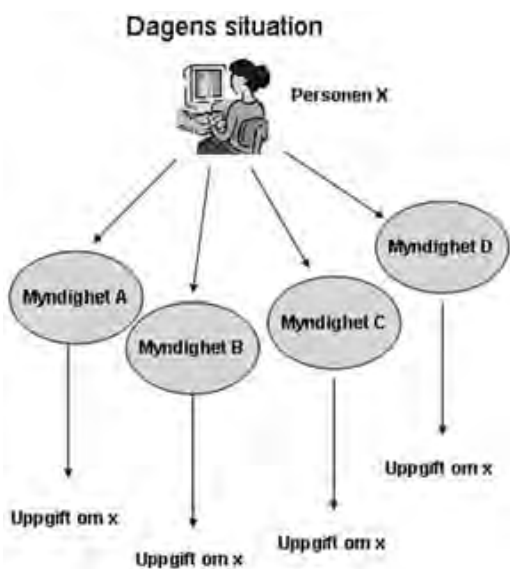
59) Nydén, M., 2000

60) I Erik Rydings "Konsten att luras utan att ljuga" redovisas den klassiska historien om kaptenen och styrmannen. Samma teknik kan lika gärna användas om politiska motståndare, konkurrenter eller människor som man har ett horn i sidan till.

Det är också detta som måste vara utgångspunkten för en kritisk granskning av relationen mellan staten, myndigheterna och medborgarna – inte tekniska frågor, inte bekvämlighetsfrågor eller ekonomiska frågor – utan huruvida en omfattande allmän hantering av privat information är förenlig med den västerländska synen på mänskliga fri- och rättigheter.

Den i grunden förändrade relationen

Tidigare kan relationen mellan myndigheter och medborgare i grunden sägas ha varit asymmetrisk – den enskilde har alltid haft mer information om sig själv eller det ärende saken gäller än myndigheten och har lämnat ifrån sig just så mycket information som myndigheten har behövt för att kunna hantera ärendet. Myndigheten å sin sida har fattat beslut om vilka uppgifter man behöver om vederbörande utifrån just perspektivet att ett visst ärende skall kunna avgöras. Relationen kan ses på sätt som framgår i figur 15.

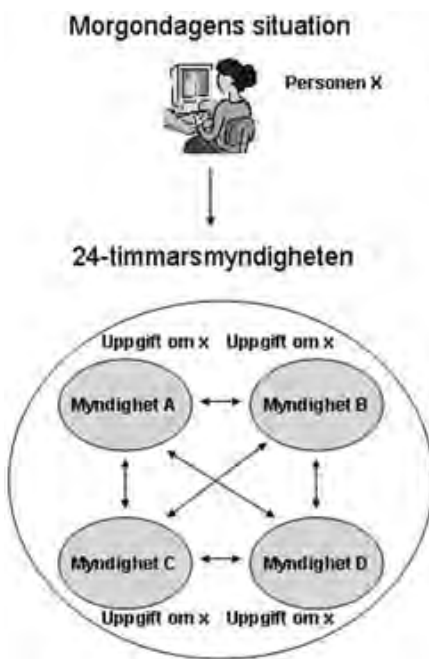


Figur 15. Dagens datarelation mellan medborgare och myndighet.

Figuren är självklart förenklad – redan idag finns grunddata om enskilda personer (t.ex. personnummer) vilka delas mellan många

myndigheter. Men huvudregeln är ändå den att myndigheter samlar in uppgifter om individer för att kunna lösa *sina* myndighetsuppgifter på ett rättssäkert sätt. Detta innebär också att informationen står i direkt relation till det regelverk som är upprättat för handläggningen av ärendet. Detta i sin tur innebär att det finns transparens i hanteringen för den som vill ta reda på varför vissa uppgifter skall lämnas – i den ideala situationen skall man genom att ta del av regelverket kunna se motiveringen till varför vissa uppgifter krävs av myndigheten. Även om detta i praktiken knappast låter sig göras alltför ofta så finns genom kopplingen mellan myndighet, regelverk och datafångst åtminstone denna möjlighet i teorin.

Jämför man denna situation med hur bilden ser ut om intentionerna bakom 24-timmarsmyndigheten genomförs fullt ut så framstår skillnaderna klart.



Figur 16. Datarelationen medborgare–myndighet efter 24-timmarsmyndigheten.

Här följer samhället – och myndigheterna – principen att en uppgift om en person enbart registreras *en* gång på *en* plats. När dessa data

sedan behövs av andra myndigheter hämtas de från den myndighet som lagrat dem. Den myndighet som lagrar data ansvarar också för att de är korrekta och uppdaterade och för att den tekniska miljön är funktionell. Från datateknisk och effektivitetssynpunkt och en medborgerlig bekvämlighetssynpunkt är detta en betydligt mer rationell arbetsmodell. Så vad är då problemet?

Det grundläggande problemet är att integritetsfrågor inte kan bedömas eller rättfärdigas utifrån datatekniska, effektivitetsmässiga eller bekvämlighetsmässiga argument. Integritetsfrågor skall i stället bedömas utifrån argument om *risk och konsekvenser*. Och i *detta perspektiv* kan den nya relationen mellan medborgare och myndighet bli problematisk.

Myndigheter är också människor

24-timmarsmyndigheten bygger till synes på en i grunden superrationalistisk tanke om hur myndigheter skall fungera och hur de skall hantera medborgarna, d.v.s. "kunderna". Detta är i sig knappast förvånande – svensk förvaltningspolitik har alltid haft ett drag av samhällsingenjörskap. Mot denna maskinmässiga syn på förvaltningen kan ställas en helt annan syn – förvaltningen som en organisation vars främsta uppgift är att klara sig – "the noble art of muddling through".⁶¹

Utgångspunkten här är snarast den att myndigheter är organisationer som alla andra organisationer, med fel, brister och förtjänster. Och som ofta fattar beslut och genomför åtgärder – inte för att i första hand uppnå de mål som riksdag och regering ställt upp utan för att klara budgeten, hantera personalproblem och för att växa i makt och inflytande. Kanske

inte en så glamorös syn på myndigheter, men förmodligen en betydligt mer korrekt än den rationalistiska maskinmodellen. Och tar man sin utgångspunkt i detta kapitelns inledning, nämligen att avtalsförslag alltid skall läsas utifrån perspektivet att parterna blir oense, är detta en betydligt mer givande infallsvinkel ur vilken man bör betrakta fenomenet 24-timmarsmyndigheten.

Empiriskt stöd för en organisationsmodell saknas inte. Den undersökning som redovisats tidigare och även Statskontorets decemberundersökning från 2001 pekar mycket tydligt på just detta fenomen. Om man ser till fördelningen av hur långt olika myndigheter har nått inom områdena service, integritet och uppfyllande av kriterier för 24-timmarsmyndigheten så slås man av att den nästan är normalfördelad. Om den rationalistiska teorin om myndigheter hade gällt hade fördelningen knappast sett ut på detta sätt – regelverket är ju detsamma för alla myndigheter och om de agerat rationellt borde de ha kommit lika långt i IT-utvecklingen. Här visas snarast att IT-mognaden hos myndigheter utvecklas på ett till synes oberoende sätt, dvs. har mycket lite med styrning från departement eller annat att göra. En gissning är att IT-mognaden hos myndigheterna har betydligt mer att göra med hur myndigheten uppfattar *nyttan* med webbplatsen än med diverse styrsignaler från regering och departement. Faktorer som budget, tillgång till kompetens, möjlighet att frigöra resurser m.m. spelar med stor säkerhet också en större roll än program utan andra resurser än direktiv.

Nu skall detta inte betraktas som en anomaly, som ett tillfälligt tillstånd som inom kort övergår i den rationalistiska modellen förut-

61) Den kanske bästa beskrivningen av dessa två paradigmen återfinns i Allison, Graham T. och Philip Zelikow, "Essence of Decision: Explaining the Cuban Missile Crisis", 2 utg. Reading, MA: Longman, 1999. Här analyseras utifrån bl.a. dessa två perspektiv hur mycket man kan förklara av den amerikanska förvaltningens agerande under Kubakrisen.

sägbara och styrbara system – nej, det skall betraktas som normaltillståndet. Det är så här det är – och det blir inte annorlunda. Myndigheterna är organisationer som organisationer är mest, och det faktum att regelverket är tillkommet via riksdag och regering påverkar nog förhållandevis lite det vardagliga arbetet.

Ett exempel på detta kan hämtas från Datainspektionens rapport om skyddade personuppgifter i folkbokföringen. Här undersöker inspektionen hur de myndigheter som hämtar uppgifter ur folkbokföringsregistret hanterar dessa data i sina system – alltså i princip exakt så som 24-timmarsmyndighetens fjärde steg är tänkt att fungera. Folkbokföringsuppgifterna lagras av en myndighet (skattemyndigheten) och lämnas därifrån enligt offentlighetsprincipen ut till andra myndigheter – kommuner, statliga myndigheter, kyrkliga myndigheter m.fl. I dessa organisationer används ofta folkbokföringsuppgifterna i den mottagande myndighetens egna system. Datainspektionen konstaterar i sin inspektion:⁶²

Däremot finns en inte obetydlig risk för att spärrmarkerade personuppgifter hos kommunerna kommer i orätta händer när uppgifterna finns registrerade i de kommunala förvaltningarnas administrativa register. Anledningen är att den sekretess som gäller inom folkbokföringen inte överförs från kommunernas befolkningsregister till de kommunala förvaltningarnas administrativa register. Personuppgifterna kan dock omfattas av annat sekretesskydd vid den enskilda kommunala förvaltningen. Det föreligger exempelvis sekretess inom socialtjänsten för uppgift om enskilds personliga förhållanden. Vid flera kommunala förvaltningar saknas dock bestämmelser om sekretess som kan omfatta den enskildes personuppgifter.

I folkbokföringsregistret finns alltså spärrmarkeringar som talar om för användaren av registret att uppgiften är skyddad och inte skall lämnas ut. I rapporten konstateras att när andra myndigheters handläggare har direkt tillgång till folkbokföringsregistret fungerar oftast spärrmarkeringarna utan problem. Men när data skall flyttas till t.ex. kommunens eget register faller spärrmarkeringen bort, och plötsligt har personens skydd i praktiken upphört! Detta har inte skett genom dålig kompetens, illvilja eller av andra icke legala orsaker, utan därför att IT-systemen inte är kompatibla och för att kostnaden för att göra dem kompatibla sannolikt är för hög. Det är inte ens säkert att den hämtande myndigheten är medveten om problemet eftersom man enbart använder de data som rutinmässigt hämtas från folkbokföringen. Av naturliga skäl kan man inte se det som inte finns därför att det fallit bort i importen.

Konsekvensen av resonemanget ovan är ganska given. I takt med att styrbarheten av myndigheterna minskar och andra faktorer spelar en allt större roll för myndighetens beteende kommer också riskerna för medborgaren vid hantering av arbetsuppgifter att öka. Om lagringen, uppdateringen och kontrollen av data är beroende av personaltillgång, sjukskrivningar, kompetensnivåer m.fl. vanliga organisatoriska bekymmer, så kommer också riskerna för att data blir fel, inte uppdaterade eller lagrade på ett osäkert sätt att öka. Att i en sådan situation applicera en centralistisk modell där myndigheterna skall lita på varandra för lagring, uppdatering och andra datatekniska insatser ökar självfallet riskerna. En rubrik ur *Dagens IT* kan illustrera situationen (figur 17). Här redovisas hur stationerna för bilbesiktning runt om i landet

62) Datainspektionen 1999:3: Skyddade uppgifter i folkbokföringen, 3

tvingades stänga eftersom de centrala datorerna klickade. Nu kan man tycka att denna kalamitet inte var särskilt stor – men som ett exempel på vad som riskerar hända med centraliserade datalager kan det fungera bra. Om det hade gällt skatteuppgifter eller personuppgifter – hade det då varit lika harmlöst?

Nu kan man (med rätta) hävda att det inte är realistiskt att alla myndigheter lagrar sina egna data om de personer man interagerar med. Detta vore i hög grad ineffektivt. Men att gå till den motsatta änden, vilket är 24-timmarsmyndighetens konsekvens – att alla data om en enskild person enbart lagras en gång av en myndighet – är också att gå för långt.

Tyngdpunkten i argumentationen här är att det vore att skapa en för hög risk från integritetsskyddssynpunkt att centralisera samhällets data om medborgaren till en enda myndighet. Erfarenheten lär oss att myndigheter

delar egenskaper med andra organisationer och att icke-optimalt beteende inte är anomalier utan snarare ett normaltillstånd. Ur integritetsperspektivet är det mot denna bakgrund bättre om centralisering av data hålls på en lagom nivå.

Rätt data till fel ändamål

En grundläggande regel för datainsamling är att data enbart skall användas för det ändamål de insamlades för. Grunden för detta är självklar – data samlas oftast in för ett specifikt ändamål, och metoden för insamlingen liksom lagringen av data är oftast kopplad direkt till motivet för insamlingen. Därmed också sagt att man inte utan vidare kan använda data insamlade för ändamål X som ett underlag för ändamål Y. Detta har också uppmärksamats av EU i personuppgiftsdirektivet.⁶³

The screenshot shows a newspaper website with a navigation bar at the top containing links like 'Affärsvärlden', 'Ny Teknik', 'dagensit.se', 'Dagens Medicin', 'Elektroniktidningen', 'Miljörapporten', and 'Konsultguiden'. Below the navigation is a banner for 'Vinn en matlagningskurs!' featuring a photo of a person. A secondary navigation bar includes categories like 'Allmänt', 'Börsen', 'Internationellt', 'Nätaffärer', 'Kariär', 'Telekom', 'Produkter', and 'Tjänster'. The main content area is dated 'Tisdag 19 mar' and features an article titled 'Datorkrångel slog ut bilbesiktningen'. The article text states that 175 inspection stations across the country were closed on Tuesday morning due to a system failure. A sidebar on the left lists various news items, and a right sidebar contains an advertisement for 'Nu kan du vinna Det Trådlösa Kontoret Klicka här!' featuring a pug dog.

Figur 17. Artikel om utslagningen av Bilprovningen (Dagens IT 02-01-10).

63) EU, 1999 COM(1999) 337 final 99/0153 (COD), 9

Further processing for compatible purposes

1. Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.

Även om direktivet tillåter data att användas för andra ändamål än för vilka de samlats in så är ändå detta hanterande omgivet av förhållandevis starka spärrar. Bland annat krävs uttryckligt tillstånd i regelverket hos den europeiska myndighet som skall övervaka hanteringen av persondata.

Ett exempel kan illustrera problematiken. Vid flera olika kontakter med myndigheter förväntas individen uppge storleken på sin bostad – det kan gälla bostadsbidrag, fastighetstaxering eller andra legala eller fiskala ärenden. Varför då inte göra det bekvämt för vederbörande och lagra alla data på ett ställe så slipper man hålla reda på detta? Därför att de olika uppgifterna hämtas på olika sätt och vid olika tidpunkter och är därför inte helt jämförbara. Detta kan resultera i två lösningar; den första är *minimallösningen* och innebär att man nöjer sig med de gemensamma data som finns – inte de som behövs – vilket innebär att underlaget för beslut blir sämre. Man avstår i detta fall från att samla in korrekta uppgifter eftersom det sannolikt finns *nästan korrekta* uppgifter till hands. Den andra är *bruttolösningen*, dvs. man samlar in alla data som alla myndigheter behöver inom ett område. Detta innebär att samhället måste lagra data som tillfredsställer alla myndigheters behov vid olika tillfällen, och därför är man tvungen att skapa ett register med mycket mer information än vad som krävs för att de enskilda myndigheterna skall kunna lösa sina uppgifter. Risken för att man skapar centrala dataregister med avsevärda informationsmängder blir

stor. Situationen kan enkelt beskrivas; myndigheten A behöver data X, Y och Z, myndigheten B behöver data Y, Z och V medan myndigheten C behöver data Y, T och W. Med den minimalistiska lösningen lagras data X, Y och Z – vilket innebär att ingen av myndigheterna får sitt behov tillgodosett. Alternativet är att lagra X, Y, Z, T, V och W, vilket tillgodoser samtliga myndigheters behov men samtidigt skapar ett system med sammantaget överflödigt data om personen ifråga. Vem garanterar att kombinationen av data inte används på ett sätt som inte är avsett?

Grundtankarna i 24-timmarskonceptet riskerar att i praktiken skapa en situation liknande denna. Även om ambitionen är god – att en person inte skall behöva gå runt till olika myndigheter för att hämta uppgifter som behövs för att genomföra ett ärende – är risken ändå stor att systemet med delad information mellan myndigheter, när det har byggts ut kommer att skapa det integritetshot som beskrivits ovan. I en värld där myndigheter agerar efter ett rationalistiskt paradigm uppstår inte denna situation – problemet är bara, vilket konstaterats ovan, att i verkliga livet är det inte rationalitet som styr handlandet utan betydligt oftare "muddling through".

Kan man prata med en agent?

En konsekvens av tankarna bakom 24-timmarsmyndigheten är införandet av en omfattande automation i myndighetshanteringen. Simuleringar, blankettifyllande via Internet, avancerade fråga-svar-funktioner – detta blir vardagsmat i en framtida myndighetsstruktur som bygger på en *front-office-* respektive *back-office-* lösning av den typ som skisserats av Statskontoret. Detta i sin tur kommer att kräva en omfattande automatisk hantering. Av rena arbetstekniska skäl kommer den e-aktiva medborgaren att behöva mötas av en virtuell tjänsteman. Det finns inga möjligheter för

någon myndighet att bemanna verksamheten så att idén bakom den ständigt öppna myndigheten kan förverkligas, utan stora resurser kommer att behöva läggas på att skapa automatiserade system. Men vad kan då detta innebära?

En första konsekvens blir att myndighetens ärenden måste översättas till regler som kan tillämpas automatiskt. Denna process är långt ifrån enkel och kan, vilket bl.a. har visats av Magnusson-Sjöberg, innebära att personer som inte har något verksamhetskunnande eller rättslig kunskap skapar översättningen från lag/förordning/regel till datatekniskt regelverk.⁶⁴ Den tänkta modellen med myndigheter som har huvudansvar för vissa typer av data och som sedan delar med sig av dessa data till andra gör inte denna bild enklare. Man får här en ökad risk för uttunning av verksamhetskunnandet i flera led – först i den myndighet som har att hantera ärendet, sedan i den eller de myndigheter som skall stötta den första myndigheten genom tillhandahållandet av data.

Den första myndigheten har inte kunnande om alla de data och datakällor som skall ingå i översättningen från förordning till datasystemets regel, utan enbart de data som myndigheten själv samlar in och lagrar. Den andra myndigheten har sannolikt inte kunskap om alla de tillämpningar som de data som de lagrar är tänkta att användas i och kan därför inte heller ta hänsyn till dessa vid lagring, uppdatering eller motsvarande. Det tidigare redovisade exemplet från Datainspektionens inspektion av hanteringen av folkbokföringsdata är även här illustrativt. De företag som konstruerade kommunernas datasystem där folkbokföringsdata användes kände sannolikt inte till skattemyndighetens system med spärrmarkering, vilket innebar att denna funktion

föll bort på kommunal nivå. Eftersom de inom kommunen som använder systemen sannolikt inte har varit med och konstruerat dem och inte heller har kunskap om principerna för skattemyndighetens lagring av data blir effekten att den information som skulle skydda den personliga integriteten kan falla bort utan att någon saknar den. Eftersom skattemyndigheten bara tillhandahåller data och inte ser den slutliga användningen har inte heller denna myndighet möjlighet att upptäcka misstag och fel i hanteringen.

Den tyngre invändningen mot den automatiserade rättshanteringen har emellertid inget att göra med de problem som kan uppstå inom myndigheterna. Den handlar i stället om hur den enskilde möter myndigheten.

Som har visats i redovisningen i undersökningen av de 94 myndigheterna finns i augusti 2001 enbart ett fåtal myndigheter som har någon form av interaktiv dialog över nätet med medborgaren. Statskontorets undersökning visar också att antalet myndigheter med simuleringar eller andra former av automatisk behandling av data är litet. Det finns därför heller inga data om hur personer har reagerat på att interagera med myndigheter på detta sätt. Däremot kan man föra resonemang om de tänkbara effekterna.

En första punkt är att många, för att inte säga de allra flesta, i Sverige kommer att välkomna en möjlighet att agera gentemot myndigheterna elektroniskt. Något som talar för detta är den stora acceptans som banktransaktioner över Internet har fått. Även amerikanska undersökningar om hur "e-citizens" ser på "e-government" tyder på att de allra flesta som använder Internetkoppling till myndigheterna skattar denna service högt.⁶⁵

64) Magnusson-Sjöberg, C., 1992, 508–510

65) Pew Internet & American Life Project, 2002: The rise of the e-citizen: How people use government agencies' web sites.

Q: How much does the Internet improve your interactions with government?

The percent who say it improves their interactions

	A lot	Some	Only a little	Not at all
Federal government	20	29	25	23
State government	18	27	27	26
Local government	11	19	18	48

Tabell 1. Amerikanska medborgares uppfattning om effekten på interaktionen med myndigheter av elektronisk hantering.

Uppenbarligen uppfattar många amerikanska medborgare att kontakten med myndigheterna förbättras via Internet och det finns knappast något skäl att tro att situationen skulle vara annorlunda i Sverige.

Samtidigt skall man nog se dessa siffror mot ljuset av att en "äkt interaktivitet" ännu inte sett dagens ljus, dvs. en situation där myndigheten per automatik hanterar ett stort antal av medborgarens ärenden. Det är nog snarare så, vilket också stöds av den amerikanska undersökningen, att Internet i dagsläget gör det lättare för medborgare att få information från myndigheterna och att detta sker på ett betydligt lättare sätt än tidigare. Den tidigare redovisade undersökningen av svenska myndigheters utbud på webben stöder också denna slutsats – information om verksamheten är idag för den absoluta majoriteten av myndigheter den enda tjänsten på Internet.

Sannolikt kommer saken i ett annat läge när man skall börja genomföra faktiska ärenden via Internet och detta blir det enda sättet att utföra dem på. För det finns knappast någon anledning att tro att myndigheterna i längden kommer att behålla såväl manuell som elektronisk betjäning – inte när besparingspotentialen av det fjärde steget är så stor.

När medborgaren t.ex. skall deklarerera sin årsinkomst via Internet och systemet inte tillåter vissa typer av handlingar som var möjliga vid manuell hantering – då riskerar också förtroendet för systemet att minska drastiskt. Det är orealistiskt att tro att det går att göra ett deklARATIONssystem som tar hänsyn till alla varianter, och det är lika orealistiskt att tro att det kommer att fungera smärt- och felfritt att översätta legala regler till dataregler. Att lägga ut en förenklad självdeklaration på Internet med i grunden mycket svagt integritetsskydd, vilket nu är fallet, är något helt annat än att hantera alla typer av deklARATIONER på Internet utan manuella alternativ.⁶⁶

EU har i sitt direktiv behandlat denna fråga och konstaterat att detta inte är en rättssäker modell.⁶⁷

Article 21

Automated individual decisions

No one shall be subject to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, reliability or conduct, unless the decision is expressly authorised by a

66) Vid 2002 års deklARATION kan man genomföra en förenklad självdeklARATION över Internet. Säkerhetskontrollen innebär att deklARANTEN får ett kontrollnummer i den papperskopia man får hemsänd och kan ange denna i stället för att under-teckna deklARATIONEN. Ännu är det inte utrett vad som skulle hända om någon kom över någon annans kontrollnummer och deklARERADE I DENNAS ställe.

66) EU, 1999, COM(1999) 337 final 99/0153 (COD)

legal provision which also lays down measures to safeguard the data subject's legitimate interests.

Även om denna paragraf är något tänjbar kan man ändå konstatera att EU enbart genom att lyfta in frågan har observerat att det finns en potentiell konflikt mellan en automatiserad rättsprocess och medborgarens intressen – och åtminstone delvis ställt sig på individens sida.

Försvarsperspektiv

Internet är resultatet av en amerikansk försvarsatsning. Systemet med "paketförmedling" av data togs fram för att garantera att militär information skulle kunna sändas till olika amerikanska militära inrättningar även om landet varit utsatt för en kärnvapenattack som kunde förutses slå ut de flesta förbindelserna. Kravet var här att samma information skulle kunna gå många vägar och inte vara beroende av en enda väg som kunde skäras av.

Synsättet här kan beskrivas som "riskaversion". Även om man bygger aldrig så säkra förbindelser mellan två punkter kan man inte eliminera risken att förbindelsen skärs av samtidigt som konsekvenserna av att risken skulle bli en händelse är så stora att det är oacceptabelt. Resultatet blir således att man bygger system med redundans – om inte data kan gå den ena vägen kan de gå den andra. Denna modell används idag inom nästan all hantering av systemkritiska data eftersom det är ett sätt att minimera konsekvenserna av ett avbrott i kommunikationerna. I grunden kan samma synsätt appliceras på samhällets hantering av persondata och det är precis detta som enligt min mening inte har gjorts när man diskuterar det fjärde steget.

Ur ett försvarsperspektiv är det ett grundläggande krav att känslig myndighetsinfor-

mation om medborgare inte kan nås, störas eller förändras av någon annan – vare sig "den andra" är en främmande makt, en kriminell organisation eller "bara" en hacker. I takt med att samhället mer och mer får karaktären av ett informationssamhälle blir det också denna information som i allt högre grad kommer att vara samhällsbärande. Utredningen *Säkerhet i en ny tid* konstaterade:⁶⁸

En annan sida av utvecklingen är att samhället har blivit starkt beroende av IT. IT har blivit den viktigaste komponenten för informationsförsörjning, oavsett om det gäller information till privatpersoner, företagsinformation, teknisk information till styrsystem för andra teknikområden, eller någon annan typ av information. Information är en av de mest värdefulla tillgångarna i dagens samhälle. Den behöver skyddas likaväl som de fysiska tillgångarna. Viktiga samhällsfunktioner kan bli svårt störda, med i värsta fall katastrofala följder, om deras IT-stöd skulle störas eller slås ut. IT är i sig beroende av områdena elförsörjning och telekommunikationer för sin funktion (telekommunikationer kan med ett visst synsätt även betraktas som en del av IT), men IT utgör ändå något väsentligt mer än dessa båda områden tillsammans.

Detta är naturligtvis sant, även om utredningen här nog i första hand inte tänkte på personinformation i sitt konstaterande. Jag skulle dock vilja gå så långt att jag hävdar att personinformationen kanske är en än viktigare datamängd ur ett försvarsperspektiv – såväl ur psykologisk synvinkel som ur en försörjningsmässig och fysisk. Nyckelpersonerna inom dessa områden blir lätta att identifiera och därmed sårbara.

Den grundläggande informationen om enskilda individer – personnummer, bostadsförhållanden, ekonomiska förhållanden, släkt-

68) SOU 2001:41: Säkerhet i en ny tid, 187

skap, kontakter med myndigheter m.m. – är lika vital för den som vill störa samhällsordningen som för den som vill bevara den. Den tidigare citerade utredningen tar också detta som sin utgångspunkt för förslag:⁶⁹

All offentlig förvaltning skall bedrivas med betryggande säkerhet i internt arbete, arbete mellan myndigheter, arbete gentemot medborgarna och internationellt. Förvaltningen skall erbjuda en hög servicegrad och kunna nå elektroniskt samt kunna erbjuda tjänster för spridning och hämtning av information via allmänna kommunikationsmetoder. Detta skall ske med god tillförlitlighet, tillgänglighet och säkerhet. Det skall gå att säkert kommunicera inom landet och med omvärlden. Elektroniska affärer skall kunna bedrivas säkert. Ett informationssamhälle för alla förutsätter även att hela den infrastruktur som informationen beror av är säker och har hög tillgänglighet. Krav ställs på förebyggande säkerhetsåtgärder, på säkerhetsåtgärder vid upptäckt av intrång och på reaktiva åtgärder. Säkerhetsåtgärderna skall medge upptäckt vid försök till intrång samtidigt som de skall ge tillräckligt med tid för att hindra eller begränsa intrånget. Tilltron till ny informationsteknik är i mycket stor grad beroende av tilltron till de tekniska systemens säkerhet. Det inkluderar tilltro till att systemen bevarar och garanterar sekretess, äkthet och riktighet avseende den information som hantearas. I förvaltningssammanhang är detta viktigt, inte minst för den personliga integriteten och medborgarnas trygghet.

Samtidigt som utredningen konstaterar detta grundläggande krav på IT-säkerhet kan man konstatera att denna utredning är den första egentliga statliga utredning som tar ett helhetsperspektiv på säkerhetsfrågor där IT ing-

år – och att detta sker år 2001 när i stort sett alla myndigheter har en mycket aktiv IT-verksamhet med registrering, webbplatser m.m. Det anmärkningsvärda med utredningen är knappast vad som sägs eller de förslag som läggs fram, utan snarare att det inte har sagts betydligt tidigare. Man kan läsa utredningen så att den konstaterar att de grundläggande säkerhetskraven för samhällets hantering av IT idag inte är uppfyllda och att man redovisar förslag för att dessa krav skall bli uppfyllda. Detta är knappast heller någon unik svensk position – det norska Direktoratet for sivilt beredskap har i en rapport till Stortinget den 2 april 2002 konstaterat att stora delar av det norska samhället riskerar att slås ut vid en IT-attack, och att riskerna för IT-sabotage är betydligt större än risken för terroristattacker av det slag som drabbade USA den 11 september 2001.⁷⁰

Om man tar sin utgångspunkt i den ovan redovisade inställningen att förvaltning och myndigheter är som organisationer är mest, alltså inte rationalistiska utan mer av typen "muddling through" är konstaterandet om hotens dignitet inte förvånande. För att en organisation skall fördela om resurser från daglig verksamhet till skydd av olika system krävs sannolikt att något har hänt som har ökat medvetenheten om behovet av skydd. Det vore på sätt och vis orationellt att lägga stora resurser på skydd av funktioner som aldrig har mankerat på ett avgörande sätt. Ett bevis för att så faktiskt är fallet finner vi i förordet till Överstyrelsen för civil beredskaps skrift *IT – incidenthantering*:⁷¹

Försöksverksamheten har visat på brister i myndigheternas organisation när det gäller hanteringen av

69) Ibid, 196

70) *Dagens IT* 020402 resektive Direktoratet for sivilt beredskap, <http://www.dsb.no>

71) ÖCB, 2001: IT – incidenthantering

IT-incidenter. Vanligt är exempelvis att det inte finns etablerade rapporteringsvägar inom organisationen när något har hänt. Många incidenter upptäckts förmodligen aldrig.

Samma observation görs av revisionsföretaget Ernst & Young i en granskning av dataviruset Nimdas effekter Västra Götalandsregionen.⁷²

De intervjuede driftenheterna har inte haft några rutiner för att löpande bedriva säkerhetsmässigt systemunderhåll. Detta är en väsentlig anledning till att regionen drabbas i så hög grad. Det har inte funnits någon etablerad krisorganisation eller rutin för incidenthantering att aktivera.

I sammanhanget kan det också påminnas om att Nimdaattacken skedde enbart ett och ett halvt år efter millenniebuggsproblematiken, där nästan alla svenska IT-ansvariga gjorde omfattande genomgångar av systemen. Tydligt sjönk medvetenheten eller säkerhetstänkandet snabbt undan.

Även om Nimdaattacken var allvarlig och kostade stora pengar för många offentliga system har ingenting hänt i den omfattningen att viktiga samhällsfunktioner har hotats på grund av störningar i IT-system – sannolikt beroende på att antalet samhällskritiska IT-system fortfarande är relativt få och professionellt skötta. Men även om ingenting avgörande har hänt har *förutsättningarna* förändrats och kommer att fortsätta förändras i takt med att allt fler myndigheter inför datasystem med känsliga uppgifter och beslutsstödssystem. Vi har en situation och en hotbild om det finns ett fåtal datasystem med personuppgifter som sköts av professionella organisationer och en helt annan situation och en helt annan hotbild om vi har många datasystem med personuppgifter som sköts av myndigheter som har helt

andra kärnuppgifter än att sköta datasystem. Det första försvarsperspektivet är givetvis att främmande makt utnyttjar informationen i systemen för att skaffa sig kunskap om personer som är viktiga inom totalförsvaret. Här gäller åter att risken för intrång ökar på ett språngartat sätt ju mer komplexiteten i systemet ökar. Ett systems komplexitet definieras som antalet element i ett system och dess attribut, graden av interaktionen mellan elementen samt graden av inbyggd ordning i systemet. Eller uttryckt på ett annat sätt, ju större variation, desto större komplexitet. Ju mer komplext ett system är, desto svårare är det att förstå och kontrollera det och desto svårare att definiera systemets gränser och följaktligen, desto svårare att förutsäga systemets beteende. Ju mer komplext ett system är och ju mer dynamisk dess omgivning är, desto oftare måste kontrollmekanismerna avläsa de objekt som skall kontrolleras och återföra styrbeslut till systemet för att systemet ska kunna styras mot sitt mål. Om den tidigare framförda tesen om att myndigheter inte är rationalistiska till sin natur är korrekt så innebär detta att risken för intrång ökar till en nivå där den övergår till säkerhet – och kontrollmekanismerna kommer inte att ha möjlighet att åtgärda problemet därför att komplexiteten blir för hög.

Detta är ett passivt hot. Någon väljer att samla information om utvalda personer för att eventuellt använda i ett senare skede. Men systemen kan lika gärna användas för betydligt mer aktiva hot.

Det andra försvarsperspektivet är att en främmande makt använder samhällets digitala infrastruktur för att slå ut samhällets grundläggande funktioner utan att detta nödvändigtvis framstår som ett angrepp i någon form. På grund av den ovan redovisade ökningen i komplexitet kommer det att vara

72) Ernst & Young, 2001: Nimda – granskning av händelser i IT-verksamheten 2001

svårt att skilja medvetna angrepp från olycks- händelser eller från intrång av typen hacker – som inte uppfattas som angrepp utan snarare som någon form av "elektronisk graffiti". En skicklig motståndare kommer också att kunna dölja sina angrepp så att det liknar t.ex. ett virusangrepp. Det tidigare refererade Nimdaviruset kostade mycket stora belopp för många organisationer – enbart Västra Göta- landsregionen uppskattade kostnaderna till cirka 2 Mkr – men har inte klassats som "sam- hällsfarligt" utan uppfattas nog mer som "sådant som händer". Om en främmande makt av något slag väljer att utnyttja samhäl- lets sårbarhet inom IT-området kommer man nog inte att använda ett så relativt harmlöst angreppssätt som ett datavirus – men heller inte ett helt uppenbart angrepp. Nimdaviru- set och dess härjningar i samhällets olika system visade klart att sårbarheten finns där, men framförallt att de organisationer som idag använder datasystem i sin kärnverksam- het inte har en säkerhetsorganisation som är kapabel att hantera störningsriskerna.⁷³ I en situation där många olika myndigheter är ansvariga för data med betydelse för den per- sonliga integriteten blir risken för fel så stor att den "är så sannolik att den nästan är sann".

Det allvarligaste hotet från en tilltagande komplexitet torde dock vara att allmänhetens tilltro till systemen och till samhället i stort försvagas om systemen inte klarar sina upp- gifter eller om de inte hanteras på ett förtroen- deingivande sätt. Jämförelsen kan här gö- ras med reaktionerna på elavbrotten under 1999–2001. Likheterna mellan IT-system och elsystem är också påtagliga – det rör sig om komplicerade tekniska system av nätkaraktär

med många aktörer med olika grad av ansvar. Avbrott innebär också omedelbar arbetsför- lust i de båda systemen.

Styrelsen för psykologiskt försvar har i sin mätning av upplevda hot och risker 2001 bl.a. frågat ett representativt urval av svenskar om hur man ser på hotet från teknisk sårbarhet, bl.a. dåliga elledningar.⁷⁴ Över 45 procent av de tillfrågade var oroade eller mycket oroade av detta. I samma undersökning konstateras också att över hälften av de tillfrågade var oro- ade eller mycket oroade av datahackers.

Denna oro har egentligen liten grund i verkliga förhållanden – andelen strömavbrott har minskat från 1999 till 2000, men detta speglas knappast i opinionen.⁷⁵ Det man i stället kan se i detta exempel är sannolikt två helt olika kalkyler. Ur leverantörens kalkyl kostar det mer att ha en mycket hög leverans- säkerhet än att åtgärda akuta problem när de inträffar, i synnerhet eftersom leveranssäker- heten i grunden redan är så hög. Ur medbor- garens perspektiv är det knappast en fråga om pengar utan om en samhällelig infrastruktur som bara ska fungera. Det går knappast att avgöra vilken inställning som är rätt och detta är i sammanhanget inte heller intressant. Det som är intressant är att när en ekonomisk prin- cip möter en princip om vad samhället skall garantera så uppstår oro om de inte hamnar på samma slutsats. Samma resonemang kan föras om datasystem i samhällets regi med integritetskänsliga uppgifter. Mängden data om enskilda personer växer lavinartat. Den enskildas beroende i det dagliga livet av fun- gerande myndighetssystem ökar i samma takt. Detta ställer krav på myndigheter som förmår att hantera en ökande komplexitet och

73) Nimdaviruset var känt sedan länge innan det slog till mot svenska servrar. Många organisationer hade tidigt – hösten 2000 – åtgärdat problemet och drabbades inte men många hade ignorerat varningar och uppdateringar – ganska precis så som man skulle förvänta sig att organisationer betar sig om de inte är rationella i sitt agerande.

74) Bennulf, M., 2001: Opinion 2001

75) Statens energimyndighet, 2002

som har förståelse för vilka krav som ställs på myndigheterna för att medborgarna skall känna trygghet i hanteringen. Detta är inte en situation som idag är för handen. Enbart två myndigheter bland de 94 undersökta hade någon form av integritetsdeklaration, dvs. kunde tala om för användaren hur data som samlades upp i interaktionen skulle hanteras. Denna observation om myndigheternas okänslighet inför medborgarnas förväntningar stöds också om man ser till hur medborgarnas data i praktiken hanteras. Datainspektionen konstaterar:⁷⁶

Information om människor som myndigheter samlar in för sin verksamhet kan då komma att användas för andra ändamål och i andra verksamheter än de som uppgifterna ursprungligen samlades in för. Detta upplevs av många som ett intrång i den personliga integriteten. Varje år får Datainspektionen klagomål från personer som vänder sig emot att en myndighet har sålt uppgifter om deras namn och adress till externa intressenter för exempelvis marknadsföringsändamål, till kreditupplysningsföretag, inkassobolag eller till marknadsundersökningar. Försäljningen är alltså en effekt av myndigheternas IT-verksamhet som allmänheten inte alltid vill godta och det är viktigt att förtroendet för användningen av modern teknik hos myndigheterna inte skadas till följd av det sätt på vilket tekniken används.

Efter att ha genomfört en undersökning bland myndigheterna kan Datainspektionen konstatera att många myndigheter säljer information om enskilda personer, och detta utan stöd i lag eller författning:⁷⁷

Datainspektionen finner det anmärkningsvärt att

flera myndigheter säljer information utan något stöd i författning eller regeringsbeslut. Det är av stor vikt att datalagens regler efterlevs på denna punkt. Under 1990-talet har Datainspektionen flera gånger påtalat för olika statliga och kommunala myndigheter att de inte har rätt att sälja sin information, då denna intention har framkommit när t.ex. ett företag ansökt om tillstånd hos Datainspektionen att samköra sina register med myndighetens. Det är viktigt att klargöra att författningsreglering av ett personregister inte automatiskt innebär att personuppgifterna dessutom får säljas samt att myndigheten själv inte har rätt att besluta att de personuppgifter myndigheten samlat in skall säljas.

Samtidigt konstateras också att i och med att datalagen upphörde den 1 oktober 2001 och PuL börjat gälla så upphörde också det generella förbudet emot att sälja information och i stället införs ansvaret för personuppgiftsombudet att tillse att myndigheten följer reglerna i personuppgiftslagen.

Det finns således all anledning att befara att en utveckling mot 24-timmarsmyndigheten skulle kunna medföra svåra ansträngningar på förtroendet för myndigheternas sätt att hantera integritetskänsliga data. Den ökande komplexiteten tillsammans med myndigheternas arbetssätt och ovana vid datasäkerhetsarbete gör det mer än troligt att de krav på integritetsfull behandling som en person har rätt att ställa kommer att åsidosättas – allt oftare och med allt tydligare konsekvenser ju mer spritt ansvaret för personuppgifter blir samtidigt som samma uppgifter görs tillgängliga för allt fler. När detta har inträffat och kommit till allmän kännedom så kommer vi också att få precis den misstro mot det politiska systemet

76) Datainspektionen, 1998: Försäljning av myndighetsinformation, 3

77) Ibid, 8

och dess förmåga att hantera integritetskänslig information som EU-direktivet om personuppgifter var tänkt att motverka.

Integritet eller offentlighet?

EU – och då särskilt parlamentet – har uppvisat en tilltagande aktivitet för att skydda den enskildes integritet och rätt till informationen om sig själv. Detta visas inte enbart genom tillkomsten av personuppgiftsdirektivet utan även av det faktum att parlamentet i december 2001 förkastade kommissionens förslag till teleskyddsdirektiv, där det bl.a. föreslogs att teleoperatörer skulle spara loggar av digitala transmissioner (exempelvis e-post). Detta skulle ha kunnat medföra att exempelvis teleoperatörer och Internetleverantörer skulle ha blivit tvungna att föra register över e-brev, telefonsamtal m.m., som myndigheter skulle ha kunnat använda, bl.a. i brottsbekämpande syfte.⁷⁸ Nu ser det ut som om detta direktiv kommer att skjutas på framtiden.

EU-parlamentet har tidigare också visat stort intresse för Echelon, det i huvudsak USA-styrda spionsatellitesystemet vilket sägs kunna följa digitala sändningar i realtid.

Man kan säga att den svenska regeringen har valt en annan väg när man skall implementera EUs direktiv, vilket bl.a. syns i den tidigare refererade hanteringen av personuppgiftslagen. Regeringen valde här en förhållandevis sträng tolkning av direktivet när det gällde privatpersoners och journalisters möjlighet att komma åt och publicera personliga data, men valde samtidigt en strategi som i praktiken gjort den möjligt för myndigheter att hantera data hur man vill, med hänvisning till offentlighetslagstiftning. Den stränga tolkningen för privatpersoner innebar i stort sett

att det inte var möjligt för någon att publicera personuppgifter av något slag utan den omtalades medtycke. Denna position har sedermera mjukats upp avsevärt, bl.a. genom Ramsbodomen under sommaren 2001 och genom EUs ställningstagande till "Bodils hemsida".⁷⁹ Resultatet av detta ser ut att bli, om inte helt, så näst intill fritt fram, för privatpersoner och journalister att offentliggöra information om andra – antingen i form av journalistik, samhällsdebatt eller i form av konst.

Denna debatt om PuL har dominerat debatten om offentlighet i Sverige under senare tid och har då kommit att ställas emot offentlighetsprincipen. IT-debattören Anders Olsson gör följande observation:⁸⁰

Både offentlighetsprincipen och integritetsskyddet utgör fundament i ett öppet och demokratiskt samhälle, men relationen dem emellan är spänningsfylld. Hur man ska finna en balans mellan offentligt och privat i informationssamhället är mycket omdiskuterat. Medan en del menar att de nya i stort sett obegränsade möjligheterna att lagra, inhämta och bearbeta information om den enskilde gör det motiverat att stärka integritetsskyddet, anser andra att allmänhetens rätt att läsa myndigheters handlingar, den s.k. offentlighetsprincipen, är allt för viktig för att urholkas bara för att samhället byter teknik för informationsbehandling.

Två observationer kan göras utifrån detta. Den första observationen gäller Sveriges förhållande till EU i denna fråga. Kulturkrock är nog den beskrivning som kommer först i tanke. Inom EU finns en tradition av sekretess och personlig integritet som bl.a. har inneburit ett skydd för personuppgifter men också en mycket stängd förvaltning. I Sverige har

78) *Computer Sweden* 2001-12-07, <http://computersweden.idg.se/text/011207-cs49>

79) Se <http://www.pul.nu> för information.

80) Olsson, A., 1999: Elektronisk demokrati

offentlighetsprincipen lett till det motsatta förhållandet – en mycket öppen förvaltning men också en nästan obefintlig personlig integritet. Det kan bli mycket svårt för Sverige att i längden leva upp till EUs principer utan att vi blir tvingade att göra en ny avvägning mellan offentlighet och integritet.

Den andra observationen är att debatten i Sverige har haft en slagsida mot de negativa konsekvenserna av ett stärkt integritetsskydd. PuL har framställts som ett hot mot journalister och debattörer eftersom det enligt vissa tolkningar skulle ha kunnat göra det mycket svårare att komma åt uppgifter om enskilda individer. Antalet synpunkter som har framhållit problemen från integritetssynpunkt med en allt mer sammanvävd och komplex förvaltning har varit få. Allt som oftast hörs enstaka röster om behovet av starkare skydd för information om privatpersoner, men dessa synpunkter tenderar att drunkna i all den teknologioptimism som framhåller de ekonomiska eller effektivitetsmässiga fördelarna med en allt mer datoriserad offentlig förvaltning:⁸¹

De senaste åren har en tendens kunnat skönjas från regering, riksdag och myndigheter att betrakta elektronisk information inte i första hand som en universell medborgerlig rättighet, utan snarare som en ekonomisk tillgång eller råvara som bör kapitaliseras när den efterfrågas av aktörer på informationsmarknaden. Utgångspunkten är att den kunskap som finns i allmänna handlingar har ett värde, som både myndigheter och kommersiella företag i ökande grad försöker omsätta i pengar. Inte minst har försäljning av offentlig information börjat ses som inkomstkälla i besparingstider, och

flera myndigheter är redan storsäljare av information i elektronisk form. [...] Det som står på spel är den samhällslösning som är varit djupt förankrad i de historiska erfarenheter vi ovan försökt skissera: Sverige som ett land där det trots avstånd och klassbarriärer råder en grundläggande jämlikhet mellan människorna. Medborgaren håller snabbt, och under allmänt tiggande, på att förvandlas till kund hos den offentliga informationsmarknaden. Det blåser alltså en besvärande motvind när den statliga förvaltningen nu ska försöka lyfta fram sin demokratiroll i framtidens informationssamhälle, och för att ta ett steg framåt kan man först tvingas ta två steg tillbaka.

Den demokratiaspekt som lyfts fram av forskarna Ilshammar och Larsmo är värd en tydligare debatt än vad som nu är fallet. Man kan ha olika uppfattning om var gränsen skall gå mellan integritetsskydd, offentlighet och effektivitet, men det torde vara ostridigt att den elektroniska utvecklingen nu går i en rasande takt inom myndighetsområdet, och att denna utveckling har sin utgångspunkt i en rationalistisk syn på organisationer som i stort saknar empiriskt stöd. Konsekvensen kan bli att vi inom en nära framtid kan komma att befinna oss i en situation där förvaltningen i samhället i grunden har förändrats och antagit en "storebror-ser-dig"-roll – allt utan debatt därför att skyddet för offentligheten har skymt skyddet för den personliga integriteten. Detta skulle i förlängningen kunna leda till att förtroendet för samhällseliga institutioner drastiskt minskas och därmed få menliga effekter för såväl medborgare som samhälle.

81) Ilshammar, L. & Larsmo, O., 1998: Ett steg framåt, två tillbaka – förvaltningens viktigaste demokratiuppgift i IT-samhället är att försvara 1700- och 1800-talens demokratiska framsteg

BILAGA

Tabell I. Undersökta egenskaper på myndigheternas webbplatser.

Undersökt egenskap	Värde	Kommentar
Integritetsdeklaration	Ja/Nej	Integritetsdeklarationen skall redovisa hur webbansvarigt organ förfar med de uppgifter man samlar in, vilka uppgifter detta är och huruvida man vidarebefordrar dem till andra
Information om vidarebefordring	Ja/Nej	Om webbhållaren har för avsikt att skicka data om besökare vidare till någon annan skall detta framgå här
Steg innan besökaren når en webbkarta	Numeriskt värde, 99 = ej förekomst	En stor webbsajt med mycket information och många kräver en lätthittad webbkarta
Steg innan besökaren finner en personallista	Numeriskt värde, 99 = ej förekomst	Ofta söker en besökande kontakt med någon på myndigheten – en komplett lista med personal hjälper till
Steg innan besökaren finner myndighetens adress	Numeriskt värde, 99 = ej förekomst	Myndighetens adress skall finnas på första sidan enligt Toppledarforums anvisningar
Finns sökfunktion?	Ja/Nej	Eftersom en myndighets webbsajt kan antas innehålla mycket information är en bra sökfunktion ofta helt nödvändig
Finns diarium på nätet?	Ja/Nej	Diariet innehåller en löpande redovisning av de handlingar som myndigheten tagit emot och skickat. Det skall vara tillgängligt för alla utan krav på legitimation eller motsvarande
Finns myndighetens regleringsbrev på nätet?	Ja/Nej	Regleringsbrevet ger viktig information om myndighetens dialog med sin uppdragsgivare – staten. Den visar också hur verksamheten finansieras och vilka större planerade förändringar som finns
Finns myndighetens årsredovisning på nätet?	Ja/Nej	Årsredovisningen innehåller mycket information om vad myndigheten presterat. Tillsammans med regleringsbrevet ger det den intresserade en bra bild av vad som hänt och vad som kan förväntas hända
Kan myndighetsfunktion utföras via nätet?	Ja/Nej	Myndighetsfunktion kan vara av många slag – från att ta emot ansökningar till att lämna kvalificerad information

forts.

Tabell 1. Undersökta egenskaper på myndigheternas webbplatser.

Undersökt egenskap	Värde	Kommentar
Kan besökaren genomföra någon form av interaktiv dialog med myndigheten över nätet?	Ja/Nej	En interaktiv dialog innebär oftast att användaren av webbplatsen kan ställa frågor eller få beräkningar m.m., utförda direkt på webbplatsen
Kan besökaren ladda ned dokument?	Ja/Nej	De flesta myndigheter producerar dokument som en besökare kan tänkas vilja ladda hem – allt från broschyrer till böcker
Finns en avdelning som kräver inloggning?	Ja/Nej	En del myndigheter har särskilda extranät där vissa kunder (motsv.) kan genomföra interaktiva tjänster efter inloggning
Kan användaren ange namn på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sitt namn i klartext på myndighetens webbsida?
Kan användaren ange adress på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sin adress i klartext på myndighetens webbsida?
Kan användaren ange telefonnummer på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sitt telefonnummer i klartext på myndighetens webbsida?
Kan användaren ange faxnummer på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sitt telefaxnummer i klartext på myndighetens webbsida?
Kan användaren ange e-postadress på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sin e-postadress i klartext på myndighetens webbsida?
Kan användaren ange personnummer på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sitt personnummer i klartext på myndighetens webbsida?
Kan användaren lämna kreditkortsnummer på webbplatsen?	Ja/Nej	Finns möjlighet för användaren att lämna sitt kreditkortsnummer i klartext på myndighetens webbsida?
Kan användaren ange en särskild kod för att komma åt en stängd avdelning på myndighetens webbplats?	Ja/Nej	Har användaren fått en särskild kod från myndigheten som används för att öppna vissa avdelningar eller för att hämta särskild information?

För att på ett enkelt sätt kunna jämföra de olika myndigheternas samlade tjänsteutbud till användaren har ett numeriskt index skapats, där svaret "ja" givit 3 poäng och där svaret "nej" givit 0 poäng. I de tre fall där antalet webbsteg som användaren behöver göra har noterats (personlista, webbkarta, adress) har värdet "0 steg" givits 3 poäng, värdet "1 steg" 2 poäng och värdet "2 steg" 3 poäng. Övriga antal steg har givit 0 poäng.

Tabell 2. Integritetshot- och servicevariabler i undersökningen.

Variabel	Sammanställning
Integritetshot	Poäng inloggning + Poäng namn + Poäng personadress + Poäng telefonnummer + Poäng faxnummer + Poäng personnummer + Poäng kreditkortsnummer + Poäng särskild kod + Poäng e-postadress
Servicegrad	Poäng webbkarta + Poäng personal + Poäng adress + Poäng sökfunktion + Poäng diarium + Poäng regleringsbrev + Poäng ladda ner dokument + Poäng årsredovisning + Poäng myndighetsfunktion + Poäng interaktiv dialog + Poäng integritetsdeklaration + Poäng vidarebefordran

Tabell 3. Myndigheter med hög grad av navigeringsmöjlighet.

Myndighet	http
Bokföringsnämnden	http://www.bfn.se/
Boverket	http://www.boverket.se/
Brottsförebyggande rådet	http://www.bra.se/
Distansutbildningsmyndigheten	http://www.distum.se/
Finansinspektionen	http://www.fi.se/
Konkurrensverket	http://www.kkv.se/indexns.html
Livsmedelsverket	http://www.slv.se/HeadMenu/livsmedelsverket.asp
Riksskatteverket	http://www.rsv.se/
Rikstrafiken	http://www.rikstrafiken.se/
Räddningsverket	http://www.srv.se/intro/
Ungdomsstyrelsen	http://www.ungdomsstyrelsen.se/kategori/

Tabell 4. Myndigheter med låg grad av navigeringsmöjlighet.

Myndighet	http
Statens Bostadsfinansieringsaktiebolag, SBAB	http://www.sbab.se/
Forskningsrådet för miljö, areella näringar och samhällsbyggande	http://www.formas.se
Centrala studiestödsnämnden	http://www.csn.se/
Lantmäteriet	http://www.lantmateriet.com/
Statens institutionsstyrelse	http://www.stat-inst.se/
Lotteriinspektionen	http://www.lotteriinsp.se/
Jämställdhetsombudsmannen	http://www.jamombud.se/
Statens institut för särskilt studiestöd	http://www.sisus.se/
Delegationen för IT i skolan	http://www.itis.gov.se/
Överstyrelsen för Civil Beredskap	http://www.ocb.se/
Premiepensionsmyndigheten	http://www.ppm.nu/
Arbetsgivarverket	http://www.arbetsgivarverket.se/
Kammarkollegiet	http://www.kammarkollegiet.se/
MISTRA	http://www.mistra-research.se/
Institutet för arbetsmarknadspolitisk utvärdering	http://www.ifau.se/
Integrationsverket	http://www.integrationsverket.se/
ESO – Expertgruppen för studier i offentlig ekonomi	http://www.regeringen.se/info_rosenbad/departement/finans/eso/index.html
Fiskeriverket	http://www.fiskeriverket.se/
Statens bostadskreditnämnd	http://www.bkn.se/
Institutet för Framtidsstudier	http://www.framtidsstudier.se/
Fastighetsmäklarnämnden	http://www.fastighetsmaklarnamnden.se/
Domstolsväsendet	http://www.dom.se/
Gentekniknämnden	http://www.genteknik.se/
Nationella sekretariatet för genusforskning	http://www.genus.gu.se/ikorthet.html
Institutet för tillväxtpolitiska studier	http://www.itps.se/
Turistrådet	http://www.swetourism.se/index.htm
Rättsmedicinalverket	http://www.rmv.se/
Småhusskadenämnden	http://www.smahusskadenamnden.se/
Centrala försöksdjursnämnden	http://www.cfn.se/

Tabell 5. Myndigheter med hög grad av direkta tjänster på webben.

Myndighet	http
Glesbygdsverket	http://www.glesbygdsverket.se/
Statens institut för särskilt studiestöd	http://www.sisus.se/

Tabell 6. Myndigheter med låg grad av direkta tjänster på webben.

Myndighet	http
Statistiska centralbyrån	http://www.scb.se/
Folkhälsoinstitutet	http://www.fhi.se/
Distansutbildningsmyndigheten	http://www.distum.se/
Statens kulturråd	http://www.kur.se/
Konsumentverket	http://www.konsumentverket.se/
Specialpedagogiska institutet	http://www.sit.se/i
MISTRA	http://www.mistra-research.se/
Barnombudsmannen	http://www.bo.se/
Statens fastighetsverk	http://www.sfv.se/
Rättsmedicinalverket	http://www.rmv.se/
Turistrådet	http://www.swetourism.se/index.htm
Banverket	http://www.banverket.se/

Tabell 7. Myndigheter med låg grad av öppenhet.

Myndighet	http
Jordbruksverket	http://www.sjv.se/
Domstolsväsendet	http://www.dom.se/
Fastighetsmäklarnämnden	http://www.fastighetsmaklarnamnden.se/

Tabell 8. Sammantagen servicepoäng (normaliserad) för de undersökta myndigheterna.

Myndighet	Navigering	Tjänster	Öppenhet	Poäng
Glesbygdsverket	83	100	58	80
Finansinspektionen	100	67	50	72
Räddningsverket	100	67	50	72
Konkurrensverket	100	33	75	69
Radio- och TV-verket	83	67	42	64
Boverket	100	33	58	64
Vägverket	67	67	50	61
Bokföringsnämnden	100	33	50	61
Elsäkerhetsverket	83	67	25	58
Tullverket	83	67	25	58
Riksskatteverket	100	67	0	56
Statskontoret	50	67	50	56
Ungdomsstyrelsen	100	67	0	56
Brottsförebyggande rådet	100	33	33	55
Riksrevisionsverket	83	33	50	55

forts.

Tabell 8. Sammantagen servicepoäng (normaliserad) för de undersökta myndigheterna.

Myndighet	Navigering	Tjänster	Öppenhet	Poäng
Rikstrafiken	100	33	17	50
Akademiska hus AB	83	33	33	50
IT-kommissionen	83	33	33	50
Arbetsförmedlingen – AMS	50	67	25	47
Bilprovningen	50	67	25	47
Rikspolisstyrelsen	50	67	25	47
Statens pensionsverk	50	67	25	47
Sveriges Radio	50	67	25	47
Arbetsmiljöverket	50	33	58	47
Datainspektionen	83	33	25	47
Institutet för arbetsmarknadspolitisk utvärdering	0	67	67	45
Ekonomistyrningsverket	50	33	50	44
Kemikalieinspektionen	50	33	50	44
Kärnkraftsinspektionen	50	33	50	44
Livsmedelsverket	100	33	0	44
Läkemedelsverket	50	33	50	44
Naturvårdsverket	50	33	50	44
Socialstyrelsen	50	33	50	44
Barnombudsmannen	50	0	75	42
Jordbruksverket	67	33	25	42
Skolverket	50	0	75	42
Statens geotekniska institut	50	33	42	42
Statens haverikommission	50	33	42	42
Väg- och transportforskningsinstitutet	50	67	8	42
Handikappombudsmannen	33	33	58	41
Apoteket	67	33	17	39
Folkhälsoinstitutet	50	0	67	39
Patent- och registreringsverket	50	67	0	39
Brottsoffermyndigheten	50	33	33	39
Totalförsvarets forskningsinstitut	83	33	0	39
Vetenskapsrådet	50	33	33	39
ESO – Expertgruppen för studier i offentlig ekonomi	0	67	42	36
Allmänna reklamationsnämnden	17	33	58	36
Distansutbildningsmyndigheten	100	0	8	36
Institutet för kvalitetsutveckling	33	67	8	36
Luftfartsverket	50	33	25	36
Nämnden för offentlig upphandling	50	33	25	36
Statens institut för särskilt studiestöd	0	100	8	36
Statens strålskyddsinstitut	50	33	25	36
Delegationen för IT i skolan	0	67	33	33

forts.

Tabell 8. Sammantagen servicepoäng (normaliserad) för de undersökta myndigheterna.

Myndighet	Navigering	Tjänster	Öppenhet	Poäng
Integrationsverket	0	33	67	33
Jämställdhetsombudsmannen	0	33	67	33
Konsumentverket	50	0	50	33
Statens energimyndighet	50	33	17	33
Diskrimineringsombudsmannen	33	33	33	33
Verket för innovationssystem	33	33	33	33
Centrala studiestödsnämnden	0	67	25	31
Fiskeriverket	0	67	25	31
Statens institutionsstyrelse	0	67	25	31
Arbetsgivarverket	0	33	58	30
Sprängämnesinspektionen	50	33	8	30
Systembolaget	33	33	25	30
Riksförsäkringsverket	50	33	0	28
Specialpedagogiska institutet	83	0	0	28
Forskningsrådet för miljö, areella näringar och samhällsbyggande	0	33	42	25
Statens bostadskreditnämnd	0	33	42	25
Statens fastighetsverk	50	0	25	25
Statistiska centralbyrån	50	0	25	25
Statens Bostadsfinansieringsaktiebolag, SBAB	0	67	0	22
Institutet för Framtidsstudier	0	33	33	22
Konjunkturinstitutet	33	33	0	22
Alkoholinspektionen	17	33	8	19
Domstolsväsendet	0	33	25	19
Fastighetsmäklarnämnden	0	33	25	19
Överstyrelsen för Civil Beredskap	0	33	25	19
Lotteriinspektionen	0	33	17	17
Statens kulturråd	50	0	0	17
Centrala försöksdjursnämnden	0	33	8	14
Institutet för tillväxtpolitiska studier	0	33	8	14
Nationella sekretariatet för genusforskning	0	33	8	14
Premiepensionsmyndigheten	0	33	8	14
Gentekniknämnden	0	33	0	11
Kammarkollegiet	0	33	0	11
Lantmäteriet	0	33	0	11
MISTRA	0	0	33	11
Småhuskadenämnden	0	33	0	11
Turistrådet	0	0	33	11
Rättsmedicinalverket	0	0	25	8
Banverket	17	0	0	6

Tabell 9. Myndigheter som tar emot alla typer av direkt personligt identifierande information.

Myndighet	http
Vetenskapsrådet	http://www.vr.se
Arbetsförmedlingen – AMS	http://www.ams.se/
Statskontoret	http://www.statskontoret.se/
Naturvårdsverket	http://www.viron.se/
Forskningsrådet för miljö, areella näringar och samhällsbyggande	http://www.formas.se
Lantmäteriet	http://www.lantmateriet.com/
Elsäkerhetsverket	http://www.elsak.se/
Brottsförebyggande rådet	http://www.bra.se/
Arbetsmiljöverket	http://www.av.se
Skolverket	http://www.skolverket.se/
Socialstyrelsen	http://www.sos.se/
Kärnkraftsinspektionen	http://www.ski.se/
Rikspolisstyrelsen	http://www.police.se/
Diskrimineringsombudsmannen	http://www.do.se/index.oois
Statens energimyndighet	http://www.stem.se/

Tabell 10. Myndigheter med starkt integritetshot.

Myndighet	http
Vetenskapsrådet	http://www.vr.se
Arbetsförmedlingen – AMS	http://www.ams.se/
Patent- och registreringsverket	http://www.prv.se/
Statens Bostadsfinansieringsaktiebolag, SBAB	http://www.sbab.se/
Centrala studiestödsnämnden	http://www.csn.se/
Premiepensionsmyndigheten	http://www.ppm.nu/

Tabell 11. Normerad lista över myndigheternas integritetshot.

Myndighet	E-post	Starkt hot	Svagt hot	Integritetshot-poäng
Vetenskapsrådet	100	75	100	89
Arbetsförmedlingen – AMS	100	75	100	89
Statens Bostadsfinansieringsaktiebolag, SBAB	100	75	75	78
Patent- och registreringsverket	100	75	75	78
Statskontoret	100	25	100	67
Statistiska centralbyrån	100	50	75	67
Naturvårdsverket	100	25	100	67
Lantmäteriet	100	25	100	67
Institutet för kvalitetsutveckling	100	50	75	67
Forskningsrådet för miljö, areella näringar och samhällsbyggande	100	25	100	67
Centrala studiestödsnämnden	0	75	75	67
Statens energimyndighet	100	0	100	56
Socialstyrelsen	100	0	100	56
Skolverket	100	0	100	56
Rikspolisstyrelsen	100	0	100	56
Kärnkraftsinspektionen	100	0	100	56
Glesbygdsverket	100	25	75	56
Folkhälsoinstitutet	100	25	75	56
Elsäkerhetsverket	100	0	100	56
Distansutbildningsmyndigheten	100	50	50	56
Diskrimineringsombudsmannen	100	0	100	56
Datainspektionen	100	25	75	56
Brottsförebyggande rådet	100	0	100	56
Arbetsmiljöverket	100	0	100	56
Ungdomsstyrelsen	0	25	75	44
Statens kulturråd	100	0	75	44
Statens institutionsstyrelse	100	0	75	44
Sprängämnesinspektionen	100	0	75	44
Riksrevisionsverket	100	0	75	44
Lotteriinspektionen	100	0	75	44
IT-kommissionen	100	0	75	44
Boverket	100	0	75	44
Bilprovningen	100	25	50	44
Akademiska hus AB	100	0	75	44
Överstyrelsen för Civil Beredskap	100	0	50	33
Statens institut för särskilt studiestöd	100	25	25	33
Specialpedagogiska institutet	0	50	25	33
Riksförsäkringsverket	0	0	75	33
Premiepensionsmyndigheten	0	75	0	33

forts.

Tabell 11. Normerad lista över myndigheternas integritetshot.

Myndighet	E-post	Starkt hot	Svagt hot	Integritetshot-poäng
Konsumentverket	100	0	50	33
Konjunkturinstitutet	100	0	50	33
Jämställdhetsombudsmannen	100	0	50	33
Jordbruksverket	0	0	75	33
Handikappombudsmannen	0	25	50	33
Delegationen för IT i skolan	0	25	50	33
Brottsoffermyndigheten	0	0	75	33
Bokföringsnämnden	0	0	75	33
Vägverket	0	50	0	22
Verket för innovationssystem	0	50	0	22
Systembolaget	0	50	0	22
Sveriges Radio	100	25	0	22
Kammarkollegiet	100	0	25	22
Finansinspektionen	0	50	0	22
Arbetsgivarverket	0	50	0	22
Statens pensionsverk	0	25	0	11
Riksskatteverket	0	25	0	11
MISTRA	0	25	0	11
Alkoholinspektionen	0	25	0	11
Väg- och transportforskningsinstitutet	0	0	0	0
Turistrådet	0	0	0	0
Tullverket	0	0	0	0
Totalförsvarets forskningsinstitut	0	0	0	0
Statens strålskyddsinstitut	0	0	0	0
Statens haverikommission	0	0	0	0
Statens geotekniska institut	0	0	0	0
Statens fastighetsverk	0	0	0	0
Statens bostadskreditnämnd	0	0	0	0
Småhusskadenämnden	0	0	0	0
Rättsmedicinalverket	0	0	0	0
Räddningsverket	0	0	0	0
Rikstrafiken	0	0	0	0
Radio- och TV-verket	0	0	0	0
Nämnden för offentlig upphandling	0	0	0	0
Nationella sekretariatet för genusforskning	0	0	0	0
Läkemedelsverket	0	0	0	0
Luftfartsverket	0	0	0	0
Livsmedelsverket	0	0	0	0
Konkurrensverket	0	0	0	0

forts.

Tabell 11. Normerad lista över myndigheternas integritetshot.

Myndighet	E-post	Starkt hot	Svagt hot	Integritetshot- poäng
Kemikalieinspektionen	0	0	0	0
Integrationsverket	0	0	0	0
Institutet för tillväxtpolitiska studier	0	0	0	0
Institutet för Framtidsstudier	0	0	0	0
Institutet för arbetsmarknadspolitisk utvärdering	0	0	0	0
Gentekniknämnden	0	0	0	0
Fiskeriverket	0	0	0	0
Fastighetsmäklarnämnden	0	0	0	0
ESO – Expertgruppen för studier i offentlig ekonomi	0	0	0	0
Ekonomistyrningsverket	0	0	0	0
Domstolsväsendet	0	0	0	0
Centrala försöksdjursnämnden	0	0	0	0
Barnombudsmannen	0	0	0	0
Banverket	0	0	0	0
Apoteket	0	0	0	0
Allmänna reklamationsnämnden	0	0	0	0

REFERENSER

- Allison, G. T. & Zelikov, P.;** 1999: *Essence of Decision: Explaining the Cuban Missile Crisis*, 2a utg, Reading, MA: Longman
- Andreason, T.;** 1998: Samhällsansvar på ideell grund – med Internet som verktyg.
I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Associated Press:** *Agencies Can't Purge Computer White House Among Those Affected by Ruling*, Denver Rocky Mountain News, 1998-11-04, pp 44A.
- Barber, B.R.;** 1999: En plats för kommers eller en plats för oss? IT i demokratiskt ljus.
I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Bedst pa Nettet,**
<http://www.bedstpaanettet.dk>
- Bennulf, M.;** 2001: *Opinion 2001 – nya hot och risker. Den svenska allmänhetens syn på samhället, säkerhetspolitiken och försvaret*, Styrelsen för psykologiskt försvar, meddelande 160
- Commission Nationale de l'Informatique et des Libertés,** 2001-12-31,
<http://www.cnil.fr/cnil/index.htm>
- Computer Sweden:** 2001-12-07;2002-01-28
- Consumers International,** 2001: *Privacy@net*, Office for Developed and Transition Economies, London
- Culman, M.J.;** 1999: *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*, The McDonough School of Business, Georgetown University, Washington D.C.
- Dagens IT:** Ny statlig upphandling för 24-timmarsmyndigheter, 2002-03-07
- Dagens IT:** 2002-04-02
- Dahlbom, B.;** 1998: En demokratisk framtid.
I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Datainspektionen,** 1998: *Försäljning av myndighetsinformation*, Datainspektionens rapport december 1998
- Datainspektionen,** 1999: *Frivilligt integritetsskydd på Internet*, Datainspektionens rapport 1999:2
- Datainspektionen,** 1999: *Skyddade uppgifter i folkbokföringen*, Datainspektionens rapport 1999:3
- Ds 2000:34:** *Samhällets grundläggande information*

- Edmar, M.**, 1999: *Internetpublicering – en juridisk vägledning*, Kungliga Ingenjörsvetenskapsakademien, IVA M 326
- Electronic Privacy Information Center**, 2001-12-31, <http://www.epic.org/>
- Ellegård, K.**, 1999: I spänningsfältet mellan social intressegemenskap och geografisk närhet försätter IKT den geografiskt förankrade demokratin i kläm?. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Ernst & Young**, 2001: *Västra Götalandsregionen – Nimda – granskning av händelser i IT-verksamheten 2001*, Rapport 2001-11-20
- EU**, 1999, COM(1999) 337 final 99/0153 (COD): Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, Brussels
- EU**, 2000, KOM(2000) 385 slutlig 2000/0189 (COD): Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om behandling av personuppgifter och skydd för privatlivet inom sektorn för elektronisk kommunikation, Bryssel
- Gøtze, J.**, 1998: Nätet ger Danmark demokratielektioner. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Hansson, K.**, 1998: Ärat vare ditt Namn – om rätten att ha och inte ha ett namn i Cyberspace. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Ilshammar, L. & Larsmo, O.**, 1998: Ett steg framåt, två tillbaka – förvaltningens viktigaste demokratiuppgift i IT-samhället är att försvara 1700- och 1800-talens demokratiska framsteg. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Ilshammar, L.**, 1999: IT i demokratin eller IT-demokrati. Teknologi och demokratisering i historisk perspektiv. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- IT-kommissionen**, 1998: *Mobila agenter*, <http://www.itkommissionen.se/observ/>
- IT-kommissionen**, 2001: *En utvecklad infostruktur – motorn i e-Sverige?*, OH-serie, <http://www.itkommissionen.se/>
- Johansson, M.**, 1999: Skola och demokrati. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Klein, K.**, 1999: www.oneworld.net. Internet och den kosmopolitiska demokratin. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Konsumentverket**, 2001: Pressmeddelande 2001-01-25
- Ljunggren, S-B.**, 1998: *Demokrati i det högfrekventa samhället*, KFB-rapport 1998:20
- Magnusson-Sjöberg, C.**, 1992: *Rättsautomation – särskilt om statsförvaltningens datorisering*, Norstedts Juridik

- Manning, W.W.**, 1997: Should you be on the Net? (law enforcement agencies). *The FBI Law Enforcement Bulletin*, Vol.66, 1997-01-01, 18(5).
- Martinsson, J.**, 1999: IT-valet? Internets betydelse för valkampanjerna. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- McAllester, M.**, 1998: Identity Crisis/ Theft of personal information, commercial abuses and terrorist threats fuel debate over the future of the Net., *Newsday*, 1998-03-09, C03.
- Morge, S.**, 1999: *Krisinformation på Internet*, Styrelsen för psykologiskt försvar
- Nationalencyklopedin**, Nätupplaga, <http://www.ne.se>
- Nielsen, J.**, 2000: *Designing web usability*, New Riders Publishing, Indianapolis
- Nydén, M.**, 2000: *Myndigheter, Internet och integritet*, Styrelsen för psykologiskt försvar, meddelande 153
- Ohlin, T.**, 1998: Förändrad kontakt mellan medborgare och myndighet. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Ohlin, T.**, 1999: Sprid medborgarmakten! I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Olsson, A.**, 1999: *Elektronisk demokrati*, Demokratiutredningens skrift nr 16, SOU 1999:16
- Parliamentary Office of Science and Technology**, "Electronic Government Information Technologies and the Citizen"
- PEW Internet & American Life Project**, 2000a: *Trust and privacy online: Why Americans want to rewrite the rules*, <http://www.pewinternet.org>
- PEW Internet & American Life Project**, 2001: *Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users*, <http://www.pewinternet.org>
- PEW Internet & American Life Project**, 2001: *Fear of Online Crime: criminal suspects' e-mail and new laws to protect online privacy*, <http://www.pewinternet.org>
- PEW Internet & American Life Project**, 2002: *The rise of the e-citizen: How people use government agencies' Web sites*, <http://www.pewinternet.org>
- Proposition 1995/96:90**: Registerbaserad folk- och bostadsräkning år 2000 m.m.
- Proposition 1995/96:125**: Åtgärder för att bredda och utveckla användningen av informationsteknik
- Proposition 1997/98:44**: Personuppgiftslag
- Proposition 1997/98:136**: Statlig förvaltning i medborgarnas tjänst
- Proposition 1999/2000:86**: Ett informations-samhälle för alla
- Proposition 1999/2000:117**: Lag om kvalificerade elektroniska signaturer m.m.
- Proposition 2001/02:09**: Vissa socialförsäkringsfrågor

- Ranerup, A.**, 1999: Elektronisk debatt i kommunal politik. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Regeringen**, 2002: <http://www.justitie.regeringen.se/justitiefragor/lagstiftning/pul/missbruk.html>
- Regeringens skrivelse 1998/99:2**: *Informationssamhället inför 2000-talet.*
- Regeringskansliet**, 1998: *En förvaltning i demokratins tjänst*
- Riksarkivet**, 2000: *Dokumentation av IT-system, en kartläggning*
- Rikspolisstyrelsen**, 2000: *Rapport angående elektronisk identifiering*
- Ryding, E.**, 1971: *Konsten att luras utan att ljuga*. Nya Doxa
- Segerlund, C.Ö.**, 1997: *IT för samhällsservice, demokrati och folkbildning i Sverige*, Teldok rapport 113
- Sjögren, J.**, 1998: *På Begäran: Information och Tjänster. I: Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- SOU 1996:40**: *Elektronisk dokumenthantering*
- SOU 1997:146**: *Grunddata – i samhällets tjänst*
- SOU 1997/98:39**: *Integritet · Offentlighet · Informationsteknik*
- SOU 1997/98:136**: *Statlig förvaltning i medborgarnas tjänst*
- SOU 1998:58**: *IT och nationalstaten – fyra framtidsscenarier*
- SOU 1998:115**: *Distansarbete*
- SOU 1999:85**: *Bredband för tillväxt i hela landet*
- SOU 1999:106**: *Konsumenter och IT – en utredning om datorer, handel och marknadsföring*
- SOU 1999:117**: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII
- SOU 1999:125**: *Politikens medialisering*, Demokratiutredningens forskarvolym III
- SOU 1999:131**: *Marknaden som politisk aktör*, Demokratiutredningens forskarvolym XI
- SOU 2001:3**: *Offentlighetsprincipen och den nya tekniken*
- SOU 2001:28**: *Yttrandefrihetsgrundlagen och Internet. Utvidgat grundlagsskydd och andra frågor om tryck och yttrandefrihet*
- SOU 2001:41**: *Säkerhet i en ny tid*
- SOU 2002:18**: *Personlig integritet i arbetslivet*
- Statens energimyndighet**, 2002: *Avbrottsstatistik, pressmeddelande 2002-01-30*
- Statens institut för kommunikationsanalys**, 2002, *Fakta om informations- och kommunikationsteknik i Sverige 2002*
- Statstjänstemannaförbundet**: 2000, 7:16
- Statskontoret**, 1999: *IT-kostnader i statsförvaltningen – en förstudie av 24 myndigheter*

- Statskontoret**, 1998: *Offentlig förvaltning och demokrati i informationssamhället*
- Statskontoret**, 1999: *Informationstjänster i fokus*
- Statskontoret**, 1999:38: *Organisations styr- och verksamhetsformer i kommuner och landsting*
- Statskontoret**, 2000: *24-timmarsmyndigheten*, <http://www.statskontoret.se/24/200021/rapport.html>, 2002-01-01
- Statskontoret**, 2000:40: *Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster*
- Statskontoret**, 2001: *Att bygga en nyttig nationell infrastruktur*, PM
- Statskontoret**, 2001, *Internet och datoranvändning i Sverige år 2000*, Rapport 28
- Statskontoret**, 2002: *Utveckling av 24-timmarsmyndigheter – lägesrapport december 2001*, Rapport 2002-12-21
- STATT**, 2000: *Någon vet var Du är*, Sveriges Tekniska Attachéer, Rapport 2000-03-31
- Styrelsen för psykologiskt försvar**, 1998: *Kriser och kriskommunikation* (utbildningsmaterial)
- Teknologirådet**, 2000: *Kommunen på nettet*, Teknologirådets rapporter 2000/4
- Tippler, J., & Douyle, M.**, 1998: Englands medborgarkontor (CAB) står på medborgarnas sida. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Tängdén, E.**, 1998: Kommunen och demokratin i informationssamhället. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- United States General Accounting Office**, 2000: *Internet Privacy – Agencies Efforts to Implement OMB’s Privacy Policy*, GAO/GGD00191
- Wells Branscomb, A.**, 1994: *Who Owns Information? From Privacy to Public Access*, New York
- Wihlborg, E.**, 1999: Platsbundna gemenskaper med virtuella kopplingar. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Åström, J.**, 1999: Digital demokrati? Idéer och strategier i lokal ITpolitik. I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Östberg, O.**, 1998: Ett förvaltningspolitiskt ackord. I: *Offentlig förvaltning och demokrati i informationssamhället*, Statskontoret 1998:2
- Östlund, B.**, 1999: Vidgar IT gapet mellan generationerna? I: *IT i demokratins tjänst*, Demokratiutredningens forskarvolym VII, SOU 1999:117
- Överstyrelsen för Civil Beredskap**, 2002: *IT-incidenthantering*, Rapport

SPFs SENASTE RAPPORTER

- 188 **Larsson, Larsåke:** *11 september – Svenska myndigheters kommunikation vid terrorattentaten i USA 2001.* Stockholm 2002.
- 187 **Granström, Kjell (redaktör):** *Göteborgskravallerna – Identitetsskapande och attitydförändringar genom deltagande i fredliga demonstrationer och våldsamma upplopp.* Stockholm 2002.
- 186 **Nord, Lars & Strömbäck, Jesper:** *Tio dagar som skakade världen – En studie av mediernas beskrivningar av terrorattacker i USA och kriget i Afghanistan hösten 2001.* Stockholm 2002.
- 185 **Leth, Göran & Thurén, Torsten:** *Revolutionen i Belgrad 2000 – Fakta och förklaringar i några svenska medier.* Stockholm 2002.
- 184 **Nordström, Gert Z:** *Terrorkriget i kvällspressen. En studie av hur Aftonbladet och Expressen presenterade Attentatet mot USA den 11 september 2001, Vedergållningen mot Afghanistan den 7 oktober, Jakten på Usama bin Ladin.* Stockholm 2002.
- 183 **Sjöstedt, Gunnar & Stenström, Paula:** *Vilseledning på Internet – En analysansats.* Stockholm 2002.
- 182 **Hedquist, Rolf:** *Trovärdighet – en förutsättning för förtroende.* Stockholm 2002.

SPFs SENASTE MEDDELANDEN

- 162 **Stütz, Göran:** *Opinion 2002 – Den svenska allmänhetens syn på samhället, säkerhetspolitiken och försvaret hösten 2002.* Stockholm 2002. [www.psyodef.se]
- 161 **Olausson, Ulrika:** *”Vi kommer bara ihåg våldsamheterna” – Medborgare om Göteborgskravallerna och medierapporteringen.* Stockholm 2002.
- 160 **Bennulf, Martin:** *Opinion 2001. Nya hot och risker. Den svenska allmänhetens syn på samhället, säkerhetspolitiken och försvaret.* Stockholm 2001.
- 159 **Palm, Lars & Nilsson, Anna:** *Föreställningen började innan publiken anlät: En analys av regeringens folkbildningsinsats om EMU.* Stockholm 2001.
- 158 **Norling, Anna:** *Olycksplats Borlänge bangård.* Stockholm 2001.
- 157 **Malešič, Marjan:** *Peace Support Operations, Mass Media, and the Public in Former Yugoslavia.* Stockholm 2000.



24-TIMMARSHOTET

– Om förvaltningens förvandling och hotet mot den personliga integriteten

Införandet av 24-timmarsmyndigheten kan i en nära framtid innebära att alla svenska myndigheter kopplas ihop i ett gigantiskt datanät. Detta får återverkningar på personlig integritet och effektivitet. I denna studie diskuteras och analyseras denna potentiella konflikt.

Michael Nydén är fil. dr. i statskunskap