BILAGA 1: UTREDNINGS-DIREKTIVEN

INNEHÅLL:

Regeringens direktiv till Datalagskommittén (dir. 1995:91)

Inledning

Vid sitt sammanträde torsdagen den 15 juni 1995 beslutade regeringen direktiv för utredningen (dir. 1995:91). Direktiven innehåller följande.

Sammanfattning av uppdraget

En parlamentariskt sammansatt kommitté tillkallas med uppgift att analysera på vilket sätt ett kommande EG-direktiv om skydd för personuppgifter skall införlivas i svensk lagstiftning samt lägga fram förslag till en ny lag på området.

Kommittén skall också föreslå de ändringar i tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet som är motiverade för att grundlagsregleringen skall vara anpassad till den nya tekniken och terminologin på området.

Bakgrund

Datalagen (1973:289) syftar till att skydda den enskilde mot otillbörligt intrång i den personliga integriteten till följd av att personuppgifter registreras med hjälp av automatisk databehandling (ADB). Datainspektionen har till uppgift att pröva ansökningar om tillstånd och utöva tillsyn enligt datalagen.

Lagen kom till år 1973 och var den första lagen i världen av denna typ med nationell räckvidd. Sedan dess har utvecklingen inom informationstekniken (IT) medfört en alltmer ökande datoranvändning i samhället. Detta har bl.a. lett till att många europeiska länder infört någon form av speciallagstiftning till skydd för den personliga integriteten.

Datalagens grundläggande drag är oförändrade trots att det nu är över tjugo år sedan den tillkom. Lagen får därför i dag såväl innehållsmässigt som till sin lagtekniska utformning anses vara föråldrad.

Utvecklingstakten inom informationstekniken har sedan datalagens tillkomst varit i det närmaste explosionsartad. ADB-tekniken har kommit att användas på de flesta områden och den har fått en allt större betydelse för samhällsutvecklingen. Ett exempel på teknikens nya landvinningar är den kraftigt ökade användningen av globala datanätverk, t.ex. Internet, som lett till tidigare oförutsedda möjligheter att snabbt och billigt överföra information från en dator till en annan via telenätet. Utvecklingen har också medfört att olika medier används i en kedja, exempelvis satelliter, faxar, telefoner, datorer och papper. Likaså har s.k. multimedia fått ett vidgat utrymme.

Denna utveckling leder till att personuppgifter registreras, kommuniceras, bearbetas, lagras osv. i en ständigt ökande takt. Utvecklingen medför också ökade risker för att den enskildes personliga integritet kränks.

Redan vid datalagens tillkomst förutsattes att den skulle ses över inom en snar framtid. Så har också skett i olika etapper. Den senaste utredningen på området, Datalagsutredningen, lade fram sitt slutbetänkande En ny datalag (SOU 1993:10) i februari 1993.

Jämsides med Datalagsutredningens arbete pågick inom EG ett arbete med att ta fram ett direktiv om skydd för personuppgifter. Något direktiv fanns inte när Datalagsutredningen presenterade sitt slutbetänkande. Detta var en av orsakerna till att regeringen i proposition 1993/94:116 Normgivningsfrågor på dataskyddsområdet, m.m. gjorde bedömningen att utarbetandet av en ny datalag borde anstå till dess det fanns ett slutligt ställningstagande av EU:s medlemsländer till ett direktivförslag.

EU:s ministerråd har den 20 februari 1995 antagit en gemensam ståndpunkt i fråga om ett förslag till ett direktiv om skyddet för enskilda personer med avseende på behandlingen av personuppgifter och om det fria flödet av sådana uppgifter, det s.k. dataskyddsdirektivet, och ett slutligt ställningstagande till förslaget till direktiv förväntas under innevarande år. Det finns därför inte längre skäl att vänta med att inleda det angelägna arbetet med en ny lagstiftning på området.

Förslaget till dataskyddsdirektiv

Syftet med direktivförslaget är att skapa en gemensam, hög nivå på integritetsskyddet för att därigenom möjliggöra ett fritt flöde av personuppgifter

medlemsländerna emellan. Medlemsstaterna får inom den ram som ges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Dessa preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen.

I förslaget har man strävat efter flexibla lösningar som lämnar utrymme för medlemsstaterna att införliva direktivet på ett sätt som är förenligt med den nationella lagstiftningstraditionen på området och som tar hänsyn till att integritetsskyddet varierar från ett land till ett annat.

I arbetet med direktivet har Sverige agerat hårt för att få till stånd sådana lösningar att direktivet inte står i motsättning till den svenska offentlighetsprincipen och annan grundlagsreglering. De svenska ansträngningarna på detta område har varit framgångsrika. Det finns i den gemensamma ståndpunkten inte någon bestämmelse som står i strid med en tillämpning av den svenska offentlighetsprincipen. För att undanröja alla eventuella oklarheter vid tolkningen av direktivets förenlighet med offentlighetsprincipen, har på svenskt initiativ tagits in en klausul i förslagets ingress som gör det möjligt att ta hänsyn till offentlighetsprincipen när direktivets bestämmelser införlivas i nationell rätt.

Huvuddragen i direktivförslaget är följande.

Direktivet är tillämpligt på all behandling av personuppgifter och således också på manuella register, dock endast på sådana manuella register som är sökbara utifrån särskilda kriterier. Direktivet är inte tillämpligt på sådan behandling av personuppgifter som faller utanför gemenskapsrätten (t.ex. den som gäller allmän säkerhet, statens säkerhet eller statens verksamhet på straffrättens område) och inte heller på register för personligt bruk. Behandling av personuppgifter för journalistiska, konstnärliga och litterära ändamål undantas från direktivets materiella bestämmelser.

Personuppgifter får samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål och uppgifterna får inte senare användas på ett sätt som är oförenligt med ursprungsändamålet.

Personuppgifter får behandlas endast när samtycke lämnats, när det är nödvändigt för att fullgöra ett avtal i vilket den registrerade är part, när det finns en i författning reglerad förpliktelse att behandling av uppgifterna skall ske, när det är nödvändigt för att skydda den enskildes grundläggande intressen, när det är nödvändigt att utföra en arbetsuppgift i det allmännas intresse eller slutligen, om det i övrigt skett en intresseavvägning som resulterat i att behandling av personuppgifter skall få ske.

Känsliga uppgifter (ras, religion, politisk åsikt, facklig tillhörighet, hälsotillstånd etc.) får inte behandlas. Dock gäller vissa undantag, bl.a. vid

den enskildes uttryckliga samtycke, för ideella föreningars medlemsregister, för hälso- och sjukvårdens administration och vid författningsreglerad skyldighet.

Medlemsstaterna skall bestämma på vilka villkor personnummer får behandlas.

När personuppgifter samlas in skall de registrerade informeras om bl.a. vem som är registeransvarig och vad uppgifterna skall användas till.

All behandling av personuppgifter skall enligt huvudregeln anmälas till en tillsynsmyndighet. Medlemsstaten kan dock genom bransch- och sektorsreglering eller motsvarande från anmälningsskyldigheten undanta sådan behandling av personuppgifter som inte kränker enskildas fri- och rättigheter.

Behandling av personuppgifter som innebär särskilda integritetsrisker får inte förekomma utan att tillsynsmyndigheten först givit tillstånd till detta.

Den registrerade skall ha rätt att få sina rättigheter enligt den nationella lagen prövade av tillsynsmyndigheten och domstol.

Överföring av personuppgifter till ett tredje land får i princip endast ske om det mottagande landet har en acceptabel skyddsnivå.

Tillsynsmyndigheten skall vara ett oberoende organ. Den skall ha undersökningsbefogenheter och befogenheter att effektivt ingripa mot otillåten behandling av personuppgifter.

Medlemsstaterna skall införliva direktivet i nationell rätt inom tre år. För de automatiska register som redan finns är föreskrivet en övergångsperiod på ytterligare tre år. För redan existerande manuella register är övergångsperioden utsträckt till, som längst, tolv år.

Handlingsbegreppet m.m.

En fråga som är av central betydelse för lagstiftningen på IT-området är tryckfrihetsförordningens (TF) bestämmelser om allmänna handlingars offentlighet (2 kap.).

Till främjande av ett fritt meningsutbyte och en allsidig upplysning skall, enligt 2 kap. 1 § TF, varje svensk medborgare ha rätt att ta del av allmänna handlingar. Rätten att ta del av allmänna handlingar får begränsas endast om det är påkallat med hänsyn till vissa särskilt i TF angivna intressen, t.ex. rikets säkerhet, intresset att förebygga eller beivra brott, skyddet för enskilds personliga eller ekonomiska förhållanden. Begränsning av rätten att ta del av allmänna handlingar skall anges noga i en sär-

skild lag, sekretesslagen (1980:100), eller i en annan lag som sekretesslagen hänvisar till. Sekretesslagen innehåller också bestämmelser om bl.a. registrering och hemligstämpling av allmänna handlingar (15 kap.). Sekretesslagen utgör tillsammans med datalagen en viktig del av integritetsskyddet i Sverige inom den offentliga sektorn.

Rätten att ta del av allmänna handlingar utgör grunden för det offentliga arkivväsendet. I arkivlagen (1990:782), som innehåller grundläggande föreskrifter om arkiv hos såväl statliga som kommunala myndigheter, finns bestämmelser om vad som ingår i en myndighets arkiv samt om vård och gallring av arkiv.

Rätten att ta del av material hos myndigheterna har från början gällt ”handlingar”. Med detta begrepp har ursprungligen avsetts pappersdokument. Genom 1949 års TF klargjordes att det också omfattade kartor, ritningar och bilder. År 1974 infördes nya bestämmelser i TF som slog fast att i princip samma regler som gällde för handlingar av traditionell typ skulle tillämpas på tekniska upptagningar inklusive ADB-upptagningar. Med upptagning för ADB skulle avses en uppgift som är fixerad på någon form av datamedium och som antingen finns i eller kan matas in i en datamaskin. I begreppet upptagning för ADB skulle också ligga att informationen var läsbar endast med ADB-teknik (prop. 1973:33). Den 1 januari 1978 fick TF:s regler om allmänna handlingars offentlighet en helt ny lydelse. I sak innebar den nya lydelsen dock inte någon större förändring.

Data- och offentlighetskommittén, DOK (Ju 1984:06) tillkallades år 1984 för att utreda användningen av personnummer i samhället. Kommittén fick genom tilläggsdirektiv (dir. 1984:48) i uppdrag att också utreda de problem som ansågs vara förenade med offentlighetsprincipens tillämpning på upptagningar för automatisk databehandling (ADB). Kommittén skulle särskilt överväga åtgärder för att stärka offentlighetsprincipen när det gällde dess egentliga syfte att ge medborgarna möjligheter till kontroll och insyn i myndigheternas verksamhet.

Kommittén avlämnade i december 1988 sitt slutbetänkande Integritetsskyddet i informationssamhället 5 (SOU 1988:64), där offentlighetsprincipens tillämpning på upptagningar för ADB behandlades.

I proposition 1990/91:60 om offentlighet, integritet och ADB lämnade härefter regeringen förslag som syftade till att stärka offentlighetsprincipen i fråga om ADB-upptagningar. I propositionen föreslogs vissa ändringar i tryckfrihetsförordningen. Departementschefen delade DOK:s uppfattning att svårigheterna med ADB-upptagningar i den praktiska tillämpningen av offentlighetsprincipen inte bör lösas genom någon genomgripande ändring

av de grundläggande bestämmelserna i 2 kap. TF. Oavsett vilka begrepp man använder sig av kommer sannolikt samma problem att kvarstå från offentlighetssynpunkt. Nya begrepp skulle enligt departementschefen tvärtom skapa fler problem än de skulle lösa. Departementschefens slutsats var att det inte fanns skäl att ändra begreppsapparaten i TF i fråga om ADB-upptagningar. Förslagen antogs av riksdagen (bet. 1990/91:KU11, rskr. 1990/91:160, bet. 1991/92:KU2, rskr. 1991/92:3).

I januari 1995 publicerades LEXIT, en rapport som är resultatet av ett utredningsarbete för vilket Datainspektionen ansvarat. I rapporten redovisas rättsliga hinder från rent verksamhetsmässiga utgångspunkter för en rationell IT-användning i förvaltningen. Där förordas bl.a. att datalagen skall ersättas av en teknikoberoende, mer generellt utformad integritetsskyddslagstiftning. Vidare påpekas att begreppet handling är svårt att applicera i en medievärld där bild, text och ljud förenas samt att arkivlagstiftningen blir allt svårare att tillämpa på grund av nuvarande handlingsbegrepp.

Uppdraget

Datalagstiftning

Enligt 2 kap. 3 § andra stycket regeringsformen skall varje medborgare i den utsträckning som närmare anges i lag skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av ADB.

Den nuvarande datalagen får mot bakgrund av utvecklingen på området anses vara såväl innehållsmässigt som till sin lagtekniska utformning föråldrad. Behovet av en total revision av datalagen är därför stort.

I och med att EU-rådet har antagit en gemensam ståndpunkt i fråga om direktivet om skydd för personuppgifter har den tidigare osäkerheten om den slutliga utformningen av direktivet till stor del undanröjts. Det föreligger därmed inte längre något hinder för det fortsatta arbetet med att revidera datalagen.

En kommitté skall därför tillkallas för att ta fram en ny lagstiftning på området. Utgångspunkten för kommitténs arbete skall vara att tillförsäkra den enskilde ett fullgott integritetsskydd i IT-samhället. Intresset av ett starkt integritetsskydd får dock inte hämma användningen av ny teknik i samhällsutvecklingen och får inte heller försvåra behandling av personuppgifter för forsknings- eller statistikändamål.

Ett dataskyddsdirektiv innebär inte att man skall anta en gemensam lag för hela EU. Ett direktiv är endast bindande i fråga om det resultat som skall uppnås och överlämnar åt medlemsstaterna att själva välja form och metod för detta. Dataskyddsdirektivet utgör därför en ram inom vilken medlemsländerna genom nationell lagstiftning skall införliva de principer som fastställs i direktivet. Medlemsländerna får själva bestämma i vilken utsträckning de vill utnyttja den spännvidd som kan finnas i de olika bestämmelserna.

Kommittén skall i sitt arbete utgå från hur en svensk lagstiftning bör utformas med beaktande av utvecklingen på området och de i sammanhanget långvariga erfarenheter vi har av den nuvarande datalagen. Utifrån denna utgångspunkt skall kommittén analysera på vilket sätt en sådan framtidsanpassad och modern lagstiftning kan göras förenlig med vad som anges i EG-direktivet.

Kommittén skall i sitt arbete bl.a. beakta utvecklingen på IT-området samt även den fortsatta utveckling som kan överblickas. Kommittén skall utgå från att en kommande lag skall vara teknikoberoende.

Datalagsutredningens slutbetänkande En ny datalag (SOU 1993:10), som till stor del bygger på EG-kommissionens förslag till direktiv från oktober 1992 kan, tillsammans med remissynpunkterna på betänkandet, utgöra ett värdefullt underlag i utredningens arbete.

Allmänna handlingars offentlighet

Till främjande av ett fritt meningsutbyte och en allsidig upplysning skall varje svensk medborgare ha rätt att ta del av allmänna handlingar. Detta är ett uttryck för offentlighetsprincipen. Genom denna skall rättssäkerheten, effektiviteten i förvaltningen och effektiviteten i folkstyret garanteras. Offentlighetsprincipen ger medborgarna möjlighet till kontroll och insyn i myndigheternas verksamhet. Offentlighetsprincipen är en viktig del i det svenska rättssystemet. Reglerna i TF om allmänna handlingars offentlighet skall ses över med hänsyn till utvecklingen på IT-området. Syftet med översynen är inte att förändra offentlighetsprincipen utan att överväga hur den skall kunna tillämpas under nya tekniska förutsättningar. Lagstiftningen måste vara anpassad till dagens förhållanden, och om möjligt även till framtidens. Den skall utformas så oberoende som möjligt av tekniska begrepp och termer. Allmänhetens tillgång till information skall vara oberoende av vilket sätt myndigheterna valt för att registrera denna information.

Kommittén skall särskilt överväga om begreppet handling i TF är ändamålsenligt eller om det bör ersättas. Utgångspunkten har tidigare varit att information hos en myndighet i princip alltid har funnits på ”papper” och att med handling (konventionell handling) förståtts t.ex. ett pappersdokument. Med den utveckling som ägt rum har med handling också kommit att förstås tekniska upptagningar inklusive ADB-upptagningar. Med den nya tekniken blir anknytningen till ett pappersdokument inte längre självklar.

Varje sammanställning av sakligt sammanhängande uppgifter som en myndighet kan göra med hjälp av tillgängliga program är att anse som en handling hos myndigheten. Förutsättningen är endast att sammanställningen skall kunna göras med rutinbetonade åtgärder. Därmed avses att det skall vara fråga om en begränsad arbetsinsats och utan nämnvärda kostnader. De konstellationer av uppgifter som kan göras tillgängliga på detta sätt brukar benämnas potentiella handlingar. En sådan handling är också att betrakta som allmän, under förutsättning att den förvaras hos myndigheten och är inkommen till eller upprättad hos myndigheten. En annan fråga som på nytt kan behöva analyseras utifrån utvecklingen mot globala nätverk är innebörden av den s.k. biblioteksregeln i 2 kap. 11 § andra stycket TF.

En anpassning av bestämmelserna som reglerar allmänna handlingars offentlighet till nya tekniska förutsättningar skall således göras och förslag till grundlagsändringar läggas fram. En förändring av TF:s grundbegrepp eller rent av införandet av en ny begreppsapparat kan bli aktuell. Kommittén skall även redovisa hur dess förslag påverkar reglerna om arkiv.

Övrigt

Kommittén skall ha stor frihet att ta upp de ytterligare frågor som den finner behöver övervägas inom ramen för uppdraget.

Regeringen tillsatte i maj 1994 en utredning med uppgift att utarbeta sådana förslag till rättslig reglering som kan behövas i samband med inrättandet av s.k. elektroniska anslagstavlor och för användningen av elektroniska dokument inom både förvaltningen och näringslivet (dir. 1994:42). Utredningsarbetet skall vara avslutat senast den 1 november 1995.

I september 1994 tillsatte regeringen en utredning om nya medier och grundlagarna m.m. (dir. 1994:104, tilläggsdirektiv dir. 1995:14). Kommittén har bl.a. till uppgift att analysera hur tryckfrihetsförordningen och yttrandefrihetsgrundlagen skall tillämpas på nya medier som används

vid förmedling av yttranden och annan information till allmänheten. Mot bakgrund av den analysen skall utredningen undersöka frågan om ett grundlagsskydd för moderna medier som nu inte har ett sådant skydd. Utredningsarbetet skall enligt direktiven vara avslutat vid utgången av 1996.

Kommittén bör hålla sig informerad om resultatet av dessa utredningars arbete och vid behov samverka med dem. Kommittén skall samråda med kommissionen för att främja en bred användning av informationsteknik (IT-kommissionen) som har i uppdrag att belysa olika rättsliga frågor inom det området.

För kommittén gäller regeringens direktiv att pröva offentliga åtaganden (dir. 1994:23), att redovisa de regionalpolitiska konsekvenserna av framlagda förslag (dir. 1992:50) och att redovisa jämställdhetspolitiska konsekvenser (dir. 1994:124). Kommittén skall bevaka den internationella utvecklingen på området.

Utredningsarbetet skall vara avslutat senast den 31 mars 1997.

BILAGA 2:

EG-DIREKTIVET

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

INNEHÅLL:

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

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av Fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 100a i detta,

med beaktande av kommissionens förslag([1]),

med beaktande av Ekonomiska och sociala kommitténs yttrande([2]),

i enlighet med det förfarande som anges i fördragets artikel 189b([3]), och med beaktande av följande:

1) Gemenskapens målsättningar som uttryckts i fördraget, såsom detta ändrats genom Fördraget om Europeiska unionen, består i att förverkliga en allt fastare sammanslutning av de europeiska folken, i att upprätta allt närmare relationer mellan de stater som förenas i gemenskapen, i att säkerställa ekonomiska och sociala framsteg i sina länder genom gemensamma åtgärder för att undanröja de barriärer som delar Europa, i att fortgående förbättra levnadsvillkoren för dess folk, i att bevara och stärka fred och frihet och i att främja demokratin på grundval av de grundläggande rättigheter som erkänns i medlemsstaternas grundlagar och lagar liksom i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

([1]) EGT nr C 277, 5.11.1990, s. 3, och EGT nr C 311, 27.11.1992, s. 30.

([2]) EGT nr C 159, 17.6.1991, s. 38.

([3]) Europaparlamentets yttrande av den 11 mars 1992 (EGT nr C 94, 13.4.1992, s. 198), bekräftat den 2 december 1993 (EGT nr C 342, 20.12.1993, s. 30) rådets gemensamma ståndpunkt av den 20 februari 1995 (EGT nr C 93, 13.4.1995, s. 1) och Europaparlamentets beslut av den 15 juni 1995 (ännu inte offentliggjort i EGT).

2) Systemen för databehandling av uppgifter är till för människornas skull. Oavsett fysiska personers medborgarskap eller hemvist måste systemen respektera dessa personers grundläggande fri- och rättigheter – särskilt rätten till privatlivet – och bidra till ekonomiska och sociala framsteg, handelns utveckling och enskilda personers välfärd.
3) Upprättandet av den inre marknaden och dennas funktion, som i enlighet med artikel 7a i fördraget innebär fri rörlighet för varor, personer, tjänster och kapital, förutsätter inte bara att personuppgifter fritt kan överföras från en medlemsstat till en annan utan också att enskilda personers grundläggande rättigheter skyddas.
4) Inom gemenskapen behandlas och används personuppgifter allt oftare inom olika ekonomiska och samhälleliga områden. Framstegen på informationsteknikens område har gjort det avsevärt lättare att behandla och utbyta sådana uppgifter.
5) Den ekonomiska och sociala integration som är en följd av upprättandet av den inre marknaden och dennas funktion i enlighet med artikel 7a i fördraget kommer med nödvändighet att leda till en betydande ökning av flödet av personuppgifter över gränserna mellan samtliga aktörer på de ekonomiska och samhälleliga områdena, oavsett om dessa aktörer tillhör den privata eller den offentliga sektorn. Utbytet av personuppgifter mellan företag i olika medlemsstater kommer att öka. De nationella myndigheterna i de olika medlemsstaterna måste som ett led i tillämpningen av gemenskapsrätten samarbeta och utbyta personuppgifter för att kunna fullgöra sina åligganden eller utföra arbetsuppgifter för en myndighet i en annan medlemsstat inom det område utan inre gränser som den inre marknaden innebär.
6) Det ökade vetenskapliga och tekniska samarbetet liksom det samordnade införandet av nya telekommunikationsnät inom gemenskapen nödvändiggör och underlättar dessutom det gränsöverskridande flödet av personuppgifter.
7) Skillnaden i skyddsnivå mellan medlemsstater vad gäller enskilda personers fri- och rättigheter, särskilt rätten till privatliv med avseende på behandling av personuppgifter, kan hindra översändande av sådana uppgifter från en medlemsstats territorium till en annans. Denna skillnad kan därför utgöra ett hinder för att utöva en rad ekonomiska aktiviteter på gemenskapsnivå, snedvrida konkurrensen och hindra myndigheterna att fullgöra de skyldigheter som åligger dem enligt gemenskapsrätten. Denna skillnad i skyddsnivå beror på olikheter i nationella lagar och andra författningar.
8) För att hindren mot flöden av personuppgifter skall kunna avskaffas måste skyddsnivån när det gäller enskilda personers fri- och rättigheter med avseende på behandlingen av sådana uppgifter vara likvärdig

i alla medlemsstater. Denna målsättning är av grundläggande betydelse för den inre marknaden men kan inte uppnås genom åtgärder endast av medlemsstaterna, i synnerhet med tanke på omfattningen av de skillnader som för närvarande finns mellan nationell lagstiftning på området och med tanke på behovet av att samordna lagstiftningen i medlemsstaterna för att säkerställa en sådan enhetlig reglering av det gränsöverskridande flödet av personuppgifter som överensstämmer med målsättningen för den inre marknaden enligt artikel 7a i fördraget. Det är därför nödvändigt att gemenskapen vidtar åtgärder för att åstadkomma en tillnärmning av lagstiftningen.

9) Eftersom tillnärmningen av de nationella lagstiftningarna kommer att leda till ett likvärdigt skydd kommer medlemsstaterna inte längre att kunna hindra det fria flödet av personuppgifter mellan dem under hänvisning till enskilda personers fri- och rättigheter, särskilt rätten till privatliv. Medlemsstaterna kommer att få ett handlingsutrymme, som i samband med genomförandet av detta direktiv också kommer att kunna utnyttjas av näringslivet och arbetsmarknadens parter. Medlemsstaterna kommer därför att i sin nationella lagstiftning särskilt kunna ange de allmänna villkor som skall gälla för behandlingen av uppgifter. Medlemsstaterna skall härvid sträva efter att förbättra det skydd som deras nuvarande lagstiftning ger. Inom ramen för detta handlingsutrymme och i enlighet med gemenskapsrätten kan skillnader uppkomma vid genomförandet av direktivet, vilket kan påverka flödet av uppgifter såväl inom en medlemsstat som på gemenskapsnivå.

10) Ändamålet med den nationella lagstiftningen om behandling av personuppgifter är att skydda grundläggande fri- och rättigheter, särskilt den rätt till privatlivet som erkänns både i artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och i gemenskapsrättens allmänna rättsprinciper. Av denna anledning får tillnärmningen av denna lagstiftning inte medföra någon inskränkning i det skydd de ger, utan skall i stället syfta till att garantera en hög skyddsnivå inom gemenskapen.

11) De principer om skydd för enskilda personers fri- och rättigheter, särskilt rätten till privatlivet, som detta direktiv innehåller, utgör en precisering och en förstärkning av principerna i Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter.

12) Principerna för skyddet måste gälla för all behandling av personuppgifter som utförs av en person vars verksamhet regleras av gemenskapsrätten. En fysisk persons behandling av uppgifter uteslutande för

personliga ändamål eller för hemmabruk, såsom korrespondens eller förande av adressregister, skall dock inte omfattas.

13) Sådan verksamhet som avses i avdelningarna V och VI i Fördraget om Europeiska unionen och som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område faller inte inom tillämpningsområdet för gemenskapsrätten, dock med förbehåll för medlemsstaternas skyldigheter enligt artiklarna 56.2, 57 eller 100a i Fördraget om upprättandet av Europeiska gemenskapen. Sådan behandling av personuppgifter som är nödvändig för att skydda statens ekonomiska välstånd omfattas inte av detta direktiv, när behandlingen har samband med frågor om statens säkerhet.
14) För närvarande görs inom ramen för informationssamhället betydande framsteg såvitt avser tekniken för att uppta, överföra, bearbeta, registrera, lagra eller lämna ut ljud- eller bilduppgifter om fysiska personer; detta direktiv bör därför tillämpas på behandling av sådana uppgifter.
15) Behandlingen av sådana uppgifter omfattas av detta direktiv endast om den sker med hjälp av automatisk databehandling eller om de uppgifter som behandlas ingår eller avses ingå i ett register som är uppbyggt efter vissa med utgångspunkt i för enskilda personer utformade kriterier för att underlätta tillgång till de berörda uppgifterna.
16) Behandlingen av ljud- och bilduppgifter – exempelvis i samband med videoövervakning – omfattas inte av detta direktiv om den utförs för att tillgodose den allmänna säkerheten, försvaret, statens säkerhet eller statens verksamhet på straffrättens område eller till annan verksamhet som inte faller inom gemenskapsrättens tillämpningsområde.
17) När det gäller behandling av ljud- och bilduppgifter för journalistiska ändamål eller i litterärt eller konstnärligt skapande, särskilt på det audiovisuella området, skall direktivets principer i enlighet med bestämmelserna i artikel 9 tillämpas restriktivt.
18) För att undvika att en enskild person förvägras det skydd som tillkommer honom enligt detta direktiv skall varje behandling av personuppgifter inom gemenskapen ske i enlighet med lagstiftningen i en av medlemsstaterna. Med hänsyn till detta bör behandlingen av uppgifter som utförs av någon som på uppdrag av en registeransvarig som är etablerad i en medlemsstat regleras av den statens lagstiftning.
19) Etablering på en medlemsstats territorium förutsätter effektiv och faktisk verksamhet med hjälp av en stabil struktur. Härvid har den berörda verksamhetens rättsliga form inte avgörande betydelse, oavsett om det är fråga om en filial eller om ett dotterbolag som är en juridisk person. Om den ansvarige är etablerad på flera medlemsstaters territorier, särskilt genom dotterbolag, måste han för att undvika varje

kringgående garantera att varje verksamhet uppfyller bestämmelserna i den nationella lagstiftning som gäller för aktiviteterna.

20) Den omständigheten att den registeransvarige är etablerad i ett tredje land får inte utgöra ett hinder för det skydd som enskilda personer ges i detta direktiv. I sådana fall skall på behandlingen av uppgifter til??lämpas den medlemsstats lagstiftning som innehåller de hjälpmedel som används för behandlingen. Det bör finnas garantier för att de rättigheter som följer av detta direktiv respekteras i praktiken.
21) Detta direktiv påverkar inte de territorialitetsregler som gäller på straffrättens område.
22) Medlemsstaterna bör i sin lagstiftning eller genom andra bestämmelser som antas för att genomföra detta direktiv närmare ange de allmänna villkoren för att en behandling skall vara tillåten. Särskilt artikel 5 jämförd med artiklarna 7 och 8 tillåter medlemsstaterna att, oavsett de allmänna regler som gäller, ange särskilda villkor för behandlingen av uppgifter på särskilda områden och för de olika kategorier av uppgifter som behandlas i artikel 8.
23) Medlemsstaterna har befogenhet att genomföra skyddet för enskilda personer både genom en generell lagstiftning om skydd för enskilda personer såvitt avser behandling av personuppgifter och genom särskild lagstiftning som till exempel om statistiska institut.
24) Sådan lagstiftning som rör skydd för juridiska personer med avseende på behandling av uppgifter som angår dem berörs inte av detta direktiv.
25) Principerna för skyddet måste avspeglas dels i de förpliktelser som åvilar personer, myndigheter, företag, institutioner, organ eller andra registeransvariga särskilt med avseende på uppgifternas kvalitet, den tekniska säkerheten, anmälningar till tillsynsmyndigheten och de omständigheter under vilka behandling får utföras, dels i de rättigheter som tillkommer enskilda personer, vilkas personuppgifter blir föremål för behandling, att bli informerade om att behandling sker, att få tillgång till uppgifterna, att begära rättelse och att under vissa omständigheter invända mot behandlingen.
26) Principerna för skyddet måste gälla all information som rör en identifierad eller identifierbar person. För att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person. Skyddsprinciperna gäller inte för uppgifter som gjorts anonyma på ett sådant sätt att den registrerade inte längre är identifierbar. En sådan uppförandekodex som avses i artikel 27 kan vara ett användbart redskap för att ge vägledning

om hur uppgifter kan göras anonyma och behållas i en form som gör det omöjligt att identifiera den registrerade.

27) Enskilda personer skall skyddas både i samband med automatisk databehandling av uppgifterna och i samband med manuell behandling. Omfattningen av detta skydd får inte faktiskt bero på den teknik som används eftersom detta skulle kunna skapa en allvarlig risk för kringgående. När det gäller manuell behandling omfattar detta direktiv endast register och inte ostrukturerade akter. Särskilt innehållet i ett register måste vara strukturerat efter bestämda kriterier som avser enskilda personer, för att lätt ge tillgång till personuppgifter. I enlighet med definitionen i artikel 2 c) kan de olika kriterier som gör det möjligt att fastställa de enskilda delarna av en strukturerad samling personuppgifter och de olika kriterier som reglerar möjligheten att få tillgång till en sådan samling utformas av varje medlemsstat. Akter eller grupper av akter liksom dessas omslag, vilka inte är strukturerade enligt särskilda kriterier, faller inte under några omständigheter inom detta direktivs tillämpningsområde.

28) Varje behandling av personuppgifter måste vara laglig och korrekt gentemot berörda personer. Uppgifterna måste särskilt vara adekvata, relevanta och nödvändiga med hänsyn till de ändamål för vilka de behandlas. Dessa ändamål skall vara uttryckligt angivna, berättigade och bestämda vid tiden för insamling av uppgifterna. Sådana ändamål med behandlingen som läggs fast sedan uppgifterna samlats in får inte vara oförenliga med de ändamål som ursprungligen angavs.

29) Senare behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål kan – förutsatt att medlemsstaterna ger lämpliga garantier – inte allmänt sett anses oförenliga med de ändamål för vilka uppgifterna tidigare samlades in. Dessa garantier skall särskilt hindra att uppgifterna används för att vidta åtgärder mot eller fatta beslut som rör en viss person.

30) För att vara tillåten skall en behandling av personuppgifter dessutom utföras med den registrerades samtycke eller vara nödvändig för ingående eller utförandet av förpliktelser i enlighet med ett avtal som är bindande för den registrerade, eller fordras enligt lagstiftning vid utförandet av något som är i det allmännas intresse eller är ett led i myndighetsutövning eller vara i en fysisk eller juridisk persons intresse förutsatt att skyddet av den registrerades fri- och rättigheter inte går före. För att särskilt garantera jämvikt mellan de berörda intressena och för att samtidigt säkerställa en effektiv konkurrens får medlemsstaterna närmare ange på vilka villkor användning och utlämnande till tredje man av personuppgifter får äga rum inom ramen för tillåtna aktiviteter som av företag och andra organ utövas i deras lö-

pande verksamhet. Medlemsstaterna får även närmare ange på vilka villkor personuppgifter i marknadsföringssyfte får vidarebefordras till tredje man, oavsett om detta sker kommersiellt eller av välgörenhetsorganisationer, föreningar eller stiftelser, exempelvis av politisk karaktär, men förutsatt att regler iakttas som har till syfte att ge den registrerade möjlighet att invända mot att de uppgifter som rör honom behandlas utan att behöva ange sina skäl och utan att åsamkas kostnader för detta.

31) Behandling av personuppgifter måste även anses tillåten när den utförs för att skydda ett intresse som är av avgörande betydelse för den registrerades liv.

32) Det ankommer på den nationella lagstiftningen att avgöra om den som ansvarar för en behandling som utförs i det allmännas intresse eller vid myndighetsutövning skall vara en myndighet eller något annat offentligrättsligt eller civilrättsligt subjekt, såsom exempelvis en yrkesorganisation.

33) Uppgifter som på grund av sin natur kan kränka grundläggande fri- och rättigheter eller privatlivets helgd får inte behandlas utan samtycke av den registrerade. Dock måste det finnas en uttrycklig möjlighet att för att tillgodose särskilda behov, i synnerhet när behandlingen av uppgifterna utförs för ändamål som har samband med hälso- och sjukvården av personer som är underkastade tystnadsplikt eller för att genomföra berättigade åtgärder av vissa föreningar eller stiftelser vilkas syften är att skydda utövningen av vissa grundläggande fri- och rättigheter.

34) När det av hänsyn till viktiga allmänna intressen är nödvändigt, måste medlemsstaterna kunna avvika från förbudet mot att behandla känsliga kategorier av uppgifter på sådana områden som exempelvis folkhälsa och socialskydd, särskilt för att säkerställa kvalitet och lönsamhet när det gäller förfaranden som används i samband med ansökningar om förmåner och tjänster inom sjukförsäkringssystemet, i samband med vetenskaplig forskning och i samband med offentlig statistik. Dock åligger det medlemsstaterna att sörja för att det finns lämpliga och konkreta garantier för att skydda enskilda personers grundläggande rättigheter och privatliv.

35) Myndigheters behandling av personuppgifter för officiellt erkända religiösa sammanslutningars räkning för att uppfylla målsättningar som uttrycks i grundlagen eller folkrätten utförs för att tillgodose viktiga samhälleliga intressen.

36) Om det i samband med att allmänna val hålls för att det demokratiska systemet skall fungera är nödvändigt att de politiska partierna i vissa medlemsstater samlar in uppgifter om enskilda personers politiska

uppfattning får behandling av sådana uppgifter tillåtas av hänsyn till viktiga allmänna intressen, på villkor att bestämmelser om lämpliga garantier föreskrivs.

37) För sådan behandling av personuppgifter som sker för journalistiska ändamål eller för konstnärligt eller litterärt skapande – särskilt på det audiovisuella området – bör det fastställas undantag från eller begränsningar i förhållande till vissa bestämmelser i detta direktiv så långt detta är nödvändigt för att förena enskilda personers grundläggande rättigheter med yttrandefriheten, särskilt den rätt att ta emot och lämna upplysningar som särskilt fastslås i artikel 10 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. För att åstadkomma en avvägning mellan de grundläggande fri- och rättigheterna åligger det medlemsstaterna att besluta om nödvändiga undantag och begränsningar såvitt avser de generella åtgärder som har avseende på uppgiftsbehandlingens berättigande, åtgärder för att vidareföra uppgifter till tredje land och tillsynsmyndighetens befogenheter. Detta får dock inte leda till att medlemsstaterna beslutar om undantag från åtgärder som vidtas för att säkerställa behandlingens säkerhet. Den tillsynsmyndighet som är behörig på området bör utrustas med i vart fall vissa befogenheter att utövas efter behandlingen i fråga, exempelvis befogenhet att med jämna mellanrum offentliggöra en rapport eller att överlämna ärenden till rättsliga myndigheter.

38) En korrekt behandling av uppgifter förutsätter att de registrerade kan få kännedom om behandlingen och att de – när uppgifter samlas in hos dem – kan få korrekt och fullständig information med hänsyn till de närmare omständigheterna vid insamlingen.

39) I vissa fall rör behandlingen uppgifter som den registeransvarige inte har samlat in direkt från den registrerade. Vidare kan utlämnande av uppgifter till tredje man vara tillåten även om utlämnandet inte kunde förutses när uppgifterna samlades in från den registrerade. I samtliga dessa fall skall den registrerade informeras när uppgifterna registreras eller senast när uppgifterna för första gången lämnas ut till tredje man.

40) Det är dock inte nödvändigt att ställa detta krav om den registrerade redan känner till informationen. Detta krav behöver inte heller ställas om registreringen eller utlämnandet uttryckligen regleras i lagstiftningen eller om lämnande av information till den berörda personen visar sig vara omöjligt eller innebära oproportionerligt stora ansträngningar, vilket skulle kunna vara fallet i samband med behandling för historiska, statistiska eller vetenskapliga ändamål. I detta sammanhang kan antalet registrerade, uppgifternas ålder och de kompensatoriska åtgärder som kan vidtas tas i beaktande.

41) Alla måste kunna utöva sin rätt att få tillgång till uppgifter som rör dem och som är föremål för behandling, för att i detalj kunna försäkra sig om att uppgifterna är korrekta och om att behandlingen är tillåten. Av samma anledning måste var och en ha rätt att få reda på den logik som gäller för den automatiska databehandlingen av uppgifter som rör honom, åtminstone såvitt avser sådana automatiska beslut som avses i artikel 15.1. Denna rättighet får inte kränka affärshemligheten eller upphovsrätten, särskilt inte den upphovsrätt som skyddar programvaran. Detta bör dock inte få resultera i att den registrerade nekas all information.
42) Medlemsstaterna kan av hänsyn till intresset hos den registrerade eller till andras fri- och rättigheter begränsa rätten till tillgång till uppgifter och information. De kan till exempel besluta att tillgång till uppgifter av medicinsk art endast får erhållas genom förmedling av någon som är yrkesmässigt verksam inom hälso- och sjukvården.
43) Rätten till tillgång till uppgifter och information samt vissa skyldigheter hos den registeransvarige kan inskränkas av medlemsstaterna i den utsträckning som det är nödvändigt för att skydda till exempel statens säkerhet, försvaret, allmän säkerhet eller viktiga ekonomiska eller finansiella intressen som är av betydelse för en medlemsstat eller för unionen, liksom för brottsutredningar och åtal och åtgärder som rör överträdelser av etiska regler som gäller för sådana yrken som särskilt regleras i lagstiftning. På förteckningen över undantag och begränsningar bör upptas de uppgifter för övervakning, tillsyn eller reglering som är nödvändiga på de tre sistnämnda områdena, nämligen allmän säkerhet, ekonomiska och finansiella intressen samt beivrande av brott. Uppräkningen av uppgifter på dessa tre områden påverkar inte undantag eller begränsningar av hänsyn till statens säkerhet och försvaret.
44) För att uppfylla vissa av de nämnda målsättningarna kan medlemsstaterna på grund av bestämmelser i gemenskapsrätten tvingas att avvika från bestämmelserna i detta direktiv om rätten till tillgång till uppgifter, skyldigheten att informera enskilda personer och kvaliteten på uppgifterna.
45) I sådana fall då uppgifter av hänsyn till allmänna intressen, på grund av myndighetsutövning eller av hänsyn till en persons berättigade intressen kan bli föremål för tillåten behandling, skall varje berörd person ändå, på berättigade och avgörande skäl som avser hans särskilda situation, ha rätt att invända mot att uppgifter som rör honom själv behandlas. Medlemsstaterna har dock möjlighet att anta bestämmelser av motsatt innehåll.

46) Skyddet för de registrerades fri- och rättigheter förutsätter såvitt avser behandling av personuppgifter att lämpliga tekniska och organisatoriska åtgärder vidtas både när systemet för behandlingen utformas och när själva behandlingen sker, särskilt för att garantera säkerheten och för att på så sätt hindra all otillåten behandling. Det åligger medlemsstaterna att säkerställa att de registeransvariga respekterar dessa åtgärder. Åtgärderna skall garantera en lämplig säkerhetsnivå med hänsyn till den nuvarande utvecklingsnivån och till kostnaderna för genomförandet under hänsynstagande till de risker som behandlingen innebär och arten av de uppgifter som skall skyddas.

47) När ett meddelande som innehåller personuppgifter översänds genom förmedling av en organisation för telekommunikation eller elektronisk post, vars enda ändamål är att översända sådana meddelanden, blir det normalt den från vilken meddelandet härrör och inte den person som erbjuder nämnda tjänst som anses ansvara för behandlingen av personuppgifterna. De som erbjuder sådana tjänster kommer dock normalt att anses som ansvariga för behandlingen av de ytterligare personuppgifter som fordras för att tjänsten skall kunna användas.

48) Anmälningsförfarandet är avsett för att göra en behandlings syfte och viktigaste egenskaper allmänt kända för att säkerställa att behandlingen sker i enlighet med de nationella åtgärder som vidtas för att genomföra detta direktiv.

49) För att undvika olämpliga administrativa formaliteter kan medlemsstaterna besluta om undantag från och förenklingar av anmälningsplikten såvitt avser sådana fall då behandlingen sannolikt inte kommer att kränka de berörda personernas fri- och rättigheter, förutsatt att detta är i överensstämmelse med en åtgärd som vidtagits av en medlemsstat och som särskilt anger begränsningarna. Medlemsstaterna kan även besluta om undantag och förenklingar i fall då någon som utsetts av den registeransvarige försäkrar sig om att de utförda behandlingarna inte kommer att kränka de registrerades fri- och rättigheter. Den person som sålunda utsetts att skydda uppgifterna måste – vare sig han är anställd av den registeransvarige eller inte – ha möjlighet att utöva sin verksamhet på ett fullständigt oberoende sätt.

50) Undantag från anmälningsplikten och förenklad anmälan bör kunna tillåtas särskilt då det är fråga om behandling av uppgifter som endast syftar till att ett register skall föras, som är avsett för att i enlighet med nationell lagstiftning ge allmänheten information och som är tillgängligt för allmänheten eller var och en som kan styrka att han har ett berättigat intresse.

51) Det förhållandet att den registeransvarige omfattas av förenklat anmälningsförfarande eller är undantagen från anmälningsplikt befriar honom inte från de övriga förpliktelser som följer av detta direktiv.
52) I detta sammanhang måste en efterföljande kontroll från den behöriga myndighetens sida i allmänhet anses som en tillräcklig åtgärd.
53) Vissa typer av behandling – till exempel behandling som har till ändamål att utesluta den berörde från möjligheten att utöva en rättighet, motta en förmån eller ingå ett avtal eller sådan behandling som innebär användning av ny teknik – kan på grund av sin natur, sin omfattning eller sitt ändamål innebära särskilda risker för att de registrerades fri- och rättigheter skall kränkas. Medlemsstaterna kan om de önskar det precisera dessa risker i sin lagstiftning.
54) Med tanke på omfattningen av den behandling av uppgifter som utförs i samhället torde det antal behandlingar som innebär särskilda risker vara mycket begränsat. Medlemsstaterna måste föreskriva att tillsynsmyndigheten eller den som utövar tillsyn i samråd med tillsynsmyndigheten företar en förhandskontroll av dessa behandlingar innan de utförs. Sedan en sådan förhandskontroll genomförts får tillsynsmyndigheten i enlighet med den nationella lagstiftningen som gäller för myndigheten yttra sig över eller tillåta behandlingen. En sådan kontroll kan även företas som ett led i det nationella parlamentets förberedande arbete med en åtgärd eller som ett led i arbetet med en åtgärd som grundas på en sådan lagstiftande åtgärd som definierar behandlingens art och anger lämpliga skyddsåtgärder.
55) För de fall då den registeransvarige inte respekterar de registrerades rättigheter måste det i medlemsstatens lagstiftning finnas möjlighet till rättslig prövning. Personer som lider skada till följd av otillåten behandling skall ha rätt till ersättning av den registeransvarige, vilken kan befrias från skadeståndsansvar om han kan visa att han inte är ansvarig för skadan, särskilt i fall då han kan påvisa att ett fel begåtts av den registrerade eller i fall av force majeure. Sanktioner skall vidtas mot såväl privaträttsliga som offentligrättsliga subjekt som överträder de nationella bestämmelser som antagits för att genomföra detta direktiv.
56) Gränsöverskridande flöden av personuppgifter är nödvändiga för den internationella handelns utveckling. Det skydd som genom detta direktiv tillförsäkras enskilda personer inom gemenskapen hindrar inte att personuppgifter överförs till sådana tredje länder som garanterar en adekvat skyddsnivå. Frågan om skyddsnivåns adekvans skall bedömas med hänsyn till alla de omständigheter som har samband med en överföring eller en grupp av överföringar.

57) Om ett tredje land inte garanterar en adekvat skyddsnivå skall överföring av personuppgifter till det landet förbjudas.
58) Undantag från detta förbud skall under vissa omständigheter kunna medges om den registrerade lämnar sitt samtycke, om överföring är nödvändig för ett avtal eller ett rättsligt anspråk, när skyddet av väsentliga samhällsintressen kräver det, till exempel vid internationellt utbyte av uppgifter mellan skattemyndigheter eller tullmyndigheter eller mellan socialförsäkringsmyndigheter eller om överföringen utförs med utgångspunkt i ett register som upprättats genom lagstiftning och som är avsett att vara tillgängligt för allmänheten eller för personer som har ett berättigat intresse. En sådan överföring bör inte omfatta alla uppgifter eller hela kategorier av uppgifter som finns i registret. När registret är avsett att vara tillgängligt för personer med ett berättigat intresse skall överföringen göras endast på begäran av dessa personer eller om de själva är mottagarna.
59) Särskilda åtgärder kan vidtas för att uppväga en otillräcklig skyddsnivå i ett tredje land om den registeransvarige ställer lämpliga garantier. Bestämmelser om förfaranden för förhandling mellan gemenskapen och tredje land måste antas.
60) Överföring till tredje land får i vilket fall som helst endast utföras i enlighet med bestämmelser som medlemsstaterna antagit för genomförande av detta direktiv, särskilt artikel 8 i detta.
61) Medlemsstaterna och kommissionen måste på sina respektive kompetensområden uppmuntra berörda delar av näringslivet att anta uppförandekodexar för att underlätta genomförandet av detta direktiv med beaktande av de särskilda former av behandling som utförs på vissa områden och med respekt för de nationella bestämmelser som antagits för dess genomförande.
62) För skyddet av enskilda personer med avseende på behandlingen av personuppgifter är det av avgörande betydelse att medlemsstaterna inrättar oberoende tillsynsmyndigheter.
63) Dessa myndigheter måste ges nödvändiga resurser för att utföra sina uppgifter, såsom befogenhet att – särskilt när det gäller klagomål från enskilda personer – undersöka och intervenera samt befogenheter att inleda rättsliga förfaranden. De måste även bidra till att garantera insyn i behandlingen av uppgifter i de medlemsstater under vilkas jurisdiktion de hör.
64) Tillsynsmyndigheterna i de olika medlemsstaterna kommer att behöva bistå varandra i samband med utförandet av de uppgifter som åligger dem för att säkerställa att skyddsreglerna respekteras på ett tillfredsställande sätt i hela Europeiska unionen.

65) En arbetsgrupp för skydd av enskilda personer i samband med behandling av personuppgifter skall inrättas på gemenskapsnivå. Gruppen skall vid utförandet av sina uppgifter vara fullständigt oberoende. Gruppen skall med hänsyn till sin särskilda karaktär ge kommissionen råd och bidra till den enhetliga tillämpningen av de nationella regler som antagits för att genomföra detta direktiv.

66) Med avseende på överföring av uppgifter till tredje land fordrar genomförandet av detta direktiv att kommissionen ges befogenhet att besluta om genomförandet och att ett förfarande i enlighet med riktlinjerna i rådets beslut 87/373/EEG([1]) införs.

67) Den 20 december 1994 träffade Europaparlamentet, rådet och kommissionen en överenskommelse om ett ”modus vivendi” beträffande genomförandeåtgärder för rättsakter som antagits i enlighet med förfarandet i artikel 189b i Romfördraget.

68) De principer för skyddet av enskilda personers fri- och rättigheter, och då särskilt rätten till privatliv, som i detta direktiv uppställs med avseende på behandling av personuppgifter skall för vissa områdens vidkommande kunna kompletteras eller preciseras med hjälp av särskilda bestämmelser som skall överensstämma med dessa principer.

69) Medlemsstaterna bör ges en frist på högst tre år räknat från ikraftträdandet av de nationella bestämmelser som antas för att genomföra detta direktiv, så att de stegvis kan tillämpa de nya nationella bestämmelserna på alla sådana behandlingar som redan påbörjats. För att möjliggöra ett kostnadseffektivt genomförande av dessa bestämmelser skall medlemsstaterna tillåtas att under ytterligare en tidsperiod, som löper ut tolv år efter dagen för antagandet av detta direktiv, vidta åtgärder för att säkerställa att då befintliga manuella register bringas i överensstämmelse med vissa av direktivets bestämmelser. Uppgifter som ingår i dessa register och som behandlas manuellt under denna förlängda övergångsperiod skall dock när det är föremål för en ytterligare sådan behandling bringas i överensstämmelse med dessa bestämmelser.

70) Det är inte nödvändigt att den registrerade på nytt lämnar sitt samtycke till att den registeransvarige fortsätter att behandla känsliga uppgifter, när en sådan behandling är nödvändig för genomförandet av att avtal som har slutits på grundval av frivilligt och informerat samtycke före dessa bestämmelsers ikraftträdande.

71) Detta direktiv hindrar inte en medlemsstat från att anta bestämmelser för att reglera sådan marknadsföring som riktar sig till konsumenter

---

([1]) EGT nr L 197 av den 18.7.1987, s. 33.

som har hemvist inom dess territorium, förutsatt att dessa regler inte rör skyddet av enskilda personer med avseende på behandling av personuppgifter.

72) Detta direktiv gör det möjligt att vid genomförandet av dessa bestämmelser ta hänsyn till principen om allmänhetens rätt till tillgång till allmänna handlingar.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1

ALLMÄNNA BESTÄMMELSER

Artikel 1

Direktivets syfte

1. Medlemsstaterna skall i enlighet med detta direktiv skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter.

2. Medlemsstaterna får varken begränsa eller förbjuda det fria flödet av personuppgifter mellan medlemsstaterna av skäl som har samband med det under punkt 1 föreskrivna skyddet.

Artikel 2

Definitioner

I detta direktiv avses med

a) *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (*den registrerade*). En identifierbar person är en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet,

b) *behandling av personuppgifter* (*behandling*): varje åtgärd eller serie av åtgärder som vidtas beträffande personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring,

c) *register med personuppgifter* (*register*): varje strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

d) *registeransvarig*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. När ändamålen och medlen för behandlingen bestäms av nationella lagar och andra författningar eller av gemenskapsrätten kan den registeransvarige eller de särskilda kriterierna för att utse honom anges i nationell rätt eller i gemenskapsrätten,

e) *registerförare*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ som behandlar personuppgifter för den registeransvariges räkning,

f) *tredje man*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ än den registrerade, den registeransvarige, registerföraren och de personer som under den registeransvariges eller registerförarens direkta ansvar har befogenhet att behandla uppgifterna,

g) *mottagare*: den fysiska eller juridiska person, den myndighet, den institution eller det andra organ till vilket uppgifterna utlämnas, vare sig det är en tredje man eller inte. Myndigheter som kan komma att motta uppgifter inom ramen för ett särskilt uppdrag skall dock inte betraktas som mottagare,

h) *den registrerades samtycke*: varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom.

Artikel 3

Tillämpningsområde

1. Detta direktiv gäller för sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg liksom för annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Detta direktiv gäller inte för sådan behandling av personuppgifter

— som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i Fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när behandlingen

har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område,

— av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll.

Artikel 4

Tillämplig nationell rätt

1. Varje medlemsstat skall tillämpa de nationella bestämmelser som den för genomförandet av detta direktiv antar för behandlingen av personuppgifter när

a) behandlingen utförs som ett led i verksamhet inom den medlemsstats territorium, där den registeransvarige är etablerad. Om en registeransvarig är etablerad inom flera medlemsstaters territorier skall han vidta nödvändiga åtgärder för att säkerställa att alla verksamheter uppfyller kraven enligt den tillämpliga nationella lagstiftningen,

b) den registeransvarige inte är etablerad inom en medlemsstats territorium utan på en plats där medlemsstatens lagstiftning gäller på grund av folkrätten,

c) den registeransvarige inte är etablerad på gemenskapens territorium och för behandling av personuppgifter använder databehandlad eller icke databehandlad utrustning som befinner sig på den nämnda medlemsstatens territorium, om inte sådan utrustning endast används för att låta uppgifter passera genom gemenskapen.

2. Under de omständigheter som avses i punkt 1 c) måste den registeransvarige utse en företrädare som är etablerad inom den berörda medlemsstatens territorium, utan att detta i övrigt påverkar de eventuella rättsliga åtgärder som kan komma att inledas mot den ansvarige själv.

KAPITEL II

ALLMÄNNA BESTÄMMELSER OM NÄR PERSONUPPGIFTER FÅR BEHANDLAS

Artikel 5

Medlemsstaterna skall inom de begränsningar som bestämmelserna i detta kapitel innebär, precisera på vilka villkor behandling av personuppgifter är tillåten.

AVDELNING I

PRINCIPER OM UPPGIFTERNAS KVALITET

Artikel 6

1. Medlemsstaterna skall föreskriva att personuppgifter

a) skall behandlas på ett korrekt och lagligt sätt,

b) skall samlas in för särskilda, uttryckligt angivna och berättigade ändamål; senare behandling får inte ske på ett sätt som är oförenligt med dessa ändamål. Senare behandling av uppgifter för historiska, statistiska eller vetenskapliga ändamål skall inte anses oförenlig med dessa ändamål förutsatt att medlemsstaterna beslutar om lämpliga skyddsåtgärder,

c) skall vara adekvata och relevanta och inte får omfatta mer än vad som är nödvändigt med hänsyn till de ändamål för vilka de har samlats in och för vilka de senare behandlas,

d) skall vara riktiga och, om nödvändigt, aktuella. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga eller ofullständiga i förhållande till de ändamål för vilka de samlades in eller för vilka de senare behandlas, utplånas eller rättas,

e) förvaras på ett sätt som förhindrar identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna samlades in eller för vilka de senare behandlades. Medlemsstaterna skall vidta lämpliga skyddsåtgärder för de personuppgifter som lagras under längre perioder för historiska, statistiska eller vetenskapliga ändamål.

2. Det åligger den registeransvarige att säkerställa att punkt 1 efterlevs.

AVDELNING II

PRINCIPER SOM GÖR ATT UPPGIFTSBEHANDLING KAN TILLÅTAS

Artikel 7

Medlemsstaterna skall föreskriva att personuppgifter får behandlas endast om

a) den registrerade otvetydigt har lämnat sitt samtycke, eller

b) behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås, eller

c) behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige, eller
d) behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade, eller
e) behandlingen är nödvändig för att utföra en arbetsuppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den registeransvarige eller tredje man till vilken uppgifterna har lämnats ut, eller
f) behandlingen är nödvändig för ändamål som rör berättigade intressen hos den registeransvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter som kräver skydd under artikel 1.1.

AVDELNING III

SÄRSKILDA BEHANDLINGSKATEGORIER

Artikel 8

Behandlingen av särskilda kategorier av uppgifter

1. Medlemsstaterna skall förbjuda behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv.

2. Punkt 1 gäller inte om
a) den registrerade har lämnat sitt uttryckliga samtycke till en sådan behandling, utom när det enligt medlemsstatens lagstiftning anges att förbudet i punkt 1 inte kan upphävas genom den registrerades samtycke, eller
b) behandlingen är nödvändig för att fullgöra de skyldigheter och särskilda rättigheter som åligger den registeransvarige inom arbetsrätten, i den omfattning detta är tillåtet enligt en nationell lagstiftning som föreskriver lämpliga skyddsåtgärder, eller
c) behandlingen är nödvändig för att skydda den registrerades eller någon annan persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke, eller
d) behandlingen utförs inom ramen för berättigad verksamhet hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen endast rör sådana organs medlemmar eller personer som

på grund av organets ändamål har regelbunden kontakt med detta och uppgifterna inte lämnas ut till tredje man utan den registrerades samtycke, eller

e) behandlingen rör uppgifter som på ett tydligt sätt offentliggörs av den registrerade eller är nödvändiga för att kunna fastslå, göra gällande eller försvara rättsliga anspråk.

3. Punkt 1 gäller inte när behandlingen av uppgifterna är nödvändig med hänsyn till förebyggande hälso- och sjukvård, medicinska diagnoser, vård eller behandling eller administration av hälso- eller sjukvård eller när dessa uppgifter behandlas av någon som är yrkesmässigt verksam på hälso- och sjukvårdsområdet och som enligt nationell lagstiftning eller bestämmelser som antagits av behöriga nationella organ är underkastad tystnadsplikt eller av en annan person som är ålagd en liknande tystnadsplikt.

4. Under förutsättning av lämpliga skyddsåtgärder och av hänsyn till ett viktigt allmänt intresse får medlemsstaterna antingen i sin nationella lagstiftning eller genom ett beslut av tillsynsmyndigheten besluta om andra undantag än de som nämns i punkt 2.

5. Behandling av uppgifter om lagöverträdelser, brottmålsdomar eller säkerhetsåtgärder får utföras endast under kontroll av en myndighet eller – om lämpliga skyddsåtgärder finns i nationell lag – med förbehåll för de ändringar som medlemsstaterna kan tillåta med stöd av nationella bestämmelser som innehåller lämpliga och specifika skyddsåtgärder. Ett fullständigt register över brottmålsdomar får dock föras endast under kontroll av en myndighet.

Medlemsstaterna får föreskriva att uppgifter som rör administrativa sanktioner eller avgöranden i tvistemål också skall behandlas under kontroll av en myndighet.

6. De undantag från punkt 1 som anges i punkterna 4 och 5 skall anmälas till kommissionen.

7. Medlemsstaterna skall bestämma på vilka villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas.

Artikel 9

Behandling av personuppgifter och yttrandefriheten

Medlemsstaterna skall med avseende på behandling av personuppgifter som sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande besluta om undantag och avvikelser från bestämmelserna i detta kapitel, kapitel IV och kapitel VI endast om de är nödvändiga för att förena rätten till privatlivet med reglerna om yttrandefriheten.

AVDELNING IV

INFORMATIONSPLIKT TILL DEN REGISTRERADE

Artikel 10

Information vid insamling av uppgifter från den registrerade

Medlemsstaterna skall föreskriva att den registeransvarige eller hans företrädare i vart fall skall ge den person från vilken uppgifter om honom själv samlas in följande information, utom i fall då han redan känner till informationen:

a) Den registeransvariges och dennes eventuella företrädares identitet.
b) Ändamålen med den behandling för vilken uppgifterna är avsedda.
c) All ytterligare information, exempelvis
   — mottagarna eller de kategorier som mottar uppgifterna,
   — huruvida det är obligatoriskt eller frivilligt att besvara frågorna samt eventuella följder av att inte svara,
   — förekomsten av rättigheter att få tillgång till och att erhålla rättelse av uppgifter som rör honom,

   i den utsträckning som den ytterligare informationen – med hänsyn till de särskilda omständigheter under vilka uppgifterna samlas in – är nödvändig för att tillförsäkra den registrerade en korrekt behandling.

Artikel 11

Information när uppgifterna inte har samlats in från den registrerade

1. Om uppgifterna inte har samlats in från den registrerade, skall medlemsstaterna föreskriva att den registeransvarige eller hans företrädare vid tiden för registreringen av personuppgifter eller, om utlämnande till en tredje man kan förutses, inte senare än vid den tidpunkt då uppgifterna

först lämnas ut, skall ge den registrerade åtminstone följande information, utom när den registrerade redan känner till informationen:

a) Den registeransvariges och dennes eventuella företrädares identitet.
b) Ändamålen med behandlingen.
c) All ytterligare information, exempelvis
   — de kategorier av uppgifter som behandlingen gäller,
   — mottagarna eller de kategorier som mottar uppgifterna,
   — förekomsten av rättigheter att få tillgång till och att erhålla rättelse av de uppgifter som rör honom,

   i den utsträckning som den ytterligare informationen – med hänsyn till de särskilda omständigheter under vilka uppgifterna samlas in – är nödvändig för att tillförsäkra den registrerade en korrekt behandling.

2. Bestämmelserna i punkt 1 skall inte gälla när det – särskilt i samband med behandling för statistiska ändamål eller historiska eller vetenskapliga forskningsändamål – visar sig omöjligt eller innebära en oproportionerligt stor ansträngning att ge information eller om registrering eller utlämnande uttryckligen föreskrivs i författning. I sådana fall skall medlemsstaterna föreskriva lämpliga skyddsåtgärder.

AVDELNING V

DEN REGISTRERADES RÄTT ATT FÅ TILLGÅNG TILL UPPGIFTER

Artikel 12

Rätt till tillgång

Medlemsstaterna skall säkerställa att varje registrerad har rätt att från den registeransvarige

a) utan hinder och med rimliga intervall samt utan större tidsutdräkt eller kostnader
   — få bekräftelse på om uppgifter som rör honom behandlas eller inte och information om åtminstone ändamålen med behandlingen, de berörda uppgiftskategorierna och mottagarna eller mottagarkategorierna till vilka uppgifterna utlämnas,
   — få begriplig information om vilka uppgifter som behandlas och all tillgänglig information om varifrån dessa uppgifter kommer,
   — få kännedom om den logik som används när uppgifter som rör honom behandlas på automatisk väg åtminstone såvitt avser sådana automatiska beslut som avses i artikel 15.1,

b) i förekommande fall få sådana uppgifter som inte behandlats i enlighet med bestämmelserna i detta direktiv rättade, utplånade eller blockerade, särskilt om dessa är ofullständiga eller felaktiga,
c) få genomfört att en tredje man till vilken sådana uppgifter utlämnats underrättas om varje rättelse, utplåning eller blockering som utförts i enlighet med punkt b), om detta inte visar sig vara omöjligt eller innebär en oproportionerligt stor ansträngning.

AVDELNING VI

UNDANTAG OCH BEGRÄNSNINGAR

Artikel 13

Undantag och begränsningar

1. Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de skyldigheter och rättigheter som anges i artiklarna 6.1, 10, 11.1, 12 och 21 i fall då en sådan begränsning är en nödvändig åtgärd med hänsyn till

a) statens säkerhet,
b) försvaret,
c) allmän säkerhet,
d) förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken,
e) ett viktigt ekonomiskt eller finansiellt intresse hos en medlemsstat eller hos Europeiska unionen, inklusive monetära frågor, budgetfrågor och skattefrågor,
f) en tillsyns-, inspektions- eller regleringsfunktion som, även om den är av övergående karaktär, är förbunden med myndighetsutövning i de under punkterna c), d) och e) nämnda fallen,
g) skydd av den registrerades eller andras fri- och rättigheter.

2. Under förutsättning av lämpliga rättsliga garantier får medlemsstaterna, i synnerhet om uppgifterna inte används för åtgärder eller beslut som avser särskilda registrerade personer, i fall då det uppenbarligen inte föreligger någon risk att den berörda personens privatliv kränks, genom lagstiftning begränsa de rättigheter som anges i artikel 12 när uppgifterna endast behandlas för ändamål som har med vetenskaplig forskning att göra eller när uppgifterna endast lagras i form av personuppgifter under en begränsad tid som inte överstiger den tid som är nödvändig för att framställa statistik.

AVDELNING VII

DEN REGISTRERADES RÄTT ATT GÖRA INVÄNDNINGAR

Artikel 14

Den registrerades rätt att göra invändningar

Medlemsstaterna skall tillförsäkra den registrerade rätten att

a) åtminstone i de fall som avses i artikel 7 e) och f) när som helst av avgörande och berättigade skäl som rör hans personliga situation motsätta sig behandling av uppgifter som rör honom, utom när den nationella lagstiftningen föreskriver något annat. När invändningen är berättigad får den behandling som påbörjats av den registeransvarige inte längre avse dessa uppgifter,

b) efter anmodan och utan kostnader motsätta sig behandling av personuppgifter som rör honom och som den registeransvarige bedömer kan komma att behandlas för ändamål som rör direkt marknadsföring, eller att bli informerad innan personuppgifter för första gången lämnas ut till tredje man eller används för tredje mans räkning för ändamål som rör direkt marknadsföring, och att uttryckligen få erbjudande om att utan kostnader motsätta sig ett sådant utlämnande eller sådan användning.

Medlemsstaterna skall vidta nödvändiga åtgärder för att säkerställa att de registrerade känner till den rättighet som anges i första stycket i b).

Artikel 15

Databehandlade beslut

1. Medlemsstaterna skall ge varje person rätten att inte bli föremål för ett beslut som har rättsliga följder för honom eller som märkbart påverkar honom och som enbart grundas på automatisk behandling av uppgifter som är avsedda att bedöma vissa personliga egenskaper hos honom, exempelvis hans arbetsprestationer, kreditvärdighet, pålitlighet och uppträdande.

2. Om inte annat följer av övriga bestämmelser i detta direktiv skall medlemsstaterna föreskriva att en person får bli föremål för ett beslut av det slag som avses i punkt 1 om beslutet

a) fattas som ett led i ingåendet eller fullgörandet av ett avtal, förutsatt att den registrerades begäran om ingående eller fullgörande av avtalet har bifallits eller att det vidtas lämpliga åtgärder för att skydda hans

berättigade intressen, exempelvis möjligheten för honom att göra sin uppfattning gällande, eller

b) tillåts i lagstiftning som innehåller bestämmelser till skydd för den registrerades berättigade intressen.

AVDELNING VIII

SEKRETESS OCH SÄKERHET VID BEHANDLING

Artikel 16

Sekretess vid behandling

Den som utför arbete under den registeransvarige eller registerföraren, liksom registerföraren själv, och som får tillgång till personuppgifter, får behandla dem endast enligt instruktion från den registeransvarige, om han inte är skyldig att göra det enligt lag.

Artikel 17

Säkerhet vid behandling

1. Medlemsstaterna skall föreskriva att den registeransvarige skall genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling.

Dessa åtgärder skall med beaktande av den nuvarande tekniska nivån och de kostnader som är förenade med åtgärdernas genomförande åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som skall skyddas.

2. Medlemsstaterna skall föreskriva att den registeransvarige, när behandlingen utförs för dennes räkning, skall välja en registerförare som kan ge tillräckliga garantier vad gäller de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som måste vidtas och tillse att dessa åtgärder genomförs.

3. När uppgifter behandlas av en registerförare skall hanteringen regleras genom ett avtal eller genom en annan rättsligt bindande handling mellan registerföraren och den registeransvarige och i handlingen skall särskilt föreskrivas att

— registerföraren endast får handla på instruktioner från den registeransvarige,
— de skyldigheter som anges i punkt 1, såsom de definieras i lagstiftningen i den medlemsstat i vilken registerföraren är etablerad, även skall åvila registerföraren.

4. För att säkra bevisning skall de delar av avtalet eller den rättsligt bindande handlingen som rör skyddet av uppgifter och de krav som rör åtgärder som anges i punkt 1 föreligga i skriftlig eller därmed jämförlig form.

AVDELNING IX

ANMÄLAN

Artikel 18

Anmälningsplikt gentemot tillsynsmyndigheten

1. Medlemsstaterna skall föreskriva att den registeransvarige eller hans eventuella företrädare före genomförandet av en behandling eller en serie behandlingar som helt eller delvis genomförs på automatisk väg och som har samma eller flera närbesläktade ändamål skall underrätta den tillsynsmyndighet som avses i artikel 28.

2. Medlemsstaterna får endast i följande fall och på följande villkor föreskriva om undantag från anmälningsplikten eller förenklad anmälningsplikt:

— Om medlemsstaten för de typer av behandling, i samband med vilka det med hänsyn till de behandlade uppgifterna inte är sannolikt att de registrerades fri- och rättigheter kränks, anger behandlingens ändamål, vilka uppgifter eller kategorier av uppgifter som behandlas, vilka registrerade eller kategorier av registrerade som avses, till vilka mottagare eller kategorier av mottagare uppgifterna lämnas ut samt hur länge uppgifterna skall bevaras och/eller
— om den registeransvarige i enlighet med den nationella lagstiftning som gäller för denne, utser ett uppgiftsskyddsombud, som särskilt skall ha till uppgift
  — att på ett oberoende sätt säkerställa den interna tillämpningen av de nationella bestämmelser som antagits till följd av detta direktiv,

— att föra ett register över de behandlingar som utförs av den registeransvarige, vilket register skall innehålla den information som nämns i artikel 21.2,

för att på detta sätt säkerställa att de registrerades fri- och rättigheter sannolikt inte kommer att kränkas som en följd av behandlingarna.

3. Medlemsstaterna får föreskriva att punkt 1 inte skall gälla för en sådan behandling vars enda syfte är förandet av ett register, som enligt lagar eller andra författningar är avsett att förse allmänheten med information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse.

4. Medlemsstaterna får föreskriva undantag från anmälningsplikten eller ett förenklat anmälningsförfarande för sådan behandling som avses i artikel 8.2 d).

5. Medlemsstaterna får föreskriva att vissa eller alla icke-automatiska behandlingar av personuppgifter skall anmälas eller att ett förenklat anmälningsförfarande skall gälla för dem.

Artikel 19

Anmälans innehåll

1. Medlemsstaterna skall precisera vilka uppgifter som anmälan skall innehålla. Den skall åtminstone innehålla

a) den registeransvariges och dennes eventuella företrädares namn och adress,
b) ändamålen med behandlingen,
c) en beskrivning av den eller de kategorier av registrerade som berörs och av de uppgifter eller kategorier av uppgifter som hänför sig till dem,
d) mottagarna eller de kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut,
e) föreslagna överföringar av uppgifter till tredje land,
f) en allmän beskrivning som gör det möjligt att preliminärt bedöma lämpligheten av de åtgärder som i enlighet med artikel 17 vidtagits för att trygga säkerheten i behandlingen.

2. Medlemsstaterna skall ange villkoren för anmälan till tillsynsmyndigheten av förändringar som rör den i punkt 1 angivna informationen.

Artikel 20

Förhandskontroll

1. Medlemsstaterna skall bestämma vilka behandlingar som kan innebära särskilda risker för den registrerades fri- och rättigheter och skall säkerställa att dessa behandlingar kontrolleras innan de påbörjas.

2. Sådana förhandskontroller skall utföras av tillsynsmyndigheten när den mottagit anmälan från den registeransvarige eller från uppgiftsskyddsombudet, som i tveksamma fall skall rådfråga tillsynsmyndigheten.

3. Medlemsstaterna kan också utföra sådana kontroller som ett led i det nationella parlamentets förberedande arbete med en åtgärd eller som ett led i arbetet med en åtgärd som grundas på en sådan lagstiftande åtgärd, som definierar behandlingens art och anger lämpliga skyddsåtgärder.

Artikel 21

Behandlingarnas offentlighet

1. Medlemsstaterna skall vidta åtgärder för att tillse att behandlingarna görs offentligt tillgängliga.

2. Medlemsstaterna skall föreskriva att tillsynsmyndigheten skall föra ett register över sådana behandlingar som har anmälts i enlighet med artikel 18.

Registret skall innehålla åtminstone den information som anges i artikel 19.1 a)–e).

Registret skall vara allmänt tillgängligt.

3. För sådan behandling som inte omfattas av anmälningsplikt skall medlemsstaterna föreskriva att de registeransvariga eller något annat organ, som medlemsstaterna utser, på lämpligt sätt skall tillhandahålla var och en som begär det åtminstone den information som anges i artikel 19.1 a)–e).

Medlemsstaterna får föreskriva att denna bestämmelse inte skall tillämpas på sådan behandling vars enda ändamål är att föra ett register, som i enlighet med lagar eller andra författningar är avsett att ge allmänheten information och som är tillgängligt för allmänheten eller för var och en som kan styrka ett berättigat intresse.

KAPITEL III

RÄTTSLIG PRÖVNING, ANSVAR OCH SANKTIONER

Artikel 22

Rättslig prövning

Medlemsstaterna skall – utan att det påverkar möjligheten att utnyttja något administrativt förfarande, till exempel vid den tillsynsmyndighet som avses i artikel 28, som kan användas innan ett ärende anhängiggörs hos en rättslig instans – föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på ifrågavarande behandling.

Artikel 23

Ansvar

1. Medlemsstaterna skall föreskriva att var och en som lidit skada till följd av en otillåten behandling eller av någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av detta direktiv, har rätt till ersättning av den registeransvarige för den skada som han har lidit.

2. Den registeransvarige kan helt eller delvis undgå detta ansvar om han bevisar att han inte är ansvarig för den händelse som orsakade skadan.

Artikel 24

Sanktioner

Medlemsstaterna skall anta lämpliga bestämmelser för att säkerställa att detta direktiv genomförs fullständigt och skall särskilt besluta om de sanktioner som skall användas vid överträdelse av de bestämmelser som antagits för att genomföra detta direktiv.

KAPITEL IV

ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

Artikel 25

Principer

1. Medlemsstaterna skall föreskriva att överföringen av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring till tredje land endast får ske om ifrågavarande tredje land – utan att detta påverkar tillämpningen av de nationella bestämmelser som antagits till följd av de andra bestämmelserna i detta direktiv – säkerställer en adekvat skyddsnivå.

2. Bedömningen av om skyddsnivån i ett tredje land är adekvat skall ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Härvid skall särskilt beaktas uppgiftens art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredje land liksom de regler för yrkesverksamhet och säkerhet som gäller där.

3. Medlemsstaterna och kommissionen skall informera varandra när de anser att ett tredje land inte erbjuder en adekvat skyddsnivå enligt punkt 2.

4. Om kommissionen i enlighet med ett sådant förfarande som beskrivs i artikel 31.2 finner att ett tredje land inte erbjuder en sådan adekvat skyddsnivå som beskrivs i punkt 2 i denna artikel, skall medlemsstaterna vidta de åtgärder som är nödvändiga för att hindra överföring av uppgifter av samma slag till ifrågavarande tredje land.

5. Vid lämpligt tillfälle skall kommissionen inleda förhandlingar för att avhjälpa den situation som uppstått när kommissionen kommit till den slutsats som anges i punkt 4.

6. Kommissionen kan, i enlighet med det i artikel 31.2 angivna förfarandet, konstatera att ett tredje land genom sin interna lagstiftning eller på grund av de internationella förpliktelser som – särskilt till följd av sådana förhandlingar som anges i punkt 5 och som gäller skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter – åligger landet har

en skyddsnivå som är adekvat i den mening som avses i punkt 2 i denna artikel.

Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut.

Artikel 26

Undantag

1. Med undantag från artikel 25 skall medlemsstaterna – om det inte finns tvingande regler om detta i deras lagstiftning – föreskriva att överföring av personuppgifter till ett tredje land som inte har en adekvat skyddsnivå i den mening som avses i artikel 25.2 får ske om

a) den registrerade otvetydigt har samtyckt till den planerade överföringen, eller
b) överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den registeransvarige eller för att på den registrerades begäran genomföra åtgärder som vidtas innan avtalet ingås, eller
c) överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den registeransvarige och tredje man i den registrerades intresse, eller
d) överföringen är nödvändig eller bindande enligt författning av skäl som rör viktiga allmänna intressen eller för att fastslå, göra gällande eller försvara rättsliga anspråk, eller
e) överföringen är nödvändig för att skydda intressen som är av avgörande betydelse för den registrerade, eller
f) överföringen görs från ett offentligt register som enligt lagar eller andra författningar är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, i den utsträckning som de i lagstiftningen angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

2. Utan att detta påverkar tillämpningen av punkt 1 får en medlemsstat til??låta överföring av personuppgifter till ett tredje land som inte säkerställer en skyddsnivå som är adekvat enligt artikel 25.2, om den registeransvarige ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter. Sådana garantier kan framgå av lämpliga avtalsklausuler.

3. Medlemsstaten skall informera kommissionen och de övriga medlemsstaterna om de överföringar som tillåtits enligt punkt 2.

Om en medlemsstat eller kommissionen på grunder som är berättigade med hänsyn till skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter gör en invändning skall kommissionen vidta lämpliga åtgärder i enlighet med det förfarande som avses i artikel 31.2.

Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut.

4. Om kommissionen i enlighet med det förfarande som anges i artikel 31.2 beslutar att vissa standardavtalsklausuler erbjuder tillräckliga garantier enligt punkt 2, skall medlemsstaterna vidta nödvändiga åtgärder för att följa kommissionens beslut.

KAPITEL V

UPPFÖRANDEKODEX

Artikel 27

1. Medlemsstaterna och kommissionen skall uppmuntra utarbetande av uppförandekodexar som – med beaktande av de särskilda förhållandena på olika områden – skall bidra till att på ett riktigt sätt genomföra de nationella bestämmelser som medlemsstaterna antar för att genomföra detta direktiv.

2. Medlemsstaterna skall föreskriva att branschorganisationer eller andra organ som företräder andra kategorier av registeransvariga, som har upprättat förslag till nationella kodexar eller som avser att ändra eller utöka existerande nationella kodexar, kan lägga fram dessa för bedömning av den nationella myndigheten.

Medlemsstaterna skall föreskriva att denna myndighet bland annat skall kontrollera att de förslag som har lagts fram för myndigheten är i överensstämmelse med de nationella bestämmelser som antagits till följd av detta direktiv. Om myndigheten anser det lämpligt skall den inhämta synpunkter från de registrerade eller deras företrädare.

3. Förslag till gemenskapskodexar och förslag till ändringar eller tillägg till existerande sådana kodexar kan läggas fram för den arbetsgrupp som avses i artikel 29. Denna arbetsgrupp skall bland annat avgöra om de förslag som lagts fram för gruppen är i överensstämmelse med de nationella bestämmelser som antagits för att genomföra detta direktiv. Om gruppen an-

ser det lämpligt skall den inhämta synpunkter från de registrerade eller deras företrädare. Kommissionen kan tillse att de kodexar som godkänts av arbetsgruppen offentliggörs på lämpligt sätt.

KAPITEL VI

TILLSYNSMYNDIGHET OCH ARBETSGRUPP FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLINGEN AV PERSONUPPGIFTER

Artikel 28

Tillsynsmyndighet

1. Varje medlemsstat skall tillse att det utses en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av detta direktiv.

Dessa myndigheter skall fullständigt oberoende utöva de uppgifter som åläggs dem.

2. Varje medlemsstat skall tillse att tillsynsmyndigheten hörs när sådana lagar eller andra författningar utarbetas som rör skyddet av enskilda personers fri- och rättigheter med avseende på behandlingen av personuppgifter.

3. Varje tillsynsmyndighet skall särskilt ha

— undersökningsbefogenheter, såsom befogenhet att få tillgång till uppgifter som blir föremål för behandling och befogenhet att inhämta alla uppgifter som är nödvändiga för att sköta tillsynen,
— effektiva befogenheter att ingripa, som till exempel att kunna avge yttranden i enlighet med artikel 20 innan en behandling äger rum, och se till att sådana yttranden i lämplig omfattning offentliggörs, att kunna besluta om blockering, utplåning eller förstöring av uppgifter, att kunna besluta om tillfälligt eller slutligt förbud mot behandling, att kunna ge den registeransvarige varning eller tillrättavisning eller att kunna hänvisa saken till nationella parlament eller till andra politiska institutioner,
— befogenhet att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av detta direktiv har överträtts eller att uppmärksamma de rättsliga myndigheterna på dessa överträdelser.

Sådana beslut av tillsynsmyndigheten som går en part emot kan överklagas till domstol.

4. Var och en kan, på egen hand eller företrädd av en organisation, vända sig till tillsynsmyndigheten med begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter. Den berörda personen skall informeras om vilka följder hans begäran har fått.

Var och en kan i samband med tillämpningen av de nationella bestämmelser som har antagits med stöd av artikel 13 i detta direktiv till tillsynsmyndigheten ge in en begäran om att få kontrollera om en behandling är tillåten. Den berörda personen skall informeras om vilka följder hans begäran har fått.

5. Varje tillsynsmyndighet skall regelbundet upprätta en rapport om sin verksamhet. Denna rapport skall offentliggöras.

6. En tillsynsmyndighet har, oavsett vilken nationell lagstiftning som gäller för den aktuella behandlingen, behörighet att inom sin egen medlemsstats territorium utöva de befogenheter som i enlighet med punkt 3 åligger den. Varje myndighet kan av en myndighet i en annan medlemsstat anmodas att utöva sina befogenheter.

De övervakande myndigheterna skall i den utsträckning som det behövs samarbeta med varandra, särskilt genom att utbyta användbar information.

7. Medlemsstaterna skall föreskriva att tillsynsmyndighetens ledamöter och personal, även sedan deras anställning upphört, skall ha tystnadsplikt med avseende på förtrolig information som de har tillgång till.

Artikel 29

Arbetsgrupp för skydd av enskilda med avseende på behandlingen av personuppgifter

1. En arbetsgrupp för skydd av enskilda med avseende på behandling av personuppgifter, hädanefter kallad ”arbetsgruppen” inrättas härmed.

Arbetsgruppen skall vara rådgivande och oberoende.

2. Arbetsgruppen skall vara sammansatt av en företrädare för den eller de tillsynsmyndigheter som utsetts av varje medlemsstat, av en företrädare för den eller de myndigheter som har inrättats för gemenskapens institutioner och organ samt av en företrädare för kommissionen.

Varje medlem av arbetsgruppen skall utses av den institution eller av den eller de myndigheter som han företräder. När en medlemsstat har fler tillsynsmyndigheter än en, skall dessa utse en gemensam företrädare. Detsamma skall gälla för de myndigheter som inrättats för gemenskapens institutioner och organ.

3. Arbetsgruppen skall fatta beslut med enkel majoritet av tillsynsmyndigheternas företrädare.

4. Arbetsgruppen skall välja sin ordförande. Ordförandens mandattid skall vara två år. Mandatet kan förlängas.

5. Arbetsgruppens sekretariatsuppgifter skall ombesörjas av kommissionen.

6. Arbetsgruppen skall själv fastställa sin arbetsordning.

7. Arbetsgruppen skall behandla frågor som förts upp på dess dagordning av ordföranden, antingen på dennes eget initiativ eller på begäran av en företrädare för tillsynsmyndigheterna eller för kommissionen.

Artikel 30

1. Arbetsgruppen skall

a) utreda varje fråga som rör tillämpningen av de nationella bestämmelser som antagits för genomförandet av detta direktiv, för att bidra till en enhetlig tillämpning av bestämmelserna,
b) yttra sig till kommissionen om skyddsnivån inom gemenskapen och i tredje land,
c) ge kommissionen råd om varje föreslagen ändring av detta direktiv, om vilka ytterligare eller särskilda åtgärder som bör vidtas för att skydda fysiska personers fri- och rättigheter med avseende på behandling av personuppgifter och om alla andra föreslagna gemenskapsåtgärder som rör sådana fri- och rättigheter,
d) avge yttranden om de uppförandekodexar som utarbetas på gemenskapsnivå.

2. Om arbetsgruppen konstaterar förekomsten av sådana skillnader mellan medlemsstaternas lagstiftning eller praxis, som kan vara till nackdel för likvärdigheten i skyddet för personer med avseende på behandlingen av personuppgifter inom gemenskapen, skall gruppen informera kommissionen om detta.

3. Arbetsgruppen kan på eget initiativ utfärda rekommendationer i alla frågor som rör skyddet av personer med avseende på behandlingen av personuppgifter inom gemenskapen.

4. Arbetsgruppens yttranden och rekommendationer skall framläggas för kommissionen och den kommitté som avses i artikel 31.

5. Kommissionen skall informera arbetsgruppen om det sätt på vilket den har tagit hänsyn till yttrandena och rekommendationerna. För att göra detta skall kommissionen utarbeta en rapport som också skall framläggas för Europaparlamentet och rådet. Rapporten skall offentliggöras.

6. Arbetsgruppen skall utarbeta en årsrapport om situationen rörande skyddet för fysiska personer med avseende på behandlingen av personuppgifter inom gemenskapen och i tredje land, som den skall översända till kommissionen, Europaparlamentet och rådet. Rapporten skall offentliggöras.

KAPITEL VII

GEMENSKAPENS ÅTGÄRDER FÖR GENOMFÖRANDE

Artikel 31

Kommittén

1. Kommissionen skall biträdas av en kommitté som är sammansatt av företrädare för medlemsstaterna och som har kommissionens företrädare som ordförande.

2. Kommissionens företrädare skall förelägga kommittén ett förslag till åtgärder. Kommittén skall yttra sig över förslaget inom en tid som ordföranden bestämmer med hänsyn till hur brådskande ärendet är.

Yttrandet skall avges med den majoritet som anges i artikel 148.2 i fördraget. Vid omröstning i kommittén skall medlemsstaternas röster vägas på det sätt som anges i den artikeln. Ordföranden skall inte rösta.

Kommissionen skall besluta om åtgärder som skall ha omedelbar verkan. Om emellertid åtgärderna avviker från kommitténs yttrande, skall kommissionen omedelbart underställa rådet ärendet. I detta fall gäller följande:

— Kommissionen skall uppskjuta genomförandet av åtgärderna under en tidsfrist om tre månader räknad från meddelandedatum,
— Rådet kan med kvalificerad majoritet fatta ett avvikande beslut inom den tidsfrist som anges i den första strecksatsen.

SLUTBESTÄMMELSER

Artikel 32

1. Medlemsstaterna skall sätta i kraft de lagar och andra författningar, som är nödvändiga för att följa detta direktiv, senast tre år efter dess antagande.

När en medlemsstat antar dessa bestämmelser skall de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen skall göras skall varje medlemsstat själv utfärda.

2. Medlemsstaterna skall se till att sådan behandling som redan pågår när de nationella bestämmelser som antas till följd av detta direktiv träder i kraft bringas i överensstämmelse med dessa bestämmelser inom tre år från denna tidpunkt.

I fråga om sådana uppgifter som redan finns i manuella register vid ikraftträdandet av de nationella bestämmelser som antas för att genomföra detta direktiv får medlemsstaterna, med avvikelse från föregående stycke, föreskriva att behandlingen skall bringas i överensstämmelse med artiklarna 6–8 i detta direktiv inom tolv år räknat från dagen för direktivets antagande. Medlemsstaterna skall dock ge den registrerade rätt att på begäran och särskilt i samband med att han utövar sin rätt till tillgång till uppgifter, erhålla rättelse, utplåning eller blockering av uppgifter som är ofullständiga, felaktiga eller lagrade på ett sätt som inte är förenligt med de legitima ändamål som den registeransvarige vill uppnå.

3. Med undantag från punkt 2 kan medlemsstaterna under förutsättning av lämpliga skyddsåtgärder föreskriva att uppgifter som endast bevaras för historisk forskning inte behöver överensstämma med artiklarna 6–8 i detta direktiv.

4. Medlemsstaterna skall till kommissionen överlämna texten till de nationella bestämmelser som de antar inom det område som omfattas av detta direktiv.

Artikel 33

Kommissionen skall första gången senast tre år efter den tidpunkt som anges i artikel 32.1 och därefter regelbundet till rådet och Europaparlamentet avge en rapport om genomförandet av detta direktiv, eventuellt försedd med lämpliga ändringsförslag. Rapporten skall offentliggöras.

Kommissionen skall särskilt undersöka tillämpningen av detta direktiv på behandling av ljud- och bilduppgifter som rör fysiska personer och skall framlägga alla lämpliga förslag som med beaktande av informationsteknikens och informationssamhällets utveckling, visar sig nödvändiga.

Artikel 34

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Luxemburg den 23 oktober 1995

På Europaparlamentets vägnar	*På rådets vägnar*
K. HÄNSCH	L. ATIENZA SERNA
Ordförande	*Ordförande*

_____

BILAGA 3: CYBERSPACE, REAL LIFE OCH JURIDIKEN

—

Rapport av Christian Wettergren och Björn Pehrson

Kungl. Tekniska Högskolan/Teleinformatik

INNEHÅLL:

Cyberspace, Real Life och juridiken

—

Datalagskommitténs betänkande ur teknisk synvinkel

Av
doktoranden Christian Wettergren och
professorn Björn Pehrson

1 Introduktion

Denna rapport diskuterar ett antal aspekter som är relevanta för den kommande datalagstiftningen, och Datalagskommitténs betänkande. Den är skriven ur ett tekniskt perspektiv, och diskuterar speciellt aspekter som rör säkerhet och den privata sfären. Rapporten utgår från de praktiska erfarenheter som författarna har av datasäkerhetsarbete i en Internetmiljö, och de problemställningar som uppkommit där. Det finns ett underliggande antagande att dessa problemställningar kommer att sprida sig till övriga IT-sektorer allteftersom. Internet utgör därmed ett tidigt test på kommande problem.

Rapportens huvudsakliga författare är doktorand Christian Wettergren, men prefekt Björn Pehrsons synpunkter är invävda i texten, och författarna har diskuterat innehållet i rapporten.

De grundläggande egenskaperna hos Cyberspace i kontrast mot den fysiska världen diskuteras i avsnitt 2. Den typ av personuppgifter som ej kopplas till den fysiska identiteten utan till den elektroniska diskuteras i avsnitt 3. Persondatalagens möjlighet att initiera en nödvändig förbättring av datasäkerheten i samhället diskuteras i avsnitt 4. Mängden ”fria personuppgifter” som finns i samband med privat kommunikation och privat be-

arbetning diskuteras i avsnitt 5. En sammanfattning av de konkreta förslagen avslutar rapporten i avsnitt 6.

2 Egenskaper hos ”Cyberspace”

I och med IT-revolutionen flyttar verksamheter från den fysiska världen in i Cyberspace. Denna flytt sker eftersom IT erbjuder en rationell hantering av många verksamheter, och IT dessutom är flexibel på ett helt annat sätt än fysiskt realiserade verksamheter. Ekonomiskt sett utgör IT ett helt nytt fenomen; enbart fasta kostnader, och rörliga kostnader nära noll. Denna ekonomiska drivkraft är mycket stark, och kommer att påverka hela samhället de närmaste decennierna.

I samband med denna IT-revolution uppkommer frågor om säkerheten och integriteten hos den nya verksamheten. Cyberspace har andra egenskaper än den fysiska världen, och därför uppkommer andra frågeställningar än då verksamheten sker i den fysiska världen. Nedan diskuteras några viktiga egenskaper hos Cyberspace, som drastiskt skiljer sig från den fysiska världen.

Först och främst måste man uppmärksamma att buggar alltid existerar i alla system[488], och att även om man kan reducera antalet kraftigt leder detta till alltför stora utvecklingskostnader. En del av dessa allmänna buggar får säkerhetsrelevans, och blir därmed *säkerhetshål*. Vi kan därför inte förvänta oss att bygga det helt säkra systemet. I stället måste målet bli att kostnaderna för att lokalisera och designa en framgångsrik attack överstiger den förväntade vinst attacken kan ge. Detta förfarande är analogt med hur det fungerar i den fysiska världen, det som har värde måste skyddas ”tillräckligt”. En av de viktigaste egenskaperna hos IT är dess fenomenala förmåga att automatisera verksamheter. Marginalkostnaden att utföra en procedur fler gånger när den väl kan utföras en gång med IT är

488 Fel och svagheter finns givetvis i alla mänskliga konstruktioner. Dessa imperfektioner utgör dock ett mycket större hot i IT-världen, jämfört med de traditionella teknologierna. I IT är det område varifrån en imperfektion kan utnyttjas mycket större än i fysiska konstruktioner. Dessutom sker allting snabbt och automatiskt i Cyberspace. En ytterligare faktor av vikt i IT är att IT är transitiv till sin natur, dvs. att om A och B kan kommunicera, och B och C kan kommunicera, betyder det att A och C också kan kommunicera. Påverkan förblir inte lokal. Detta sammantaget leder till att en angripare har betydande skalfördelar i Cyberspace jämfört med den fysiska världen.

obetydlig. Detta innebär att aktioner som skulle kräva en stor organisation med betydande resurser om de utfördes i den fysiska världen kan utföras av enskilda individer i Cyberspace. Dessa aktioner kan givetvis vara av kriminell art. Ett illustrativt exempel är till exempel att *Swedish Hacker Association* lyckades obemärkt ”dyrka 150 000 lås” i Cyberspace, dvs. gissa 150 000 användares lösenord. Tänk er motsvarande aktion i den fysiska världen! Den obetydliga kostnaden för replikation och automatisering är ytterst viktig då man resonerar om lagstiftningen i Cyberspace.

Tyvärr är grundtekniken i IT-systemen inte robust nog. En till synes obetydlig bugg kan utnyttjas mycket effektivt av en angripare, och effekten av buggen kan lätt förstoras till att omfatta hela system. Ofta kombinerar en angripare ihop effekten av flera buggar och systemets medvetna funktion till en attackkedja som uppnår angriparens mål. Eftersom grundtekniken är i stort sett densamma över hela IT-världen, är svagheterna i stort sett desamma överallt. Dessutom blir de åtgärder som behövs för att göra tekniken mer robust likartad. Målet måste vara att grundtekniken skall bli såpass robust att ”vanliga” programmerarmisstag inte skall kunna utnyttjas och förstoras, utan att effekterna förblir lokala runt buggen.

Orsaken till IT:s oerhörda vitalitet kan sägas bero på att informationen kan flöda fritt inom systemet. Nya program laddas ner över Nätet, olika meddelanden skickas mellan användare, automatiska sökmotorer samlar på sig all information i enorma databaser. Det som behövs för att utföra en attack är *information*, och det som behövs för att skydda ett system är *information*. Kostnaden för att utföra en attack beror alltså på hur stora kostnaderna är för att införskaffa den nödvändiga informationen. Införskaffandet kan antingen ske genom att man själv skapar informationen, vilket ofta innebär arbetstid, eller byter den till sig från någon som har informationen. Dessvärre finns det en välorganiserad *Computer Underground*, där information byts utan kostnad. Dessutom drivs medlemmarna av ett brinnande intresse för IT-system, och arbetar därför gärna gratis, eller för en viss status i denna subkultur. Vi kan därför konstatera att kostnaderna för en attack på ett system i dag ligger nära noll. I värsta fall behöver angriparen investera någon arbetsvecka för att ta sig in.

En annan egenskap hos Cyberspace som inte uppmärksammats ordentligt ännu är den oerhörda *transitivitet* som informationen får i systemet. System som man trodde var helt separerade kan visa sig vara *nära* i Cyberspace genom att de delar på någon resurs. Informationen kan då rinna iväg åt icke-förväntade eller icke-önskade håll. En medveten angripare kan därför ofta hitta ”bakvägar” in i systemen.

I IT-system agerar ett antal olika personer, ”parter”, samtidigt. Säkerhetsfunktionerna måste förhindra att de olika parterna otillbörligt påverkar de andra parterna. Säkerhetsfunktionerna i moderna IT-system byggs nästan alltid efter det jag kallar *Systemparadigmen.* Med det menar jag att separationen av parterna uppnås genom att en ytterligare part, *Systemet*, införs, som tillser denna separation. Eftersom *Systemet* separerar parterna måste alla parter lita på *Systemet*, och den som kontrollerar *Systemet* har möjlighet att förfalska varje parts medverkan i IT-systemet. Filosofin bakom *Systemparadigmen* går ut på att *Systemet* ska göras säkert. Tyvärr brukar *Systemet* bli stort och komplext, och innehåller därför buggar. Erfarenheten visar att *Systemet* nästan alltid kan komprometteras på något sätt.

Systemparadigmen håller på att ersättas av andra paradigmer. I öppna system, med allmän och delad nätinfrastruktur, kan inte nätet antas vara del av *Systemet*. I detta koncept sammanbinds de olika parterna av en komponent som ingen part litar på, och det finns ingen omfattande *System*-komponent, utan varje part hanterar sina egna behov själva. För att uppnå robust säkerhet bör komponenterna *distribueras ut* i systemen, och *göras så små och* därmed *många*, som möjligt.

Vi behöver antagligen ompröva var på spektrat *flexibilitet–säkerhet* vi vill befinna oss för olika verksamheter och funktioner. Vissa kritiska funktioner skall kanske göras väsentligt mindre flexibla än vad de är i dag?

Enskilda personers aktiviteter i Cyberspace lämnar omfattande spår efter sig. En viktig konsekvens av att IT-teknologin är så billig och att informationen kan rör sig så fritt är att det är relativt enkelt och billigt att samla in och sammanställa sådana spår till en heltäckande bild av vad en viss person företar sig. I de fall IT används i samband med fysisk verksamhet kan denna typ av informationsinsamling även komma att omfatta aktiviteter i den fysiska världen.[489] Det är därför mycket viktigt att minimera informationsläckaget från olika IT-tjänster ut i systemet.

Grundläggande bestäms säkerheten i Cyberspace av **ekonomiska kalkyler**. Om kostnaden för att bryta sig in i ett system blir kännbar för angriparen kommer vederbörande att vara mer tveksam i att attackera. Ökande kostnader stänger ute allt fler angripare. Få angripare är motiverade om kostnaderna för attacken överstiger den förväntade vinsten, multiplicerat med sannolikheten för en lyckad attack. Denna fundamentala ekvation be-

---

489 Ett exempel är det läckage av geografisk plats som ägaren av en GSM-telefon läcker in i GSM-*systemet*. Denna information används numera regelbundet av polisen.

stämmer hur omfattande säkerhetsproblem vi kan komma att få. Tyvärr är kostnaderna i dag i det närmaste noll, som vi konstaterat tidigare[490]. Följaktligen kan vi vänta oss problem framöver.

IT-tekniken förändrar maktbalansen mellan olika parter, eftersom den ekonomiska grunden för deras verksamhet förändras. Applicerat på brottsbekämpning betyder det att den eviga kampen mellan brottslingar och polis får nya förutsättningar i Cyberspace. Det går inte att avgöra åt vilket håll maktbalansen tippar, eftersom båda parters verksamhet påverkas. Eftersom läget är så osäkert kommer båda sidor försöka stärka sina positioner, och vad som är önskvärt beror på vilka värderingar man har. Vi kan konstatera att vare sig en polisstat med omfattande övervakning av oskyldiga personer ”för säkerhets skull”, eller total anarki är attraktiv för de flesta[491]. Det i någon mån ”neutrala alternativet” är att bygga IT-system som har liknande ekonomisk trade-off mellan polismakt och brottslingar som den i dag existerande fysiska världen har. Detta är ju i praktiken inte görligt, men kan utgöra en utgångspunkt för diskussionen.

3 Personuppgifter kopplade till elektroniska identiteter

I lagförslaget utgår man ifrån begreppet *personuppgift*. Detta begrepp utgår från den historiskt viktiga *databasen*, som registrerar fakta och uppgifter om människor. Databasen övervakar alltså människorna i den fysiska

---

490 Värdet av informationen, och därmed den potentiella vinsten, i IT-system kommer att öka med tiden, vilket alltså innebär att vi i stället måste öka *kostnaden för en attack*. Att lyckas med detta kommer att bli svårt. Det skulle vara mycket svårt att förhindra hackers att byta information med varandra. En viktig faktor i en attacks förväntade vinst är hur många gånger den kan upprepas på ett identiskt sätt, det vill säga hur stor replikationsfaktorn är. Det går att minska replikationsfaktorn genom att ha diversitet i IT-systemen, men detta är dyrt. Replikationsfaktorn kan också reduceras genom att koppla bort IT-system från kommunikationsmöjligheter, men detta är oftast inte ett alternativ. En angripare kan också avskräckas på grund av efterräkningar, men det förutsätter att man vet vem angriparen är, och det kan man ofta inte göra i Cyberspace. Det slutliga alternativet är att *drastiskt öka den tekniska kostnaden för ett intrång genom att på något sätt förändra grundtekniken i IT-systemen*. Hur dessa ändringar av grundtekniken skall se ut är en grannlaga forskningsuppgift.

491 Detta är givetvis kulturberoende. Svenskar torde ha större tilltro till Staten än exempelvis många amerikanska medborgare.

verkligheten. Eftersom personuppgifter inte enbart förekommer i databaser, har begreppet generaliserats till att omfatta sökbara samlingar av personuppgifter.

> [Avsnitt 1 Gällande rätt i huvuddrag]
> Med *personuppgift* avses upplysning som avser enskild person. Det kan vara upplysningar om namn, personnummer, födelsedatum, nationalitet, utbildning, familj och anställningsförhållanden. Även andra typer av upplysningar av mindre personlig karaktär räknas som personuppgifter. Enligt lagmotiven avses även uppgifter om en persons bostadsförhållanden, banktillgodohavanden, fastighets- eller bilinnehav och upplysningar i övrigt om en persons ekonomiska ställning. […]
>
> En personuppgift kan hänföras till en viss person antingen direkt genom själva uppgiften eller med hjälp av en identitetsuppgift som också ingår i registret. Även register som innehåller identitetsuppgifter av sådan art att bara den invigde kan utläsa vilka personer som finns registrerade omfattas av datalagen. Likaså omfattas statistiska uppgifter där beteckningar som också återfinns på dokument gör det möjligt att knyta uppgifterna till en viss person.

> [Avsnitt 3.2.2.2 Personuppgifter och den registrerade]
> **Med *personuppgift* avses varje upplysning som avser en identifierad eller identifierbar fysisk person (*den registrerade*).** En person är identifierbar om han eller hon kan identifieras direkt eller indirekt, t.ex. genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans eller hennes fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Kopplingen till den fysiska personen är stark, och det är logiskt med tanke på dagens situation. En annan typ av *”personuppgifter”* kan dock bli viktig inom de närmaste åren, som inte tydligt ingår i definitionen ovan, nämligen *uppgifter som knyts till den elektroniska identiteten.*

Personuppgifter om den elektroniska identiteten innebär att man samlar in uppgifter om ett subjekts aktiviteter i Cyberspace, utan att för den skull försöka knyta uppgifterna till en fysisk person. Man behöver inte ens försöka tillse att man enbart samlar uppgifter om en enstaka persons aktiviteter. Dessa uppgifter kan man sedan använda för marknadsföring, övervakning, marknadsundersökningar, skräddarsydda tjänster (*personalisering)* och bevisinsamling.

Denna typ av personuppgifter kan komma att utgöra en väg runt lagstiftningen, och kan bli nog så viktig för företagen.

> […] I punkt 26 i ingressen betonas att man, för att avgöra om en person är identifierbar, skall beakta alla hjälpmedel som kan komma att användas för

> att identifiera personen. Däremot gäller inte direktivet för uppgifter som har gjorts anonyma på ett sådant sätt att personen inte längre är identifierbar.
>
> […] I kommissionens förklaring anges som exempel på direkt identifiering att personen kan identifieras genom namnet. Indirekt identifiering kan vara när personen kan identifieras genom ett telefonnummer, ett bilregistreringsnummer, ett socialförsäkringsnummer eller ett passnummer. Ett annat exempel är när identifieringen av en person sker 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 andra personer. Det framgår vidare av kommissionens förklaring att 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.

Eftersom uppgifterna inte nödvändigtvis knyts till *enskild* person, kan företagen argumentera att detta inte är personuppgifter i lagens mening. Uppgifterna kan bli alltmer detaljerade, men det är inte säkert att de därför innebär att man kan identifiera den fysiska individen. Och vad händer om den fysiska individen namnger sig själv i samband med någon tjänst? Tidigare var det ju inget personregister, men i och med detta blir det ett? En analogi med den fysiska världen skulle kunna vara omfattande övervakning med kameror och mikrofoner. Eftersom individerna inte är identifierade så rör det sig inte om personuppgifter, men denna omfattande övervakning utgör ändå ett omfattande integritetsintrång. Analogin haltar dock, eftersom uppgifter insamlade i Cyberspace är väsentligt mer lättbearbetade än video och ljud.

Dessa cyber-personuppgifter kan bli mycket detaljerade, jämfört med de traditionella personuppgifterna. Insamling av beteendeuppgifter i Cyberspace är mycket billigt, jämfört med om man skulle samla in samma uppgifter i den fysiska världen. Bearbetningen av dessa uppgifter sker dessutom i samma medium, vilket innebär att det inte finns några omfattande konverteringskostnader. Ytterligare en förvärrande faktor är att individen inte har någon möjlighet att avgöra om han/hon är övervakad eller inte i Cyberspace. En motsvarande omfattande fysisk övervakning skulle vara synlig, alternativt kräva stora investeringar för att inte synas. Ett *förslag* är att tjänster som är allmänt tillgängliga måste deklarera om de loggar användaren, vad som loggas och hur länge denna information sparas. Man kan också tänka sig att reglera handeln med dylika personuppgifter mellan företag.

De flesta av dagens IT-system läcker personuppgifter till omgivningen. Avlyssning av den allmänna nätstrukturen avslöjar dels *vilka* användare

som kommunicerar med varandra, dels *vad* de gör. De som använder samma server kan ofta iaktta varandras aktiviteter. Kvarvarande spår i olika datorer kan ofta berätta för en senare användare vad som företagits med datorn. Mycket få program och applikationer utvecklas med tanke på att minimera denna typ av läckage. Det har förekommit fall i USA där headhunters har kontrollerat vilka användare som arbetat sent för att hitta lämpliga kandidater att rekrytera. Det kan noteras att det enda verktyg vi har för att åtgärda detta problem är kryptering.

IT-revolutionen har inte hunnit så långt ännu, och användning av personuppgifter knutna till elektroniska identiteter har inte kommit i allmän bred användning ännu. Konceptet används dock bl.a. i Postens webbplats *Torget* med hjälp av så kallade *Cookies*.[492] I USA är *personalisering* av webbsidor det senaste, vilket också baserar sig på personuppgifter knutna till en elektronisk identitet. När alltfler verksamheter flyttas till Cyberspace kommer denna typ av personuppgifter att bli allt viktigare.

Rent tekniskt går registrering av dylika personuppgifter till som så att varje aktör i ett system bär på något kännetecken, en *markör*. En markör kan antingen vara en redan existerande särskiljande datamängd, eller så kan denna datamängd läggas till vid interaktionen. Aktiviteter som aktören utför loggas med markören som nyckel. Det behöver inte finnas en absolut koppling mellan aktören i Cyberspace och *en* enskild individ, utan man kan ha markerat *en (liten) grupp individer* med en markör. Det kanske räcker med att registrera ett hushålls vanor, exempelvis. Det är möjligt att välja markörer som aktören *är tvungen att använda* för att kunna utnyttja tjänsterna. Det är också möjligt att välja markörer som används av flera tjänsteleverantörer, vilket underlättar korskorrelering av insamlad information. Ett exempel på markör kan vara att använda en persons publika nyckel som knutits till ett nationellt ID-kort, eller datorns ändnodsadress (IP-nummer). Dessa markörer är besvärliga att byta.

Tidigare integritetsproblem kommer att blekna jämfört med de problem vi potentiellt har framför oss. Jag tror att det är viktigt att fortlöpande följa integritetsproblematiken, och att vara beredd att reglera avarterna. En möjlighet vore att ge Datainspektionen ett uppdrag att utgöra allmänhetens *integritetsombudsman*. Jag ser det som mycket viktigt att samhället initie-

---

492 Så här ser ett utdrag ut ur en Cookie-fil:

```
.torget.se     TRUE   / FALSE        1291165200 TorgetUser   851564382
www-elec.enst.fr FALSE      /      FALSE    946511999  RoxenUserID  0x59
.socialstudies.com TRUE     /      FALSE  946684799    INTERSE sl67231788
www.dn.se      FALSE  FALSE   859839554  DNetVisits   6
```

rar och stödjer forskning som syftar till att ta fram system som minimerar integritetsproblemet. Vi kan inte förvänta oss att marknaden tar tag i detta problem.

4 Hur få en positiv utveckling på datasäkerhetsområdet?

Datasäkerhet är ett oerhört eftersatt område i dag, och medvetenheten om säkerhetsbristerna är låg. I princip samtliga datorsystem går att bryta sig in i med relativt små resurser. Som nämnts tidigare är det kapital en inbrottstjuv behöver *information*, och denna typ av information är normalt sett billigt att få tag på.

Militären har fått upp ögonen för denna fara, och kallar ämnet för ”*information warfare”*. De undersöker problemen ur både defensiv och offensiv synvinkel. Rapporterna [1] [2] [3] målar en skrämmande bild där alla datorsystem kan manipuleras, och där dessa manipulationer kan få dramatiska konsekvenser med försörjningskriser, störtande flygplan och krockande tåg. De militära analytikerna noterar att användningen av detta ”vapen” inte begränsar sig till nationalstater, utan även små grupper med begränsade resurser kan nyttja det.

För att tillse att otillåtna samkörningar mellan persondataregister ej sker måste man ha en hög datasäkerhetsnivå i systemen, annars kan en part med ont uppsåt omärkligt bryta sig in i de intressanta persondataregistren, kopiera persondata, och sedan genomföra samkörningen med egen utrustning.

Med utgångspunkt i mitt tekniska kunnande och baserat på en del av den litteratur jag har läst håller jag det inte för orimligt att främmande makt har fullständig access till vissa av våra persondataregister med känsligt innehåll. Den amerikanska militären hävdar att det är av avgörande strategisk vikt att de besitter ”*information high ground*”, dvs. att de har tillgång till all information de behöver. Det är sannolikt att den amerikanska signalspaningsorganisationen NSA har säkrat fri tillgång till intressanta register.[493] Jag bedömer det som fullt möjligt att även betydligt

493 Enligt obekräftade rykten, som bland annat återgetts i Washington Post, hade NSA genom avlyssning fullständig tillgång till all intern information hos EU-kommissionen. NSA hade modifierat en hårdvarukomponent i kommissionens PC-maskiner för att uppnå detta. Tyvärr saknas referenser på denna händelse.

mindre organisationer kan skaffa sig tillgång till dessa register. *Jag bedömer det som mycket svårt att skydda stora samlingar av intressanta persondata från otillbörligt intrång.*

Enligt den nu gällande datalagen (1973) får Datainspektionen utfärda föreskrifter om hur behandlingen skall genomföras med hänseende på kontroll och säkerhet (6 § DL).

> 6 § DL Lämnas tillstånd till inrättande och förande av personregister, skall datainspektionen, i den mån det behövs för att förebygga risk för otillbörligt intrång i personlig integritet, meddela föreskrift om
> …
> 4. den tekniska utrustningen,
> …
> 10. kontroll och säkerhet,
> …

EU:s dataskyddsdirektiv reglerar säkerheten vid behandling av personuppgifter närmare. Dataskyddsdirektivet skall omsättas i nationell lag, i och med Datalagskommitténs betänkande och den efterföljande behandlingen.

> Artikel 17: Säkerhet vid behandling
>
> 1. Medlemsstaterna skall föreskriva att den registeransvarige skall genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling.
>
> Dessa åtgärder skall med beaktande av den nuvarande tekniska nivån och de kostnader som är förenade med åtgärdernas genomförande åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som skall skyddas.
>
> 2. Medlemsstaterna skall föreskriva att den registeransvarige, när behandlingen utförs för dennes räkning, skall välja en registerförare som kan ge tillräckliga garantier vad gäller de tekniska säkerhetsåtgärder och de organisatoriska åtgärder som måste vidtas och tillse att dessa åtgärder genomförs.

> 3. När uppgifter behandlas av en registerförare skall hanteringen regleras genom ett avtal eller genom en annan rättsligt bindande handling mellan registerföraren och den registeransvarige och i handlingen skall särskilt föreskrivas att
> — registerföraren endast får handla på instruktioner från den registeransvarige,
> — de skyldigheter som anges i punkt 1, såsom de definieras i lagstiftningen i den medlemsstat i vilken registerföraren är etablerad, även skall åvila registerföraren.

Datalagskommittén diskuterar inte säkerhetskraven närmare, utan refererar till skrivningarna i dataskyddsdirektivet. Jag tror att dessa paragrafer kan komma att bli viktiga de närmaste åren, och skulle gärna se en skärpning av kraven.

Till att börja med är det orimligt att lägga samma säkerhetskrav oberoende av datasamlingens omfattning och struktur. För privat användning av en mindre mängd persondata i en ostrukturerad samling torde dagens kommersiella produkter med lösenordsskydd vara tillräckligt.

Eftersom automatiska bearbetningar är praktiskt taget utan kostnader i Cyberspace, utgör de **stora** samlingarna av strukturerade persondata problemet. Små register som är organiserade efter olika kriterier, och använder olika databasteknik, eller på annat sätt har olika struktur, leder till omfattande manuellt efterarbete. Dessutom blir inte alla intrång identiska, eftersom systemen är olika, vilket ytterligare fördyrar hopsamlandet av informationen.

De stora persondatasamlingarna sitter däremot i mitten av stora informationsbehandlingssystem med tillhörande stora accessnät ut i organisationens administration. Ofta räcker det med *ett* intrång i ett sådant system för att en angripare skall få tag på den information som han är ute efter. Dessutom leder det stora accessnätet till att det finns många vägar in i systemet, och databastekniken är mer standardiserad.

Dessa stora informationsbehandlingssystem leder till kraftiga rationaliseringsvinster för organisationen. Samtidigt ökar risken för intrång i registret kraftigt med *storleken*. De stora registren bör därför ha större säkerhetskrav på sig än de små registren.

De investeringar som dessa ökade krav orsakar, leder till samhällsekonomiska vinster, eftersom de minskar sårbarheten i samhället. Det är troligt att hotet från *”information warfare”* kommer att leda till att staten i vilket fall tvingas genomföra program för att minska sårbarheten hos de mest kritiska IT-systemen, för att trygga *informationsförsörjningen*. De stora administrativa systemen hör till dessa kritiska system.

Mitt förslag är att förstärka kraven på säkerhet i samband med större persondatasamlingar. Innehavare av stora register bör vara skyldiga att demonstrera att säkerheten är tillfredsställande inför exempelvis en expertkommitté. Denna kontroll bör ske regelbundet. Att ha en koppling till *state-of-the-art* innebär tyvärr bara att det eftersatta området datasäkerhet inte rör sig framåt. **Kraven bör vara målrelaterade**, och inte produktrelaterade. Ett minimum är att varje organisation skyddar sig mot de kända attacker som finns. Organisationen bör också skydda sig mot attacktyper som är troliga att utnyttjas allmänt inom en snar framtid. Man bör också notera att organisationer med resurser alltid kan använda mer avancerade och okända attacktyper på systemet. Om innehållet i registren är känsligt, eller hotbilden på annat sätt visar att kvalificerade attacker är troliga, bör organisationen vara skyldig att skydda sig mot dessa hot också.

Jag tror också att det är viktigt att säkerhetsbestämmelserna förknippas med reella och kännbara påföljder. Nuvarande 23 § DL kan leda till att den registeransvarige får ersätta skada orsakad på grund av brott mot 20 § DL, exempelvis mot föreskrifter angående kontroll och säkerhet (6 § 1 st. 10 DL). EU:s dataskyddsdirektiv innehåller följande:

> Artikel 23: Ansvar
>
> 1. Medlemsstaterna skall föreskriva att var och en som lidit skada till följd av en otillåten behandling eller av någon annan åtgärd som är oförenlig med de nationella bestämmelser som antagits till följd av detta direktiv, har rätt till ersättning av den registeransvarige för den skada som han har lidit.
>
> 2. Den registeransvarige kan helt eller delvis undgå detta ansvar om han bevisar att han inte är ansvarig för den händelse som orsakade skadan.

I Datalagskommitténs föreslagna lydelse av persondatalagen har detta formulerats:

> 31 § Den persondataansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av
> a) de tekniska möjligheter som finns,
> b) vad det skulle kosta att genomföra åtgärderna,
> c) de särskilda risker som finns med behandlingen av personuppgifterna, och
> d) hur pass känsliga de behandlade personuppgifterna är.
>
> När den persondataansvarige anlitar ett persondatabiträde, skall den persondataansvarige förvissa sig om att persondatabiträdet kan genomföra de sä-

kerhetsåtgärder som måste vidtas och se till att persondatabiträdet verkligen vidtar åtgärderna.

Skadestånd

43 § Den persondataansvarige skall ersätta den registrerade för den skada som en behandling av personuppgifter i strid med denna lag eller föreskrifter som har meddelats med stöd av lagen har fört med sig. Ersättning skall betalas också för ren förmögenhetsskada och för den kränkning av den personliga integriteten som behandlingen har inneburit.

Ersättningsskyldigheten enligt första stycket kan i den utsträckning det är skäligt sättas ned eller helt falla bort, om den persondataansvarige visar att felet inte berodde på honom eller henne.

Först föreslår jag alltså att fallet e) att åtgärderna skall relateras till antalet registrerade i persondataregistret, inkluderas i 31 § ovan.

Jag föreslår vidare att den registeransvarige skall kunna hållas skadeståndsskyldig även vid fall av *intrång av tredje man*. 43 § andra stycket kan tolkas så att vid intrång av tredje man är inte den persondataansvarige skadeståndsskyldig med avseende på intrång i den personliga integriteten, eftersom *”felet inte berodde på honom eller henne”*.

Skadeståndsansvaret bör vidare vara strikt, så att intrång av tredje man i ett register *alltid* leder till en viss skadeståndskostnad för den persondataansvarige. Skadeståndets storlek kan dock reduceras om den persondataansvarige kan demonstrera att tillräckliga målrelaterade åtgärder vidtagits för att tillse säkerheten i behandlingen och lagringen av registret, på liknande sätt som i den föreslagna 43 §.

5 ”Fria” personuppgifter

Den föreslagna persondatalagen innehåller ett antal undantag från när lagen tillämpas.

Undantag för privat användning av personuppgifter

6 § Denna lag gäller inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur.

Undantag med hänsyn till yttrandefriheten

7 § Bestämmelserna i 9–29 och 33–46 §§ samt 47 § första stycket och 49 § skall inte tillämpas på

a) sådana förfaranden som är skyddade enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen,

b) spridningen av sådana yttranden som är skyddade enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, eller
c) sådan behandling av personuppgifter som annars sker uteslutande för journalistiska ändamål eller konstnärligt eller litterärt skapande.

10 § Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller när behandlingen är nödvändig
a) för att fullgöra ett avtal med den registrerade,
b) för att på den registrerades begäran vidta åtgärder innan ett avtal träffas,
c) för att den persondataansvarige skall kunna fullgöra en rättslig skyldighet,
d) för att skydda vitala intressen för den registrerade,
e) för att utföra en arbetsuppgift av allmänt intresse,
f) för att den persondataansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller
g) för ändamål som rör ett berättigat intresse hos den persondataansvarige eller hos sådana tredje män till vilka personuppgifterna lämnas ut när detta intresse väger tyngre än den registrerades intresse.

Dessutom kan uppgift föras över till tredje land, där undantag från lagstiftningen kan trädda in.

34 § Utan hinder av 33 § är det tillåtet att föra över personuppgifter till tredje land, om den registrerade har samtyckt till överföringen eller när överföringen är nödvändig för att
a) fullgöra ett avtal mellan den registrerade och den persondataansvarige,
b) på den registrerades begäran vidta åtgärder innan ett avtal träffas,
c) ingå eller fullgöra ett sådant avtal mellan den persondataansvarige och tredje man som är i den registrerades intresse,
d) rättsliga anspråk skall kunna fastställas, göras gällande eller försvaras, eller
e) skydda vitala intressen för den registrerade.

Det är också tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter.

En del av dessa undantag rör det fall då den registrerade själv har lämnat medgivande om behandling, en del fall rör tryck- och yttrandefriheten, och ytterligare fall rör rent privat behandling. Resultatet av dessa undantag kommer att bli att en stor mängd av ”fria” persondatauppgifter kommer att existera.

IT innebär att intressegrupper lätt kan formas och kommunicera med varandra. Dessa nya fora behöver inte ha en fast form, utan kan uppkomma spontant och upplösas spontant. De kan dessutom vara helt baserade på personlig kommunikation inom en liten grupp av individer. Att delta i

dessa fora är en grundläggande rättighet såväl med avseende på mötesfrihet som föreningsfrihet (2 kap. 1 § RF). I många fall rör sig detta om privat kommunikation – ett cybermöte – och *Yttrandefrihetsgrundlagen* (YGL) och *Tryckfrihetsförordningen* (TF) borde då inte appliceras, dvs. ingen ansvarig utgivare, ingen ”självsanering”, inga genmälen. Det faktum att denna kommunikation sker över elektroniska infrastrukturer bör inte påverka denna grundläggande rätt att kommunicera. Enligt den föreslagna 6 § ovan har varje person dessutom rätt att behandla personuppgifter för privat verksamhet. Rimligen borde denna rent privata bearbetning kunna baseras på information som erhållits genom privat kommunikation. Dessutom skulle efterlevnaden av en lag som förbjöd denna typ av behandling inte kunna kontrolleras.

Det är troligt att mängden ”fria personuppgifter” kommer att växa kraftigt framöver. De självmant lämnade uppgifterna kommer att öka, och de privata mottagarna kommer att kunna lagra dessa uppgifter[494]. Dessa uppgifter kan sedan komma att spridas i andra hand i privata möten eller i småskaliga ”massmedier”, som nyhetsbrev och diskussionsgrupper. Vi kan redan konstatera att det förekommer ryktesspridning på Internet som är mycket livskraftig. Om ett rykte uppfattas som trovärdigt och angeläget sprids det vidare, och det är därför troligt att vi kommer att få se betydligt fler ärekränkningsmål framöver.

Nätets gränslöshet ställer dock till problem när det gäller ärekränkning, eftersom olika nationer har olika ärekränkningslagar. Traditionella massmedier kommer antagligen ställa upp på självsanerande kontrollverksamhet, men kommer ”nya massmedier” att göra det?[495] Det är inte särskilt troligt, och var gränsen mellan ”slutet möte” och ”massmedier” ska dras kan verkligen diskuteras. Min erfarenhet från Internettjänsten Usenet[496] är att man inte nödvändigtvis kan förvänta sig en ”god samtalston”, till stor del baserat på det faktum att deltagargruppen är så heterogen, och att exponeringen för diametralt motsatta åsikter får vissa deltagare att tappa fatt-

---

494 Det är vanligt att flitiga e-post-användare har stora mängder e-post lagrade, ibland uppåt flera tusen stycken. Denna e-post är full med personuppgifter, och kan sökas i baserat på ämne, avsändare, datum eller valfritt nyckelord.

495 Se exempelvis den omskrivna servern Flashback (http://www.flashback.se) med tillhörande nyhetsbrev Flashback News Agency (FNA), som går ut till omkring 12 000 svenska prenumeranter.

496 Ett världsomspännande diskussionsforum med ämnesrelaterade möten där deltagare från hela världen deltar.

ningen.[497] Denna situation leder ibland till en upptrappning, som emellanåt slutar i en större mängd stämningar för förtal mellan kontrahenterna.

> 12 § I de fall där behandling av personuppgifter bara är tillåten när den registrerade har lämnat sitt samtycke enligt 10, 15 eller 34 § har den registrerade rätt att när som helst återkalla ett lämnat samtycke. Ytterligare personuppgifter om den registrerade får därefter inte behandlas.
>
> En registrerad har utöver vad som följer av första stycket och 11 § inte rätt att motsätta sig sådan behandling av personuppgifter som är tillåten enligt denna lag.

Denna rätt att återkalla uppgifter lämnade med samtycke kan rent praktiskt vara ogörligt för denna typ av ”fria personuppgifter” som diskuteras. Spridningen av dessa uppgifter är okontrollerbar. Inlägg i diskussionslistor hamnar exempelvis hos alla prenumeranter av diskussionslistan, och vissa av dem kan ha lämnat listan vid tidpunkten då begäran om ett ”återkallande” skickas ut.

I grunden finns det en fundamental motsättning mellan rätten till privat kommunikation och allmänhetens och enskildas oro för att bli ”registrerade”. Om och hur denna motsättning bör regleras är oklart för mig. Jag tror att det är viktigt att vara medveten om att en större mängd ”fria personuppgifter” kommer att ackumuleras i IT-systemen, och jag föreslår att Datainspektionen får i uppdrag att fortlöpande undersöka omfattningen av det integritetsintrång denna information utgör. Jag tror också att är viktigt att nya system som minimerar mängden ”fria personuppgifter” med hög identifikationsgrad utvecklas.[498]

6 Sammanfattning

I Cyberspace gäller andra fundamentala begränsningar än vad som gäller i den fysiska världen, och det gör att andra problemställningar blir aktuella.

---

497 Denna typ av exponering för extrema åsikter och främmande uppfattningar kommer också att öka kraftigt i omfattning, och det är mycket svårt att åtgärda. Min uppfattning är att vi måste bli mer toleranta mot dylika yttringar. Det innebär dock inte att de skall stå oemotsagda.

498 Vid KTH/Teleinformatik har vi nyligen genomfört två examensarbeten (OnTheMove-projektet) som syftat till att ta fram ett system med pseudonymer. I detta system antar vi att man kommunicerar, men identifikationsgraden kan varieras, och varje fysisk person har flera pseudonymer, vilket försvårar korrelationen mellan fysisk person och yttrande.

Datalagen (1973) sysslade med *register*; datasamlingar om fakta om den fysiska världen och individer i den. Allteftersom verksamheter flyttar från den fysiska världen till Cyberspace, kommer mer och mer uppgifter att enbart röra Cyberspace. De fundamentala egenskaperna hos Cyberspace kommer därför att bli viktiga.

Ett förslag är att *tjänster som är allmänt tillgängliga måste deklarera om de loggar användaren, vad som loggas och hur länge denna information sparas.* Man kan också tänka sig att reglera handeln med dylika personuppgifter mellan företag.

Den föreslagna definitionen av *personuppgift* är bra, men den tar ej hänsyn till identiteter som enbart rör sig i Cyberspace, utan explicit koppling till den fysiska individen. Detta kan utgöra en väg runt den föreslagna persondatalagen. Det är inte heller säkert att enbart *enskild* individ kan råka ut för integritetsintrång, utan även *en liten grupp av individer* kan råka ut för detta.

Ett förslag är att ge Datainspektionen en allmän roll som allmänhetens *Integritetsombudsman.* DI skulle då få ett fortlöpande uppdrag att tillvarata individens integritet under IT-revolutionens fortskridande. Det är viktigt att samhället initierar och stödjer forskning som syftar till att ta fram system som minimerar integritetsproblemet. Det föreslås också att omfattningen av *vidtagna säkerhetsåtgärder skall göras beroende av storleken på persondatasamlingen*. Det föreslås att den föreslagna 31 § kompletteras med

e) att åtgärderna skall relateras till antalet registrerade i persondataregistret

Att ha en koppling till datasäkerhetens *state-of-the-art* innebär tyvärr bara att det eftersatta området datasäkerhet inte rör sig framåt. *Kraven bör vara målrelaterade,* och inte produktrelaterade.

Det föreslås vidare att den persondataansvarige skall kunna hållas skadeståndsskyldig även vid fall av *intrång av tredje man*. Skadeståndsansvaret bör vidare vara strikt, så att intrång av tredje part i ett register *alltid* leder till en viss skadeståndskostnad för den persondataansvarige. Detta förslag rör 43 § andra stycket.

I grunden finns det en fundamental motsättning mellan rätten till privat kommunikation och allmänhetens och enskildas oro för att bli ”registrerade”. Om och hur denna motsättning bör regleras är oklart. Det är viktigt att vara medveten om att en större mängd ”fria personuppgifter” kommer att ackumuleras i IT-systemen. Vi föreslår att Datainspektionen

får i uppdrag att fortlöpande undersöka omfattningen av det integritetsintrång denna ”fria” information utgör. Det är också viktigt att nya system som minimerar mängden ”fria personuppgifter” med hög identifikationsgrad utvecklas.

Detta arbete har finansierats av EU genom ACTS-projektet OnTheMove. För mer information om OnTheMove, se http://www.sics.se/~onthemove/.

Denna bilaga finns tillgänglig på http://www.it.kth.se/~cwe/phd/dalk/.

Referenser

[1] Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, *Strategic Information Warfare: A New Face of War,*
http://www.rand.org/publications/MR7MR661/MR661.html
http://www.rand.org/publications/MR7MR661/MR661.pdf

[2] Robert H. Anderson, Anthony C. Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: ‘The Day After… Cyberspace II’*
http://www.rand.org/publications/MR/MR797/

[3] *Information War and the Air Force: Wave of the Future? Current Fad?*
http://www.rand.org/publications/IP/IP149/

BILAGA 4: PERSONLIG INTEGRITET

—

Rapport av Göran Collste

Centrum för tillämpad etik
Universitetet i Linköping

INNEHÅLL:

Behandling av personuppgifter och personlig integritet. En etisk analys

Av Göran Collste

I denna studie är det två frågor som står i fokus: Vad betyder personlig integritet? Är personlig integritet något viktigt och värdefullt? Studien inleds med exempel på några situationer där personlig integritet har aktualiserats. Med hjälp av dessa exempel görs ett försök att precisera innebörden i begreppet kränkning av personlig integritet. Efter att ha behandlat frågan hur man sett på personlig integritet inom svensk tradition ställs frågan om personlig integritet är en rättighet. Avslutningsvis behandlas några exempel på hur respekten för personlig integritet kan komma i konflikt med andra värden.[499]

1 Några exempel

A. I förtroende berättade A för P att han för något år sedan försökt ta sitt liv. När A fick reda på att P talat med några arbetskamrater om detta kände han att hans personliga integritet blivit kränkt.
B. När B går ut bland människor, känns det som alla stirrar på honom. Han upplever att hans personliga integritet blir kränkt.
C. Fröken C har valt att ställa upp och medverka i en pornografisk tidskrift. När X får reda på det, hävdar hon att Cs personliga integritet blir kränkt, vilket C förnekar.
D. Tidningen x-pressen publicerade en lista över de tio rikaste personerna i länet. D fanns med på listan och upplevde publiceringen som en kränkning av sin personliga integritet.

---

499 Ett tack riktas till deltagare i seminariet för tillämpad etik vid Linköpings universitet för värdefulla synpunkter på denna studie.

E. En diskett med datajournaler från en vårdcentral råkade i orätta händer. Es journal fanns med och när hon fick reda på detta upplevde hon att hennes personliga integritet blivit kränkt.
F. Flygbolaget LINSAS installerar datoriserade övervakningssystem för att kunna kontrollera hur mycket personalen använder bokningssystemet. F arbetar med bokning och upplever det nya systemet som en kränkning av hennes personliga integritet.
G. Den utvecklingsstörda flickan G blir utsatt för ett övergrepp av en vårdare. När X får reda på detta hävdar hon att Gs personliga integritet blivit kränkt.
H. Under semestern hade inbrottstjuvar gått igenom Hs lägenhet. H upplevde att hans personliga integritet blivit kränkt.

2 Vad är personlig integritet?

Vi står här inför ett antal skilda händelser som har det gemensamt att någon uppfattat att en handling utförts som medfört att de berörda personernas integritet blivit kränkt. Finns det något gemensamt mellan de olika händelserna som kan leda oss fram till en definition av vad personlig integritet är? Är det i samtliga fall rimligt att hävda att de berördas personliga integritet verkligen blivit kränkt?

Kan en persons integritet kränkas utan att personen själv är medveten om detta (fall C)? En analogi skulle kunna vara att en person som lever i en diktatur utan frihet (vilket kan visas genom avsaknad av yttranderätt, föreningsrätt osv.) trots detta inte upplever sig ofri.

Kan en person uppleva sig kränkt utan att vara kränkt (ev. fall B), dvs. den subjektiva upplevelsen av kränkning motsvaras inte av en faktisk kränkning? Svaren på dessa frågor får bilda underlag för ett förslag till avgränsning av begreppet personlig integritet.

Självkontroll

Ett återkommande element i beskrivningar av personers upplevelser av integritetskränkning är upplevelsen av en förlorad kontroll över sin egen person eller över en viss typ av uppgifter om sig själva. Vi ser det i exemplet där flickan G blir utsatt för ett övergrepp, i exemplet A där A förlorade kontrollen över uppgiften att han försökt begå självmord, liksom i exempel E där fru E förlorat kontrollen över uppgifter i datajournalen. I exemplet F

är det känslan av att vara kontrollerad av någon annan som upplevs som en integritetskränkning.

När det gäller personliga uppgifter som man upplever att man förlorat kontrollen över behöver det inte handla om sådana uppgifter som endast är tillgängliga för de berörda personerna själva. I exemplen hade uppgifterna lämnats ut till en vän respektive till sjukvårdspersonal, men de berörda personerna hade själva kontroll över vilka andra som fått ta del av uppgifterna.

Känsliga uppgifter om personer: det privata och det avvikande

Vilka uppgifter om personer är integritetskänsliga? Det tycks inte vara vilka uppgifter som helst som man vill ha kontroll över. Exemplen A och E handlar om självmordsförsök respektive uppgifter i sjukdomsjournaler, dvs. uppgifter som gäller personliga förhållanden, det privata.

Å andra sidan är inte detta något som är självklart. I exempel B tycks det som om herr B uppfattar sig kränkt av att andra ser hans ansikte. I vår kultur kan vi uppfatta en sådan upplevelse som orimlig, ja till och med patologisk, men i andra kulturer kan detta vara en naturlig reaktion. Bildförbud och den muslimska kvinnans beslöjande av delar av sitt ansikte är uttryck för detta.

Det finns också uppenbarligen personer som inte delar majoritetens uppfattning om var gränsen ska dras mellan personliga uppgifter som hör till de skyddsvärda och de som kan göras offentliga. Fröken C som medverkar i en pornografisk tidskrift drar gränsen mellan vad som hör till det privata och det offentliga på ett annat sätt än X.

Är det möjligt att dra någon bestämd gräns mellan uppgifter som är integritetskänsliga och därmed hör till privatlivet och sådana som inte är det? I den engelskspråkiga världen används *privacy* för det som i den svenska diskussionen betecknas *personlig integritet*. Den amerikanske filosofen W A Parent definierar *privacy* på följande sätt:

> ”Privacy is the condition of not having undocumented personal knowledge about one possessed by others.”

Parent avgränsar själv de personliga uppgifter det handlar om som

> ”…facts about a person which most individuals in a given society at a given time do not want widely known about themselves.”[500]

Vilken typ av uppgifter det rör sig om varierar mellan olika samhällen. I USA, liksom i Sverige, hör säkerligen uppgifter om personers sexualvanor och alkoholvanor dit. När sådana uppgifter om oss blir offentliga upplever de flesta detta som en integritetskränkning. I Sverige där religion blivit en privatsak kan uppgifter om personers religiösa uppfattningar räknas som tillhörande det privatas område, till skillnad från i USA.

Det kan ifrågasättas om information om privatlivet, för att falla in under begreppet *privacy*, inte får vara dokumenterad. Parents motivering för denna avgränsning är att informationen blir offentlig i och med att den dokumenteras och därmed, definitionsmässigt, upphör att vara privat. Möjligen kan denna avgränsning vara förnuftig när det gäller begreppet *privacy*, dock knappast när det gäller begreppet personlig integritet. En integritetskränkande uppgift som sprids om en person kan vara kränkande såväl första som andra som de ytterligare gånger som denna uppgift ges spridning.

Men är det verkligen möjligt att bygga myndigheters handlande, såsom exempelvis lagstiftning för behandling av personuppgifter, på en – antagen – majoritetsuppfattning eller för att använda Parents uttryck, på vad ”…most individuals in a given society…” uppfattar som kränkande? Mot detta talar att det finns personer som kan uppleva sådant som för majoriteten är trivialt, t.ex. offentliggörande av uppgifter om personers längd, som ytterligt känsliga. En vuxen person som är 1 m 30 cm kan uppleva sig kränkt av att hans längd meddelas offentligt. Ett annat problem är att det i mångkulturella samhällen blir svårt att uppnå en bred enighet. Jag ska återkomma till frågan om skillnaden mellan ”objektiva” och ”subjektiva” integritetskränkningar.

Den personliga integritetens extension

Vad innefattas i begreppet ”person” när vi talar om ”personlig integritet”? Var går gränsen mellan jaget/personen och resten av världen? Eller, med

---

500 Parent, W A, Privacy, Morality and the Law, i Philosophy and Public Affairs, 1983, s. 216.

andra ord, vilken extension (utbredning) har den personliga integriteten? Frågorna är inte alldeles lätta att besvara. Kroppen hör till personen, men en person är inte endast en levande kropp. Själen eller psyket, medvetandet, karaktär och personliga egenskaper, idéer och uppfattningar, hör också dit. När man talar om vad en person är, är det knappast rimligt att i platonsk anda dra någon gräns mellan kroppen och själen. Exempelvis när den utvecklingsstörda flickan G blir kränkt är det dels genom ett rent kroppsligt övergrepp, men nära förknippat med detta är den psykiska upplevelsen av övergreppet.

Människan är en social varelse. Vi står i olika typer av förbund med andra människor och vi kan leva oss in i deras upplevelser och känslor. Därmed kan vi också uppleva oss kränkta när andra som står oss nära kränks. Om mitt barn kränks kan jag uppleva det som att jag kränks. Vad som hör till det personliga tycks kunna beskrivas som sfärer. En person består av kropp och själ eller psyke där också andra personer gör sina avtryck. I denna mening kan man kanske säga att också delar av den sociala omgivningen ”ingår” i personen. Dessa sfärer är inflätade i varandra.

Vi såg att H upplevde inbrottet som en kränkning av den personliga integriteten. Upplevelsen han ha sin grund i att inbrottstjuven ”rotade” i sådant som H uppfattar som en del av sin privata sfär. H kan också ha upplevt det som en kränkning av sin person att inbrottstjuven tog Hs ägodelar. Det gör han kanske därför att han ser sin egendom som en viktig del av sitt jag, sin person. Hans personliga sfär innefattar också hans egendom. Andra personer skulle kanske inte uppfatta inbrottet som en kränkning av sin person (däremot som en kränkning av sin äganderätt). Här har vi ett exempel på hur upplevelser av kränkning kan skifta mellan olika individer.

Exemplet illustrerar också att det går att göra en distinktion mellan kränkning av person och kränkning av personlig integritet. Den personliga integriteten kränks när det sker ett intrång i personens privatliv, eller med andra ord när personen förlorar kontrollen över sin privata sfär. Enligt detta förslag till begreppsanvändning är kränkning av person ett vidare begrepp än kränkning av personlig integritet. Alla kränkningar av personlig integritet är kränkningar av personen men vissa kränkningar av personen kan inte betecknas som kränkningar av den personliga integriteten.

I andra kulturer där individen utgör en del av en större gemenskap som klanen, stammen etc. dras gränsen för såväl personens som den personliga

integritetens extension på ett annat sätt än hos oss.[501] Även denna aspekt på personlig integritet är således kulturbunden.

Att vara kränkt och att uppleva sig kränkt

Går det att skilja mellan att vara kränkt och att uppleva sig kränkt, mellan rimlig och orimlig, t.ex. sjuklig upplevelse av kränkning, mellan objektiv och subjektiv kränkning? Svaret är betydelsefullt bland annat därför att om man vill lagstifta om vilken typ av personuppgifter som kan ingå i offentliga register, så måste en sådan lag grundas på en uppfattning om var gränsen går mellan rimlig och orimlig upplevelse av kränkning.

Vi kan illustrera frågan med hjälp av ett fyrfältsdiagram:

	Kränkt	Icke kränkt
Upplever sig kränkt	1	2
Upplever sig icke kränkt	3	4

Ruta 1 innebär att man är kränkt och att man upplever sig kränkt, ruta 2 att man inte är kränkt men upplever sig kränkt, ruta 3 att man är kränkt men inte upplever sig kränkt och ruta 4 att man inte är kränkt och inte upplever sig kränkt.

Som vi sett tidigare kan en persons integritet kränkas på olika sätt. Det kan exempelvis ske genom ett kroppsligt eller psykiskt övergrepp och genom att uppgifter om personens privatliv sprids om honom eller henne.

Mitt förslag när det gäller att avgränsa vad det är rimligt att uppfatta som integritetskränkande uppgifter om personer, anknyter till Parents generalisering. En objektiv integritetskränkning föreligger när uppgifter som de flesta individer i ett visst samhälle inte vill ska spridas om sig görs offentliga. Avgränsningen blir därmed socialt grundad. Utöver detta kan enskilda individers upplevelser av att vara kränkta uppfattas som faktiskt grundade om det finns rimlig grund för upplevelsen. Ett exempel på rimlig grund kan vara att man har ett lyte eller något annat man skäms över och som man därmed inte vill att andra ska få kunskap om.

---

501 Mbiti, J S, African religions and philosophy, London 1969, s. 104 ff.

Exempel på subjektiva upplevelser av kränkning som inte uppfyller villkoret ”rimlig grund” är upplevelser som bygger på felaktig information. Personen P trodde, felaktigt, att A hade spridit känsliga uppgifter om honom och kände sig därmed kränkt. Andra upplevelser av kränkning som inte uppfyller villkoret ”rimlig grund” är upplevelser som kan betecknas som irrationella eller patologiska[502].

Med utgångspunkt i detta förslag till avgränsning kan fallet A ovan, mannen vars självmordsförsök blev känt, se som ett exempel på 1, fröken C som medverkar i pornografiska tidskrifter kan utgöra ett exempel på 3. Att en persons förmögenhet blir allmänt känd kan knappast uppfattas som en kränkning av hans personliga integritet. Fallet D är därmed ett exempel på 2, liksom B som upplever att alla stirrar på honom. B är exempel på 2 om inte han exempelvis har stora bölder i ansiktet. Då finns det ett rimligt skäl till varför han upplever sig kränkt om hans ansikte visas offentligt. Mannen som är 1.30 lång har ett rimligt skäl för att inte vilja att hans längd offentliggörs, något som för personer med normallängd kan göra detsamma.

Kan bara personer kränkas?

Det förekommer i den filosofiska diskussionen olika försök att avgränsa begreppet person. Syftet med sådana avgränsningar är vanligen att dra en gräns mellan de individer som har och de som inte har moralisk status. Exempel på sådana avgränsningar är Harry Frankfurts, som med person avser individ som kan ha önskningar av andra ordningen, dvs. önskningar om att ha vissa önskningar snarare än andra[503] och Jonathan Glover som hävdar att personer är individer med självmedvetande[504].

Denna typ av avgränsningsförsök har kritiserats för att de fungerar diskriminerande när det gäller vilka mänskliga individer som har moralisk

---

502 Vi kan lätt föreställa oss upplevelser av integritetskränkning som inte är rimliga. Det är dock inte så lätt att karakterisera dessa. Det finns en risk för att man antingen gör sig skyldig till ett cirkelresonemang eller utgår från ett problematiskt normalitetskriterium när man hävdar att de upplevelser som inte är rimligt grundade, är irrationella eller patologiska.

503 Frankfurt, H, Freedom of the Will and the Concept of a Person, Journal of Philosophy, 1970.

504 Glover, J, Jag. Den personliga identitetens filosofi och psykologi. Stockholm 1990, s. 80.

status. Moralisk status förutsätter rationell förmåga, vilket små barn och utvecklingsstörda saknar. När integritet definieras i termer av respekt för personers ”åsikter, önskningar och värderingar”[505] finns risken att en liknande begränsning av vilka individer som har en personlig integritet som är skyddsvärd görs. Det skulle exempelvis kunna leda till att den utvecklingsstörda flickan G inte har någon personlig integritet som kan kränkas. Hon kan ju tänkas vara så gravt utvecklingsstörd att hon inte utvecklat några ”åsikter, önskningar och värderingar”.

Slutsats: begreppet personlig integritet

Vilken innebörd har begreppet personlig integritet? Eftersom det är lättare att identifiera kränkning av personlig integritet än begreppet personlig integritet i sig, väljer jag att utgå från begreppet kränkning av personlig integritet:

Personers integritet kränks i den mån som
1) det sker ett intrång i deras privata sfär och/eller
2) uppgifter om dem, som det finns rimliga skäl att beteckna som integritetskänsliga, sprids ut. Dessa uppgifter kan gälla personers egenskaper, uppfattningar eller handlingar.

3 Personlig integritet i svensk tradition

De ökade tekniska möjligheterna att samla in uppgifter om individer genom exempelvis modern elektronik, datateknik och genteknik har gjort det nödvändigt för samhällets beslutsfattare och lagstiftare att reflektera över innebörden av begreppet personlig integritet och hur den personliga integriteten skall skyddas. Sedan 1970 har flera utredningar behandlat frågor om hur personlig integritet skall skyddas från otillbörlig avlyssning, från kränkande registrering och från övervakning och kontroll på arbetsplatsen.

Den svenska samhällsutvecklingen under 1900-talet kännetecknas av framväxten av ”det starka samhället”. Stat, kommun och landsting har haft uppgiften att på olika sätt skapa förutsättningar för ett gott liv för medborgarna. Man kunde tänka sig att denna betoning på samhällsgemenskapens intressen skulle lett till att myndigheter, i den sociala ingenjörskonstens in-

505 Hermerén, G, Kunskapens pris, Stockholm 1986, s. 156.

tresse, fått rätten att utveckla datoriserade personregister utan hänsyn till den enskilde individens personliga integritet. Ser man till utredningar och till den lagstiftning som genomförts i Sverige under de senaste 30 åren finner man dock att denna farhåga tycks vara obefogad. I stället var Sverige det första land som lagstiftade om dataskydd genom datalagen som stiftades 1973 och betecknas i en internationell jämförande studie som en ”modell” i detta avseende.[506]

Kanske har detta att göra med den gamla tradition av offentlighet och öppenhet som rått i Sverige, en tradition som går tillbaka till 1700-talets myndighetsutövning. Offentlighetsprincipen har hindrat myndigheter att i hemlighet samla in personliga integritetskänsliga uppgifter om medborgarna.

Ett återkommande konstaterande i de utredningar som behandlat frågan är att det är svårt att definiera begreppet personlig integritet. Vanligen används begreppet skydd för personlig integritet synonymt med skydd för privatlivet eller ”privatlivets helgd”[507]. När det gäller arbetslivet uppfattas skyddet för personlig integritet som detsamma som ”en fredad sektor” för den enskilde.[508] I utredningen *Data och integritet*, SOU 1972:47, där regler för dataregistrering för första gången formuleras av svenska myndigheter, anknyter man till den socialliberale filosofen John Stuart Mills begrepp ”privat sfär”, dvs. en gräns inom vilken den enskilde får bestämma över sig själv, och till de amerikanska juristerna Brandeis och Warrens ”privacydoktrin” som fastställer en ”right to be alone”[509]. I utredningar som syftar till att reglera hantering av genetisk information hävdas att ”Genetisk integritet är en del av den personliga integriteten”[510]

Vilka uppgifter om individer är det då som bör skyddas? Enligt den utredning som behandlar skydd för avlyssning bör den enskilde ”…åtnjuta skydd mot utomståendes insyn i hans privata förhållanden”[511].

De utredningar som har till uppgift att utforma regler för dataregistrering anger vissa personuppgifter som är känsliga. De uppgifter som nämns

---

506 Michael, J, Privacy and Human Rights. An International and Comparative Study, with Special Reference to Developments in Information Technology. Aldershot 1994, s. 53.

507 SOU 1972:47, Data och integritet, s. 56.

508 Ds 1989:24, Datatekniken och den personliga integriteten i arbetet, s. 115.

509 SOU 1972:47, s. 56.

510 Ds 1996:13, Genetisk integritet, s. 25.

511 SOU 1970:47, Skydd mot avlyssning, s. 56.

i utredningen *Data och integritet* är bl.a. uppgifter om begångna brott, påföljder, tvångsåtgärder och nykterhetsvård liksom om enskilda personers uppfattningar i politiska och religiösa frågor. Uppgifter om betyg och inkomst hör också till de personuppgifter som enligt utredningen bör skyddas.[512] Liknande personuppgifter nämns i det förslag till ny datalag som lades fram 1993. Här tillkommer dock uppgifter om ras och etniskt ursprung.[513] De personuppgifter som kan uppfattas som känsliga i arbetslivet är bl.a. uppgifter om de anställdas arbetsprestationer, värdeomdömen om arbetstagare samt de anställdas hälsouppgifter.[514] De utredningar som reglerar genetisk information understryker att information om personers arvsanlag hör till de uppgifter som är integritetskänsliga.

Hur ser man då på skyddet av personlig integritet i förhållande till andra värden? Det finns en enighet om att skyddet för personlig integritet måste avvägas mot andra värden. Det kan således i vissa fall vara nödvändigt att använda övervakningsapparatur eller föra register, även om detta utgör ett hot mot vissa individers integritet.

I utredningen *Skydd mot avlyssning* hävdas att myndigheter måste kunna göra ”…mer eller mindre vittgående undantag” från integritetsskyddet.[515] I utredningen *Data och integritet* tar man avstånd från tanken att integritetsskydd innebär detsamma som att bli lämnad i fred. Det finns samhälleliga krav på medborgarna i form av beskattning och upplysningar om personliga förhållanden[516]. Denna typ av dataregistrering av personuppgifter kommer möjligen i konflikt med Brandeis och Warrens mycket snäva definition: rätten att bli lämnad ifred. I *En ny datalag* hävdar man att vissa ”övergripande intressen” kan få begränsa integritetsskyddet i samband med upprättandet och användandet av dataregister. Man avstår dock från att precisera i vilka fall detta kan ske.[517]

Information om individers arvsanlag bör skyddas genom att individer själva bestämmer om användningen, hävdas i *Genetisk integritet*. Om individen anser att han eller hon kan ha nytta av att dela med sig av infor-

512 SOU 1972:47, s. 59 f.

513 SOU 1993:10, En ny datalag, s. 418.

514 Ds 1989:24, s. 16.

515 SOU 1970:47, s. 56.

516 SOU 1972:47, s. 56.

517 SOU 1993:10, s. 161.

mation kan detta vara möjligt, så länge inte detta också innebär att information om anhörigs arvsanlag förmedlas.[518]

Några mer utförliga motiveringar till varför det är viktigt att skydda den enskildes integritet formuleras inte. Man tycks se det som ett självklart värde eller rättighet i demokratiska samhällen. Det konsekvensetiska argument som man anför i utredningen Genetisk integritet är bl.a. att individer kan löpa risk att diskrimineras i arbetslivet och i andra sammanhang om deras arvsanlag blir kända[519].

4 Är personlig integritet en rättighet?

Ofta hävdas att personlig integritet är en rättighet. Om man med rättighet menar ”valid claim”,[520] dvs. välgrundat anspråk, som implicerar skyldigheter för omgivningen, kan vi precisera påståendet att personlig integritet är en rättighet på följande sätt: Varje person har ett välgrundat anspråk att andra personer handlar på ett sådant sätt att hans eller hennes personliga integritet respekteras.

Vad betyder det då att se personlig integritet som en rättighet? Enligt rättsfilosofen Ronald Dworkin är det i varje samhälle nödvändigt att hävda vissa individuella rättigheter för att förhindra att den enskilde individens fundamentala intressen eller den enskildes värdighet blir kränkt till förmån för majoritetens intressen eller önskningar.[521]

Tillämpad på personregister innebär satsen att personlig integritet är en rättighet och att medborgarna har berättigat anspråk att myndigheter och andra registerinnehavare hanterar register på ett sådant sätt att medborgarnas personliga integritet respekteras.

Varför har då medborgarna ett sådant anspråk? Vilka skäl kan anföras för att personlig integritet är en rättighet? Det går att anföra en rad skäl för detta. Några utgår från att personlig integritet är viktigt i sig, andra att det har ett instrumentellt värde, dvs. det bidrar till att något annat värde realiseras.

---

518 Genetisk integritet, Ds 1996:13, s. 25.

519 A.a.

520 Feinberg, J, Social Philosophy, Englewood Cliffs 1973, s. 67.

521 Dworkin, R, Taking Rights Seriously, London 1977.

1) Respekt för personers integritet utgör en del av respekten för personer. Att respektera personer eller som Immanuel Kant uttrycker det: behandla personer som ”ändamål” och aldrig enbart som medel[522], kan ses som en grundläggande plikt som inte ytterligare behöver motiveras.

   Man kan tänka sig ett samhälle där den personliga integriteten inte alls respekteras när det gäller insamlande av personuppgifter, DDR utgör ett näraliggande historiskt exempel. I ett sådant samhälle riskerar personer att förlora sin känsla av att vara unika, att vara autonoma eller med andra ord sin moraliska personlighet. I ljuset av detta exempel framstår respekten för personlig integritet som ett nödvändigt villkor för att personers autonoma jag eller moraliska personlighet skall kunna utvecklas.
2) Det finns en utbredd oro hos allmänheten att myndigheter samlar uppgifter om dem som kan användas för att kontrollera dem. Denna oro talar för att det upplevs negativt av personer att veta eller att misstänka att deras personliga integritet blir kränkt.
3) Den som har kunskap om en person kan därigenom få makt över personen. Om integritetskänsliga uppgifter om en person sprids till obehöriga personer kan dessa utsätta personen för påtryckningar och tvång. Till obehöriga personer kan här, förutom enskilda individer, också exempelvis arbetsgivare räknas. Som utredaren av skyddet för personers genetiska integritet påpekar kan en arbetsgivare som har tillgång till en anställds genetiska information använda denna kunskap mot den enskildes intresse vid beslut om avskedanden eller liknande. Genetisk information kan också användas av försäkringsbolag på ett sätt som strider mot den enskildes intresse.[523]
4) I ett samhälle där det finns fördomar mot vissa vanor eller personliga egenskaper kan det medföra att personer utsätts för trakasserier eller blir till åtlöje om upplysningar om sådana vanor och egenskaper sprids till obehöriga.

Vi finner således att det finns flera starka skäl för ståndpunkten att det är viktigt att respektera personers integritet och därmed se den personliga integriteten som en rättighet. Det är dock knappast rimligt att se rättigheten till personlig integritet som absolut. Det kan ju tänkas att det finns situationer där andra moraliska värden står på spel och som skulle motivera att

---

522 Kant, I, Grundlegung zur Metaphysik der Sitten, Hamburg 1965, s. 52.

523 Ds 1996:13.

den enskilde individens personliga integritet sätts åt sidan. Vi ska illustrera detta med ett fiktivt exempel:

> En person A är bärare av en sjukdom som vid hudkontakt utsätter en annan person för förgiftning som, om inte motåtgärder vidtas, dödar personen inom en vecka. A antecknar i sin dagbok vilka personer han träffar men han vägrar att lämna ut dessa anteckningar.

Onekligen innebär det en kränkning av As personliga integritet att mot As vilja med list eller tvång ta reda på innehållet i dagboken. Här verkar det dock rimligt att hävda att det finns andra och överordnade värden som motiverar en kränkning av detta slag: Det är oskyldiga människors liv som står på spel.

Med den engelske filosofen W D Ross kan vi se rättigheten till personlig integritet som en *prima facie*-rättighet[524]. Den är en giltig och välgrundad rättighet som dock i en konkret handlingssituation kan sättas ur spel om den kommer i konflikt med någon annan rättighet som väger tyngre.

5 Behandling av personuppgifter och rättigheten till personlig integritet

En övergripande fråga inför utvecklingen av ett datasamhälle är om det är önskvärt att allt fler och mer omfattande dataregister upprättas. Vilka följder får detta för samhällsklimat, demokrati och medborgarnas förtroende för politiker och myndigheter? Dessa viktiga socialetiska frågor kommer jag inte här att ta upp. I stället är det den mer begränsade frågan hur en avvägning mellan å ena sidan värdet av olika typer av personregistrering och sambearbetning och å andra sidan det eventuella hotet mot individers personliga integritet som kommer att behandlas.

Ett argument mot att upprätta datoriserade personregister kan vi kalla ”polisstatsargumentet”. Argumentet innebär att man inte bör upprätta personregister därför att de i en annan tänkbar politisk situation där diktatur råder kan användas av makthavarna för att förfölja medborgarna. Visst skulle systemet i DDR fungerat ännu effektivare och mer förtryckande med en utbyggd datoriserad personregistrering. Å andra sidan kan ”polisstatsargumentet” användas mot många verksamheter i samhället. Även polismakten, militären, tidningar och TV kan i en annan politisk si-

524 Ross, W D, The Right and the Good, Indianapolis 1988.

tuation användas som medel för förtryck. Detta utgör dock knappast ett argument mot att det finns en poliskår, tidningar etc. i ett demokratiskt samhälle där mänskliga fri- och rättigheter respekteras!

Ett annat argument mot personregister eller sambearbetning av register innebär att om man tillåter en viss typ av register, t.ex. register över vilka personer som är HIV-positiva, så kommer vi snart ha registrerat alla som är sjuka, vare sig det gäller halsfluss eller blindtarmen. Detta argument betecknas ibland ”the slippery slope argument” eller på svenska ”det sluttande planets argument”. Inte heller detta argument är särskilt övertygande. Det finns inget logiskt samband mellan den ena typen av register och den andra. Det är ju fullt möjligt att formulera kriterier för vilken typ av register som bör tillåtas, kriterier som därmed utesluter andra typer av register.

Det finns anledning att göra en rad distinktioner när man diskuterar frågan vilken typ av behandling av personuppgifter som kan hota den personliga integriteten.

1. Slutna och öppna system

En första distinktion är mellan öppna och slutna system. Öppna system är de system som alla kan ha tillgång till, slutna de som kräver tillgång till en ”nyckel”, dvs. det finns någon form av behörighetskrav för att få tillgång till uppgifter i registret.

Det kan förefalla som om denna distinktion löser problemet med hotet mot den personliga integriteten. Om nämligen integritetskänsliga uppgifter om individer samlas i slutna system, så kan endast de personer som har anledning att ta del av dessa uppgifter ha tillträde till de slutna systemen. Erfarenheten visar dock att denna uppfattning inte håller. Genom slarv med säkerhetsrutiner, misstag och avsiktligt intrång kan slutna system öppnas. Då det inte finns några system som med säkerhet är slutna, måste diskussionen om risker för kränkning av den personliga integriteten även föras när det gäller sådana register.

2. Avsikt och resultat

Vi måste också skilja mellan den avsikt som finns bakom registeranvändningen och de effekter som registret kan ha. Exempelvis kan avsikten med en sambearbetning av två olika register vara att uppnå något effektivitetsmål för myndigheten medan effekten kan vara att integritetskänsliga uppgifter får spridning.

3. Individmål eller samhällsmål
Syftet med att registrera personuppgifter kan antingen vara att uppnå ett individmål eller ett samhällsmål. Exempel på individmål är hälsojournaler som upprättas för att vara ett medel för individens hälsa, exempel på samhällsmål är att upprätta register som underlättar skatteindrivning.

4. Samtycke – icke samtycke
Register kan föras med den registrerades samtycke eller utan. Om ett informerat samtycke inhämtats från den enskilde personen är risken mindre att den personliga integriteten kommer att kränkas.

5. Identifiering – avidentifiering
Personuppgifter kan antingen föras så att de enskilda personerna går att identifiera genom namn och/eller personnummer eller också kan registret vara avidentifierat. Det går då inte att spåra vilka personuppgifter som gäller en bestämd individ. Dessa s.k. avidentifierade register utgör inte något hot mot personlig integritet.

6 Värdekonflikter

Många personregister är okontroversiella när det gäller risken för integritetskränkningar då de inte innehåller någon information som är integritetskänslig. När register som innehåller integritetskänslig information ska upprättas uppstår en värdekonflikt mellan å ena sidan värdet av att upprätta registret och å andra sidan den risk för integritetskränkning som uppstår.

Vi har tidigare hävdat att personlig integritet är en prima facie-rättighet. Det innebär att individer har moraliskt välgrundade anspråk att deras personliga integritet skyddas. Med beaktande av svårigheten att skydda personuppgifter i register kan en utgångspunkt för diskussionen om personregister vara att villkor för att få upprätta register där det finns integritetskänslig information är att dessa är avidentifierade eller baserade på informerat samtycke. Om dessa villkor inte kan uppfyllas måste det finnas starka skäl för att upprätta register. De mål som kan uppnås genom personregister kan då inte inom ramen för rimliga kostnader uppnås på annat sätt.

Vid beslut om behandling av personuppgifter, exempelvis genom upprättandet av dataregister, är det också nödvändigt att göra någon form av sannolikhetsbedömning av risken för integritetskränkning. Värdet av de mål som uppnås genom registrering måste vägas mot en bedömning av värdet av skyddet för den personliga integriteten och den sannolika risk

som föreligger att integritetskänsliga personuppgifter läcker ut ur systemet. Diskussionen om ett systems legitimitet gäller därför förutom frågan vilka känsliga uppgifter som ingår också frågan vilken säkerhet som är möjlig att uppnå och vilket eller vilka värden som systemet kan realisera.

Vilka värdekonflikter ger upprättandet av personregister upphov till? Vilka värden eller rättigheter är det som står emot varandra? Dessa frågor bör ställas och svaren preciseras inför varje upprättande av register och inför varje sambearbetning av registeruppgifter. Här ska jag endast antyda några värdekonflikter på en mer generell nivå.

Tre huvudtyper av register som gett upphov till offentlig diskussion kommer att behandlas. Register förs bl.a. av samhällsekonomiska skäl, av hälso- och sjukvårdsskäl och för brottsbekämpning.

Register med identifierbara personuppgifter upprättas för att upprätthålla en god skatteförvaltning och för att sociala förmåner och bidrag skall utbetalas på ett korrekt sätt. I det moderna, storskaliga samhället har denna typ av dataregister blivit nödvändig för att hushålla med begränsade ekonomiska resurser på ett optimalt sätt. Skattesystemet motiveras också av att det är ett medel att omfördela resurser i samhället för att uppnå en ökad jämlikhet. De värden som ligger till grund för denna typ av register är således både ekonomisk utveckling och jämlikhet.

Även om enskilda personer kan uppleva det som integritetskränkande att uppgifter om deras inkomst eller förmögenhet registreras är det svårt att uppfatta denna upplevelse som sakligt grundad. Det föreligger således knappast någon objektiv kränkning och därmed inte heller någon värdekonflikt.

Utifrån vårt förslag till precisering av begreppet personlig integritet kan en person som är berättigad till socialbidrag eller arbetslöshetsersättning uppleva det som en kränkning att han eller hon för att få bidrag måste registreras som bidragsmottagare respektive arbetslös. Onekligen kan vissa typer av offentliggörande av sådana uppgifter om den enskilde innebära en integritetskränkning. I detta sammanhang, när uppgifterna registreras i slutna register, kan man se det som en registrering som den enskilde ger sitt samtycke till, en registrering av detta slag är ju en nödvändig förutsättning för bidragssystemen och det finns därmed inte skäl för den registrerade att uppleva registreringen som kränkande.

Datoriserade journaler är ett exempel på behandling av personuppgifter inom hälso- och sjukvårdsområdet. Journaler innehåller ofta integritetskänsliga uppgifter. Dessa system har ett instrumentellt värde genom att de kan förbättra vården och därmed patienternas hälsa. Under förutsättning att

patienterna får information om hur datajournalen används kan även denna form av behandling av personuppgifter legitimeras utifrån ett informerat samtycke. Den som inte vill finnas med i en journal kan välja att avstå från sjukvård.

Ett av de mest omdiskuterade datoriseringsprojekten under senare år är FAS 90. FAS 90 är en förkortning för ”Framtida ADB-verksamhet för socialförsäkringen på 90-talet och därefter”. I FAS 90, som på grund av en proteststorm aldrig kom att realiseras, skulle sjukförsäkringsregistret med personuppgifter, sjukfallsregistret för redan pågående fall och historikregister för avslutade sjukdomsfall sammanföras med syftet att kunna upptäcka hälsovådliga arbetsplatser och arbetsmiljöer. De lokala sjukfallsregistren, som innehåller mycket integritetskänslig information, skulle finnas att tillgå på lokala socialförsäkringskontor.

FAS 90 ställde stora krav på en säker hantering av slutna system. Kritiker menade att det skulle vara omöjligt att undvika att uppgifter från ett stort antal lokala register läckte ut, trots stränga säkerhetskrav.

Genom FAS 90 skulle kunskapen om skadliga arbetsmiljöer öka och åtgärder för att förbättra dessa kunna vidtagas. Det värde som systemet syftade till att realisera var således en förbättad folkhälsa, vilket mer precist betyder bättre hälsa och minskad risk att dö i förtid för ett stort antal individer. Ett ställningstagande till denna typ av register förutsätter en vägning mellan å ena sidan värdet av en förbättrad folkhälsa och å andra sidan möjliga risker för integritetskränkningar. Man bör också ställa frågan om inte folkhälsovärdet kan uppnås på annat sätt.

Även frågan om upprättande av register över HIV-positiva individer väcker principiella frågor. Ett register av detta slag har motiverats med att det är nödvändigt för att begränsa spridningen av sjukdomen aids, t.ex. i samband med blodgivning. Det kan onekligen ses som en kränkning av den HIV-positives integritet att bli registrerad på detta sätt. Ser vi personlig integritet som en prima facie-rättighet finns det dock skäl att hävda att det sociala målet att begränsa spridningen av aids eller med rättighetstermer; medborgarnas rättighet att inte utsättas för HIV-smitta, väger så tungt att det berättigar att HIV-positiva personer utsätts för denna kränkning.

I samband med brottsbekämpning har man i USA öppna system med integritetskänsliga personuppgifter. Ett exempel är formerna för efterlysning av brottslingar. Där kan man på postkontor se fotografier av efterspanade brottslingar med personuppgifter. Man har uppenbarligen gjort den bedömningen att brottsbekämpning väger tyngre än respekten för brottslingars personliga integritet. I Sverige har man gjort en annan bedömning.

Register över brottslingar aktualiserar också en värdekonflikt. Skälet att föra register över brottslingar eller brottsmisstänkta personer är att det är ett viktigt led i brottsbekämpning att i spaningsarbete kunna leta i ett register efter möjlig gärningsman. Ytterst kan detta motiveras av medborgarnas behov av säkerhet och trygghet för liv och egendom.

Ett register över dömda brottslingar kan uppfattas som ett berättigat undantag från integritetsskyddet av ett annat skäl. Den som medvetet begår ett brott har därigenom ställt sig utanför det skyddsnät som omfattas av medborgarna i samhället. Han eller hon kan inte göra anspråk på alla de rättigheter som tillkommer den vanlige medborgaren. Genom att begå brottet har brottslingen själv valt att kunna bli utsatt för en integritetskränkning av detta slag.

Sambearbetning

Den etiska diskussionen om behandling av personuppgifter har bl.a. handlat om det berättigade i att sambearbeta olika register. När Arbetsmarknadsstyrelsen 1994 önskade sambearbeta register över personer som mottar arbetslöshetsersättning och personer som mottar ersättning från allmänna försäkringskassan väckte detta en omfattande debatt. Syftet med sambearbetningen var att kunna spåra personer som fuskar genom att för samma tid få del av båda typerna av ersättning.

Ett motiv som låg bakom sambearbetningen var det som vi sett ligger bakom ekonomiska register över huvud taget, dvs. att uppnå ett så optimalt resursutnyttjande som möjligt. Därutöver motiverades sambearbetningen med att man därigenom kunde motverka fusk och lagbrott, dvs. det fanns både etiska och juridiska motiv bakom sambearbetningen.

Är denna typ av sambearbetning av personregister moraliskt berättigad? Den som svarar nej på frågan kan hävda att åtgärden motiveras av en misstanke att de som uppbär arbetslöshetsersättning gör sig skyldiga till fusk. Att misstänkas för att ha fuskat innebär en kränkning av den personliga integriteten. Det som skiljer denna typ av ”brottsbekämpning” från annan är då att man frångår principen om att presumera individens oskuld innan en undersökning vidtas.

Den som svarar ja på frågan kan hävda att åtgärden inte föranleds av att varje person som mottar bidrag är misstänkt för fusk, utan att endast denna misstanke gäller några få. Därmed frångår man inte heller principen att presumera individens oskuld, åtminstone inte i större utsträckning än vid

en vanlig polisiär trafikkontroll. Att sambearbeta register på detta sätt innebär således inte i sig att de registrerades personliga integritet blir kränkt.

Denna typ av etisk konflikt kan naturligtvis enklast lösas genom att man innan man utför välmotiverade sambearbetningar inhämtar de registrerades informerade samtycke till att sådana bearbetningar kommer att genomföras.

7 Sammanfattning

I denna studie har jag hävdat att en kränkning av en persons integritet är en typ av kränkning av personen som sker när det görs ett intrång i personens privata sfär och/eller när det mot hans eller hennes vilja sprids uppgifter om egenskaper, uppfattningar och handlingar som det finns grund för att uppfatta som känsliga.

Man har rättighet till personlig integritet i första hand därför att respekten för den personliga integriteten är en del av respekten för personen, vilket kan uppfattas som en grundläggande plikt, men också för att det medför negativa följder om personers integritet inte respekteras. Rättigheten till personlig integritet kan dock inte vara absolut. Det finns situationer där andra värden än respekten för personlig integritet bör väga tyngre och därmed avgöra handlingens utfall.

BILAGA 5: ALLMÄNHETENS INSTÄLLNING

—

Rapport av Johan Åhlfeldt

Institutionen för socialmedicin
Uppsala universitet

INNEHÅLL:

Uppgiftslämnande och dataregistrering. Allmänhetens inställning 1970–1995

Av Johan Åhlfeldt

Inledning

I ett modernt samhälle används uppgifter om enskilda individer i en mängd olika sammanhang, både av offentliga och privata användare. Sedan automatisk databehandling blev kommersiellt gångbar i slutet av 1960-talet har bearbetningar av personuppgifter med hjälp av automatisk databehandling ökat mycket kraftigt. Det har inte bara ersatt manuella rutiner eller bearbetningar med annan äldre teknik utan också möjliggjort en ökad behandling av personuppgifter över huvud taget. I början av 1970-talet var bearbetning av uppgifter om enskilda med hjälp av automatisk databehandling relativt sällsynt och inskränkte sig till ett litet antal stora datorsystem, företrädesvis inom den offentliga sektorn men också inom stora företag i den privata sektorn. Tidiga datorsystem inom den offentliga sektorn byggdes ut inom folkbokföring och beskattning, den officiella statistiken och den statliga forskningen, hos polis- och åklagarväsendet samt hos försvaret. Inom den privata sektorn fanns tidigt datorsystem med personregister inom bank- och kreditväsendet. I dag möter den enskilde behandling av personuppgifter överallt. Många av de stora datorsystemen med centrala personregister är förvisso kvar men antalet mindre användare har också ökat. Tekniken har möjliggjort en både utvidgad och fördjupad användning av personuppgifter med stora möjligheter till utbyte av uppgifter mellan olika personregister. Detta har underlättats genom den utbredda användningen av gemensamma och unika identitetsbeteckningar – personnummer.

Sverige införde tidigt en dataskyddslagstiftning med syfte att reglera både privat och offentlig användning av automatisk databehandling av personuppgifter och värna den enskildes integritet, datalagen (1973:289). In-

rättande och förande av personregister krävde tillstånd från Datainspektionen. Undantagna var endast personregister vars inrättande beslutats av regering eller riksdag. Upptagningar på medium för automatisk databehandling hade en osäker status i tryckfrihetsförordningen då det inte klart framgick om de var att betrakta som allmänna handlingar. Frågan påkallade en snar lösning eftersom personuppgifter efterfrågades med stöd av offentlighetsprincipen av både privata och offentliga användare. Sekretesskyddet hade också allvarliga brister, särskilt när det gällde utbyte av uppgifter om enskilda individer myndigheter emellan. Dessa problem gav upphov till farhågor hos allmänheten om en ökad kontroll och en okontrollerad spridning av personuppgifter i samhället.

Syfte, metod och avgränsningar

Syftet med denna PM är att redogöra för forskningsläget om allmänhetens inställning till användningen av personuppgifter med hjälp av automatisk databehandling i samhället. I genomgången skall särskilt uppmärksammas hur allmänhetens inställning förändrats över tid och om inställningen varierar mellan olika grupper i samhället och mellan olika regioner. I Sverige har Statistiska centralbyrån (SCB) undersökt allmänhetens inställning till personregister på data, särskilt med hänsyn till användningen av ADB för framställning av officiell statistik. SCB har även undersökt allmänhetens attityder till Statistiska centralbyrån som producerar (ansvarade) för merparten av den officiella statistiken. Bakgrunden till dessa undersökningar var tilltagande problem med att upprätthålla en hög svarsfrekvens i statistiska undersökningar som SCB och andra statistikproducenter samt företrädare för forskningen började uppleva i början av 1970-talet.

I denna redogörelse undersöker jag användningen av personuppgifter i både privat och offentlig sektor. Personuppgifter är uppgifter om enskilda fysiska personer som kan hänföras till enskild person med namn, personnummer eller annan beteckning som gör det möjligt att identifiera den enskilde. Jag ansluter mig här till samma definition av begreppet som förekommer i datalagen (1973:289) och som avses med uppgift om enskild i allmän handling i sekretesslagen (1980:100). Behandling av personuppgifter sker i dag i mycket stor utsträckning med hjälp av automatisk databehandling (ADB). Denna användning har väckt farhågor om de registrerades personliga integritet. Datalagen har till uppgift att förhindra otillbörliga intrång i de registrerades personliga integritet i samband med inrättande

och förande av personregister. Denna redogörelse handlar uteslutande om behandling av personuppgifter med sådan teknik. Användning av avidentifierade eller anonymiserade uppgifter om enskilda faller utanför denna rapport liksom manuell behandling av personuppgifter. Det har diskuterats om inte statistikproduktionen och forskningen i mycket högre grad än i dag kan klara sin verksamhet med användning av sådana uppgifter. Denna fråga liksom frågan om behovet av personregister för olika ändamål behandlas inte här. Hanteringen av personuppgifter med data för uteslutande privat bruk omfattas inte heller av redogörelsen.

Att lämna en redogörelse över kunskapsläget om allmänhetens inställning till behandlingen av personuppgifter i samhället är en mycket omfattande uppgift. För att ge en bra överblick måste framställningen göras systematiskt. Det faktum att forskningsresultat saknas på vissa områden är av intresse i sig. Till min hjälp har jag ansett det nödvändigt att utveckla begrepp som kan relateras till varandra och analytiskt belysa rapportens frågeställningar.

Att jämföra människors föreställningar och attityder över en tidsperiod på över 20 år är problematiskt eftersom de teknologiska, sociala, legala och politiska förutsättningarna för behandling av personuppgifter i hög grad har förändrats. De föreställningar och attityder människor i dag redovisar eller redovisade vid tidigare undersökningstillfällen är vid tidpunkten resultatet av ett komplicerat samspel mellan olika faktorer. Särskilt iögonfallande är naturligtvis den snabba teknologiska utvecklingen på området. Insamling, bearbetning, bevarande och utlämnande av personuppgifter äger rum i situationer där enskilda individer träder in i bestämda sociala relationer till de som samlar in och behandlar personuppgifter. Dessa situationer har också förändrats i termer av auktoritet, demokratisering och utbildning för att nämna några betydelsefulla förändringar, om än inte lika dramatiskt. Även om vi analytiskt kan definiera begrepp som ”personuppgift” och ”personregister” med giltighet över tid, refererar dessa till olika innehåll vilket i sin tur styr människornas erfarenhetsrum och förväntningshorisont.

Jämförelse över tid möjliggörs genom ett antal undersökningar om allmänhetens syn på automatisk databehandling och integritet, alltsedan utvärderingen av folk- och bostadsräkningen 1970 till vår undersökning ”Medborgarna och forskningen” 1995. Jag skall här kortfattat presentera dessa undersökningar.

År 1976 genomförde Statistiska centralbyrån en undersökning om allmänhetens inställning till integritetsfrågor i allmänhet och till SCB:s sta-

tistikproduktion i synnerhet. Undersökningen gjordes på uppdrag av en inom verket tillsatt utredning rörande uppgiftslämnar- och bortfallsproblem i statistikproduktionen. SCB hade uppmärksammat att vägrarbortfallet i urvalsundersökningar ökat, trots stora informationsinsatser riktade till uppgiftslämnarna. Den nyinrättade tillstånds- och tillsynsmyndigheten Datainspektionen hade aviserat en restriktivare hållning mot metoder för att kompensera bortfall i urvalsundersökningar, imputering och indirekta intervjuer. Undersökningen genomfördes som en del av SCB:s Omnibus, och var en intervjuundersökning som omfattade personer kyrkobokförda i Sverige i åldern 16–74 år. Urvalet omfattade 1 271 personer och svarsfrekvensen uppgick till 78 procent.[525] SCB har redovisat resultatet i rapporten *SCB och allmänheten* (SCB, Stockholm, 1977). De flesta frågor i undersökningen redovisas i tabellform uppdelat på variablerna kön, utbildning, boenderegion och yrkesställning.

Under början av 80-talet hade integritetsfrågorna fått ökad aktualitet i debatten. Våren 1984 tillsattes en statlig kommitté, Data- och offentlighetskommittén (DOK), som hade till uppgift att utreda användningen av personnummer i samhället. Statistiska centralbyrån genomförde samma år ytterligare en undersökning om integritetsfrågor och allmänhetens inställning till SCB. Resultatet från denna undersökning redovisades i rapporten *Data och integritet* (SCB, Stockholm 1985). Till vissa delar replikerade denna undersökning den tidigare från 1976. Undersökningen genomfördes med hjälp av besöksintervjuer och vände sig till befolkningen i åldern 18–74 år. Urvalet omfattade 1 020 personer och av dessa medverkade 75 procent.[526] De flesta frågor i undersökningen redovisades i en tabellbilaga till rapporten. Svarsfrekvensen för dessa variabler särredovisas mot bakgrundsvariablerna kön, ålder och utbildning. Vissa variabler särredovisades också mot boenderegion och kunskap om datorer.

DOK gav 1986 Statistiska centralbyrån i uppdrag att undersöka allmänhetens inställning till personregister och personnummer. SCB kompletterade för egen räkning frågeformuläret med några frågor om allmänhetens uppfattning om statistikproduktionen. Undersökningen genomfördes med hjälp av en postenkät till personer i åldern 16–74 år. Urvalet omfattade 1 200 personer och den vägda svarsfrekvensen efter två på-

---

525 *SCB och allmänheten. Resultat från en intervjuundersökning våren 1976.* Statistiska centralbyrån, I/Utredningsinstitutet, Stockholm 1977-01-17.

526 Data och integritet. Allmänhetens kunskaper och attityder allmänt och till SCB. Statistiska centralbyrån/Utredningsinstitutet, Stockholm, mars 1985.

minnelser beräknades till 78 procent.[527] Resultatet av undersökningen redovisades dels i Data- och offentlighetskommitténs betänkande SOU 1987:31 *Integritetsskyddet i informationssamhället 4*, (Stockholm 1987) dels i SCB:s rapport *SCBs image 1986* (SCB, Stockholm 1987). I betänkandet redovisades inga råtabeller och redovisningen av svarsfördelningar för vissa frågor är ofullständig. I SCB:s rapport fanns en tabellbilaga men redovisningen omfattade endast frågorna som SCB själv ansvarade för.

Förutom dessa tre attitydundersökningar har Statistiska centralbyrån gjort utvärderingar av informationskampanjerna i samband med Folk- och bostadsräkningarna FoB 65, FoB 70, FoB 75 och FoB 80. Dessa undersökningar kom i ökad omfattning att innehålla frågor om integritet och registrering av personuppgifter för statistikproduktion.[528] Våren 1975 genomförde SCB på uppdrag av en utredning om integritetsskyddsåtgärder inom statistikproduktionen, en undersökning om olika personuppgifters känslighet.[529]

Inom forskningsprojektet ”Medborgarnas deltagande i forskning – Effektivitet och legitimitet i användning av personuppgifter i forskning och statistik” vid Institutionen för socialmedicin, Uppsala universitet genomfördes i samarbete med Hälsodatakommittén (S 1994:31) under våren 1995 en postenkätundersökning. Syftet var att undersöka allmänhetens inställning till att bidra med personuppgifter och i vissa fall mänsklig vävnad för forskning. Ett annat syfte var att undersöka allmänhetens inställning till att redan befintliga uppgifter hos myndigheter och företag används för forskning och statistik. Undersökningspopulationen omfattade personer i åldern 18–74 år och urvalet uppgick till 1 501 personer. Den vägda svars-

---

527 *SCBs image 1986*. Statistiska centralbyrån/utredningsinstitutet, Stockholm 1987.

528 Wärneryd, Bo ”Allmänhetens inställning till folk- och bostadsräkningen 1970” *Statistisk tidskrift* 1972:3. Rudén, Britt. *Information om FoB 75*, SCB, U/UI, Stockholm 1976-02-25. Davidsson, G. *FoB 80. Utvärdering av informationskampanjen. Allmänheten*. Statistiska centralbyrån, Stockholm 1982. Undersökningen omfattade personer i åldern 16 år och äldre och genomfördes som en besöksintervju med telefonuppföljning. Urvalet omfattade 807 personer och svarsfrekvensen uppgick till 83 procent.

529 Langlet, Pieter. *Undersökning rörande personuppgifters känslighet*. SCB U/UI, Stockholm 1975-10-29. Undersökningen ingick i SCB:s Omnibus juni 1975. Svarsfrekvensen var ovanligt låg, endast 64 procent. Personuppgifter om ekonomi, vilket parti man hade röstat på i riksdagsval och kontakter med vårdgivande myndigheter ansågs mest känsliga.

frekvensen efter två påminnelser och telefonuppföljning beräknades till 69 procent.[530] Några frågor från SCB:s tidigare undersökningar upprepades för att möjliggöra jämförelser över tid. De flesta av dessa frågor kom dock att omarbetas antingen genom att svarsalternativen eller frågornas formulering ändrades något. Med ledning av resultatet från en provundersökning förtydligades bl.a. frågan om överföring av redan insamlade folkbokföringsuppgifter. För urvalspersonen betonades att det handlade om uppgifter med personnummer.[531]

Begreppslig ram

Behandling av personuppgifter kan förstås som en process som antingen syftar till att framställa upplysningar som ett led i att vidta administrativa åtgärder/fatta beslut om enskilda, eller som syftar till att producera generell kunskap om människa och samhälle. Till det förra fallet räknas all administration och beslutsfattande mot enskilda för att fördela och leda arbete, för att sälja och köpa varor och tjänster, eller för att administrera individens skyldigheter och rättigheter gentemot offentlig myndighet. Exempel på sådana ändamål kan vara anställning, arbetsledning, försäljning, hälso- och sjukvård, barnomsorg, taxering och folkbokföring. För den enskilde har besluten som fattas eller åtgärderna som vidtas positiva eller negativa

---

530 Undersökningen genomfördes inom ramen för forskningsprojektet *Medborgarnas deltagande i forskning – Effektivitet och legitimitet i användningen av personuppgifter i forskning och statistik* med stöd från Socialvetenskapliga forskningsrådet (SFR) SFR-93-0135:1A. Projektledare var professor Tom R Burns, Sociologiska institutionen. Övriga projektmedlemmar var professor Claes-Göran Westrin, Institutionen för socialmedicin och FK Johan Åhlfeldt, Sociologiska institutionen och Institutionen för socialmedicin, Uppsala universitet. Hälsodatakommittén (S 1994:31) bidrog till undersökningens finansiering och medverkade i konstruktionen av frågeformuläret i vissa delar.

531 I SCB:s undersökning från 1984 löd frågan ”För bl.a. folkbokföring och beskattning har myndigheterna personregister på data. Där finns t ex följande uppgifter om Dig: personnummer, namn, civilstånd, adress, antal barn, inkomst, fastighetsinnehav och medborgarskap. Tycker Du att det är riktigt att de här uppgifterna skulle kunna föras över till ”. I vår undersökning var ingressen till frågan, de uppräknade myndigheterna och företagen desamma som i SCB:s fråga. Själva frågan fick följande lydelse: ”Tycker Du att det är riktigt att uppgifter med personnummer om folkbokförda skall få föras över till…”. Detta förtydligande bedömdes som nödvändigt eftersom flera i provundersökningen hade uppgivit att deras ställningstagande var beroende av om uppgifterna var avidentifierade eller ej.

konsekvenser. Individen blir behandlad för en sjukdom eller skada han lider av, den anställde får sin arbetsinsats utvärderad och den kreditsökande får en kredit beviljad.

I det senare fallet är intresset för individen helt underordnat. Här är det i stället många individers handlingar, verksamheter eller förloppet av en händelse som är av intresse. Behandlingen av personuppgifter är då ett led i utvärderingen och planeringen av sociala aktiviteter och verksamheter, eller att framställa generellt giltig kunskap om människan och samhället. Produktion av kunskap syftar inte till att fatta beslut eller vidta åtgärder mot enskilda individer i administrativt syfte och behandlingen av personuppgifter har därför inga avsedda konsekvenser för den enskilde. Exempel på sådana ändamål är journalistik, forskning, samhällsplanering och utvärdering av privata och offentliga verksamheter. Behandling av personuppgifter för dessa båda ändamål är naturligtvis centrala funktioner för både privata och offentliga samhällsinstitutioner.

Den process som vi benämner behandling av personuppgifter omfattar fyra moment, *insamling* och *bearbetning* av uppgifter om enskilda individer. När uppgifterna bearbetats tillkommer ytterligare moment i *bevarande* och *utlämnande* av personuppgifter. Två parter är alltid involverade, den som efterfrågar, samlar in och bearbetar uppgifter och den som lämnar uppgifter. Uppgiftslämnaren är oftast den som uppgifterna refererar till, dvs. att den enskilde individen lämnar uppgifter om sig själv.[532] Sedan uppgifterna samlats in och bevarats (lagrats) kan den som först samlade in uppgifterna komma att bli uppgiftslämnare om någon annan efterfrågar uppgifterna. Ett sådant utlämnande har dock alltid föregåtts av enskildas uppgiftslämnande, ibland i samband med direkt observation t.ex. en läkarundersökning.

---

532 Uppgifter om en person kan också lämnas av andra privatpersoner, t.ex. vårdnadshavare eller förmyndare. Vid sjukdom eller olycksfall kan närstående lämna uppgifter om den som insjuknat eller skadats om denne är oförmögen att göra det själv. Vardagslivet innehåller också andra situationer då vänner, grannar, arbetskamrater kan bli uppgiftslämnare om förhållanden som berör en annan person än dem själva. De som blivit vittne till brott är skyldiga att inför polis och domstol uppge vad de har iakttagit om den som är misstänkt för brott.

Uppgifter om enskilda kan också samlas in genom direkt observation. Med observation avses insamling av uppgifter genom kroppsundersökning, provtagning, iakttagelse av beteende och aktivitet. Direkt observation kan vara öppen som vid en läkarundersökning, eller dold, t.ex. när polisen bedriver spaning mot misstänkta.

Den långtgående automatiseringen har inneburit en ökad teknisk-administrativ kapacitet att behandla personuppgifter. I de olika momenten handlar det dock inte bara om ett *instrumentellt* förfogande av personuppgifter utan det finns i varierande grad inslag av *kommunikativt* handlande. Det instrumentella handlandet värderas utifrån effektivitet. Det innebär att insamling, bearbetning, bevarande (lagring) och utlämnande av personuppgifter skall ske snabbt, med hög säkerhet och till en låg kostnad. Datateknikens utveckling har i denna mening möjliggjort en ökad effektivitet som vi ännu inte ser slutet på. Det kommunikativa handlandet däremot tar sin utgångspunkt i att samförstånd om villkoren för behandling av personuppgifter måste uppnås mellan dem som uppgifterna avser och den som behandlar uppgifterna. Detta anspråk bottnar naturligtvis i de förväntade eller upplevda konsekvenserna för den enskildes personliga integritet. Samförstånd krävs för att verksamheten skall åtnjuta de berördas förtroende och acceptans både när det gäller insamling av uppgifter från individerna själva eller den vidare behandlingen av dessa. Att uppnå samförstånd handlar inte enbart om på vilka grunder ett uppgiftslämnande kommer till stånd och vilka uppgifter som lämnas ut. Den enskildes anspråk berör även honom i egenskap av registrerad och vad som sker med uppgifterna under bearbetningen (t.ex. frågan om vilka bearbetningar och för vilka ändamål de får göras), bevarandet (t.ex. hur länge uppgifterna får bevaras) och utlämnandet (t.ex. till vem och för vilka ändamål får uppgifterna lämnas ut). I uppgiftslämnarsituationen har den enskilde att ta ställning till alla momenten av behandling av personuppgifter. Under vår undersökningsperiod, då den tekniskt-administrativa kapaciteten har ökat, har betydelsen av det kommunikativa inslaget i processen också kommit att öka, både i form av uppgiftslämnarnas krav på information och medbestämmande, men också författningsregleringen och inte minst andra arrangemang i form av t.ex. etiska kommittéer och riktlinjer.

Samförstånd om formerna för behandling av personuppgifter kan uppnås på olika sätt, antingen genom överenskommelse mellan uppgiftslämnaren och den som behandlar uppgifterna eller bestämmelser i författning. Kan sådant samförstånd vid en viss tidpunkt och i en viss social situation inte uppnås kan det få till följd att den instrumentella kapaciteten inte kan utnyttjas i enlighet med dess egna tekniska och administrativa förutsättningar.

Den specifika reaktionen från uppgiftslämnarna eller de registrerade bestäms ytterst av grunden för uppgiftslämnandet, om den är ett fullgörande av ett avtal eller en plikt, eller om uppgiftslämnandet är frivilligt.

Typiska reaktioner är att människors beredvillighet att frivilligt lämna uppgifter minskar, att människor medvetet lämnar felaktiga eller ofullständiga uppgifter, att människor undandrar sig kontakt med myndigheter och företag av rädsla och olust, samt att människor ger uttryck för protester, antingen direkt till dem som efterfrågar uppgifter eller offentligt för att skapa opinion för politisk förändring. Vilken reaktion som är den typiska bestäms av den enskildes handlingsutrymme i uppgiftslämnarsituationen. ”Protest” är typisk för situationer då den enskilde av antingen formell skyldighet eller materiell nödvändighet är tvungen att lämna uppgifter. ”Sorti” är en typisk respons i situationer när uppgiftslämnandet saknar direkta konsekvenser för den enskilde, dvs. då det är frivilligt.[533]

Vi har diskuterat flera omständigheter som talar för att förhållandet mellan de instrumentella och de kommunikativa aspekterna av behandlingen av personuppgifter blivit problematiska. Det finns också omständigheter som inte inverkar restriktivt på processens instrumentella effektivitet. Hos allmänheten finns ett starkt uttryck för att myndigheterna och företagen skall utnyttja den ökade kapaciteten för att minimera kreditrisker, kartlägga hälsorisker, att hålla samhällsservice tillgänglig och rätt avpassad till befolkningens behov, att ”bidragsfusket” skall stoppas, att kriminalitet skall bekämpas – åtgärder som ofta innebär att ett stort antal och känsliga uppgifter om enskilda individer samlas in och bevaras under lång tid och att redan insamlade uppgifter sambearbetas. Med en utbredd registrering av personuppgifter i samhället måste kanske den enskilde själv balansera effektivitet och integritet, antingen det sker i form av ökade krav på information och inflytande som uppgiftslämnare och registrerad eller att som samhällsmedborgare delta i den offentliga diskussionen om denna avvägning. Detta ger upphov till intressanta frågor inför redovisningen av det empiriska materialet.

Omfattningen och djupet av behandling av personuppgifter i samhället bestäms dels utifrån vad som är tekniskt-administrativt möjligt (kostnadnytta), dels vad som är tillåtet (eller inte uttryckligen förbjudet) inom ramen för de rättsliga regler som gäller för användningsområdet (legalitet),

---

533 Sedan uppgifterna insamlats och behandlingen av personuppgifter fortsätter har den enskilde uppgiftslämnaren inte lika stora möjligheter att utöva inflytande. Uppgifter i allmänna handlingar som åtnjuter sekretess har den enskilde rätt att efterge sekretess. Datalagens 10 § ger den enskilde möjlighet att kontrollera vilka uppgifter som lagrats och om de inte är korrekta, att få uppgifterna rättade. Protest är annars en vanlig reaktion från de registrerade sedan en viss behandling uppmärksammats eller beslutats efter att uppgifterna samlats in.

dels vad som överenskommits mellan avtalsparter, dels vad som kan göras för att upprätthålla förtroende för behandlingen av personuppgifter så att t.ex. enskilda individer lämnar uppgifter över huvud taget och att lämnade uppgifter är fullständiga och sanningsenliga (legitimitet). En viss praxis för att garantera verksamhetens legitimitet kan vara stadfäst som bindande etiska regler för en bransch (t.ex. direktreklam), för en profession (läkare) eller för en verksamhet (forskningsetiska regler). För behandling av personuppgifter, där de tekniska och ekonomiska förutsättningarna förändras mycket snabbt, kan vi anta att det tekniskt-administrativa användningsområdet hela tiden varit större än det legalt tillåtna och det socialt accepterade. Det finns också ett samband mellan legalitet och legitimitet. Blir gapet mellan vad som är rättsligt tillåtet (eller inte uttryckligen förbjudet) och vad som av en större opinion betraktas som oacceptabelt finns det förutsättningar för en politisk förändring av rättsbestämmelserna.

Avvägningen mellan de instrumentella och de kommunikativa aspekterna av behandling av personuppgifter sker inte bara hos dem som behandlar uppgifter utan också hos dem som lämnar uppgifter och blir registrerade. Den enskilde individen värderar å ena sidan nyttan av en effektiv behandling för honom själv, för den grupp han tillhör eller för samhället i stort, allt efter det ändamål för vilket behandlingen vidtas, och å andra sidan villkoren för behandlingen så att hans förtroende och acceptans kan upprätthållas. Denna avvägning sker inom ramen för den sociala relation uppgiftslämnaren eller den registrerade har till den som behandlar personuppgifter.

Grunden för uppgiftslämnande bestäms av vad för slags social relation som finns mellan den enskilde individen och den som behandlar uppgifter om honom. Denna grund består antingen av ett avtal eller ett pliktförhållande. Ett avtal baseras på förväntningar om ömsesidig nytta mellan parterna och motiveras av deras egenintresse. Ett pliktförhållande baseras på förväntningar om gillande eller ogillande från omgivningen riktat mot den enskilde. Reaktionen från omgivningen kan vara legalt eller normativt sanktionerad.

Avtalet reglerar vilka prestationer som kan förväntas av parterna, t.ex. att den enskilde skall lämna ut vissa uppgifter om sig själv till den som tillhandahåller en anställning, en bostad, en vara eller en tjänst. Detta berör

den enskilde i egenskap av *anställd* och *kund*.[534] Inom det privaträttsliga området kan det också finnas bestämmelser som reglerar vilka uppgifter som över huvud taget kan efterfrågas. Det kan vara kollektivavtal och bestämmelser i författning. Grunden för uppgiftslämnande kan också baseras på medlemskap i en organisation. *Medlemmar* kan sägas ha överenskommit med medlemsorganisationen att lämna uppgifter om sig själva om det innefattas av medlemskapet. Normativt sanktionerade pliktförhållanden i den privata sektorn finns mellan *privatpersoner* och organisationer. Den kan bestå i att organisationer vädjar till allmänheten om ekonomiska bidrag eller andra frivilliga insatser. Enskilda individers uppgiftslämnande till privata företag för opinions- och marknadsundersökningar är exempel på detta. Även enskildas uppgiftslämnande till massmedia räknas hit, i den mån det inte förekommer ekonomisk ersättning.

Legala pliktförhållanden förekommer uteslutande i enskildas relation till offentlig myndighet. I ett legalt pliktförhållande är omfattningen av en uppgiftsskyldighet för den enskilde reglerad i lag. För t.ex. taxerings- och folkbokföringsändamål finns en lagstadgad uppgiftsskyldighet för den enskilde. Om den enskilde inte fullgör sin plikt riskerar han att tvångsåtgärder vidtas mot honom. Även utan en formell uppgiftsskyldighet kan den enskilde vara tvingad att lämna uppgifter om sig själv som ett villkor för att få rätten till bistånd bedömd eller för att få adekvat vård och behandling. Sanktionen i detta fall är utebliven ersättning, understöd eller vård. Den enskilde kan då sägas vara föremål för ett administrativt tvång t.ex. i fråga om hälso- och sjukvård, socialförsäkring och socialtjänst. När den enskilde är föremål för en lagstadgad skyldighet eller ett politiskt-administrativt tvång är det i relationen som *klient* till en offentlig myndighet.

Medborgarskapet kan också innebära förpliktelser som inte formulerats som lagstadgade skyldigheter eller välfärdspolitiska rättigheter. När en offentlig myndighet efterfrågar insatser från den enskilde i form av uppgiftslämnande för samhällsplanering, officiell statistik, forskning, eller i form av vävnadslämnande för vård av annan person (blodtransfusion, transplantation) och medicinsk forskning är det den enskilde i egenskap av *medborgare* myndigheten adresserar. Förpliktelsen är normativ eftersom

534 Den enskilde kan också vara anställd och kund till offentliga förvaltningar i den mån de tillhandahåller anställning, varor och tjänster och de är baserade på ett privaträttsligt avtal. Även privata medlemsorganisationer kan ha anställda.

den saknar tvångsmaktens sanktion och appellerar till den enskildes solidaritet och identifikation med det allmänna bästa.[535]

Figur 1 sammanfattar behandlingen av personuppgifter i samhällets privata och offentliga sektor med avseende på ändamålet med behandlingen och relationen mellan uppgiftslämnaren och den som använder uppgifterna. Två situationer av uppgiftslämnande särskiljs, när uppgifter inhämtas från den enskilde uteslutande på basis av uppgifter som denne lämnar, och när inhämtandet av uppgifter också (eller uteslutande) sker på basis av direkt observation av individens inre kroppsliga och själsliga tillstånd, eller individens yttre beteende. Figuren beskriver en rad olika situationer för uppgiftslämnande alltifrån ifyllandet av ett enkätformulär på frivillig grund i individens eget hem till en kroppsundersökning under tvång på anstalt.

Behandling av personuppgifter kan antingen syfta till att framställa upplysningar för administration av enskilda individer (för att fatta beslut eller vidta åtgärd), eller framställa kunskap om människa och samhälle. För administrativa ändamål baseras uppgiftslämnandet på avtal, medlemskap, administrativt och lagstadgat tvång. När uppgifter inhämtas för planering, utvärdering och forskning är enskildas uppgiftslämnande baserat på normativ förpliktelse (frivillighet).[536]

---

535 Även de lagstadgade skyldigheterna innehåller element som upprätthålls normativt. För det är ju inte enbart hotet om rättsliga sanktioner som får medborgarna att inställa sig till värnplikt och som vittnen i domstol samt att betala skatt.

536 I den senaste folk- och bostadsräkningen (FoB 90) förelåg uppgiftsskyldighet för folkbokförda att lämna hushålls- och fastighetsuppgift till Statistiska centralbyrån. Syftet med FoB 90 var enbart att skapa ett underlag för officiell statistik, samhällsplanering, forskning och allmän information, inte som tidigare att samtidigt kontrollera folkbokföringen. Undersökningen kan sägas utgöra ett undantag från sambandet mellan grund för uppgiftslämnande och ändamål med behandling av personuppgifter.

Figur 1: Behandling av personuppgifter i samhället. Enskildas uppgiftslämnande och direkt observation.

	Personuppgifter insamlas av			
	privat företag, medlemsorganisation		**offentlig myndighet**	
Verksamhetens ändamål	**administrativt**	**icke-administrativt**	**administrativt**	**icke-administrativt**
Uppgiftslämnarens relation till användare	*kund, anställd, medlem*	*privatperson*	*klient*	*medborgare*
Personuppgifter				
inhämtas genom direkt observation	kliniska undersökningar i privat hälso- och sjukvård och företagshälsovård, övervakning av anställda: **avtal**	kliniska undersökningar i privat forskning, journalistik: **frivillighet**	kliniska undersökningar i hälso- och sjukvården: **administrativt tvång**. psykiatrisk tvångsvård, kriminalvård, allmän försäkring, arbetarskydd, rättegångsbalken, polisspaning: **legalt tvång**	kliniska undersökningar i offentlig forskning, blodgivning, organdonation: **frivillighet**
lämnas av den enskilde själv	administration av kunder, anställda och medlemmar: **avtal; medlemskap**	marknads- och opinionsundersökningar, journalistik: **frivillighet**	folkbokföring, beskattning: **uppgiftsskyldighet.** allmän försäkring, hälso- och sjukvård, socialtjänst: **administrativt tvång**	statistiska urvalsundersökningar: **frivillighet**. folk- och bostadsräkning: **uppgiftsskyldighet**

Vi skall nu återvända till problematiken omkring utlämnande av befintliga uppgifter om enskilda individer hos organisationer respektive myndigheter i privat och offentlig sektor. Som vi sett av ovanstående genomgång är det uppgifter om individer i egenskap av anställda och kunder, medlemmar, klienter, privatpersoner och medborgare. Grunden för uppgiftslämnande varierar med relationen mellan den enskilde uppgiftslämnaren och den som samlar in och bearbetar uppgifterna. Uppgifter om enskilda personer har olika status beroende på var de bevaras. En grundläggande distinktion går mellan privata organisationer och offentliga myndigheter. Alla handlingar med uppgifter om enskilda i den privata sektorn är till sin natur privata. Utlämnande av uppgifter till andra än avtalsparterna får ske endast med stöd av avtalet. Statsmakterna kan dock i lag ålägga enskilda företagare och näringsidkare att lämna uppgifter till myndigheter, t.ex. arbetsgivares skyldighet att lämna kontrolluppgift om anställda till skattemyndigheten. Huvudregeln i den offentliga sektorn däremot är att allmänna handlingar med uppgifter om enskilda är offentliga och måste lämnas ut till den som efterfrågar uppgiften (TF). Känsliga uppgifter i allmänna handlingar

skyddas dock av sekretess med hänsyn till enskilds ekonomiska eller personliga förhållanden (sekretesslagen 1980:100). Sekretessen kan vara absolut eller göras till föremål för en prövning om skada och men för den enskilde om uppgiften lämnas ut. Den enskilde kan helt eller delvis efterge sekretess som gäller till förmån för honom själv.

Datalagen (1973:289) tar sin utgångspunkt i det förhållandet att behandling av personuppgifter med hjälp av automatisk databehandling kräver ett särskilt skydd för den enskildes integritet som inte kan upprätthållas med grundbestämmelserna om offentlighet och sekretess eller avtalsrätt i den privata sektorn. Lagstiftning om integritetsskydd är ett uttryck för att statsmakterna vill ha kontroll över behandlingen av personuppgifter i samhället. Den som avser att inrätta och föra ett personregister måste i dag anmäla detta till Datainspektionen och få licens. I vissa fall då känsliga uppgifter skall registreras måste den registeransvarige ansöka om tillstånd. Personregister som beslutats av statsmakterna är undantagna från tillståndsplikten.

Distinktionen mellan privat och offentligt är viktig i en diskussion om utlämnande av befintliga personuppgifter. Uppgifter kan lämnas ut från privata respektive offentliga organisationer och myndigheter och lämnas till både privata och offentliga användare. Tar vi i beaktande för vilket ändamål uppgifterna ursprungligen samlades in samt för vilket ändamål de skall användas får vi åtta olika fall att diskutera. Samutnyttjande och sambearbetning av personuppgifter är mycket vanlig och sker ofta med hjälp av automatisk databehandling. Både inhämtande och utlämnande av personuppgifter som skall ingå respektive ingår i personregister är föremål för författningsreglering genom datalagen. Vi måste också göra skillnad på om den som förfogar över uppgifter enligt lag är skyldig att lämna ut uppgifter[537] eller om det sker med stöd av avtal mellan den enskilde som uppgifterna refererar till eller med stöd av dennes frivilliga samtycke. Skall uppgifter som lämnas ut ingå i personregister hos någon annan och utlämnandet inte sker med stöd av den enskildes samtycke, författning eller tidigare tillstånd från Datainspektionen måste den som vill inrätta ett sådant personregister söka tillstånd. Den som lämnar ut uppgifter är också skyldig att

---

537 Uppgiftsskyldighet kan bestå av att en privat organisation eller myndighet enligt lag är skyldiga att regelmässigt lämna ut uppgifter om anställda, kunder, medlemmar och klienter till myndighet. Offentlighetsprincipen stadgar också en skyldighet för myndigheter att lämna ut uppgifter till den som efterfrågar dem om uppgifterna inte skyddas av sekretess.

se till att uppgifter inte används i strid med de övriga bestämmelserna i datalagen.

Vilka möjligheter har då den enskilde att få information och påverka om uppgifter som han lämnat tidigare lämnas ut till någon annan? Datainspektionen skall i sin tillståndsgivning särskilt beakta inställningen hos dem som skall komma att registreras. Det har bl.a. utmynnat i krav på underrättelse och inhämtande av samtycke från de registrerade.

All uppgiftsskyldighet för enskilda juridiska personer, kommuner och landstingskommuner till statliga myndigheter måste ha stöd i lag. I modern lagstiftning som berör inrättande och förande av centrala personregister hos myndigheter finns bestämmelser om information till de registrerade.

Figur 2: Behandling av personuppgifter i samhället. Utlämnande av uppgifter från myndigheter och medlemsorganisationer.

	Personuppgifter insamlas av			
	privat företag, medlemsorganisation		**offentlig myndighet**	
Verksamhetens ändamål	**administrativt**	**icke-administrativt**	**administrativt**	**icke-administrativt**
Den registrerades relation till användare	*kund, anställd, medlem*	*privatperson*	*klient*	*medborgare*
Personuppgifter lämnas ut av				
Företag eller medlemsorganisation (om anställda, kunder och medlemmar)	personupplysning inkassoåtgärd: **avtal**		smittskydd, kontrolluppgifter från arbetsgivare, banker och försäkringsbolag: **uppgiftsskyldighet enligt lag**	uppgiftslämnande till den officiella statistiken: **uppgiftsskyldighet enligt lag**
Myndighet (om klienter och patienter)	ärenden hos kronofogden: **offentlighetsprincipen (TF); uppgiftsskyldighet enligt lag**. patientuppgifter vid tecknande av privat försäkring: **medgivande från enskild (SekrL)**	värvning av kunder, anställda och medlemmar, urvalsdragning och bortfallsanalys: **offentlighetsprincipen (TF), Datalagen, SPAR, spärr mot direktreklam**	kontroll av rätt till förmåner: **uppgiftsskyldighet enligt lag eller offentlighetsprincipen (TF)**	samhällsinformation, urvalsdragning och bortfallsanalys, registerundersökningar: **uppgiftsskyldighet enligt lag eller offentlighetsprincipen (TF), medgivande från enskild (SekrL)**

Resultat

Redovisningen av tidigare forskningsresultat disponeras på följande sätt. Ur integritetssynpunkt är det centralt hur och från vem uppgifterna inhämtas. Jag har valt att låta detta styra framställningen. I modellen ovan har

följande situationer för uppgiftslämnande särskilts. Direkt observation, uppgiftslämnande från den enskilde själv, från företag eller organisationer om anställda, kunder och medlemmar, samt från offentlig myndighet (statlig, landstingskommunal, kommunal) om klienter. Jämförelser möjliggörs horisontellt i modellen, dvs. vi kan göra jämförelser om allmänhetens inställning till behandling av personuppgifter mellan verksamheter för olika ändamål (administrativa och icke-administrativa ändamål) inom respektive privat och offentlig sektor såväl som mellan samhällssektorer.

Direkt observation

Direkt observation förekommer i praktiker såsom kliniska undersökningar (medicinska, psykiatriska, psykologiska). Sådana praktiker finns i både privat och offentlig verksamhet, företagshälsovård, allmän och privat hälso- och sjukvård. De kan initieras av försäkringsbolag, arbetsgivare, allmän försäkringskassa, Arbetarskyddsstyrelsen, polis, åklagare och militär myndighet. När den allmänna hälso- och sjukvården tar initiativ till undersökning av enskilda benämns det screeningverksamhet. Den kan vara inriktad på att upptäcka viss sjukdom hos människor i normalriskpopulationer eller högriskpopulationer. Den enskilde själv kan också ta initiativ till att låta undersöka sig, då han har behov av det. I de flesta fall är ändamålet att vidta åtgärder eller att fatta beslut om behandling av den enskilde. Det finns dock fall där syftet kan vara att behandla annan person, t.ex. genom blodtransfusion och transplantation, eller att inhämta uppgifter för forskning. Även om den enskilde själv primärt inte är föremål för beslut eller åtgärd framkommer uppgifter i undersökningen som är av intresse för honom. Blodgivning kan ju sägas vara en mindre hälsoundersökning för den enskilde även om det inte är eller får vara motivet för den enskilde att lämna blod. En sådan situation ställer emellertid krav på att information lämnas till den enskilde och att han vid behov får en hänvisning till annan instans för adekvata åtgärder. Direkt observation genom klinisk undersökning genererar ofta känsliga uppgifter om den enskilde, uppgifter om förhållanden som den enskilde själv ofta inte känner till. Direkt observation kan också förekomma i andra praktiker än kliniska undersökningar. Övervakning av anställda av arbetsgivare kan utgöra ett led i en utvärdering av de anställdas arbetsinsatser. Med datatekniken finns möjligheter att registrera arbetets utförande av arbetstagare som betjänar elektronisk utrustning. Polisens övervakning av den allmänna ordningen, trafiken, spaning

mot enskilda som misstänks för brott är en annan praktik som ibland är dold för den som står under övervakning. Även här har modern datateknik möjliggjort en effektivare övervakning.

Statistiska centralbyrån frågade 1984 vad allmänheten uppfattade som ett intrång i privatlivet. Praktiker som kan räknas till direkt information var TV-övervakning av varuhus, TV-övervakning av offentliga platser, kroppsvisitation i tullen, poliskontroll av bilförares alkoholhalt.

Tabell 1: Syn på privatlivet, reaktion inför olika förfaranden för direkt observation, procent.

	Stör mig inte alls	Är något besvärande	Ser det som ett intrång i privatlivet	Totalt
TV-övervakning i varuhus	81	15	3	100
Poliskontroll av alkoholhalt	80	15	1	100
TV-övervakning på offentlig plats	63	20	15	100
Kroppsvisitation i tullen	45	39	13	100

Källa: *Data och integritet*, SCB 1985.

TV-övervakning på offentlig plats och kroppsvisitation i tullen förknippades mest med ett intrång i privatlivet. Män ansåg i något större utsträckning att TV-övervakning av offentlig plats var ett intrång i deras privatliv. En sådan uppfattning var mycket vanligare bland yngre än äldre och vanligare bland personer med utbildning på lägst gymnasienivå. Kvinnor ansåg oftare än män att en kroppsvisitation var ett intrång i privatlivet, 18 procent jämfört med 8 procent. För övriga bakgrundsfaktorer var skillnaderna små med en liknande tendens åt utfallet om TV-övervakning av offentlig plats. Upplevelsen av en alkoholtest i samband med bilkörning upplevdes sällan som ett intrång i privatlivet men kvinnor, yngre och personer med akademisk utbildning ansåg oftare att det var besvärande. För TV-övervakning av varuhus var tendensen den motsatta hos män som i högre utsträckning upplevde det som besvärande, men i övrigt var svarsmönstret likartat som för andra typer av direkt observation.

I undersökningen ”Medborgarna och forskningen” frågade vi om inställningen till att patientuppgifter inom hälso- och sjukvården registreras med hjälp av data. Sådana uppgifter kommer från någon form av medicinsk undersökning. I vår undersökning hade 69 % besökt öppen hälso- och sjukvård i privat eller offentlig regi de senaste 12 månaderna, 11 % hade

varit inlagda på sjukhus. Nästan hälften (49 %) uppgav att de var oroade över att obehöriga kunde få tillgång till patientuppgifter på data inom hälso- och sjukvården. Däremot var det en minoritet (17 %) som instämde i att det var besvärande att patientuppgifter bevarades på data. Flertalet (82 %) instämde i påståendet att bevarande av patientuppgifter på data gjorde vården tryggare. Inom hälso- och sjukvården har på senare tid patientnära system börjat introduceras, det kan vara system för journalhantering och provsvar som finns på avdelningsnivå.

Ett annat område för uppgiftslämnande förekommer i samband med givande av blod för transfusion eller annan vävnad för transplantation. För att bli accepterad som blod- eller plasmagivare måste den enskilde lämna en hälsodeklaration och blodprov som analyseras för att bestämma blodgrupp och antikroppar men också för att konstatera om det föreligger hinder för blodgivning, t.ex. infektionssjukdom. Enligt vår skattning hade knappt 8 procent av den vuxna befolkningen lämnat blod de senaste 12 månaderna. Om en person uttryckt en vilja att efter döden låta sin vävnad eller organ komma till användning för transplantation eller andra medicinska ändamål är de legala förutsättningarna uppfyllda för sjukvården att använda vävnad eller organ för medicinska ändamål. Viljeyttringen kan gälla all vävnad som kan användas, avse viss användning eller vissa organ. En sådan vilja kan komma till uttryck genom anmälan till donationsregister hos Socialstyrelsen, på donationskort eller muntligt till sjukvårdspersonal eller anhörig. Är den avlidnes uppfattning ej känd har närstående rätt att förbjuda ett sådant ingrepp. I vår undersökning kunde 65 procent tänka sig att deras organ användes efter döden. Om det gällde en avliden anhörig, som inte hade uttryckt någon åsikt, kunde endast 41 procent tänka sig att medge transplantation. Något färre, 60 procent, kunde tänka sig att deras organ fick användas för medicinsk forskning efter döden. Andelen osäkra var 23 procent när det gällde användning av egna organ för transplantation, 33 procent när det gällde anhörigs organ och 24 procent när det gällde egna organ eller vävnad för medicinsk forskning.

Ett intressant exempel på direkt observation är den screeningverksamhet för vissa medfödda ämnesomsättningssjukdomar hos nyfödda. bl.a. fenylketonuri (PKU). Socialstyrelsen har rekommenderat sjukvårdshuvudmännen att delta i denna verksamhet. Analyserna görs centralt på Huddinge sjukhus där ett identifierbart blodprov också sparas för framtiden. I princip alla personer födda 1965 och senare ingår i ett centralt personregister på Huddinge sjukhus med länk till ett blodprov som kan användas för framtida medicinsk forskning. Förekomsten av detta register

öppnar upp intressanta frågeställningar särskilt med anknytning till DNA/RNA-tekniken. Det är åtminstone två integritetsaspekter som får en delvis ny innebörd. Undersökning av människans arvsmassa ger kunskap om andra genetiskt besläktade individer. Frågor om samtycke och information blir här komplicerade, särskilt med tanke på att den genetiskt besläktade familjen i dag inte alltid sammanfaller med den sociala familjen och att mycket av den information som framkommer vid en genetisk undersökning är av mycket känslig natur och svår att kommunicera. Den andra frågan handlar om vävnadsprovets potentiella informationsinnehåll i takt med att den mänskliga arvsmassan kartläggs och nya metoder för diagnostik utvecklas. I en annan rekommendation har Socialstyrelsen rekommenderat patologavdelningar att tills vidare spara alla prover dels med hänvisning till patientens vård och behandling, dels med hänvisning till den medicinska forskningen behov.

Andra förfaranden med direkt observation som varit föremål för debatt och politiska överväganden är användningen av medicinska undersökningar i arbetslivet och undersökningar av människans arvsmassa med DNA/RNA-teknik i arbetslivet och vid tecknande av privata liv- och sjukförsäkringar. Övervakning av anställda med hjälp av automatisk databehandling var föremål för Datalagsutredningens överväganden.

Den enskildes uppgiftslämnande

Om inte uppgifter inhämtas genom direkt observation är den enskilde själv eller en honom närstående person uppgiftslämnare. En vårdnadshavare är uppgiftslämnare för minderåriga och en anhörig kan vara uppgiftslämnare då enskilds förmåga att själv kommunicera är nedsatt, tillfälligt eller permanent. Vi skall här inte gå in på närståendes ställning som uppgiftslämnare. I de undersökningar som redovisas här finns ingen kunskap om detta med undantag för medicinska förfaranden för transplantation, obduktion och medicinsk forskning. Andra utomstående, t.ex. vittnen vid brottsplats eller olycka har skyldighet att på uppmaning av polis eller domstol redogöra för vad de observerat. Ett vittnes uppgiftsskyldighet är ej administrativt i förhållande till honom själv utan den han vittnar mot.

Vi har tidigare diskuterat den enskildes uppgiftslämnande i olika situationer. I den privata sektorn är informationsutbyte (uppgiftslämnande) en naturlig del av ett *avtal* mellan två parter. Det handlar antingen om ett anställningsförhållande eller ett kundförhållande. Det finns bestämmelser i

författning (lag) som begränsar enskilds rätt att avtala om att vissa uppgifter lämnas ut. Uppgiftslämnande i ett anställningsförhållande kan också begränsas av kollektivavtal mellan företrädare för arbetsgivare och arbetstagare. Ett *medlemskap* i ekonomisk eller ideell förening kan också utgöra grunden för uppgiftslämnande från den enskilde till föreningen. De vanligast förekommande personregistren i den privata sektorn är kundregister, personregister för administration av personal och löner samt medlemsregister. Sådana personregister kräver oftast inte tillstånd enligt datalagen. Datalagen medger föreningar att registrera uppgifter av känslig natur om de utgör grunden för medlemskapet. Arbetsgivare får registrera uppgifter om enskilds sjukdom eller hälsotillstånd om det behövs för åtgärd om rehabilitering. *Frivillighet* som grund för uppgiftslämnande av enskilda i den privata sektorn sammanfaller med att anknytning som följer av anställning, kundförhållande eller medlemskap saknas.

Företag och organisationer har ett berättigat intresse att rekrytera nya medarbetare, kunder eller medlemmar. När ett företag tar kontakt med den enskilde i detta sammanhang finns ingen etablerad anknytning mellan företaget och den enskilde. Den enskilde är *privatperson* i förhållande till företaget. Denna har om den är riktad till enskild person föregåtts av att uppgifter om den enskilde har lämnats ut av någon annan. Till detta återkommer vi nedan. Vi återkommer även till de fall då ett företag eller organisation kontaktar den enskilde för att denne skall bidra med uppgifter om sig själv i samband med marknads- eller opinionsundersökningar. Den enskilde kan naturligtvis själv söka upp ett företag eller en organisation som han önskar att etablera en förbindelse med. När den enskilde nåtts av kontaktförsöket står det honom fritt att ta kontakt. Något uppgiftslämnande är det inte frågan om förrän den enskilde ansöker om medlemskap i förening, att bli kund till eller anställd i ett företag. Först då är ändamålet med företagets eller organisationens inhämtande av uppgifter beslutande eller åtgärdande gentemot den enskilde. Det kan finnas villkor förenade med en ansökan, t.ex. kreditupplysning, som innebär att den enskilde lämnar uppgifter om sina personliga och ekonomiska förhållanden eller informeras om att uppgifter inhämtas om honom. I de fall befintliga uppgifter skyddas av sekretess avstår den enskilde sekretessen som gäller till förmån för honom (utlämnande av patientuppgifter vid tecknande av privat pensions- eller sjukförsäkring). I författning finns regler om vilka uppgifter ett företag eller organisation får efterfråga. Ett aktuellt lagförslag i en departementspromemoria från socialdepartementet vill förbjuda att arbetsgivare och försäkringsbolag får efterfråga uppgifter om enskilda personer från

undersökningar genomförda med DNA/RNA-teknik. Det finns i ett demokratiskt samhälle en formell frivillighet att ingå avtal eller inträda som medlem i sammanslutningar. Formellt sett är parterna som skall komma överens om innehållet i ett avtal likaberättigade. Materiellt sett hänger en sådan frivillighet och möjligheterna att ställa villkor samman med resurser hos parterna som påverkas av en rad faktorer som bl.a. gett upphov till organisering av konsumenter, hyresgäster och arbetstagare i intresseföreningar men också lagstiftning för att skydda den svagare parten.

SCB frågade i undersökningar genomförda 1984 och 1986 om det var befogat att vissa myndigheter, företag och organisationer hade personregister på data.

Tabell 2: Inställning till att myndigheter och företag har personregister på data år 1984 och år 1986, procent.

	Befogat	Tveksamt	Obefogat	Vet ej	Samtliga
Försäkringskassan	91 (76)	6 (14)	2 (7)	1 (3)	100 (100)
Skattemyndigheter	84	10	4	2	100
Banker	66 (44)	21	10	2	100
Försäkringsbolag	63 (37)	20	13	3	100
Statistiska centralbyrån	53 (34)	25 (26)	18 (29)	4 (11)	100 (100)
Socialnämnderna	47 (42)	29	21	3	100
Kontokortsföretag	33 (20)	16	47	4	100
Kundregister, t.ex. på varuhus	15 (7)	14	68	3	100
Bokklubbar	8 (4)	12	77	3	100

Källa: *Data och integritet*. SCB (1985) och SOU 1987:31 *Integritetsskyddet i informationssamhället 4*. Stockholm 1987. Siffror inom parentes är tillgängliga uppgifter från 1986 års undersökning.

En mycket stor andel ansåg 1984 att personregister hos försäkringskassan, sjukhus, och skattemyndigheter var befogade. Över hälften ansåg personregister befogade hos banker, försäkringsbolag och Statistiska centralbyrån. För kundregister hos företag som tillhandahåller varor fanns inte samma stöd. Något större stöd fanns för personregister hos kontokortsföretag. När det förelåg skillnader mellan olika grupper av människor var det ofta de äldre som inte ansåg att personregister var befogade, undantagna var deras inställning till personregister hos socialnämnderna och kundregister hos varuhus som var positivare än yngre grupper. Personer med akademisk utbildning var positivare till förekomsten av personregister hos framför allt Statistiska centralbyrån, 72 % jämfört med drygt 50 %, men också till personregister hos skattemyndigheterna, socialnämnderna och

kontokortföretag, än personer med lägre utbildning. I Data- och offentlighetskommitténs undersökning 1986, som genomfördes av SCB, har andelen positiva markant minskat. Allra mest minskade stödet för de kundregister som redan två år tidigare hade lågt stöd, minskningen var över 40 %. Personregister hos försäkringskassan och socialnämnderna behöll i högre grad stöd hos allmänheten jämfört med två år tidigare. Allmänhetens inställning till dataregistrering under 80-talet återkommer vi till nedan.

En stor del av debatten och kritiken har åtminstone tidigare gällt användningen av personnummer. År 1984 uppgav 15 % att de känt obehag över att lämna ut personnummer, 10 % hade till och med vägrat att göra det. Även om personer med denna erfarenhet utgjorde en minoritet hade andelen personer med obehagskänsla fördubblats år 1986 liksom andelen som någon gång vägrat lämna sitt personnummer. I vår undersökning år 1995 uppgav 17 % att de någon gång vägrat att lämna sitt personnummer. Kritiken har också gällt användningen av personnummer. År 1984 ansåg nära 40 % att de hade tyckt att det var onödigt att lämna sitt personnummer, 1986 hade nära 55 % denna upplevelse. Dessa upplevelser och erfarenheter var vanligare hos yngre och medelålders, välutbildade och personer med stor kunskap om datorer. Särskilt tydliga var dessa upplevelser hos personer med akademisk utbildning och hos tjänstemän. Bland tjänstemän var en vägran att lämna personnummer dubbelt så vanlig jämfört med andra grupper, 14 % jämfört med 8 % bland arbetare och 5 % bland företagare. Detta gällde också akademiker (18%) jämfört med andra (7 och 11%). Skillnaderna kvarstår i vår undersökning från 1995.

Av frågan om vägran att lämna ut personnummer framgår inte vilken grund för uppgiftslämnande som gällde och inte heller konsekvenserna för den enskilde. Frågan gällde både när en myndighet eller företag bad att den enskilde skulle uppge personnummer, detta formulerades explicit i vår undersökning 1995. Stod den enskilde inför att ingå ett avtal kan resultatet ha varit att avtal inte kom till stånd, eller att villkoren för avtalets ingående ändrades till hans fördel.

Grunden för uppgiftslämnande i den offentliga sektorn kan vara legalt tvång. Tvång som innebär frihetsberövande eller åligganden för den enskilde gentemot myndigheterna måste ha stöd i lag. För enskildas uppgiftslämnande i administrativt syfte finns lagstadgad uppgiftsskyldighet i verksamheter för bl.a. folkbokföring, och beskattning. Denna skyldighet upprätthålls med straffsanktion. Inom socialförsäkringen upprätthålls uppgiftsskyldighet med sanktion om förlust av ersättning. Lämnande av felaktiga eller ofullständiga uppgifter innebär att utgiven ersättning kan

krävas tillbaka. Inom hälso- och sjukvården finns ingen formell uppgiftsskyldighet för den enskilde men myndigheterna är skyldiga att dokumentera insatser riktade mot den enskilde. Provtagning för HIV-infektion utgör enda undantaget och kan göras anonymt. Är resultatet av analysen positivt bortfaller rätt till anonymitet och uppgiftsskyldighet enligt smittskyddslagen infaller. Inom hälso- och sjukvården och socialtjänsten förutsätts snarare att den enskilde samarbetar för att bli bemött på ett adekvat sätt och få den hjälp han behöver. Särskilt inom sjukvården kan det få förödande konsekvenser för patienten om han inte lämnar riktiga och fullständiga uppgifter till sjukvårdspersonalen. När uppgiftslämnande sker för ett administrativt, beslutande eller åtgärdande ändamål säger vi att den enskilde är *klient* till den myndighet han lämnar uppgifterna. Grund för uppgiftslämnande är här ett *administrativt tvång*. När det inte finns en uttalad legal uppgiftsskyldighet för den enskilde (beskattning, folkbokföring, smittskydd osv.) står det honom i princip fritt att avstå från att begära vård eller annan hjälp från det allmänna. Det är allmänt känt att enskilda kan ha svårt att söka ekonomisk hjälp från socialtjänsten även om de är i behov av ekonomisk hjälp eftersom det anses utpekande och obehagligt. Möjligheten till anonyma HIV-test skall också ses mot denna bakgrund och att det ligger i det allmännas intresse att människor vet om de bär på infektionen eller inte. Skillnaden består i att den enskilde kan tvingas till att betala skatt men i allmänhet inte tvingas till att söka vård och behandling eller att få sjukpenning. Det finns dock föreskrifter i lag om tvångsvård. Om däremot den enskilde accepterar att ta emot vård eller behandling, ekonomisk ersättning eller understöd måste han finna sig i att lämna uppgifter som är fullständiga och sanningsenliga och att lämnade uppgifter registreras hos handläggande myndighet.

Alla människor har någon erfarenhet av uppgiftslämnande för administrativa syften. Vi kan här skilja mellan uppgiftslämnande och registrering av uppgifter för å ena sidan vanligt förekommande administrativa syften som anställning, kundförhållande, medlemskap i den privata sektorn och folkbokföring, beskattning och socialförsäkring i den offentliga sektorn och å andra sidan mer ovanligt förekommande, känsliga och utpekande administrativa syften som vård och behandling, ekonomiskt stöd från socialtjänst och tvångsåtgärder av olika slag. Erfarenhet av uppgiftslämnande för vissa sådana ändamål, har vi försökt skatta som bakgrundsvariabler i vår undersökning. Det är situationer då enskilda sökt hjälp, vård eller erhållit ersättningar för längre tids arbetslöshet och sjukdom. Av de tillfrågade hade under de senaste 12 månaderna 11 % varit in-

lagda på sjukhus, 1 % fått hjälp eller omvårdnad av socialtjänsten, 14 % hade sökt bostadsbidrag, 4 % hade sökt socialbidrag och 16 % hade varit sjukskrivna en sammanhängande period om mer än sex dagar. På frågan om urvalspersonernas huvudsakliga sysselsättning under de senaste 6 månaderna uppgav 7 % att de var arbetslösa och 1 % att de var långtidssjukskrivna. 50 % av de tillfrågade förvärvsarbetade på heltid medan 14 % förvärvsarbetade mindre än heltid. Inga frågor ställdes om tvångsåtgärder gentemot enskilda.

Det allmänna har också behov av att efterfråga information från enskilda för andra syften än administrativa. Det allmänna har ett ansvar för att framställa information om hur samhället ser ut och fungerar, särskilt att utvärdera de offentliga verksamheterna, framställa den officiella statistiken och att bedriva vetenskaplig forskning. När enskilda tas i anspråk som uppgiftslämnare för sådana ändamål finns inget administrativt intresse riktat mot honom från myndighetens sida. Uppgiftslämnandet är frivilligt. En sådan inbjudan kan riktas mot den enskilde som representant för allmänheten eller på grundval av en befintlig eller avslutad klient-relation med en myndighet. Oavsett vilken kategori den enskilde tillhör är relationen till den myndighet som efterfrågar uppgifter för sådana icke-administrativa ändamål alltid utan aktuellt administrativt eller åtgärdande intresse. Undantag är klinisk forskning där patienten erbjuds att medverka i en studie där aktiv behandling erbjuds. Även om syftet fortfarande är att utveckla nya metoder eller söka ny kunskap inom medicinen, finns också ett åtgärdande syfte riktat mot patienten. Avhängigt vilken relation undersökningsdeltagaren har eller har haft till den som genomför undersökningen eller undersökningens syfte är medverkan formellt sett frivilligt. Sedan kan de materiella grundvalen för medverkan variera. Eftersom denna relation med myndigheten är utan administrativt intresse benämner vi den enskilde *medborgare* i detta sammanhang. Grunden för uppgiftslämnande är formell *frivillighet*.

I vår undersökning frågade vi urvalspersonerna om de hade erfarenhet av uppgiftslämnande för planering, utvärdering, statistik och forskning. Vi fann det inte meningsfullt att försöka skatta sådant uppgiftslämnande i den privata och den offentliga sektorn var för sig. Grunden för sådant uppgiftslämnande är frivillighet i båda fallen. 75 % uppgav att de någon gång blivit tillfrågade att medverka i sådana undersökningar. På frågan när detta senast hade hänt uppgav 41 % att det hade inträffat åtminstone en gång under de senaste 12 månaderna. Av de tillfrågade hade 90 % deltagit vid detta tillfälle. Vår undersökning visar att efterfrågan på uppgifter från enskilda

för statistiska undersökningar är både utbredd och frekvent. Beredvilligheten att medverka är dock inte så hög som våra undersökningsdeltagare uppger. Det kan nämligen befaras att de som valt att inte deltaga i vår undersökning också har vägrat att deltaga i andra undersökningar. I SCB:s undersökning ”Data och integritet” år 1984 hade 57 % någon gång blivit ombedda att deltaga i en statistisk undersökning. Efterfrågan på uppgifter från privatpersoner/medborgare kan sägas ha ökat under perioden mellan de båda mättillfällena.

Vi undersökte det upplevda besväret av olika intrång i privatlivet. Detta säger inte uttryckligen något om hur stort berättigande sådana åtgärder har i allmänhetens ögon. Däremot kan synen på det berättigade i sådana åtgärder påverka det upplevda besväret. Vi återkommer till det nedan.

Tabell 3: Syn på privatlivet. Allmänhetens upplevelser av olika intrång i privatlivet, procent.

Hur reagerar Du	Inte alls besvärande	Inte särskilt besvärande	Ganska besvärande	Mycket besvärande	Kan inte säga	Samtliga
Om någon myndighet ber dig medverka i statistisk undersökning om hushållens privatekonomi	32	36	17	8	5	100
Om Du blir uppringd av ett företag som vill sälja varor	4	13	29	51	2	100
För reklam med Ditt namn på i brevlådan	12	30	28	29	1	100
Om ett marknadsundersökningsinstitut ber dig medverka i undersökning om hushållens inköpsvanor	22	40	22	11	4	100
Om uppgifter om att Du fått vård på sjukhus används för medicinsk forskning	30	35	14	11	10	100
Om uppgifter om Din inkomst och förmögenhet används för framställning av officiell statistik	19	30	20	26	6	100
Om myndigheter sammanställer uppgifter från olika register för att kontrollera om Du försöker skaffa Dig förmåner som Du inte har rätt till	37	26	12	18	6	100

Ingen av frågorna handlar om att den enskilde lämnar uppgifter om sig själv för administrativa ändamål. Däremot berör frågorna uppgiftslämnande för planerande, utvärderande och forskningsändamål, både i privat och offentlig regi. Flera frågor berör upplevelsen av besvär i samband med att andra än den enskilde själv lämnat ut uppgifter om honom. Den enskilde

utsätts för uppvaktning av utomstående i sitt hem på fritiden. Sådana kontaktförsök är gemensamma för både offentliga och privata undersökningsinstitut men också för företag som kontaktar den enskilde i hemmet för att värva nya kunder o.dyl. Det har föregåtts av att uppgifter om den enskilde lämnats ut av någon som förfogar över sådana, vanligast är utlämnande från SPAR-registret. Upplevelsen av besvär mellan dessa typer av kontakter skiljer sig åt markant i vår undersökning. Medan omkring 30 % upplever sig besvärade av en förfrågan om medverkan i både privata och offentliga undersökningar känner sig 60 % besvärade av adresserad direktreklam och så mycket som 80 % av företag som försöker sälja varor och tjänster per telefon. I det senare fallet är så mycket som drygt 50 % mycket besvärade.

När det gäller utlämnande av känsliga uppgifter och sekretesskyddade uppgifter för både administrativa (kontrollerande) ändamål och för forskning och statistik uppger omkring 30 % att de känner sig besvärade av att uppgifter om att de fått vård eller behandling lämnas ut för medicinsk forskning och att myndigheter sambearbetar uppgifter för att kontrollera om enskilda försöker skaffa sig förmåner de inte har rätt till. Däremot upplever sig 46 % besvärade av att uppgifter från skattemyndigheterna används för framställning av den officiella statistiken. Utgångspunkten i datalagen är att all kontakt från utomstående gentemot enskilda utgör intrång i deras privatliv. Sådana intrång kan vara tillbörliga och otillbörliga. När otillbörliga intrång skall förebyggas har datainspektionen bl.a. att ta hänsyn till inställningen hos de som skall registreras. I vissa fall får enskilda finna sig i intrång i deras privatliv eftersom sådana kan vara motiverade av starka samhällsintressen. I vår undersökning upplevs användning av befintliga uppgifter i kommersiella sammanhang och i viss utsträckning (drygt en fjärdedel) för framställning av den officiella statistiken som mest besvärande när det gäller privatlivet. Enskilda finner sig i att bli kontaktade för medverkan i statistiska undersökningar och att myndigheter sambearbetar personuppgifter för att komma åt bidragsfusk. För det senare ändamålet är nästan 20 % mycket besvärade.

SCB ställde 1984 en liknande fråga men med andra svarsalternativ. Svarsalternativen var ”stör mig inte alls”, ”är något besvärande” samt ”ser det som ett intrång i privatlivet”. På frågan om medverkan i statistisk undersökning uppgav 69 % att de inte alls blev störda, 25 % var något besvärade och endast 5 % upplevde en sådan förfrågan som ett intrång i privatlivet. Även om svarsalternativen inte är direkt jämförbara uppvisar de en likartad fördelning, dvs. om ”stör mig inte alls” jämförs med ”inte alls be-

svärande" och att "mycket besvärande" jämförs med "intrång i privatlivet". Däremot förelåg en skillnad jämfört med privat marknadsundersökning, den uppgavs i SCB:s undersökning handla om vilket tvättmedel man använde, 27 % upplevde en sådan förfrågan om medverkan som ett intrång i privatlivet. Här kan dock frågans formulering ha bidragit till den höga andelen negativa. På frågan hur de reagerade inför att bli uppringda av företag som ville sälja varor svarade 40 % att de såg det som ett intrång i privatlivet, 14 % sa att det inte störde dem alls. Direktadresserad reklam ansåg 30 % vara ett intrång i privatlivet medan 25 % sa att de inte blev störda av detta. Jämfört med vår undersökning har människor blivit mer uttalat negativa när det gäller företag som bedriver telefonförsäljning och något mindre positiva när det gäller direktreklam.

Upplevelsen av påfrestningar på privatlivet kan inte bara ställas i relation till ändamålet och nyttan med åligganden och förpliktelser för den enskilde, det kan också ha att göra med skyddet för privatlivet eller den personliga integriteten när personuppgifter behandlas. I undersökningar från 1970 och fram till 1984 har Statistiska centralbyrån konstaterat att människor har dålig kännedom om innebörden av sekretesslagen. År 1984 trodde endast en mindre del att uppgifterna fick lämnas ut fritt (7 %), men tydligast var att enskilda överskattade sekretesskyddet, 46 % trodde att sekretessen var absolut. År 1970 trodde nästan 70 % att uppgifterna bara fick användas av SCB i statistikproduktionen. Vid samma tillfälle befarade 35 % att det fanns risk för att lämnade uppgifter kunde komma ut till obehöriga. En ökande del av allmänheten tror emellertid att uppgifter som man lämnat till SCB kan komma att användas på ett sätt som man ogillar. År 1976 var andelen 9 % och år 1986 då frågan sist ställdes hade den ökat till 32 %. Om allmänhetens kännedom om sekretesskydd ser ut på samma sätt när det gäller andra myndigheter är svårt att säga. Dock kan man väl misstänka att allmänhetens föreställningar om sekretess inte medger att uppgifter dyker upp i helt andra sammanhang. För detta talar ovan redovisade överskattning av sekretesskyddet, den debatt som registreringen av sekretesskyddade uppgifter för bl.a. forskning och statistik har gett upphov till samt att reglerna, med bl.a. prövning om skada eller men för den uppgifterna handlar om, är svårbegripliga. SCB genomförde en allmän skattning av skyddet för privatlivet i undersökningarna 1976 och 1984. Vid det första undersökningstillfället upplevde 31 % att privatlivet var mindre skyddat än för fem år sedan, vid det andra tillfället hade andelen stigit till 40 %.

Vi har länge uppehållit oss vid de kommunikativa aspekterna av behandlingen av personuppgifter. Vi lade dock inledningsvis stor tonvikt vid

de tekniskt-administrativa möjligheterna som kommer med automatisk databehandling. De kan användas för att uppnå större effektivitet i behandlingen av personuppgifter. Men vilka är de ändamål för vilka behandlingen görs. Hänger inte allmänhetens inställning till registrering av personuppgifter samman med värderingen av de resultat som uppnås. Det finns inte bara en stark opinion för ökad restriktivitet mot sambearbetningar av personregister, opinionen är också stark för en ökad kontroll över samhällsutvecklingen och dess bieffekter. Allmänheten utövar ett starkt tryck på ansvariga myndigheter att ta fram kunskap om risker för människors välfärd och hälsa, t.ex. genom ökat stöd för forskningen. Ökad effektivitet kommer också enskilda till godo som bättre service för företagens kunder och myndigheternas klienter. I SCB:s undersökning 1984 instämde 44 % helt med påståendet att dataregister gör det lättare för myndigheter att ge en effektiv service åt allmänheten, ytterligare 34 % instämde delvis i påståendet. Lika stor andel instämde i påståendet att det komplicerade bidragssystemet gjorde en effektiv kontroll av enskilda nödvändig för att komma åt bidragsfusket. En sådan inställning återfanns i större utsträckning hos äldre, lågutbildade, och i arbetar- och företagarkategorin. Påståendet att datorer bidrog till en bättre service hade allmän uppslutning, inga märkbara skillnader kunde konstateras bland olika grupper.

I ett annat påstående värderades nödvändigheten att i ett modernt samhälle ha bra statistik om människornas levnadsförhållanden, 31 % instämde helt och ytterligare 27 % instämde delvis i påståendet. Bland de äldsta var denna inställning ännu något mer positiv. I SCB:s undersökning 1986 skulle angelägenheten av statistik på olika områden värderas. Över 50 % ansåg att det var viktigt med statistik om hälsotillståndet, sysselsättning och arbetslöshet, arbetsmiljön, Sveriges ekonomi, prisutvecklingen och för samhällsplanering. Mindre viktig ansågs statistik om fritidsintressen och partisympatier vara. Statistik om alkoholkonsumtion intog en mellanställning. Medan 47 % ansåg att statistik var mycket betydelsefull som underlag för samhällsplanering ansåg endast 17 % att den var mycket viktig för egen del som information om hur samhället fungerar och utvecklas. Frågorna är intressanta men olika till sin karaktär. I den första frågan uppmanas den enskilde att ta ställning till ett samhälleligt behov, i den andra till ett personligt behov. Bland äldre personer var andelen som värderade det personliga behovet av statistik som mycket viktigt högre. I den första frågan var svarsmönstret fördelat på ett likartat sätt mellan olika grupper. Dessa resultat tyder på att statistisk information bedöms viktig som ett un-

derlag åt myndigheterna att planera samhällelig service och att man anser det angeläget med initiativ på eller åtminstone bevakning av områden som arbetsmiljö och befolkningens hälsa. Områden som tillhör enskildas privatsfär behöver inte i samma utsträckning belysas med statistisk information. Endast för en mindre del, särskilt äldre, är statistisk information viktig för att själv skaffa sig kunskap om samhällsutvecklingen.

Vi ställde en liknande fråga i vår undersökning 1995, i den instämde 38 % helt i påståendet att bra statistik måste finnas för att allmänheten skall kunna bilda sig en saklig uppfattning om samhällsutvecklingen. Alla dessa påståenden är dock lätta att allmänt instämma i. På det sätt som påståendena är konstruerade kommer de inte i konflikt med andra intressen. SCB gjorde dock ett försök att bygga in en intressekonflikt i en fråga om angelägenheten av statistik på olika samhällsområden mot bakgrund av den uppoffring det innebär för enskilda att lämna uppgifter. Även här ansågs statistik om hälsotillståndet, arbetsmiljön, sysselsättning och arbetslöshet samt ungdomens yrkes- och utbildningsplaner vara mycket viktiga. Mer fritidsbetonade områden och opinionen i vissa samhällsfrågor ansågs mindre viktiga. Är detta helt enkelt ett uttryck för att allmänheten mycket väl förstår kopplingen mellan uppgiftslämnande och möjligheten att framställa statistik på olika områden och att man bestämt avvisar medverkan i statistiska undersökningar om sakområden som man antingen värderar som oviktiga eller som man i en prioritering kan avstå ifrån till förmån för sitt privatliv?

Det finns ytterligare ett sätt att studera allmänhetens beredvillighet att medverka som uppgiftslämnare i statistiska undersökningar. Eftersom medverkan är frivillig kan vi helt enkelt studera hur stor andel av de tillfrågade som vid olika tillfällen har svarat. Man kan tänka sig flera angreppssätt beroende på vad man vill studera. Det finns olika typer av undersökningar med avseende på hur enskilda lämnar uppgifter. Det kan ske skriftligt med hjälp av en enkät, eller genom en intervju. Intervjun kan genomföras som ett hembesök eller per telefon. De som någon gång blivit tillfrågade att medverka i en statistisk undersökning (76 %) blev i vår undersökning uppmanade att redovisa förhållandena vid den senaste undersökningen. Det vanligaste sättet för uppgiftslämnande var telefonintervju (47 %), därefter kom postenkäten (32 %) och besöksintervju (10 %). Vilken typ av uppgiftslämnande som innebär mest intrång i privatlivet kan inte bedömas. Man skulle kunna tänka sig att ju högre grad av personlig kontakt man blir föremål för, desto större upplevs intrånget. Det kan också vara tvärtom att ju mindre anonymt och opersonligt uppgiftslämnandet är

desto starkare tillit känner man inför att lämna uppgifter till någon utomstående. Sedan beror det också på uppgifternas känslighet. SCB:s undersökning från 1975 bekräftar att de rätt väl sammanhänger med grad av sekretesskydd i offentlig verksamhet. Känsliga områden som framträdde var ekonomi, ideologi och stigmatiserande kontakter med myndigheterna.

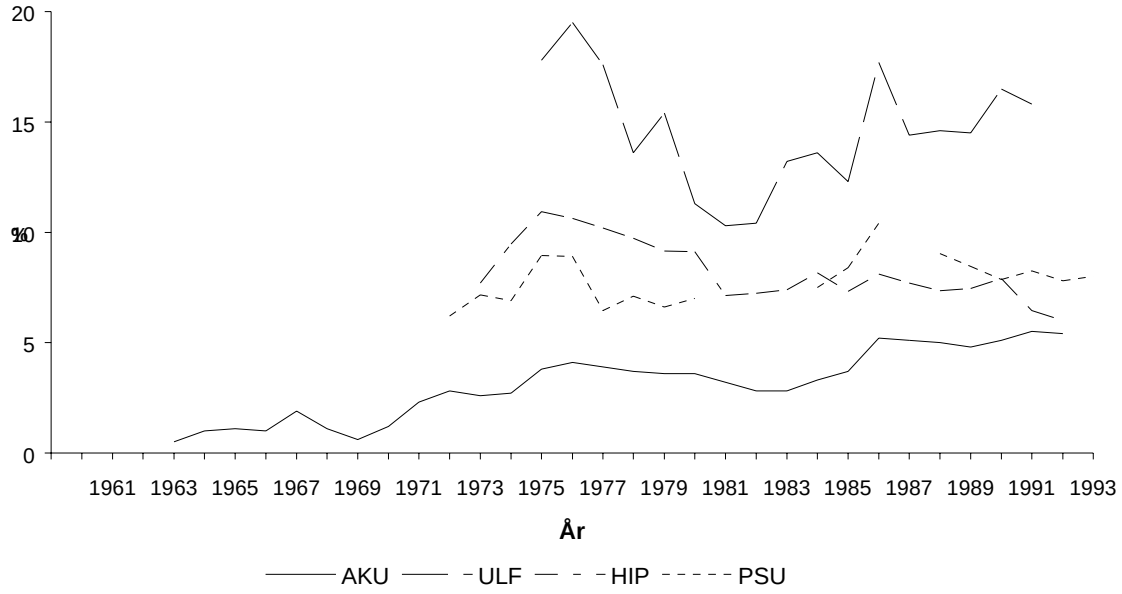
Frågornas karaktär har ett nära samband med undersökningens syfte. Vi har ovan visat hur allmänheten ser på statistik om olika sakområden. Frågan om undersökningens syfte ligger nära vem som efterfrågar uppgifterna. Är den undersökande institutionen privat eller offentlig? Det kan vara av avgörande betydelse för hur resultatet av undersökningen blir tillgängligt och kan komma till nytta. Är det medicinsk eller samhällsvetenskaplig forskning? Dessa faktorer kan antas påverka allmänhetens vilja att medverka vid ett bestämt tillfälle. Vid jämförelser av detta slag vill man dock konstanthålla alla parametrar utom den man studerar. Viljan att medverka förändras också över tid. Vid sådana jämförelser är det viktigt att jämföra likartade undersökningar vid flera undersökningstillfällen.

SCB gör ett antal undersökningar sedan lång tid. De olika undersökningarnas uppläggning har varit förhållandevis konstant över tid. Användningen av datainsamlingsmetoder varierar även om telefonintervju dominerar. Figur 3 visar utvecklingen av vägrarbortfallet i de respektive undersökningarna över tid. Arbetskraftundersökningen (AKU) är en telefonintervju som genomförts sedan början av 1960-talet. Telefonintervjun tar cirka 10 minuter att genomföra. Undersökningen om levnadsförhållanden (ULF) startade 1974 och är en besöksintervju. Intervjun tar över en timme att genomföra och berör en mängd känsliga frågor. Uppgifter inhämtas också från SCB:s inkomst- och förmögenhetsregister och registret över kontrolluppgifter. Uppgifterna till dessa register inhämtas från skattemyndigheterna. Hushållens inköpsplaner är en telefonintervju och startade 1973. Telefonintervjun tar mellan 15 och 35 minuter att genomföra, beroende på hur många följdfrågor som måste ställas. Partisympatiundersökningen (PSU) startade 1972. Det är också en telefonintervju som går snabbt att genomföra. Inkomstfördelningsundersökningen (HINK) genomförs sedan 1973. Den är en kombinerad registerundersökning och telefonintervju. Tyngdpunkten ligger på inhämtande av uppgifter från myndigheternas personregister. I PSU ingår endast röstberättigade till skillnad från de andra undersökningarna som vänder sig till populationen folkbokförda.

Utvecklingen över vägrarbortfallet låter sig analyseras över en mängd faktorer. Den enda faktorn som konstanthålls är att SCB genomför undersökningen, därför låter sig jämförelser av olika undersökande institutioner

inte göras. Det är emellertid en fördel ur en annan synvinkel, att SCB har likartade rutiner för att minimera vägran att medverka. Samtliga undersökningar har liknande status och ingår i den Officiella statistiken, varför detta ändamål inte kan jämföras med något annat. Andelen vägrare är lägst i AKU. Det är en kort telefonintervju om ett område som vi ovan konstaterat har ett stort stöd bland allmänheten. I andra telefonintervjuer är vägrarbortfallet högre. HIP och PSU berör områden som inte ansågs vara lika viktiga och som dessutom berör känsliga uppgifter som partisympati och ekonomi. HINK är numera också en telefonintervju. Fram till 1983 genomfördes den dock som en enkätundersökning. Ur integritetssynpunkt är problemet med denna undersökning att uppgifterna huvudsakligen inhämtas från befintliga personregister. Om detta var anledningen till att SCB övergav enkätundersökningen till förmån för telefonintervju kan jag inte bedöma. Det sammanfaller dock med att sambearbetningar av detta slag började debatteras. Vägrarbortfallet i undersökningen steg kraftigt mellan 1982 och 1983. Trots sambearbetningarna har undersökningen inte högre vägrarbortfall än HIP och PSU. ULF har den största andelen vägrare. Det är också den mest omfattande undersökningen av dem vi nu jämför. I ULF inhämtas personuppgifter till en del, i likhet med HINK, också från befintliga personregister. Vi kan konstatera att andelen vägrare varierar mest i denna undersökning. Någon postenkätundersökning finns tyvärr inte med i jämförelsen. Resultatet av jämförelsen tycks tyda på att graden av personlig kontakt inverkar menligt på beredvilligheten att medverka. Det kan dock bero på att uppgiftslämnandet är av mycket större omfattning i ULF än i de andra undersökningarna. Det skall nämnas att bortfallet i enkätundersökningar brukar ligga på en högre nivå, mellan 20 och 30 %. Frågeområde tycks också spela en roll för viljan att medverka. Det kan förklara att AKU har ett mycket lägre bortfall än PSU och HIP trots likheterna i övrigt.

Figur 3: Andel vägrare i urvalsundersökningar 1963-1993



Att viljan att deltaga i undersökningar har minskat över tid framgår inte omedelbart av figuren. Det är endast i AKU som det har skett en långsam ökning av andelen vägrare. Det gäller även i ULF från 1982. Där har dock andelen vägrare fluktuerat kraftigt vilket gör det svårt att konstatera om det föreligger en trend. Särskilt låg var svarsfrekvensen 1986. I HIP och PSU gick andelen vägrare upp i mitten på 70-talet för att sedan falla tillbaka till en tämligen konstant nivå. I HIP har bortfallet till och med minskat på senare år. I AKU ökade andelen vägrare snabbare 1971, 1975 och 1986. Dessa år sammanfaller rätt väl med kulmen på debatten om data och integritet i Sverige. 1970 och 1971 debatterades folk- och bostadsräkningen livligt. Det var Sveriges första debatt om personregistrering och integritet. Som ett resultat av denna och faktorer som jag berörde inledningsvis fick Sverige en datalag som började gälla 1974. En av de första konflikter som den nya tillsynsmyndigheten Datainspektionen hade var med SCB och företrädare för forskningen. Denna debatt utlöstes av att SCB överklagade Datainspektionens beslut angående föreskrifter i samband med att tillstånd lämnades för personregistret levnadsförhållanden. Denna konflikt uppmärksammades också i massmedia. Det höga bortfallet för ULF inledningsvis kan relateras till denna händelse. Förtroendet för undersökningen ökade sedan fram till 1982/83 då utvecklingen vände.

Denna vändpunkt sammanfaller med en kraftig uppgång av andelen vägrare i HINK. För AKU däremot sker ingen uppgång av bortfallet vid denna tidpunkt. Omkring 1983 debatterades samkörningar i offentligheten.

SCB hade publicerat ett förslag om en folk- och bostadsräkning helt baserad på användningen av befintliga registeruppgifter (FOBALT). För att klara detta hävdade SCB dessutom att det behövdes fyra nya centrala personregister för statistiska ändamål. SCB ville också att folkbokföringen skulle ändras så att enskilda boende i flerfamiljshus skulle folkbokföras på lägenhet i stället för fastighet. Det skulle innebära att man fick en mer rättvisande bild av hushållens sammansättning än annars med hjälp av befintliga registeruppgifter. Två av de föreslagna registren inrättades så småningom, utbildningsregistret och sysselsättningsregistret. Eftersom både ULF och HINK använder registeruppgifter ligger det nära till hands att anta att uppgången av vägrarbortfallet hade att göra med att frågor om samkörningar uppmärksammades. Särskilt som bortfallet i andra undersökningar inte ökar.

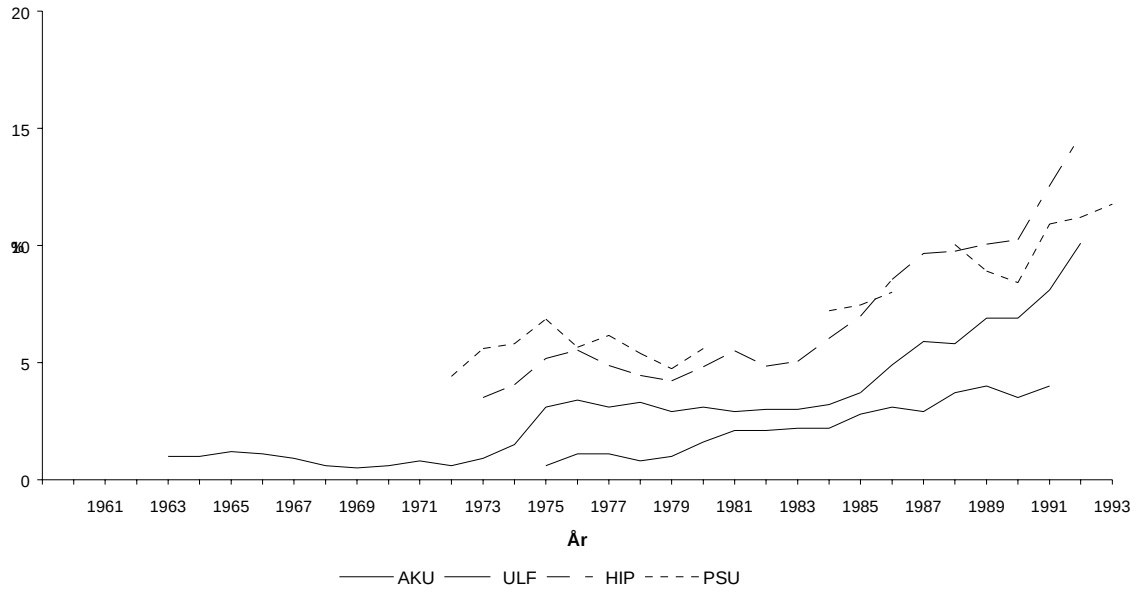
Nästa kraftiga ökning sammanfaller med debatten om forskningsprojektet Metropolit vid Stockholms universitet. Forskarna i projektet hade samlat in uppgifter om en årskull stockholmare födda 1953, dels från myndigheter, dels från individerna själva. Syftet var att studera hur uppväxtmiljön påverkade deras möjligheter senare i livet. En mängd synnerligen känsliga uppgifter hade registrerats sedan 53-ornas barndom. Uppgifter om avvikande beteende upprörde många. En mycket upprörd debatt om förutsättningarna för forskning och statistik, samt de registrerades personliga integritet fördes. Detta fick till följd att andelen vägrare ökade i samtliga undersökningar. En ökning av bortfallet kan också noteras år 1990. Då debatterades återigen folk- och bostadsräkningen. Vid denna räkning var det ett stort antal personer som trots uppgiftsskyldighet vägrade att lämna uppgifter, särskilt i Stockholmsregionen. Svarsandelen för Stockholm var 84 % före första påminnelse. Vid 1975 och 1980 års räkning hade den varit omkring 94 %.[538]

Vi har kunnat påvisa ett samband mellan offentlig uppmärksamhet och debatt om personregistrering och integritet och allmänhetens beredvillighet att medverka i urvalsundersökningar som ingår i den officiella statistiken. SCB har varit inblandad i samtliga debatter även om myndigheten inte alltid varit huvudaktör. Att döma av bortfallsutvecklingen i AKU och i ULF från början av 80-talet har offentlig uppmärksamhet om behandlingen av personuppgifter i den officiella statistiken resulterat i en minskad vilja hos

538 SOU 1993:41 *Folk- och bostadsräkningen år 1990 och i framtiden*. Stockholm 1993, (s. 66-67). Svarsandelen för hela riket var 91 % före första påminnelse. Den slutliga svarsandelen var för riket 97 %.

allmänheten att bidra med uppgifter om sina personliga förhållanden. Denna minskning har varit övergående och förtroendet har sakta återhämtats. Dock aldrig riktigt till de nivåer som gällde innan. Denna slutsats stöds bara delvis av variationer i beredvilligheten att medverka i de andra undersökningarna.

Figur 4: Andel ej anträffade i urvalsundersökningar 1963-1993

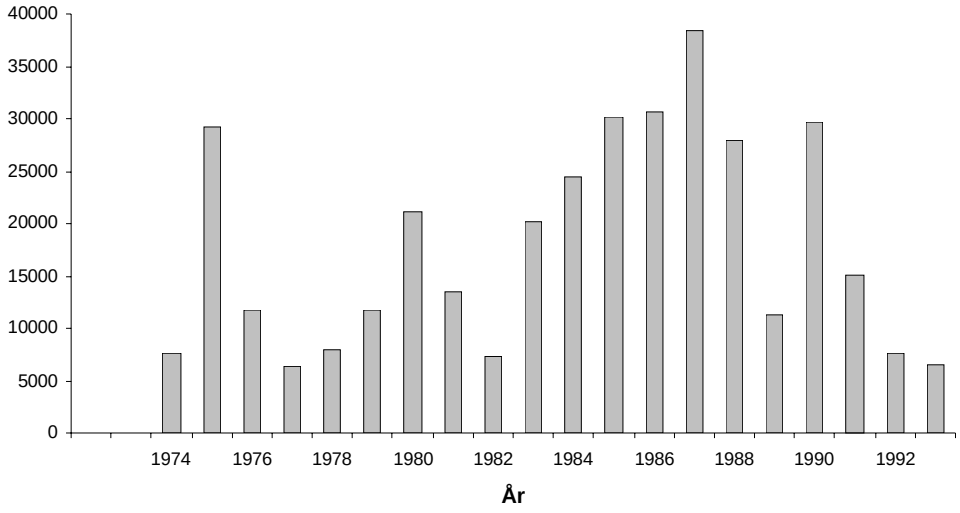


En annan svårighet att bedriva undersökningar med frivilligt uppgiftslämnande är att enskilda är svåra att anträffa, se figur 4. Det är ett resultat av ändrade levnadsvanor där arbetstiderna är mer oregelbundna, att en allt mindre del av fritiden tillbringas i hemmet och att många skaffar sig hemligt telefonnummer. Detta skall ses mot bakgrunden att en majoritet av urvalsundersökningarna genomförs med telefonintervjuer. En annan strategi att göra s.k. indirekta intervjuer, dvs. att fråga någon närstående till urvalspersonen om dennes personliga förhållanden, minskade kraftigt i mitten på 70-talet. Andelen ej anträffade har sedan 1985 åter ökat kraftigt. Det är i SCB:s telefonintervjuer ett lika stort problem som vägrarbortfallet, i AKU till och med ett större problem.

En annan indikator på allmänhetens förtroende för användningen av personuppgifter är möjligheterna till insyn genom 10 § datalagen. Enskild har rätt att en gång om året få veta om han förekommer i ett personregister och vilka uppgifter som finns om honom. I vår undersökning uppgav 11 procent av befolkningen att de någon gång begärt ett registerutdrag. För de flesta (65 %) låg den senaste begäran mer än 5 år tillbaka i tiden. Detta

tyder på att intresset för registerutdrag avtagit de senaste åren. Jag har låtit sammanställa uppgifter om antalet förfrågningar om registerutdrag hos myndigheter med ansvar för framställningen av den officiella statistiken, nämligen Statistiska centralbyrån, Socialstyrelsen och Riksförsäkringsverket. Uppgifter föreligger från SCB sedan tillkomsten av datalagen 1974.[539] Hos Socialstyrelsen finns uppgifter tillgängliga från 1985[540] och hos Riksförsäkringsverket från 1989[541], se figur 5–7. Dessa myndigheter har personregister över i princip hela den svenska befolkningen. Intresset för registerutdrag varierar mellan myndigheterna, år 1990 var ärendevolymen hos SCB 30 000, hos Riksförsäkringsverket 25 000 och hos Socialstyrelsen mindre än 5 000. Intresset har också varierat kraftigt över tid. Gemensamt för de tre är att intresset efter år 1990 markant har avtagit. Denna förändring inträffade tidigt hos Socialstyrelsen, redan efter 1986.

Figur 5: Statistiska centralbyrån, registerutdrag enligt 10 § datalagen 1974-1993, antal.

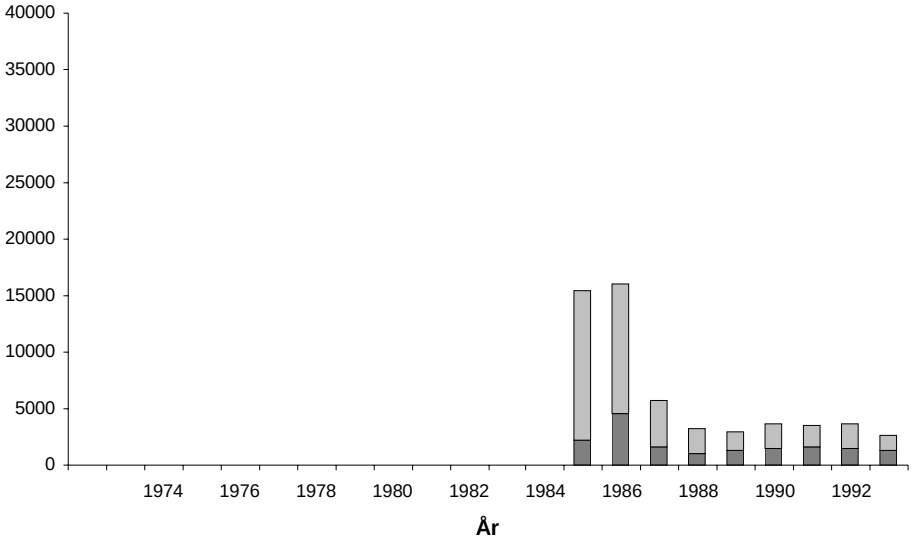


539 Muntlig uppgift av Kerstin Landgren 1994-03-07, SCB, Örebro.

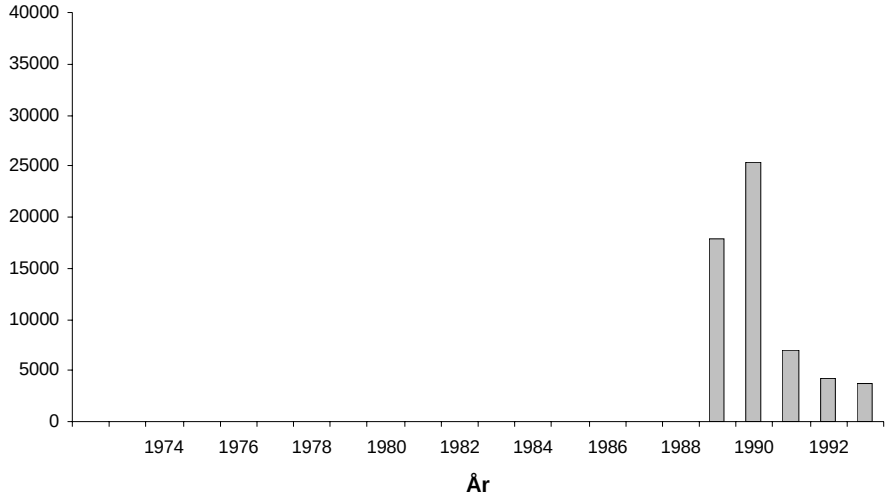
540 Muntlig uppgift Veijo Andersson 1994. Socialstyrelsen, Stockholm.

541 Muntlig uppgift av Britt-Marie Sélen 1994-03-17. Riksförsäkringsverket, ADB-avdelningen, Sundsvall.

Figur 6: Socialstyrelsen, registerutdrag enligt 10 § datalagen 1985-1993, antal



Figur 7: Riksförsäkringsverket, registerutdrag enligt 10 § datalagen 1989-1993, antal



Det är bara hos SCB som vi kan följa intresset för registerutdrag från 1974. Först 1975 gällde datalagen hela året. Hos SCB finns fyra perioder med högt intresse för registerutdrag. De kulminerar 1975, 1980, 1987 och 1990. Dessa perioder av högt intresse för registerutdrag har olika utsträckning i tiden. Den första perioden 1975 avtar året därpå. Intresset vid nästa period omkring 1980 blev inte lika stort men kan sägas omfatta föregående och nästföljande år. Från 1983 ökar intresset åter och varar fram till 1988. År 1987 inträffade en tillfällig uppgång då SCB:s högsta ärendevolym noterades med strax under 40 000 förfrågningar. Den senaste perioden av ökat intresse omfattade endast år 1990. Min hypotes att intresset varierar med

uppmärksamhet för data- och integritetsfrågor får stöd. Tidpunkter med ökat intresse för registerutdrag sammanfaller med tidpunkterna för en minskad beredvillighet att lämna uppgifter. Därtill kommer några nya. Det kan noteras att varje år med en folk- och bostadsräkning sammanfaller med ett stort intresse för registerutdrag. Vid dessa tidpunkter har åtminstone sedan FoB 85 förekommit debatter som har ifrågasatt folk- och bostadsräkningen. SCB har också på blanketten för uppgiftslämnande upplyst de uppgiftsskyldiga om deras rätt att begära registerutdrag. Därtill kommer uppgången år 1987. Enligt muntlig uppgift från SCB sammanhänger den med inrättandet av utbildningsregistret som också gav upphov till överklagande hos regeringen. Datainspektionen hade meddelat föreskrift om att 1/3 av de registrerade varje år skulle få ett registerutdrag utan att de själva begärt det. SCB överklagade beslutet hos regeringen.

Användning av uppgifter om enskilda hos myndigheter och företag

Frågan om utlämnande av uppgifter från Statens person- och adressregister (SPAR), vilket innehåller uppgifter från folkbokföring och taxering, har förekommit i SCB:s undersökningar vid tre tillfällen 1976, 1984 och 1976 och upprepades med några mindre justeringar även i vår undersökning 1995. Genom dessa undersökningar kan vi följa en utveckling över tid för ett minskat stöd för utlämnande av uppgifter från en myndighet till andra myndigheter och företag. De uppgifter det här är frågan om är var för sig offentliga hos de myndigheter som samlat in dem. Genom det statliga adress- och personregistret får de användas för uppdatering av adresser, direktreklam och urvalsdragning av dem som efterfrågar uppgifterna. Den enskilde kan begära att uppgifter om honom spärras mot direktreklam. Skall uppgifterna ingå i ett personregister krävs tillstånd från Datainspektionen om den registeransvarige saknar anknytning som följer av medlemskap, anställning eller kundförhållande. Den registeransvarige måste i sådana fall kunna åberopa särskilda skäl för att få registrera personer utan sådan anknytning. Det som får minst stöd hos allmänheten i dessa undersökningar är att uppgifter förs över till företag för kommersiell användning riktad mot privatpersoner. En mycket liten andel säger sig kunna acceptera detta. Från företagets sida handlar det om att värva nya kunder eller medlemmar. Även utlämnande av uppgifter till andra privata och offentliga

verksamheter utan anknytning till den registrerade har svagt stöd hos allmänheten. Överföring av folkbokföringsuppgifter till forskningsinstitution, Statistiska centralbyrån och Socialstyrelsen accepteras av omkring 25 %. Uppgifterna skall användas till urvalsdragningar för genomförande av bl.a. statistiska undersökningar. Verksamheter som den enskilde har anknytning till i egenskap av klient eller kund erhåller störst stöd för inhämtande av uppgifter från SPAR, dvs. överföringar av uppgifter till bank där den enskilde är kund och till socialtjänsten.

Tabell 4: Allmänhetens inställning till överföring av uppgifter från statens adress- och personregister 1995, procent.

	Ja	Kanske	Nej	Vet ej	Samtliga
Bank där du har konto	36	17	41	5	100
Socialtjänsten	30	20	40	8	100
Kreditupplysningsföretag	28	17	48	5	100
Statistiska centralbyrån	26	22	42	8	100
Forskningsinstitution	26	22	41	10	100
Socialstyrelsen	25	22	42	10	100
Försäkringsbolag där Du ej är kund	3	5	88	3	100
Reklamföretag	1	2	91	3	100

En fråga som uppmärksammats mycket är vilket inflytande enskilda skall ha över användningen av uppgifter för andra ändamål än de insamlats för. Det är en viktig dimension av begreppet personlig integritet. Utifrån principen om informerat samtycke skall den enskilde avgöra sådan användning. Det har också hävdats att den enskilde inte själv kan få bestämma fullt ut hur uppgifter om honom kommer till användning. Det finns situationer där den enskildes integritetsintresse måste få stå tillbaka till förmån för viktiga samhällsintressen. Det blir då en uppgift för politiska beslutsfattare att göra en sådan avvägning och i varje sådant fall noga ange på vilket sätt uppgifterna får användas. Vi ställde flera frågor som berörde detta. I en fråga gavs en kort beskrivning av hur uppgifter som enskilda lämnat i administrativa sammanhang också används för framställning av officiell statistik och i viss forskning. Frågan gällde vilket inflytande enskilda skulle ha över sådan användning. Mer än hälften, 59 % svarade att den enskilde måste själv bestämma om uppgifter om honom får komma till användning för forskning och statistik. En tredjedel kunde acceptera att enskilda skulle ha möjlighet att förhindra sådan användning och endast

4 % svarade att enskilda inte skulle ha möjlighet att själva avgöra detta. 6 % kunde inte ta ställning i frågan.

Det finns alltså ett starkt stöd bland allmänheten för att enskilda skall ha ett avgörande inflytande över användningen. Ytterligare en fråga ställdes som mer detaljerat angav förutsättningarna för att redan befintliga uppgifter kan få komma till nytta för forskning. Det gällde uppgifter hos försäkringskassan, 58 % instämde helt i påståendet att uppgifter inte fick användas för forskning utan urvalspersonens medgivande, ytterligare 19 % instämde delvis i påståendet. Ett motsatt påstående gällde att myndigheter inte behöver informera om uppgifter skall användas för statistik och forskning. Här var osäkerheten stor, 14 % kunde inte ta ställning till påståendet, majoriteten, 63 %, tog helt eller delvis avstånd från påståendet, 22 % instämde helt eller delvis.

Av de krav på insatser som kan ställas på den enskilde i egenskap av privatperson eller medborgare konstaterade vi tidigare att allmänheten har svårt att acceptera överföringar av uppgifter som de lämnat i något annat sammanhang för kommersiell användning. Sådan överföring har ägt rum innan den enskilde blir kontaktad genom direktreklam eller per telefon. Allmänheten upplever i mycket stor utsträckning att sådana kontaktförsök är besvärande. På liknande sätt kontaktas enskilda för medverkan i statistiska undersökningar. Detta upplevs i mindre grad som besvärande även om det saknas stöd för överföring av befintliga uppgifter för sådana ändamål. Om samhällsnyttan av sådana överföringar upplevs som angelägen kan allmänheten i högre utsträckning acceptera att detta äger rum, t.ex. vid överföringar av patientuppgifter till Socialstyrelsens cancerregister. Det upplevda besväret över att sådana överföringar sker varierar också med den förmodade nyttan. Det är i mindre grad besvärande med samkörningar för kontroll av bidragsfusk än om uppgifter används för den officiella statistiken. Även om sambearbetningar för angelägna samhällsbehov kan accepteras anser allmänheten att enskilda skall informeras och ha ett avgörande inflytande över denna användning.

BILAGA 6: LITTERATUR-FÖRTECKNING

INNEHÅLL:

OFFENTLIGT TRYCK

Departementsserien (Ds)

DsJu 1977:11	*Handlingssekretess och tystnadsplikt (Del 1) – Förslag till ny sekretesslag*
DsJu 1981:15	*Tillstånd och tillsyn enligt datalagen – Förslag till åtgärder på kort sikt m.m.* (Promemoria av Datalagstiftningskommittén)
DsC 1984:11	*Remissyttranden över statistikutredningens betänkande (SOU 1983:74) Framtida statlig statistik – En sammanställning från civildepartementet*
DsJu 1987:8	*Integritetsskyddet i informationssamhället 3 – Grundlagsfrågor* (Delbetänkande av Data- och offentlighetskommittén)
Ds 1989:24	*Datatekniken och den personliga integriteten i arbetet – en kartläggning*
Ds 1994:51	*Skyddet för enskilda personers privatliv – En studie* (gjord av Per Jermsten)
Ds 1994:80	*Elektronisk dokumenthantering inom skatteförvaltningen* (Promemoria av Per Furberg)
Ds 1996:19	*Lag om kriminalvårdsregister*
Ds 1996:38	*Moderna telekommunikationer åt alla*
Ds 1996:61	*Kassettersättning m.m.*
Ds 1996:70	*Översyn av registerlagarna inom socialförsäkringsadministrationen*
Ds 1996:71	*Rättsligt skydd för databaser*
Ds 1997:2	*Nya register för tullens brottsbekämpande verksamhet*

Statens offentliga utredningar (SOU)

SOU 1944:69	*Straffrättskommitténs betänkande med förslag till lagstiftning om brott mot staten och allmänheten*
SOU 1966:60	*Offentlighet och sekretess*
SOU 1972:47	*Data och integritet* (Delbetänkande av Offentlighets- och sekretesslagstiftningskommittén)
SOU 1972:49	*Tryckfriheten och reklamen* (Betänkande av Massmedieutredningen)
SOU 1975:22	*Lag om allmänna handlingar* (Betänkande av Offentlighets- och sekretesslagstiftningskommittén)

SOU 1975:49 *Massmediegrundlag* (Betänkande av Massmedieutredningen)
SOU 1977:19 *Radio och TV 1978–1985* (Betänkande av 1974 års radioutredning)
SOU 1978:54 *Personregister – Datorer – Integritet – Översyn av datalagen* (Delbetänkande av Datalagstiftningskommittén)
SOU 1980:8 *Privatlivets fred* (Betänkande av Integritetsskyddskommittén)
SOU 1980:31 *Offentlighetsprincipen och ADB* (Delbetänkande av Datalagstiftningskommittén)
SOU 1983:70 *Värna yttrandefriheten* (Förslag av Yttrandefrihetsutredningen)
SOU 1983:74 *Framtida statlig statistik* (Betänkande av Statistikutredningen)
SOU 1985:51 *Upphovsrätt 3 – Upphovsrätt och datorteknik* (Delbetänkande av Upphovsrättsutredningen)
SOU 1986:46 *Integritetsskyddet i informationssamhället 2 – Myndigheternas försäljning av personuppgifter m.m.* (Delbetänkande av Data- och offentlighetskommittén)
SOU 1987:31 *Integritetsskyddet i informationssamhället 4 – Personregistrering och användning av personnummer* (Delbetänkande av Data- och offentlighetskommittén)
SOU 1988:11 *Öppenhet och minne – Arkivens roll i samhället* (Betänkande av Arkivutredningen)
SOU 1988:64 *Integritetsskyddet i informationssamhället 5 – Offentlighetsprincipens tillämpning på upptagningar för automatisk databehandling* (Slutbetänkande av Data- och offentlighetskommittén)
SOU 1989:20 *Tullregisterlag m.m.* (Delbetänkande av Utredningen om lagstiftningsbehovet vid tulldatorisering [TDL-utredningen])
SOU 1989:74 *Forskningsetisk prövning – Organisation, information och utbildning* (Betänkande av Forskningsetiska utredningen)
SOU 1989:75 *Etisk granskning av medicinsk forskning – De forskningsetiska kommittéernas verksamhet* (En underlagsstudie från Forskningsetiska utredningen; Bengt Erik Eriksson)
SOU 1990:12 *Meddelarrätt – Meddelarfrihet i företag och föreningar, m.m.* (Betänkande av Meddelarskyddskommittén)

SOU 1990:43 *Förenklad statistikreglering* (Betänkande av Statistikregelutredningen)
SOU 1991:21 *Personregistrering inom arbetslivs-, forsknings- och massmedieområdena* (Delbetänkande av Datalagsutredningen)
SOU 1992:48 *Effektivare statistikstyrning – Den statliga statistikens finansiering och samordning* (Delbetänkande av 1990 års statistikutredning)
SOU 1992:84 *Ersättning för kränkning genom brott* (Delbetänkande av Kommittén om ideell skada)
SOU 1992:110 *Information och den nya InformationsTeknologin – Straff- och processrättsliga frågor m.m.* (Betänkande av Datastraffrättsutredningen)
SOU 1993:10 *En ny datalag* (Slutbetänkande av Datalagsutredningen)
SOU 1993:32 *Ny anställningsskyddslag* (Delbetänkande av 1992 års arbetsrättskommitté)
SOU 1993:83 *Statistik och integritet Del 1* (Delbetänkande av Integritetsskyddsutredningen)
SOU 1993:110 *Integritet och effektivitet på kreditupplysningsområdet* (Slutbetänkande av Kreditupplysningsutredningen)
SOU 1994:1 *Ändrad ansvarsfördelning för den statliga statistiken* (Betänkande av Genomförandekommittén)
SOU 1994:17 *Års- och koncernredovisning enligt EG-direktiv – En anpassning av den svenska redovisningslagstiftningen till EG:s fjärde, sjunde och elfte bolagsdirektiv* (Delbetänkande av Redovisningskommittén)
SOU 1994:30 *Vallagen* (Slutbetänkande av 1993 års vallagskommitté)
SOU 1994:63 *Personnummer – integritet och effektivitet* (Betänkande av Personnummerutredningen)
SOU 1994:65 *Statistik och integritet Del 2* (Slutbetänkande av Integritetsskyddsutredningen)
SOU 1994:83 *Övergång av verksamheter och kollektiva uppsägningar – EU och den svenska arbetsrätten* (Delbetänkande av 1992 års arbetsrättskommitté)
SOU 1994:105 *Ny lagstiftning om radio och TV* (Slutbetänkande av Radiolagsutredningen)
SOU 1995:86 *Dokumentation och socialtjänstregister* (Slutbetänkande av Socialtjänstkommittén)

SOU 1995:92 *EG:s arbetstidsdirektiv och dess konsekvenser för det svenska regelsystemet* (Delbetänkande av 1995 års arbetstidskommitté)
SOU 1995:95 *Hälsodataregister Vårdregister* (Betänkande av Hälsodatakommittén)
SOU 1995:115 *Ny lag om europeiska företagsråd* (Delbetänkande av 1995 års Arbetsrättskommission)
SOU 1995:122 *Reform på recept* (Delbetänkande av HSU 2000)
SOU 1995:147 *Förbättrad tillsyn över hälso- och sjukvårdspersonal* (Betänkande av Utredningen om förbättrad tillsyn över hälso- och sjukvårdspersonalen)
SOU 1996:35 *Kriminalunderrättelseregister DNA-register* (Delbetänkande av Registerutredningen)
SOU 1996:40 *Elektronisk dokumenthantering* (Betänkande av IT-utredningen)
SOU 1996:63 *Medicinska undersökningar i arbetslivet* (Betänkande av Utredningen om medicinska undersökningar i arbetslivet)
SOU 1996:72 *Rättspsykiatriskt forskningsregister* (Betänkande av Utredningen om register för forskning inom rättspsykiatrin)
SOU 1996:88 *Kameraövervakning* (Slutbetänkande av Utredningen om användningen av övervakningskameror)
SOU 1996:94 *Nationell teleadresskatalog* (Betänkande av Katalogutredningen)
SOU 1996:157 *Översyn av redovisningslagstiftningen* (Slutbetänkande av Redovisningskommittén)
SOU 1997:3 *Fastighetsdataregister* (Betänkande av Fastighetsdatautredningen)

Propositioner

Prop. 1948:230 *med förslag till tryckfrihetsförordning m.m.*
Prop. 1973:33 *med förslag till ändringar i tryckfrihetsförordningen, m.m.*
Prop. 1973:90 *med förslag till ny regeringsform och ny riksdagsordning*
Prop. 1973:123 *med förslag till ändring i tryckfrihetsförordningen*
Prop. 1975/76:160 *om nya grundlagsbestämmelser ang. allmänna handlingars offentlighet*
Prop. 1975/76:209 *om ändring i regeringsformen*
Prop. 1978/79:109 *om ändring i datalagen*

Prop. 1979/80:2 *Förslag till sekretesslag m.m.*
Prop. 1980/81:20 *om besparingar i statsverksamheten, m.m.*
Prop. 1981/82:37 *om offentlighetsprincipen och ADB*
Prop. 1981/82:189 *om ändring i datalagen m.m.*
Prop. 1984/85:133 *om skärpningar av statistiksekretessen*
Prop. 1984/85:189 *om patientjournallag m.m.*
Prop. 1986/87:116 *om ändring i datalagen*
Prop. 1986/87:151 *Ändringar i tryckfrihetsförordningen m.m.*
Prop. 1987/88:57 *om grundlagsfäst integritetsskydd*
Prop. 1988/89:85 *om upphovsrätt och datorer*
Prop. 1989/90:40 *om tullregisterlag m.m.*
Prop. 1989/90:72 *om arkiv m.m.*
Prop. 1989/90:90 *Forskning*
Prop. 1990/91:53 *om lag om folkbokföringsregister, m.m.*
Prop. 1990/91:60 *om offentlighet, integritet och ADB*
Prop. 1990/91:64 *om yttrandefrihetsgrundlag m.m.*
Prop. 1990/91:126 *om följdlagstiftning med anledning av den nya summariska processen, m.m.*
Prop. 1991/92:118 *om förenklad statistikreglering*
Prop. 1991/92:170 *Bilaga 9 Den s.k. EES-propositionen – Arbetsmarknadsdepartementet*
Prop. 1992/93:48 *Ändringar i de immaterialrättsliga lagarna med anledning av EES-avtalet, m.m.*
Prop. 1992/93:75 *Satellitsändningar av TV-program*
Prop. 1992/93:101 *om den statliga statistikens finansiering och samordning*
Prop. 1992/93:193 *om sjukförsäkringsregister hos de allmänna försäkringskassorna*
Prop. 1993/94:67 *om ändringar i lagen om anställningsskydd och i lagen om medbestämmande i arbetslivet*
Prop. 1993/94:100 *Bilaga 8 Budgetpropositionen 1994 – Finansdepartementet*
Prop. 1993/94:116 *Normgivningsfrågor på dataskyddsområdet, m.m.*
Prop. 1993/94:197 *Datapantbrev*
Prop. 1993/94:217 *En reformerad datalag*
Prop. 1993/94:224 *Ändringar i skatteregisterlagen, m.m.*
Prop. 1993/94:235 *Lag om arbetsförmedlingsregister*
Prop. 1994/95:8 *Lag om socialförsäkringsregister*
Prop. 1994/95:19 *Sveriges medlemskap i Europeiska unionen (Del 1)*
Prop. 1994/95:34 *Den svenska tullagstiftningen vid ett EU-medlemskap*
Prop. 1994/95:50 *Nya kapitaltäckningsregler m.m.*

Prop. 1994/95:93 *Elektronisk dokumenthantering inom skatteförvaltningen, m.m.*
Prop. 1994/95:100 *Bilaga 3 Förslag till statsbudget för budgetåret 1995/96 – Justitiedepartementet*
Prop. 1994/95:102 *Övergång av verksamheter och kollektiva uppsägningar*
Prop. 1994/95:144 *Riktlinjer för registrering av påföljder m.m.*
Prop. 1994/95:168 *Elektronisk dokumenthantering inom exekutionsväsendet m.m.*
Prop. 1994/95:200 *Lag om vissa personregister för officiell statistik m.m.*
Prop. 1994/95:201 *Avisering av folkbokföringsuppgifter*
Prop. 1994/95:227 *Hemlig teleavlyssning och hemlig teleövervakning*
Prop. 1995/96:90 *Registerbaserad folk- och bostadsräkning år 2000 m.m.*
Prop. 1995/96:125 *Åtgärder för att bredda och utveckla användningen av informationsteknik*
Prop. 1995/96:160 *Radio- och TV-lag*
Prop. 1995/96:162 *EG:s arbetstidsdirektiv*
Prop. 1995/96:163 *Europeiska företagsråd*
Prop. 1995/96:176 *Förstärkt tillsyn över hälso- och sjukvården*
Prop. 1996/97:5 *Forskning och samhälle*
Prop. 1996/97:27 *Läkemedelsförmåner och läkemedelsförsörjning m.m.*
Prop. 1996/97:65 *Ändringar i kreditupplysningslagen*
Prop. 1996/97:70 *Ny vallag*

Utskottsbetänkanden

KU 1987/88:19 *om grundlagsfäst integritetsskydd (prop. 1987/88:57)*
KrU 1989/90:29 *Arkiv m.m.*
LU 1989/90:37 *Skydd för företagshemligheter*
KU 1990/91:11 *Offentlighet, integritet och ADB*
KU 1992/93:32 *Förslag till en lag om personregister i riksdagens informationssystem Rixlex*
KU 1994/95:10 *Vissa datalagsfrågor*
SkU 1994/95:15 *Elektronisk dokumenthantering inom skatteförvaltningen*
LU 1994/95:27 *Elektronisk dokumenthantering inom exekutionsväsendet m.m.*
KU 1995/96:13 *Registrering av ledamöternas ekonomiska intressen*
KU 1995/96:29 *Radio- och TV-frågor*
UbU 1996/97:3 *Forskningspolitiken*

Utredningsdirektiv

Dir. 1984:48 *(Data- och offentlighetskommittén [Ju 1984:06]; tilläggsdirektiv)*

Dir. 1989:26 *(Datalagsutredningen [Ju 1989:02])*

Dir. 1992:50 *(Kommittédirektiv till kommittéer och särskilda utredare att redovisa regionalpolitiska konsekvenser)*

Dir. 1993:7 *(Personnummerutredningen [Ju 1993:01])*

Dir. 1994:23 *(Direktiv till samtliga kommittéer och särskilda utredare att pröva offentliga åtaganden)*

Dir. 1994:104 *(Mediekommittén [Ju 1994:13])*

Dir. 1994:124 *(Direktiv till samtliga kommittéer och särskilda utredare att redovisa jämställdhetspolitiska konsekvenser)*

Dir. 1995:38 *(Registerutredningen [Ju 1995:01])*

Dir. 1995:96 *(Utredningen [S 1995:07] om register för forskning inom rättspsykiatrin)*

Dir. 1995:120 *(Utredningen om fastighetsdatasystemets författningsreglering [Ju 1995:09])*

Dir. 1995:125 *(Katalogutredningen [K 1995:06])*

Dir. 1996:14 *(Pliktregisterutredningen [Fö 1996:03])*

Dir. 1996:22 *(Registerutredningen [Ju 1995:01])*

Dir. 1996:31 *(Utredningen om det allmännas skadeståndsansvar vid överträdelse av EG-rätten [Ju 1996:04])*

Dir. 1996:43 *(Grunddatabasutredningen [Fi 1996:06])*

Dir. 1996:49 *(Direktiv till samtliga kommittéer och särskilda utredare att redovisa konsekvenser för brottsligheten och det brottsförebyggande arbetet)*

Dir. 1996:55 *(Utredningen om åtgärder mot vissa bulvanförhållanden m.m. [Ju 1996:06])*

Dir. 1996:89 *(En utredning om register för skattebrottsutredningar m.m.)*

Dir. 1996:108 *(En utredning om bostadsrättsregister samt frågor om förvärv och pantsättning av bostadsrätt [Ju 1996:10])*

Dir. 1996:117 *(En utredning om en översyn av bestämmelserna inom trafikregisterområdet [K 1996:06])*

Övrigt

Statsrådsberedningens PM 1996:4; *Redaktionella och språkliga frågor i EU-arbetet*

ÖVRIG LITTERATUR

Bernitz, Ulf m.fl.; *Immaterialrätt*, 5 uppl. 1995

Blume, Peter; ”*Arbejdsmarked og persondatabeskyttelse*” i UfR B 1996 s. 427 ff.

Blume, Peter; *Personregistrering*, 3. rev. udgave, 1996

Bohlin, Alf; *Allmänna handlingar*, 1988

Bohlin, Alf; ”*Offentlighet och sekretess i myndighets forskningsverksamhet*” i Förvaltningsrättslig tidskrift 1996 s. 183 ff.

Bohlin, Alf; *Offentlighetsprincipen*, 4 uppl., 1994

Cappelen-Smith, Hans; ”*Behöver lagstiftningen om emissionsprospekt reformeras?*” i SvJT 1996 s. 205 ff.

Corell, Hans m.fl.; *Sekretesslagen – Kommentar till 1980 års lag med ändringar*, 3 uppl., 1992

Europarådet; *Data protection and the media – Study prepared by the Committee of Experts on Data Protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ)*, 1991

Evers, Jan; *EG och behandling av personuppgifter*, 1993

Fahlbeck, Reinhold; ”*Employee Privacy in Sweden*” i Comparative Labor Law Journal, volym 17, nr 1, 1995, s. 139 ff.

Fahlbeck, Reinhold; ”*Employee Privacy in Sweden*” i JT 1991–92 s. 41 ff.

Freese, Jan; *Rapport om skyddet för enskilda personers privatliv – ett mer samlat grepp?*, 1995

Gränström, Claes & Lundquist, Lennart & Fredriksson, Kerstin; *Arkivlagen – Bakgrund och kommentarer*, 1992

Hiselius, Patrik; *SCB:s statistikverksamhet och gällande rätt*, IRI-rapport 1990:7

Holmberg, Erik & Stjernquist, Nils; *Grundlagarna med tillhörande författningar*, 1980

Hultqvist, Anders; *Legalitetsprincipen vid inkomstbeskattningen*, 1995

Koktvedgaard, Mogens & Levin, Marianne; *Lärobok i immaterialrätt*, 4 uppl., 1996

Koskull, Anders von; ”*Personvärn och personalrekrytering, eller transformation och skygglappar*” i FJFT 1996 s. 391 ff.

Kring, Claes & Wahlqvist, Sten; *Datalagen med kommentarer*, 1989

Magnusson Sjöberg, Cecilia; *Rättsautomation – Särskilt om statsförvaltningens datorisering*, 1992

Michael, James; *Privacy and Human Rights – International and Comparative Study, with Special Reference to Developments in Information Technology*, 1994

Petersson, Bo; *Forskning och etiska koder*, 1994

Påhlsson, Robert; *Riksskatteverkets rekommendationer – Allmänna råd och andra uttalanden på skatteområdet*, 1995

Riksrevisionsverket; *Principer för prissättning av informationstjänster*, RRV 1995:64

Seipel, Peter; *ADB-upptagningars offentlighet – Rapport till Data- och offentlighetskommittén*, IRI-rapport 1988:1 (intagen som bilaga 2 till SOU 1988:64)

Seipel, Peter; *Juristen och datorn – Introduktion till rättsinformatiken*, 5 uppl., 1994

Seipel, Peter; *Offentlighetens begrepp – TF, ADB och allmänna handlingar*, IRI-rapport 1983:8

Statistiska centralbyrån; *Data och integritet – Allmänhetens kunskaper och attityder allmänt och till SCB*, 1985

Statistiska centralbyrån; *Datorvanor 1995 – Undersökning gjord på uppdrag av IT-kommissionen*, 1995

Statistiska centralbyrån; *SCB och allmänheten – Resultat från en intervjuundersökning våren 1976*, 1977

Statistiska centralbyrån; *SCBs image 1986 – En enkätundersökning*, 1987

Strömberg, Håkan; *Normgivningsmakten enligt 1974 års regeringsform*, Andra upplagan, 1989

Strömberg, Håkan; *Tryckfrihetsrätt och annan yttrandefrihetsrätt*, 11 uppl., 1995

Strömholm, Stig; ”*Integritetsskyddet – Ett försök till internationell lägesbestämning*” i SvJT 1971 s. 695 ff.

Suviranta, Antti; ”*Workers Privacy in Finland*” i Comparative Labor Law Journal, volym 17, nr 1, 1995, s. 45 ff.

Toppledarforum; *Elektronisk post och katalog i offentlig förvaltning – En förstudie*, 1995

Toppledarforum; *Offentlighet & IT – Vägledning för den offentliga förvaltningen*, Statskontoret 1995:14

Toppledarforum; *LEXIT – Förstudie*, 1995

BILAGA 7: SUMMARY IN ENGLISH

INTEGRITY • RIGHT-OF-ACCESS • INFORMATION TECHNOLOGY

SUMMARY

A new Personal Data Protection Act

Our task has been to conduct a review of the current Data Protection Act which has been in force since 1973. The aim has been to produce modern, technically independent legislation to protect personal integrity in the processing of personal information.

The draft we now submit for an entirely new Personal Data Protection Act is largely based upon a recent EU directive in this field. A prerequisite for being able to submit a draft law of this kind was that the directive should be in line with what is protected under the Swedish constitution or what is otherwise of particular importance from a Swedish point of view. The new legislation must not impinge upon the constitutional right for every citizen to have access to documents and data held by authorities (*the right-of-access principle*), nor upon freedom of expression or freedom of the press. This prerequisite has been fulfilled. Sweden's participation in the final negotiations enabled Sweden's viewpoints to be taken into consideration in the directive. We propose unambiguous provisions in the new Personal Data Protection Act which make clear that the Act should not be applied to an extent which would curtail rights protected by the constitution. Accordingly the proposed Act neither affects nor changes these rights.

In common with the EU directive the proposed legislation is based upon regulation of the actual handling of data containing personal infor-

mation. An alternative would be to allow the handling of personal information to remain largely free, only seeking to prevent any handling which might be deemed as misuse of that information. With due regard to the unease which many people increasingly feel towards collections of electronic data relating to themselves, we have decided that the time is not right to allow largely unrestricted handling of computer based personal information. Neither would Sweden fulfil its international commitments if we were to choose a model entirely different from that of the EU directive. However, we consider that, in the long term, a policy of constraint and legal steps against misuse would be preferable to regulation of a kind of data handling which virtually anyone can engage in.

The proposed Personal Data Protection Act may be seen as a framework which provides guidelines for all processing of personal data. The aim is that the Government and the Swedish Data Inspection Board should be able to make the regulations more precise within this legal framework. The special register statutes which include rules for many important public records, are not part of our brief. We would like to point out that these provisions must be reviewed in the coming years and be adapted to the new Personal Data Protection Act.

Purely private use of personal data is outside the bounds of the proposed Act. One such example of this worthy of mention is E-Mail between private persons.

The expression “processing of personal data” comprises everything which can be done with such data, e.g. the retrieval, collection, storage and dissemination of data. Processing of personal data which is partly or wholly automatic, i.e. largely computerised, comes under the proposed Act. Manual processing of such data (on paper) is only included if the data is to form part of a proper register.

The proposed Act defines certain basic requirements for all processing of personal data. The person responsible for the processing of personal data (*the controller*) must ensure that the data is only collected for certain expressly stated and justifiable purposes. The data may not later be used for any purpose incompatible with the ones for which the data was originally collected. Superfluous data may not be processed, and that data which is processed must be adequate and relevant. Inaccurate, misleading or incomplete data must be corrected. The data may be stored only as long as is necessary with respect to the purposes of the processing. There are special rules for data which is processed for historical, statistical or scientific purposes.

The proposed Act contains a comprehensive list of cases in which personal data may be processed. Personal data may always be processed if the individuals in question (*the data subjects*) have given their consent. In other cases the processing must be necessary for the attaining of certain stated purposes. Those situations in which processing may be undertaken without consent may be summarised as follows:

- In connection with a contract
- In order to fulfil a legal obligation
- In order to protect vital interests of the data subject
- In order to carry out a task of public interest or in connection with the exercising of official authority
- After a balance of interests where the interests of the data subject are weighed against the interests on the part of the controller

The proposed Act contains special rules applying to the processing of sensitive personal data. Sensitive data includes information relating to a person's health or sex life and data which reveals race, ethnic origin, political opinions, religious or philosophical beliefs, or membership of a trade union. Such data may only be processed in those cases listed in the Act. However, the Government or the Data Inspection Board may permit the processing of sensitive personal data in other cases provided that it is necessary on grounds of substantial public interest.

Sensitive data may be processed when the data subject has given his/her consent or when he or she has manifestly made the data public. Those cases in which data relevant to the purpose of the processing may otherwise be processed can be summarised as follows.

- In order to fulfil obligations or to exercise rights within the field of labour law
- In order to protect vital interests when the data subject is unable to give his/her consent
- In order to establish, exercise or defend legal claims
- Inside non-profit organisations sensitive data, e.g. relating to members and sympathisers may be processed, but may not be disclosed to a third party
- Within the health service
- For scientific research and statistics purposes where a research ethics committee has approved the project or where the public interests clearly override the risks to integrity

As a principal rule, data pertaining to criminal offences, etc., may only be processed by public authorities. As is the case today, the national personal identification number may only be used when it is clearly motivated by the purpose of the data processing, the importance of a definite identification or any other significant reason.

The data subjects shall be informed about the processing of their data. The proposed Act stipulates that the controller shall at his own initiative provide information about the processing to the data subject. However, in cases where data is collected from any other source than the data subject himself, it is not necessary to notify the person concerned if the registration or disclosure of the data is regulated by statute or if the effecting of the notification would involve a disproportionate effort.

The proposal states that the data subject shall have the right to request, free of charge, once per year information relating to the data being processed, i.e. a transcript from the registers. The controller shall, on request, correct any personal data which is inaccurate, misleading or incomplete, or which has otherwise not been processed in accordance with current regulations.

Certain restrictions are proposed for transfers of personal data outside the EU and the EEA.

The proposed Act contains regulations pertaining to security in the processing of personal data.

The current obligation to report processing to the Data Inspection Board should be kept to a minimum. Instead, the Board should concentrate on supervision, information and advice. The Data Inspection Board shall also issue instructions which clarify the provisions of the Act in various areas.

If anyone contravenes the proposed Act, the Data Inspection Board shall seek to achieve rectification. The proposal allows the Board to impose penalties and to bring cases aimed at erasing the personal data in question.

Broadly speaking, the penalties for violation of the proposed Act primarily comprise damages to injured data subjects. As has been the case up to now, they shall, in addition to other compensation, have a right to general (punitive) damages for the violation of their rights. In principle, there should be a strict liability for damages, i.e. damages should be paid out as soon as the rules have been broken. However, we propose that, within reason, damages shall be reduced in cases where the controller can

prove that the incorrect processing was not dependent on his or her action or failure to take action.

The proposed Act should come into force on January 1, 1999 and be fully applied to all processing commenced thereafter. For processing already underway when the Act comes into force, the former Data Protection Act should apply up until October 2001.

The principle of right-of-access in the IT society

The second part of our task has been to review the provisions of Chapter 2 of the Freedom of the Press Act concerning citizens' rights to gain access to public documents (documents received or created by an authority including manual or electronic registers) – the right-of-access principle. The aim has not been to alter this principle, but rather to investigate how it can be applied in a modern IT environment. We have set out two premises for this work:

- Right-of-access shall be as broad as possible
- The rules must be clear and simple to apply

Wide reaching right-of-access provides checks on power, thus helping to strengthen democracy. Our proposal also aims at extending in the long term the possibilities for the general public to gain benefit from the enormous amounts of data held by the public authorities.

We propose that the central concept of the right-of-access principle should be "public data" rather than "public document". The concept of data is technically neutral, and the Official Secrets Act is already based upon it. In this respect the proposed amendments do not involve any major objective changes: if one today can obtain access to a document one should according to our proposal have access to the data contained in that document. One improvement is that one no longer needs to resort to hypothetical notions, such as the expression "potential documents", for electronic records to be included in the right-of-access principle.

We propose that the concept of a document shall remain in the Act as a "storage space" for data. A document has a defined content, namely the content which the person who once wrote the document ascribed to it. It is of no significance whether the document takes the form of a piece of paper or if it exists in digital form.

We refer to those storage spaces which do not constitute documents as databases. What typifies a database is that individual elements of data are

arranged in such a way that they can be searched, and that they can be combined in various ways. Registers are typical examples of databases. Manual databases and those maintained via digital technology have the same status.

Thus data may either be found in documents or in databases.

One prerequisite for data to be public within a public authority is that it is in the keeping of that authority. In the 1970s a rule was introduced which provides that all data technically accessible to an authority is deemed as in the keeping of that authority. In the mainframe computer environment of that time, such a rule was reasonable. However, we observe that such a rule cannot be applied in a modern IT environment in which virtually everything is "technically available", e.g. via Internet. One prerequisite for the right-of-access principle to be able to function in practice is that the boundaries between authorities are maintained. Authorities otherwise will have impaired capacity for keeping their data in order, impairing the preconditions for the general public to be able to locate it.

We propose that the concept of "storage" should reassume its original meaning, but that it should also include electronic storage. The obligations of an authority to release public data should thus comprise such data as it stores, either purely physically (on paper, CD-ROM, floppy- or hard disk) or logically (in an electronic file belonging to the authority).

Data contained in an authority's library is not affected by the right-of-access principle. The new way of regarding storage means that this provision can be simplified. A book in a library should be treated in the same way regardless of whether it is printed on paper or if it is stored on a CD-ROM.

In cases where the general public want certain information, authorities are currently assumed to have a certain obligation to make extra searches and compilations over and above their normal course of work. Usually, anything which can be produced by "routine measures" is deemed to be a public document. This should also apply in future, but should be related to costs. An authority should have a duty to carry out any extra work which can be carried out without incurring significant costs. Since technology will provide even broader and cheaper opportunities to search for and compile data, the future ability of the general public to gain insight into the workings of authorities and to share in their knowledge will increase.

Regarding the actual issue of public data to the general public, we propose that the right-of-access principle be extended. According to our proposal, it should also include a right to obtain public data in electronic form.

We are aware that such a right could not be introduced generally and immediately. According to the proposed stipulation the general public's right to obtain public data on disk or via E-Mail must be adapted to the particular authority's technical capabilities. Since these are continually being improved, insight will also become more effective. There may be certain special regulations which forbid an authority to issue data in digital form, and in certain cases such an issue might be subject to secrecy legislation, but the principle should be that one has the same right to obtain data in electronic form as on paper. This should, in the long run at least, be a positive development also for the authorities who will cut down on their dependence on costly paper handling.

The right to obtain data in electronic form should not include computer programs since this might infringe upon copyright. On the other hand, we consider that there is a public interest in finding out how various authorities' computer programs work. This is especially true in cases where the authority makes automated decisions using computer programs. In order to strengthen public insight, we therefore propose that the authorities, where such programs are used, should be obliged to provide descriptions (system documentation) on how those programs work.

Our proposal for new concepts in the Freedom of the Press Act, which form part of our constitution, will necessitate consequential changes in statutes and regulations of inferior rank. We submit proposals for such changes in the Official Secrets Act and the Archives Act.

The Freedom of the Press Act does not currently stipulate what will happen to public documents when they are no longer current. Since it is of major practical importance for public insight that public data be stored and preserved, we propose the introduction of a provision in the Freedom of the Press Act which refers to the Archives Act.

The following committee members expressed dissenting opinions: Anders Christner (Christian Democrat Party), Tomas Ohlin (Liberal Party) and Inger René (Moderate Party) jointly, and Bo Edvardsson (Green Party).

Statements of opinion were submitted by Bo Edvardsson (Green Party), by Jan Evers with Rolf Nygren, and by Barbro Fischerström, Anders S Forsberg, Jan Freese and Margareta Åberg.