Motion till riksdagen 1987/88:K431

av Anders Björck m. fl. (m)

om datorers betydelse och konsekvenser

Mot.
1987/88
K431

1 Inledning

Den moderna informationsteknologin erbjuder fascinerande möjligheter. Kvalificerade matematiska beräkningar kan göras med ett fickminne. En portabel ordbehandlare kan via telefon sända färdig redigerad text rakt in i ett sätteri. Gigantiska mängder information kan lagras i en persondator. Elektroniken och datoriseringen förändrar inom varje samhällsområde förutsättningarna för människors dagliga verksamhet.

Det är inte främst möjligheten att lagra stora mängder information som har den största förändringskraften utan de avancerade möjligheterna till att sprida och hantera informationen i näst intill oändliga former. Rätt information kan sökas och finnas vid rätt tillfälle ur ett flöde av information som är universellt. Den intressanta informationen kan spridas och nå dem som behöver den.

Den moderna informationsteknologin sätter därför den enskilde i ett centrum av den tillgängliga informationen, ett centrum som inte bara är oberoende av hans geografiska placering utan också av hans placering i en viss hierarkisk struktur.

I ett samhälle där information inte längre är en bristvara utan något som finns i överskott undergrävs alltmer centralistiska idéer vare sig de präglat organisationer, företag eller politiska system.

Det är behovet av samordnad verklighetssyn och kvalificerad information som motiverar till centralisering av beslut och ansvar. I ett samhälle där informationen inte ens behöver spridas utan redan i ett visst givet utgångsläge kan sägas finnas hos den enskilde – eller det i alla fall är på den enskildes initiativ som informationen kan sökas – faller ett viktigt skäl för centraliserat beslutsfattande bort. Därmed minskar också behovet att samla information i stora centrala register.

Det är betydande krafter som kan utvecklas i takt med att vårt samhälle i allt högre grad präglas av den moderna informationsteknologin.

- Nyföretagandets möjligheter ökar. Det blir lättare att se de olika möjligheter som finns till företagande. Möjligheterna att nå mer begränsade nischer av efterfrågan ger, tillsammans med den datorstyrda produktionens möjligheter att tillverka små upplagor i långa serier, entreprenörer

1 *Riksdagen 1987/88. 3 saml. Nr K431*

bättre förutsättningar och överblick än någonsin. Det lilla företaget kan genom sin datorisering vinna de administrativa skalfördelar som tidigare enbart stora företag kunnat utnyttja.

- Kombinationen av nyföretagandets möjligheter, ett växande tjänstebehov som följer i informationssamhällets spår och kravet på kvalitativ anpassning av varor och tjänster kräver större insatser från den enskilde och ger ett spektrum av nya och växande sysselsättningsmöjligheter.
- Datoriseringen ger framför allt en möjlighet att utveckla den kvalitativa dimensionen i produkter, tjänster och i vårt arbetsliv, samtidigt med att nya sysselsättningsmöjligheter därmed öppnar sig.
- Förmågan att hantera och förmedla information och därmed kunskaper, ger skolan nya möjligheter, samtidigt som datoriseringen av tjänstesamhället ställer än mer varierade krav på kunskaper och kompetens.
- Den moderna informationsteknologin samlar inte bara våra befintliga kunskaper på ett lättillgängligt sätt utan kan också medverka till att höja samhällets totala kunskapsnivå och individens kunskapsutnyttjande. Inom forskning, massmedia och i den offentliga debatten tillför datateknologin en ny dimension.
- Medborgarnas förutsättningar att kontrollera myndigheternas maktutövning kan genom den nya informationsteknologin öka samtidigt som det finns större skäl än tidigare att av myndigheterna kräva effektivitet, produktivitet och ett tillmötesgående gentemot den enskilde medborgarens önskemål.

Det ligger i sakens egen natur att en utveckling som inom varje samhällssektor erbjuder medborgarna varierande möjligheter till information och utveckling inte kan administreras fram. Den moderna informationsteknologins användning bygger på kunskap, kreativitet och anpassning till de enskilda människorna som använder den. Av samma skäl som den verkar decentraliserande, kan man inte med centrala beslut styra och utveckla den om den skall utvecklas till människornas bästa.

Det är därför viktigt att slå fast att det som Sverige idag behöver inte är en "datapolitik" som med centrala och generella värderingar av tekniken som sådan söker föra frågan om teknikens användning samman under en samhällsövergripande politik.

Ny teknik väcker alltid oro hos en del människor. Fruktan för förändringens eventuella negativa sidor ställer ibland krav på kontroll som kan leda till att utvecklingens möjligheter försummas.

I ett land som Sverige med västvärldens mest omfattande offentliga sektor är risken för detta betydande. Datatekniken ses av vissa snarare som ett medel för kollektivets kontroll och planering av samhället, än som ett medel för att stärka medborgarnas möjligheter att både kunna kontrollera den offentliga makten och utnyttja ett ökat växande utrymme för den egna kreativiteten.

Detta har gett Sverige en i vissa delar bakvänd politik i frågor som rört datateknikens användning. I stället för att stifta lagar till skydd för den enskildes rättssäkerhet och integritet, har statsmakterna inte bara utnyttjat datatekniken till att ytterligare utvidga ett redan omfattande uppgiftsinsam-

lande och registrerande utan också till att underblåsa en föreställning om att det åvilar statsmakterna att planera för datoranvändandet i det svenska samhället. Datatekniken har snarare använts för centralisering än för det decentraliserade och öppna samhälle den ger möjlighet till.

Det finns betydande skäl att vända sig emot en sådan utveckling. Statsmakternas uppgift bör primärt vara att tillse att ny teknik – det må vara såväl datorteknik som annan ny teknik – inte inkräktar på medborgarnas rätt till liv, egendom eller integritet. Det är huvudsakligen inom dessa områden som vi i denna motion för fram konkreta krav på förändringar, samtidigt som vi pekar på de möjligheter som nu växer fram inom vissa samhällsområden och som kräver politiskt beslutsfattande.

2 Den politiska utmaningen

Datateknikens möjligheter får inte försummas genom att de risker som den kan medföra används till argument mot utnyttjande av modern datateknologi. I stället är det viktigt att statsmakterna tar ett betydande ansvar för att lagstiftningen möter de nya krav som den nya teknologin ställer när det gäller att skydda medborgarnas säkerhet, liv och egendom.

- Offentlighetsprincipen måste anpassas till datateknologin så att medborgarnas möjligheter att kontrollera myndigheterna inte urholkas.
- Den enskildes integritet måste skyddas.
- Samhällets sårbarhet måste nedbringas till en rimlig nivå.
- I sin egenskap av datoranvändare måste staten leva upp till dessa krav samtidigt som man ger skattebetalarna den effektivitet och service de har rätt att erhålla.

Tyvärr kan man knappast påstå att socialdemokratin har levt upp till denna utmaning.

- Stora centrala datasystem har byggts upp utan hänsyn till behovet av att även med ny informationsteknologi leva upp till de krav som lagar och regler ställer, vad gäller medborgarnas möjligheter till insyn. En viktig orsak till detta är att statens användning av datorer har byggt på centraliserade tekniska lösningar. För den normale medborgaren har detta lett till att tillgången på viktig information genom offentlighetsprincipen blivit svårare.
- Socialdemokratin tycks framförallt ha sett datateknologin som en möjlighet att samla och registrera personuppgifter om de enskilda medborgarna. Sedan socialdemokratin 1982 kom till makten har den enskildes rättsliga ställning vad gäller skyddet av det egna privatlivet försvagats. Det finns en mycket stark tendens hos olika företrädare för regeringen att se den enskildes integritet som "en avvägningsfråga". Från fall till fall skall frågan om den enskildes integritet avgöras av enskilda myndigheter. Det har lett till att det finns ett bristande skydd för den enskildes integritet och därmed en följande osäkerhet om var gränsen för den enskildes privatliv går.

Vad än värre är, är att avvägningsfilosofin kontinuerligt leder till att den som avväger – den offentliga maktens olika myndigheter – blir allt starkare gentemot den vars integritet avvägs – den enskilde medborgaren. Exempel på hur den offentliga makten har flyttat fram sina positioner gentemot den

enskilde medborgarens privatliv är många:

- den nya taxeringslagen ger skattemyndigheterna möjlighet att kontrollera datalagrat material hos företag och enskilda – inte bara hos den som skall revidera utan också hos tredje part – utan att det i lagen finns angivet något skydd för den enskildes integritet,
- fritidsbåtregistret är ett av många exempel på hur flera centrala register växer fram i kontrollsyfte,
- lagen om förenklad självdeklaration har inte bara skapat ett ökat personnummeranvändande utan bygger på det direkta syftet att öka antalet datasamkörningar,
- kronofogdemyndigheternas utmätningsregister, REX, ger en omfattande och spridd terminalåtkomst till känsliga personuppgifter,
- datoriseringen inom sjukvården har inte lett till någon lagstiftning som reglerar under vilka former uppgiftslämnande mellan sjukvårdens olika myndigheter och socialstyrelsen får ske, ej heller till en översyn av hur sekretesskraven uppfylls. I stället har den socialdemokratiska majoriteten i data- och offentlighetskommittén föreslagit en urholkning av sekretesslagen,
- myndighetsförsäljningen av personuppgifter fortsätter, i vissa fall utan lagligt stöd, samtidigt som data- och offentlighetskommittén har föreslagit att de nio största säljarnas försäljning skall ges särskilt lagstöd.

Sedan socialdemokratin kom till makten har riksdagen inte förelagts något förslag som stärker skyddet av den enskildes integritet annat än förbättrade möjligheter till rättelse av felaktiga personuppgifter. Om inget görs riskerar vi att se informationssamhället växa fram samtidigt som den enskilde i praktiken blir rättslös vad gäller skyddet av det egna privatlivet. Det vore förödande inte bara för vårt samhälle utan också för medborgarnas syn på datatekniken.

- Det saknas idag en klar filosofi över hur statens egna datasystem skall utvecklas. I ett slags låt-gå-filosofi byggs stora centrala system med betydande negativa effekter för sekretesskyddet, integriteten, sårbarheten och flexibiliteten i användandet.
- Sedan den socialdemokratiska regeringen 1982 tillträdde har den över huvud taget inte vidtagit någon åtgärd för att minska den sårbarhet som är konsekvensen av en utökad användning av olika dataregister. Den bristande sårbarheten beror också på en bristande förmåga hos olika myndigheter att tillämpa sekretesslagstiftningen i sammanhang där detta är nödvändigt. Exemplen med Södertäljes civila försvarsplanering och postverkets försäljning av beskrivningar av det svenska vägsystemet i datamedia visar båda på en aningslöshet som är ett generellt problem. Det är mot den bakgrunden oroande att ingenting egentligen har gjorts på grundval av de rekommendationer som sårbarhetsberedningen lämnade efter sig, lika oroande är att ansvaret för sårbarhetsproblematiken nu synes vara uppdelat på så många olika händer att det uppenbarligen utesluter nödvändigt agerande.

3 Offentlighetsprincipen och sekretessen

En begränsning av medborgarnas tillgång till allmänna handlingar till följd av myndigheternas ADB-användning kan inte accepteras. Detta skulle, i vart fall i ett längre perspektiv, t. ex. kunna innebära en risk för att myndigheterna korrumperas på det sätt som kan förekomma i andra samhällen. Det skulle också kunna få negativa effekter för den fria samhällsdebatten. En utvidgad offentlighet till följd av datoriseringen medför emellertid integritetsrisker både för individer och företag och för vår nation som sådan.

Gällande rätt på offentlighetens område anses numera innebära bl. a. att myndigheterna är skyldiga att tillhandahålla även sådana s. k. potentiella handlingar som myndigheterna inte själva behöver i sin myndighetsutövning och som aldrig ingått i en viss myndighets beslutsunderlag. Myndigheterna anses t. o. m. skyldiga att som ett utflöde av handlingsoffentligheten göra sammanställningar med nya program eller bearbeta sina databaser med program som den enskilde själv tillhandahåller.

Handlingsoffentlighetens omfattning har härigenom kommit att bestämmas av vad som är tekniskt möjligt att "ta fram" ur en databas i stället för att gränsen för insynsrätten bestäms av den berörda myndighetens verksamhetsuppgifter. Härigenom har man i motsvarande mån fjärmat sig från den grundsats som motiverade handlingsoffentligheten.

Även med avseende på uppgiftslämnandet mellan skilda myndigheter har de ovan redovisade förhållandena fått allvarliga konsekvenser. Vid den senaste översynen av sekretesslagstiftningen fann man det från integritetssynpunkt angeläget att fastslå att sekretesslagens regler även skulle gälla mellan myndigheter – t. o. m. mellan självständiga verksamhetsgrenar inom samma myndighet. Samtidigt har emellertid den tekniska utvecklingen bl. a. lett till förekomsten av de ovan nämnda potentiella handlingarna. Detta har i praktiken öppnat för ett vidgat dataflöde mellan myndigheterna. Knappast någon myndighet torde undanhålla en annan myndighet sådana sammanställningar av data som är tekniskt möjliga att ta fram ur den egna databasen om dessa sammanställningar ändå skulle utlämnas enligt offentlighetsprincipen därest någon enskild begärde detta. Härigenom kommer myndigheterna faktiskt att kunna använda "offentlighetsprincipen" för att kontrollera enskilda, medan syftet med principen är det rakt motsatta.

De nu redovisade problemställningarna måste uppmärksammas i högre grad än för närvarande. Olika former att fixera innehållet i datahandlingar genom föreskrifter från datainspektionen till den registerförande myndigheten kan vara ett sätt. Ett annat kan vara tekniska begränsningar i programmen, syftande till att enbart göra sådan databehandling möjlig som rimligtvis står i överensstämmelse med myndighetens uppgifter och ärendebehandling. Data- och offentlighetskommittén har under sin drygt tvååriga verksamhet ännu inte lagt dylika överväganden till grund för sina betänkanden.

Det finns vidare, alldeles oavsett data- och offentlighetskommitténs arbete, av skäl som framgår av ovan förda resonemang, anledning till att ytterligare precisera gränsen mellan olika myndigheter och självständiga verksamhetsgrenar vad gäller uttag i enlighet med offentlighetsprincipen. Det finns enligt vår mening starka skäl för att en myndighet skall inhämta

personuppgifter direkt från den enskilde och inte från andra myndigheter.

Detta bör framgå i berörda myndigheters instruktioner. Vad som här anförts med anledning av olika myndigheters inbördes hantering av offentliga uppgifter bör riksdagen som sin mening ge regeringen till känna.

Det finns utöver detta anledning att i betydligt högre grad än tidigare diskutera formerna för hur sekretessbelagd information på data skyddas samt under vilka former sekretessbelagd information lämnas ut.

De tekniska möjligheterna till intrång ger anledning till oro. I det avsnitt som behandlar sårbarhetsfrågor återkommer vi till skyddet av sekretessbelagd information.

Vid ett antal olika fall har det funnits anledning att rikta kritik mot vissa myndigheters sätt att hantera sekretesslagen, när de lämnar ut sekretessbelagda uppgifter till olika register.

Hälso- och sjukvårdssekretessen ställer krav på en menbedömning för varje person som man lämnar ut uppgifter om. Detta sker uppenbarligen inte i de fall då stora informationsmängder överföres från ett register till ett annat.

Den mest uppseendeväckande nonchalansen av de krav som sekretesslagen ställer är den uppgiftslämning som idag sker till socialstyrelsens forskning- och statistikregister från landstingen. Sedan data- och offentlighetskommittén i sitt betänkande SOU 1986:24 påtalat att den uppgiftsöverföring det här gäller inte är förenlig med sekretesslagen har inget skett från vare sig regeringens eller myndigheternas sida.

Detta förhållande är oacceptabelt. Uppgiftslämnandet inom och mellan hälso- och sjukvårdens olika myndigheter måste följa gällande sekretesslag. Regeringen bör därför omgående ta initiativ till nya informationsrutiner mellan socialstyrelsen och sjukvårdens olika myndigheter. En förutsättning för centrala register av det slag det här gäller, bör vara att de har stöd i en särskild registerlag. P. g. a. den tid som förflutit sedan det klargjordes att delar av landstingens uppgiftslämnande till socialstyrelsen inte är förenligt med sekretesslagen är det nu nödvändigt att detta arbete sker skyndsamt. Riksdagen bör ge regeringen till känna vad som här anförts.

Den bristande överensstämmelsen mellan sekretesslag och tillämpning i detta fall – där verksamheten är organiserad och noga planlagd och utredd – ger anledning att misstänka att en bristande överensstämmelse föreligger även i andra fall där bedömningen görs från fall till fall i en betydligt svårare beslutssituation i det vardagliga arbetet.

Kombinationen av ett ökat hanterande av sekretessbelagda uppgifter och allt större datasystem gör det angeläget att sekretess tillämpas på det sätt som avses och som lagen ger möjlighet till. Ett nyligen uppmärksammat exempel på bristande tillämpning av sekretesslagstiftningen är Södertäljes kommunala civilförsvarsplanering, som var helt öppen, trots att den rimligen borde vara sekretessbelagd.

Regeringen bör ta initiativ till en översyn av hur svenska myndigheter tillämpar sekretesslagstiftningen. Det finns två viktiga skäl till detta. Dels skulle en sådan översyn leda till en bättre tillämpning, dels skulle regering och riksdag få en bättre bild av hur den sekretess fungerar som ibland är en förutsättning för inrättandet av vissa datasystem. Vad som här sagts om en

översyn av myndigheternas tillämpning av sekretesslagstiftningen bör riksdagen som sin mening ge regeringen till känna.

Det finns emellertid ytterligare ett annat problem som följer av kommunikationen i stora datasystem och sekretessbelagda informationer.

Risken för att hemliga uppgifter kan tappas ur olika dataregister kommer troligtvis aldrig kunna förebyggas helt samtidigt som vissa register måste finnas till. Frågan om kryptering av sådan känslig information är därvid av stort intresse. Inom statistiska centralbyrån har man arbetat med att utveckla olika "säkra" krypteringsmetoder.

Enligt vår mening är emellertid säker och trovärdig kryptering endast en metod för bättre säkerhet. Kryptering kan därför inte användas som argument för inrättandet av fler register och insamlande av fler uppgifter. Däremot bör sådana metoder användas när de kan ge större säkerhet åt information som finns insamlad i befintliga register. Det bör inte nödvändigtvis gälla enbart forsknings- och statistikregister. Regeringen bör därför lämna riksdagen en redovisning över hur kryptering kan användas i olika datasystem.

Ett alternativ till kryptering är utgallring av känsliga uppgifter efter en viss tid eller när myndigheten inte längre behöver uppgiften i sådana verksamheter som inte främst rör traditionell myndighetsutövning utan där den enskilde snarare står i ett slags kundförhållande till myndigheten. Den typen av register bör i görligaste mån avidentifieras när så är möjligt. Ett exempel på denna typ av register är biblioteksverksamheten. Utlåningsregister bör sekretessbeläggas och gallras kontinuerligt.

Ytterligare ett alternativ för att skydda känsliga personuppgifter är att den enskilde bär dem med sig. Inte minst inom sjukvården skulle detta kunna vara ett alternativ med hjälp av s. k. smart cards.

Ett förfarande där sådana elektroniska kort blir bärare av vissa patientuppgifter skulle kunna kombineras med datasystem som är decentraliserade för varje sjukvårdsklinik. Genom ett sådant system skulle de som är närmast berörda i vården av en patient – patienten och den aktuella kliniken – ha en kontroll över patientjournalens uppgifter. Samtidigt skulle man genom ett system med elektronisk post – men med beaktande av sekretesslagens krav – möjliggöra överföring av information till och från kliniker.

Genom att ansvaret och kontrollen av journaluppgifterna ligger hos dem som inför patienten är ansvariga för vården, skapas ett stort förtroende för hur uppgifterna hanteras samtidigt som möjligheterna till forskning inte påverkas. Det borde vara angeläget för sjukvårdshuvudmännen och andra vårdgivare att utreda förutsättningarna för hanterande av patientjournaler med hjälp av "smart cards" eller lokalisera datasystem.

Formerna för uppgiftslämnandet enligt sekretesslagen lämnar ur den enskildes perspektiv mycket övrigt att önska. Beslut om utgiftslämnande fattas av myndigheten utan möjlighet för den registrerade – som lämnat uppgifter i tron att dessa skall stanna hos myndigheten – att reagera. Det finns därför anledning att överväga dels en underrättelse till den registrerade, dels en besvärsrätt, så att prövning kan ske av annan instans än den utlämnande myndigheten. Vad som i frågan om underrättelse till enskild och besvärsrätt anförts bör ges regeringen till känna.

4 Att skydda den enskildes integritet

Datalagen trädde i kraft 1973. Den är avsedd att vara ett skydd gentemot otillbörliga intrång i den enskildes integritet vad avser ADB-baserade personregister. Lagen slår bl. a. fast vad gäller begreppet otillbörligt intrång att inställningen som föreligger, eller kan antas föreligga, hos dem som kan registreras skall beaktas vid bedömningen av vad som är otillbörligt intrång.

Det skydd datalagen ger den enskildes integritet har i praktiken försvagats.

Den offentliga sektorns utveckling har lett till ett så omfattande registrerande att den enskilde medborgaren knappast kan ha någon överblick över var han är registrerad, lika litet som han kan ha kännedom om vilka uppgifter som finns registrerade och vem som kan få tillgång till dem.

Den enskilde kan än mindre påverka spridningen av insamlade uppgifter om den egna personen. Datatekniken erbjuder kommunikationsmöjligheter och sammanställningsmöjligheter som har lett till att sekretesskyddet i praktiken har urholkats samtidigt som myndigheterna börjat sälja de insamlade personuppgifterna.

I de flesta kontakter med det offentliga möter den enskilde krav på att uppge personuppgifter. Statliga myndighete, kommuner och landsting har alla sina register, som alla kräver sin del av den enskildes privatliv och som oftast förutsätter samkörning med andra register. Ur dessa register lämnas uppgifter vidare till andra myndigheter samt till forskning och statistik. Inom barnomsorgen, äldrevården och sjukvården ställs frågor om den enskildes privata förhållanden, vilket också är fallet när han står i bostadskö eller begär bostadsbidrag. Uppgifterna registreras och sammanställs, lagras och skickas vidare till andra myndigheter. De flesta landsting har idag omfattande patientdatabaser som innehåller uppgifter som kan anses som ytterligt integritetskänsliga.

Skyddet av den enskildes integritet bör baseras på attityden att personuppgifter tillhör den enskilde. När uppgifter måste insamlas skall detta ske med stor respekt för denne. Insamlade uppgifter bör så långt möjligt vara en sak mellan den enskilde och myndigheten. Offentlighetsprincipen utgör härvidlag en begränsning. Det faktum att insamlade uppgifter blir offentliga bör å andra sidan fungera som en restriktion för mängden av material som insamlas. Myndigheterna bör dessutom inte genom försäljning aktivt sprida uppgifterna vidare.

4.1 Vad är integritet?

Begreppet integritet är svårt att objektivt definiera utifrån den enskilde medborgarens perspektiv. I ett mer allmänt perspektiv kan det dock beskrivas enligt följande.

För det första är graden av integritet beroende av den enskildes möjlighet att bestämma andras insyn i det egna privatlivet. För det andra beror integriteten av hur stor kontroll och kännedom den enskilde har över hur insamlade uppgifter används. Det blir därmed viktigt att skydda mot insyn och att öka den enskildes kontroll över insamlade uppgifter. Svårigheten att generellt bestämma vad som för individen är känslig information är ingen

ursäkt för underlåtenhet att skydda integriteten. Tvärtom gör denna svårighet att skyddet och den enskildes kontroll bör vara så omfattande som möjligt. Därmed kan den enskilde i största möjliga mån själv dra gränsen för sin integritet.

En stor del av de frågor som gäller data och den enskildes integritet ligger idag på regeringens bord. Detta gäller frågan om en personnummerbegränsning, försäljningen av personuppgifter och metoden att med särskilda registerlagar ge riksdagen kontroll över stora centrala register. Den viktigaste frågan, nämligen den som rör innebörden i begreppet offentlig handling är fortfarande under utredning liksom ett antal andra för integriteten viktiga frågor. Vi vill i det följande peka på åtgärder som vi bedömer som angelägna i syfte att anpassa datalagen och annan lagstiftning till de hot som i dag möter den enskildes integritet.

4.2. Begränsa uppgiftslämnandet

Det avgörande hotet mot den enskildes integritet är när han eller hon tvingas lämna ifrån sig personliga uppgifter. När uppgifterna väl är lämnade har den enskilde inte längre någon kontroll eller egentlig kunskap om hur de används. Ny lagstiftning kan t. ex. tillkomma som medger nya användningsområden av insamlade uppgifter. Intrång i integriteten kan ske genom att sekretesskyddet fungerar dåligt. Tillstånd till nya samkörningar mellan olika dataregister kan lämnas. Behörighetssystem kan vara bristfälliga. Sekretess som tidigare har rått kan hävas. Mot denna bakgrund är det nödvändigt att minska myndigheternas rätt att insamla, registrera, lagra och vidarebefordra personuppgifter.

Regeringen bör därför tillsätta en delegation med uppgift att föreslå minskningar i medborgarnas uppgiftsskyldigheter.

I ett större perspektiv är den enskildes integritet direkt beroende av hur mycket den offentliga makten intervenerar i den enskildes vardag. Enkla och generella system för välfärd minskar behovet av kontroll och personuppgifter. En ökad frihet för den enskilde medborgaren, ett spritt ägande, uppluckring av offentliga monopol samt lägre skatter är exempel på politiska åtgärder som inte bara utökar utrymmet för den enskildes egna beslut och engagemang utan också stärker den enskildes integritet. Denna politik skisseras i en lång rad andra motioner som lämnas in till årets riksmöte av företrädare för moderata samlingspartiet.

4.3 Stärk datalagen

Frågan om ett grundlagsskydd för den enskildes integritet ligger på riksdagens bord. Den överenskommelse som förslaget bygger på skulle enligt vår mening kunnat vara mer långtgående vad gäller att styra användningen av insamlade uppgifter i ett register till det ändamål de insamlats för.

Det finns dock ett betydande symbolvärde och även en praktisk betydelse i det nu liggande förslaget som motiverar vår uppslutning bakom det. För att grundlagsskyddet skall kunna få en mer märkbar betydelse, krävs emellertid en förstärkning av den nuvarande datalagstiftningen.

Enligt vår mening bör ändamålet för ett register få en betydligt större betydelse för användningen av de insamlade uppgifterna än vad de idag har.

Samtidigt finns det skäl att utnyttja den praxis som utvecklats sedan datalagens tillkomst till att precisera datalagen och därmed ge den en starkare ställning.

Detta kan ske genom att man bättre än idag definierar begreppen särskilda och synnerliga skäl för tillstånd enligt datalagen. Härigenom kan man på en gång uppnå en bättre ändamålsstyrning och samtidigt vinna en ökad klarhet i datalagen.

Vad gäller prövningen av datainspektionens beslut menar vi att denna bör ske strikt enligt datalagen utan politiska avvägningar. Det finns idag en sådan erfarenhet och praxis av datalagens tillämpning att regeringsrätten och inte regeringen bör vara besvärsinstans. Datalagens skydd av den enskildes integritet blir starkare om prövningen av datainspektionens beslut enbart sker efter datalagen, utan de politiska värderingar en regering tenderar att göra.

Den kanske mest diskuterade formen för användande av insamlade personuppgifter är samkörning med andra register. Det är enligt vår mening utomordentligt viktigt att skapa en ökad restriktivitet vad gäller samkörningar. Detta gäller framförallt samkörningar som syftar till kontroll. Samtidigt är det viktigt att ge den enskilde registrerade en starkare ställning inför frågan om en samkörning skall ske.

Endast sådana kontrollsamkörningar bör tillåtas där den enskilde vid lämnandet av informationen haft klart för sig att samkörning kan komma att ske. Efter genomförd samkörning skall den enskilde få del av resultatet. Några åtgärder får inte vidtagas utan att den enskilde haft möjlighet att reagera mot eventuella felaktigheter.

Vad gäller samkörningar med andra syften är kontroll – till exempel forskning eller statistik – bör kravet på informerat samtycke skärpas i de fall en särskild registerlag inte anger under vilka former samkörningar med dessa syften får ske.

Mängden av befintliga register med persondata i det svenska samhället möjliggör en typ av forskning som på grund av kostnadsskäl annars inte hade kunnat genomföras i samma grad som idag. Det gäller framförallt projekt, som kräver att de enskilda individernas data från en tid till en annan, och från ett register till ett annat, är identifierbara.

Forskning som utan ett stort befintligt registermaterial endast hade kunnat genomföras under förutsättning av stora ekonomiska resurser kan idag genomföras med stor enkelhet med hjälp av modern datateknik och befintliga register.

Forskning och statistik är vida begrepp. Det faktum att uppgifter skall användas för dessa ändamål ger inte i sig ett skydd för integriteten.

Ur den enskildes perspektiv kan skillnaden mellan t. ex. administrativa register och forskningsregister vara liten. För den enskilde är det ett faktum att han eller hon saknar kontrollen över vart känsliga uppgifter tar vägen. Utan vetskap om vem eller vilka som får tillgång till uppgifterna blir personen beroende av att andra hanterar uppgifterna på ett sätt som är förenligt med hans värdering av den personliga integriteten.

Risken för missbruk och felaktig hantering ökar ju mer omfattande registerhanteringen blir.

Fler register och en vidare spridning av registrens innehåll leder dessutom till en större risk för att "grannen" får insyn i en uppgift som man egentligen enbart vill ha för sig själv.

Det finns av detta och av andra skäl – t. ex. rädslan för att uppgifterna används för andra ändamål än för forskning och statistik – anledning att misstänka att en ökad avoghet gentemot olika register och till insamling av uppgifter kommer att växa fram. Detta kan ta sig – och tar sig redan idag – uttryck i ofullständigheter, felaktigheter och uteblivna svar. Den typen av "civil olydnad" kan försvåra möjligheterna att använda datatekniken som sådan. Förutom att kvaliteten på de data som används för forskning blir sämre finns en betydande risk för att människor inte kommer att vilja deltaga i sådana projekt som faktiskt kräver deras aktiva medverkan.

Ett bristande förtroende för myndigheternas sätt att hantera insamlade uppgifter kommer också att drabba människors välfärd på ett orättvist och ibland farligt sätt. Exempel finns redan idag på att människor avstår från välfärdsförmåner eller vård på grund av att de hellre värnar sin personliga integritet – ett handlande som vilar på allmänna känslor av bristande förtroende och stolthet. "Ingen annan än jag och doktorn har med detta att göra."

Det är följaktligen nödvändigt att ge den enskilde en starkare rättslig ställning i frågor som rör skyddet av hans integritet. Integriteten som sådan och allmänhetens förtroende för myndigheternas hantering av personuppgifter kräver detta. Ett sådant förtroende är en förutsättning för att de uppgifter som samlas in får en sådan kvalitet att de är användbara till det syfte de samlas in för. Detta gäller inte minst om de skall användas till forskning.

Argumentet att forskningen behöver tillgång till personuppgifter och register är inte tillräckligt för att integritetsaspekter skall vika. En del av de argument som används för att longitudinell forskning skall genomföras på basis av olika register ger i konsekvensens namn anledning till insamling av ännu fler uppgifter. I en tänkt framtid skulle man därmed kunna avslöja ännu fler folksjukdomar än vad man annars hade kunnat.

"Ifall, ifall"-attityden är både farlig och meningslös. Den är farlig eftersom den leder till omfattande uppgiftskrav och krav på utnyttjande av olika register. Den är meningslös eftersom vi trots allt vet så oerhört lite om vad som i framtiden är relevanta kunskaper för de forskningsbehov som då finns. Det är i det perspektivet viktigare att slå vakt om den personliga integriteten och allmänhetens förtroende – för framtida medverkan – än om fri tillgång till befintliga registerdata.

Det finns dessutom en risk för att lättillgängligheten blir metodstyrande och att forskningsuppgifter löses genom registerforskning. Alternativen till registerforskning är dock många.

Riktade undersökningar med insamling av de för ett särskilt forskningsändamål relevanta uppgifterna är ett annat sätt, så kallade surveys ytterligare ett. Den svenska forskning som bygger på uppgifter om större populationer har präglats av tillgängliga befolkningsregister. Det är däremot inte belagt att forskningen i andra länder – ofta bedriven med en annan metodik – är sämre.

Undervisning om andra metoder för forskning än sådan som bygger på tillgång till dataregister och samkörningar bör vara ett led i berörd forskarutbildning. Det kan öka intresset för andra tillvägagångssätt och minska pressen på kompromisser med kravet på ett fullgott skydd för den enskildes integritet.

Det är viktigt och fullt möjligt att ge den enskilde en starkare ställning genom att mer konsekvent införa kravet på informerat samtycke utan att forskningen för den skull skall omöjliggöras eller försvåras mer än som är rimligt.

- Informerat samtycke bör gälla samkörning av uppgifter ur olika register samt utlämnande från sekretessbelagda register. Informerat samtycke innebär att den enskilde informeras och själv samtycker till att uppgifter om den egna personen används till ett annat ändamål än som från början avsågs.
- Datainspektionen bör kunna medge att man tillämpar passivt samtycke. Det innebär att de registrerade informeras och ges möjlighet att reagera mot att uppgifter om dem används.

Passivt samtycke bör enbart kunna tillämpas då det gäller uppgifter som från integritetssynpunkt anses mindre känsliga och när det aktuella registrets omfattning gör det orimligt att använda aktivt samtycke. Ett villkor för att passivt samtycke skall räcka bör vara att möjligheten att använda urvals- eller tvärsnittsundersökningar är uttömd.

- Det finns dock vissa register som har ett sådant innehåll att det är av betydande värde att uppgifterna kan användas för forskning utan att informerat samtycke skall vara en förutsättning.

Av bl. a. detta skäl är det lämpligt att centrala offentliga register har stöd i särskilda registerlagar, som dels ger det lagliga stödet till uppgiftsinsamlingen som sådan och dels beskriver under vilka former de insamlade uppgifterna får registreras och användas. Genom ett system med registerlagar får riksdagen kontroll över utvecklingen inom området.

I sådana registerlagar kan anges om uppgifterna får lämnas ut utan den enskildes informerade samtycke och om uppgifterna får samköras med andra register utan informerat samtycke.

- I registerlagarna bör finnas bestämmelser för hur sekretessbelagda uppgifter skall lämnas ut. Vidare bör där beskrivas formerna för hur ett beslut om utlämnande skall tas. Det bör t. ex. förutsättas att det aktuella forskningsprojektet har godkänts av en etisk kommitté. Ansvaret för utlämnandet av uppgifter skall vara klart och entydigt och ligga hos ledningen av den myndighet som för registren.

Huvudregeln skall vara att informerat samtycke skall krävas vid utlämnande av sekretessbelagda personuppgifter och vid samkörning av personregister. I undantagsfall kan datainspektionen medge passivt samtycke. Endast om det anges i särskild registerlag skall uppgifter kunna lämnas ut och samköras utan individens samtycke. Riksdagen bör som sin mening ge dessa riktlinjer för forskningens användning av dataregister till känna.

4.4 Begränsa personnummeranvändningen

Personnumret har för många kommit att bli en symbol för ett skrämmande datasamhälle där den enskilde anonymiseras och blir till ett nummer utan namn, ständigt utsatt för myndigheters kontroll och insyn, utan någon annan identitet än sitt personnummer. Förekomsten av denna känsla behöver inte överdrivas. Den är ändå ett skäl till försiktighet med personnummeranvändningen.

Det finns också betydligt mer konkreta skäl att begränsa personnummeranvändandet. Som identifikationsbegrepp har personnumret en särställning. Den utbredda användningen av personnumret – där personnumret faktiskt i många fall fått ersätta namnet – leder till att den enskilde i en mängd sammanhang lämnar efter sig ett unikt identifikationsbegrepp, tillsammans med känsliga eller okänsliga personuppgifter, när namn och adress hade räckt för det syfte man lämnar uppgifterna till. Genom att detta unika identifikationsbegrepp används inom alla samhällsområden skapas en möjlighet till insyn, kontroll och spårning av enskilda personer som ur många perspektiv är skrämmande. Detta är inte en följd av personnumrets tekniska uppbyggnad utan av dess effektivitet att helt entydigt identifiera en individ.

Personnumret ger dessutom tekniska förutsättningar som underlättar samkörning även om det inte alltid är en förutsättning för detta. Det är betecknande att de som starkast understryker hur lätt det är att samköra med andra identifikationsbegrepp ofta samtidigt pekar på de svårigheter en begränsning av personnummeranvändningen skulle innebära.

Enligt vår mening är det inte fråga om att avskaffa personnumret utan att begränsa dess användning. Det är ett effektivt identifikationsbegrepp som skall användas där den typen av säker identifikation är nödvändig. En begränsning av personnummeranvändningen bör i stället bygga på att endast vissa registeransvariga, genom särskilt lagstöd, får kräva personnummer. I övrigt bör användningen av personnummer vara frivillig.

För närvarande ligger ett förslag med denna innebörd hos regeringen varför vi inte lämnar något yrkande i denna fråga.

4.5 Försäljning av personuppgifter

Stat och kommun ägnar sig idag åt att aktivt sprida insamlade uppgifter genom att kommersiellt försälja dem.

Vi anser det principiellt felaktigt att det offentliga på detta vis säljer delar av enskilda medborgares privatliv. Offentlighetsprincipen ger inget stöd för en sådan försäljning. Tvärtom riskerar försäljningsverksamheten att skapa en "lyxklass" där vissa medborgare kan köpa offentliga handlingar i en form som offentlighetsprincipen inte ger den enskilde möjlighet att kräva.

Data- och offentlighetskommittén har lämnat förslag om en begränsning av försäljningen ur personregister. Begränsningen innebär i själva verket en legalisering av nuvarande försäljningsverksamhet. Genom att man inte tagit ställning till offentlighetsprincipens handlingsbegrepp innebär kommitténs förslag varken någon begränsning eller kontroll av vilka uppgifter och vilken information som får säljas.

Det är enligt vår mening ytterst betänkligt att myndigheter försäljer uppgifter som insamlats för speciella myndighetsändamål.

För det första innebär försäljningen att myndigheten ägnar sig åt en verksamhet som inte ingår i själva myndighetsuppgiften. För det andra leder försäljningen till en uppenbar risk att man blandar ihop behovet av uppgifter för myndighetsutövningen med den efterfrågan försäljningen ger. Det finns påtagliga integritetshot i detta, samtidigt som denna risk negativt kan påverka medborgarnas förtroende för myndigheten och dess sätt att hantera insamlade uppgifter.

För det tredje strider försäljningen mot syftet med datalagens ändamålsparagraf. Insamlade personuppgifter skall enbart användas för de ändamål de insamlats för. Existensen av SPAR-registret – som har stöd i datalagen – och försäljningen ur andra register strider mot denna paragrafs syfte att skydda den enskildes integritet. Försäljningen ur myndigheters personregister bör därför inte tillåtas. Riksdagen bör ge regeringen detta till känna.

Statens person- och adressregister bygger på uppgifter som insamlats för helt andra ändamål än för försäljning. Med sin mängd av olika uppgifter som kan levereras i olika, förutsedda och oförutsedda, sammanställningar tillhör SPAR-registret ett av de mer integritetskänsliga registren i Sverige. Försäljningen ur detta register i dess nuvarande form bör därför inte heller få ske.

Därmed försvinner motivet för detta registers särställning. Behovet av ett register för t. ex. uppdatering kan fyllas genom att SPAR omvandlas till ett renodlat adressregister som i vanlig ordning lyder under datalagen. Riksdagen bör därför fatta beslut om att avveckla SPAR.

4.6 Skydd av företagsuppgifter

Den svenska integritetsdebatten har nästan uteslutande rört de enskilda individerna och det hot som datoriseringen – främst hos myndigheterna – inneburit för intrång i den personliga integriteten. Det mycket omfattande ADB-stöd som numera är en normal del i myndighetsutövningen, innebär av samma skäl som ovan redovisats vad avser den enskilde medborgarens integritet.

Det förekommer i dag ett omfattande uppgiftsinsamlande från företagen till den offentliga sektorn. Uppgiftsinsamlandet har under åren vuxit till oerhörda volymer. Enligt beräkningar, som gjordes för flera år sedan, sänder näringslivet in mer än 50 miljoner blanketter till olika myndigheter under ett år. Volymen har snarare ökat än minskat sedan dess. Insamlandet syftar till att tillgodose samhällsapparatens underlag för styrning, kontroll och statistik. Hanteringen av dessa oerhörda volymer av data är endast möjlig med hjälp av ADB-teknik hos myndigheterna.

Lagringen av dessa data i myndigheternas databaser representerar de facto en potentiell risk för oförutsedda och obehöriga informationsuttag. Dessa risker måste elimineras. En första förutsättning för att nå detta mål är att man i högre grad än för närvarande är medveten om de sårbarhets- och integritetsrisker som dessa baser medför. Dessa frågor behandlas närmare under rubriken "Sårbarheten måste minskas".

Myndigheternas insamling av företagsuppgifter medför emellertid även ytterligare risker, som i första hand sammanhänger med hur insynsreglerna enligt offentlighetsprincipen och de gällande reglerna i sekretesslagen tillämpas.

Som ovan redovisats kommer t. ex. det skydd som sekretesslagen är tänkt att ge vad gäller uppgiftsöverföringar från en myndighet till en annan att i stor utsträckning sättas ur spel genom nuvarande praxis enligt tryckfrihetsförordningen och sekretesslagen – framför allt genom tillämpningen av informationsbegreppet "potentiell handling" vid uppgiftslagring på ADB-medium. Denna utveckling av praxis är ännu så länge bara inledd, men den kan leda till ytterst obehagliga konsekvenser om den tillåts fortsätta.

Enligt vad som anförts på annan plats i motionen bör problemen med ADB och offentlighetsprincipen angripas raskt och beslutsamt. Härigenom skulle de grundläggande integritetshoten – både för individer och företag – i väsentliga delar kunna undanröjas.

För skyddet av företagens integritet krävs emellertid också andra särskilda åtgärder. I första hand bör dessa avse insatser för att begränsa det uppgiftsinsamlande som nu förekommer hos ambitiösa myndigheter som i detta avseende givits ganska fria händer genom den s. k. ramlagstiftningstekniken. Uppgiftsinsamlandet borde i mycket större utsträckning förutsätta direkt och tydligt stöd i lag för att få förekomma. För kontrolländamål borde t. ex. endast stickprov göras även om datatekniken gör det billigt för den uppgiftsinsamlande myndigheten att bearbeta uppgifter från den totala populationen.

Det borde också klarare slås fast – såsom gäller för uppgifter om enskilda individer – att uppgifter som insamlats för ett bestämt ändamål inte skall få användas för andra ändamål än som avsågs vid uppgiftsinsamlingen – varken hos den insamlande myndigheten eller annan myndighet.

I de fall då det blir aktuellt att överlämna uppgifter rörande ett visst företag från t. ex. en myndighet till en annan – och detta inte kunnat förutses vid uppgiftsinsamlandet – bör regler övervägas som skyddar företagen genom att dessas samtycke skall inhämtas.

Det synes också vara nödvändigt att tillförsäkra företagen en laglig insynsrätt med avseende på de uppgifter som registrerats om dessa hos någon myndighet. Insynsrätten skulle kunna utformas med ledning av den särskilda paragraf i datalagen som tillförsäkrar medborgarna en insynsrätt av detta slag.

Det är också angeläget att överväga integritetsskyddsregler som förhindrar att företagen avtvingas uppgifter om affärsidéer, planer och liknande företagshemligheter som i orätta händer skulle kunna lända företaget till skada.

Behovet av skydd av företagshemligheter bör utredas i särskild ordning. Riksdagen bör ge regeringen detta till känna.

5 Sårbarheten måste minskas

Det tekniskt avancerade samhällets sårbarhet är ett stort och växande problem. Elavbrott, återkommande tillfällen av avbrott i radio- och TV-

utsändningar samt allvarliga störningar i tele- och datakommunikationslinjerna är några exempel som visar på samhällets sårbarhet i vid bemärkelse. De visar också hur dålig vårt samhälles beredskap är. Hur denna sårbarhet påverkas av den fortgående datoriseringen av samhällets olika funktioner har kartlagts och analyserats under en följd av år – först av sårbarhetskommittén (SÅRK) och senare av sårbarhetsberedningen (SÅRB).

SÅRK, som gjorde en övergripande analys, drog vid 1970-talets slut den allmänna slutsatsen att sårbarheten är oacceptabelt hög och att den kommer att öka om inte motåtgärder vidtas. Sex år senare konstaterar SÅRB att medvetenheten om denna sårbarhet visserligen ökat, men att det är tveksamt om den ökade medvetenheten hittills fått tillräckligt genomslag. Sårbarheten är, anser SÅRB, alltjämt oacceptabelt hög.

Ambitiösa insatser ifråga om kartläggning och analys samt även beträffande utveckling av nya metoder och hjälpmedel har gjorts av de nämnda utredningarna. Tyvärr har emellertid den socialdemokratiska regeringens vilja och förmåga att följa upp utredningsresultaten inte varit lika framträdande. I stället för att ta itu med de praktiska problemen när utredningsresultaten förelåg lät regeringen tiden förödas genom kompetenstvister mellan olika departement. Belysande är att det gick nästan ett helt år efter det att justitieministern bemyndigats att tillkalla en samrådsgrupp i sårbarhetsfrågor innan en sådan grupp började tillsättas och då hade ärendet flyttats till civildepartementet och sammansättningen och inriktningen blivit en annan än som ursprungligen avsetts.

Ansvaret för sårbarhetsfrågor är idag splittrat på olika myndigheter och samrådsgrupper. Något organ med ett samlat och övergripande ansvar för den nationella säkerheten, finns ej idag, trots det ansvar som nu lagts på ÖCB. Samtidigt som civildepartementet ansvarar för datafrågor lyder ÖCB under försvarsdepartementet. Uppenbarligen har detta lett till handlingsförlamning. T. ex. har SÅRB:s olika rekommendationer inte fått någon konkret uppföljning. De brister som SÅRB pekade på kvarstår. Det är därför nödvändigt att regeringen snarast till riksdagen redovisar vilka åtgärder man avser att vidta för att minska sårbarheten. Samtidigt bör regeringen till riksdagen redovisa en organisation för sårbarhetsfrågornas hantering med klara ansvarsförhållanden inom regeringskansliet. Riksdagen bör ge regeringen detta som sin mening till känna.

Vi vill i det följande beröra några av de problemområden där vi anser att snara åtgärder är påkallade.

5.1 Den civila statsförvaltningens sårbarhet

Av ett flertal rapporter (bl. a. statskontorets rapport 1986:3 och RRV:s rapport ADB–säkerhet–granskning av de civila myndigheternas ADB-säkerhetsarbete, som publicerades sommaren 1987) har framgått att det finns skrämmande brister i säkerheten hos många civila myndigheter. Sårbarhetsanalyser har i allmänhet inte genomförts och katastrofplanering i egentlig mening är bristfällig eller förekommer inte alls. Här har statsmakterna ett oavvisligt ansvar att tillse att myndigheterna åläggs att svara för en sådan planering att risken för datahaverier vare sig det beror på olyckshändelser

eller medvetna sabotagehandlingar minskar. I den ovan nämnda RRV-rapporten föreslås att alla myndigheter med ADB-register bör göra en sårbarhetsanalys och bedöma konsekvenserna av eventuella störningar. Vi delar också uppfattningen att processen hur skyddsåtgärder väljs och införs bör förbättras, liksom även utbildning och information till berörd personal. Vi anser att även en sårbarhetsanalys bör läggas till grund för beslutsfattande om varje nytt register. Detta krav bör därför ställas på statliga utredningar genom tillägg i kommittékungörelsen. Sårbarhetsanalys skall ingå i det beslutsunderlag som skall föreligga enligt förordningen om investeringar i statliga ADB-register (SFS 1981:2666). Riksdagen bör ge regeringen detta till känna.

5.2 Datakommunikationernas sårbarhet

Datakommunikation inom landet och med utlandet har under senare år ökat kraftigt i omfattning. En snabb utveckling förväntas även för de kommande åren. Mot den bakgrunden är det allvarligt att informationssäkerheten ofta är så bristfällig.

Nätverk för datakommunikation används rutinmässigt för såväl produktions- och företagsstyrning som för andra vitala tillämpningar. Detta medför att betydligt större krav på säkerhet måste ställas mot såväl avbrott och störningar som mot avlyssning och obehörigt intrång i telenätet. Det är därför angeläget att tillgången på datakommunikationslinjer av god kvalitet ökar samt att behovet av nödvändiga alternativlösningar vid störningar tillgodoses. Skyddet mot avlyssning måste snabbt vidareutvecklas genom förbättrade krypteringsmöjligheter. Regeringen bör lämna riksdagen förslag som innebär krav på kryptering vid datakommunikation av sekretessbelagd information.

5.3 Offentlighet och sårbarhetsrisker

Det är uppenbart att offentlighetsprincipen och gällande handlingsbegrepp som likställer datalagrad information hos myndigheter med traditionella allmänna handlingar skapar problem från sårbarhetssynpunkt. Dagens moderna ADB-teknik och dess oanade möjligheter till selektering och sammanställningar gör att hanteringen av en mängd i och för sig oskyldiga uppgifter kan leda till en information som kan vara äventyrlig för landets säkerhet. SÅRB hävdade att ADB-behandlad information med gängse säkerhetsteknik inte kan anses uppfylla de krav på skydd som sekretesslagen ställer. Det uppmärksammade postens transportplaneringssystem (PTP) som sammanställts ur olika offentliga register till en detaljerad digitaliserad karta, marknadsförs just med de "operativa, tekniska och strategiska" fördelar det ger, är ett exempel på detta. Sammanställningen av denna information kan vara skadlig för rikets säkerhet. Förekomsten av PTP är ett exempel på den bristfälliga hanteringen i regeringen av dessa frågor. Uppenbarligen finns det ingen som på allvar prövat om PTP kan anses godtagbart med avseende på rikets säkerhet. Informationen bör inte

sammanställas i denna form och bör ej heller saluföras som nu sker. Riksdagen bör ge regeringen detta till känna.

5.4 Forskning och utveckling

På flera områden skulle sårbarheten kunna minskas och säkerhetsarbetet förstärkas genom ett målmedvetet forsknings- och utvecklingsarbete vid universitet och högskolor. Ett uppenbart viktigt område för de offentliga forskningsinstitutionerna är de frågor som rör databrott och s. k. datavirus. På grund av prestige och företagshemligheter finns det en betydande risk för att den kunskapsuppbyggnad som idag sker isoleras inom olika organisationer och företag. Inte minst inom det juridiska området är forskning angelägen. Det finns också behov inom sådana områden som systemutveckling, organisationsutveckling, personal- och säkerhet samt systemkomplexitet och hur den skall kunna kontrolleras. Ett annat forskningsområde är hur man skall kunna mäta, utveckla och vidmakthålla datakvalitet.

6 Statliga datorer

Datorer finns nu på allt flera statliga arbetsplatser – ingen verksamhet är undantagen. Samtidigt sker det inom de statliga förvaltningarna en utveckling i riktning mot mindre system. Det är inte inom de stora administrativa datasystemen som den tekniska utvecklingen är mest märkbar – det är inom den s. k. kontorsautomationen som den snabbaste utvecklingen äger rum. Ordbehandling, elektronisk post, kalkylering, konstruktion och trycksaksproduktion är bland de viktigaste områdena.

Behovet av olika typer av system är skiftande från myndighet till myndighet. I vissa fall är persondatorer ett lämpligt val. I andra fall kan nätverk av mindre datorer erbjuda flexibla och användarvänliga lösningar. Enbart inom några få områden krävs det stora centralt belägna datorer.

Det nuvarande anslagssystemet för statliga inköp av datorer är ett uttryck för ett äldre synsätt på datorer. Förr var datorer sällsynta. Då var det måhända lämpligt att en specialiserad myndighet hade upphandlingsansvaret. Statens kostnader för datoranvändning och investeringar inom förvaltning och undervisning uppgår till ca 2 miljarder kronor.

I dag kan myndigheterna själva finanisera s. k. basdatorer och persondatorer ur sina ordinarie anslag. Investeringar i större datorer finansieras över ett särskilt anslag över civildepartementets anslag.

Att myndigheterna dels får ett anslag för förvaltningskostnader, dels får ett anslag för datorer är olyckligt. Det innebär att myndigheten inte kan göra en avvägning mellan olika slags kostnader. Dessutom förlängs beslutsgången. Det finns därför en uppenbar risk att fel sorts utrustning köpes. Satsning på s. k. basdatorer eller större system riskerar att avgöras av myndighetens anslagssituation.

Regeringen har avviserat att den undervåren avser att lägga en proposition om dataanvändningen inom statsförvaltningen. Vi utgår från att regeringen kommer att förändra budgetsystemet vad gäller inköp av större statliga datorsystem. De olika statliga myndigheterna bör själva få köpa in datorut-

rustning. Statskontoret eller privata konsulter kan under en tid hjälpa myndigheter att bygga upp en kompetens för att på egen hand köpa in datorer.

I dag är kommunikationsmöjligheterna mellan olika sorters datorer ofta dåliga. I framtiden kommer kommunikationsområdet att utvecklas mycket snabbt. Det är därför väsentligt att investeringar i nya datorer sker med hänsyn till möjligheten att skapa kommunikation mellan olika system.

Vid inköp av datorer för statens räkning är det därför nödvändigt att man alltid klarlägger vilka kommunikationsmöjligheter som kan erhållas. Datorer som bara fungerar isolerade var för sig är betydligt mindre effektivitetsbefrämjande än de som kan fungera i nätverk. Möjligheterna till kommunikation måste därför vara ett grundläggande kriterium vid de enskilda myndigheternas val av datautrustning.

Integrationsarbetena inom EG kan förväntas leda till mer utvecklade "kommunikationsprotokoll" inom offentlig förvaltning. De svenska myndigheterna måste följa utvecklingen inom EG och tillse att svensk medverkan i det europeiska integrationsarbetet inte försvåras av praktiska kommunikationsproblem.

Ur sårbarhets- och integritetssynvinkel är det väsentligt att man inom statliga myndigheter strävar efter att upprätta mindre och geografiskt begränsade system. Det ger också möjligheter till lokalt anpassnings- och utvecklingsarbete. Erfarenheterna från stora övergripande administrativa system som t. ex. SLÖR, visar också att dessa ofta kan vara ett hinder för en effektiv administration.

7 Hemställan

Med hänvisning till det anförda hemställs

1. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om behovet av åtgärder beträffande myndigheters hantering av sekretessbelagd information,

2. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om informationsrutiner mellan socialstyrelsen och sjukvårdens olika enheter,

3. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om översyn av myndigheters tillämpning av sekretesslagstiftningen,

4. att riksdagen hos regeringen begär en redovisning av användning av kryptering i enlighet med vad i motionen anförts,

5. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om utgallring och sekretessbeläggning av uppgifter i register som inte nyttjas för myndighetsutövning,

6. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om besvärsrätt vid utlämnande av uppgift,

7. att riksdagen hos regeringen begär tillsättande av en delegation i syfte att föreslå minskningar av uppgiftslämnandet i enlighet med vad i motionen anförts,

8. att riksdagen hos regeringen begär förslag till ändring i datalagen (1973:289) beträffande särskilda och synnerliga skäl för tillstånd i enlighet med vad i motionen anförts,

9. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om prövning av datainspektionens beslut,

10. att riksdagen hos regeringen begär förslag till ändring i datalagen (1973:289) beträffande information och informerat samtycke inför samkörning av dataregister i enlighet med vad i motionen anförts,

11. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om användning av persondataregister vid forskning i enlighet med vad som i motionen anförts,

12. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om försäljning av uppgifter från statliga dataregister,

[att riksdagen hos regeringen begär förslag till avveckling av SPAR i enlighet med vad i motionen anförts[1]],

13. att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om behovet av skydd för företagshemligheter,

[att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om hanteringen av sårbarhetsfrågorna inom regeringskansliet[2]],

[att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om behovet av sårbarhetsanalys i samband med utredningsförslag om inrättande av nya register[2]],

[att riksdagen hos regeringen begär förslag till krav på kryptering av sekretessbelagd information vid datakommunikation[2]],

[att riksdagen som sin mening ger regeringen till känna vad i motionen anförts om sammanställning och försäljning av information som kan vara till skada för rikets säkerhet[2]].

Stockholm den 26 januari 1988

Anders Björck (m)
Gunnar Hökmark (m) *Hans Nyhage (m)*
Elisabeth Fleetwood (m) *Inger Koch (m)*
Birger Hagård (m) *Hans Dau (m)*
Stig Bertilsson (m)

[1] 1987/88:Fi413
[2] 1987/88:Fö526

Innehållsförteckning

gotab Stockholm 1988 14457