Peter Blume

Persondata-beskyttelse i den private sektor

– retspolitiske overvejelser

FSRs Perspektiv-serie

FSRs Forlag 1995
Foreningen af Statsautoriserede Revisorer

Persondatabeskyttelse i den private sektor

Omslag ved art/Grafik
Bogen er sat med Plantin og trykt hos
N. Christensen Grafik ApS
Printed in Denmark 1995

ISBN 87-7747-142-3

Redaktionens forord

Formålet med FSRs Perspektiv-serie er på et højt teoretisk/fagligt niveau at præsentere problemstillinger inden for de fire fagområder Revision, Regnskab, Skatteret og Erhvervsret, der indgår i revisorkandidatuddannelsen.

Målgruppen for serien er de studerende ved handelshøjskoler og universiteter samt praktiserende revisorer og advokater. Det er redaktionens håb, at tillige dansk erhvervsliv vil finde emner af interesse i serien.

Det er redaktionens målsætning, at emnerne, ud over at være relevante for målgrupperne, skal synliggøre seneste forskning samt indeholde et fremtidsorienteret og gerne internationalt element og dermed give serien perspektiv.

Perspektiv-seriens redaktion består af:

Forord

I denne bog gennemføres en retspolitisk orienteret diskussion af databeskyttelsesretten i den private sektor. Bogens formål er dermed ikke i første række at redegøre for gældende ret, hvorom der henvises til Peter Blume: Personregistrering (2. udgave København 1992).

Databeskyttelsesretten har de senere år fået stadig større praktisk betydning for det private erhvervsliv. I takt med, at personrelateret information har fået stigende økonomisk og konkurrencemæssig betydning, samtidig med at den moderne informationsteknologi har vundet solidt fodfæste, er databeskyttelsesretten blevet tilsvarende vigtig.

Det må forventes, at EU inden længe gennemfører et generelt direktiv om persondatabeskyttelse og at dette udløser et behov for betydelige ændringer af dansk ret. De retspolitiske spørgsmål vil have stor aktualitet i de kommende år.

Det er mit håb, at denne bog kan yde et bidrag til denne retspolitiske debat og herved fremme en regulering, der på et fornuftigt grundlag afbalancerer erhvervslivets behov for persondataanvendelse og hensynet til beskyttelse af det enkelte menneskes personlige integritet og privatliv.

Peter Blume
København, juni 1994

Indhold

1 Den almene baggrund

1 Privatlivets fred

Beskyttelsen af privatlivets fred har en lang tradition i dansk ret. Selv om der ikke findes en almindelig regel herom i grundloven, men alene en særlig bestemmelse om boligens ukrænkelighed (§ 72), er der ikke større tvivl om, at der er tale om en rettighed, som de fleste borgere anser for meget væsentlig. Det er en form for retsværn, der har til formål at yde individet en beskyttelse både i forhold til offentlige myndigheder og til det private erhvervsliv. Det er et væsentligt karakteristikon, at behovet for privatlivsbeskyttelse ikke blot er aktuelt i forholdet mellem det offentlige og borgerne, men også har betydning mellem borgerne og erhvervslivet samt for borgerne indbyrdes. Denne beskyttelse er baseret på det grundsynspunkt, at det enkelte individ har en privat sfære, der skal værnes mod andres indtrængen, enten således at der opstilles et egentligt forbud herimod eller således, at bestemte betingelser skal være opfyldt for, at værnet om privatlivet brydes.

I en grundlæggende artikel i Harvard Law Review 1890[1] opstillede to fremtrædende jurister, Samuel D. Warren and Louis D. Brandeis, to basale rettigheder for individet. Først »the right to be let alone«, d.v.s. retten til at være i fred, hvilket kan videreføres til en antagelse om, at der er et privat råderum, som det enkelte individ har fuld ret over. For det andet »the right to selfdetermination«, d.v.s individets selvbestemmelsesret. Der er bestemte forhold, som kan betegnes »private« med den konsekvens, at individet skal være indforstået med, at andre får kendskab til disse. Som det vil fremgå nærmere i det følgende, har disse to basale rettigheder fortsat stor betydning ved en fastlæggelse af det private område

1. The Right to Privacy p. 193-220.

i det moderne samfund.

Privatlivets fred, der kan give anledning til filosofiske overvejelser af nærmest essentiel karakter, kan under en juridisk betragtningsmåde udmøntes på forskellig måde alt afhængig af, hvad der konkret er beskyttelsesobjektet. De retlige regler og de synspunkter, der betinger deres udformning, vil være forskellige om det er individets fysiske person, om det er iagttagelser af personen (fotografier og lignende), om det er individets ejendom, eller om det er information om personen, der gøres til genstand for beskyttelsesregler. De her nævnte områder har alle en eller anden form for beskyttelse i straffeloven, jfr. særligt bestemmelserne i denne lovs kapitel 27. Disse almindelige regler må dog suppleres af andre bestemmelser for at opnå en effektiv retsbeskyttelse.

Denne bogs emne er det den retlige regulering af privat/personlig information. Der er tale om et aspekt af privatlivets fred, der har påkaldt sig betydelig interesse i moderne tid, og hvor den retlige regulering har stor betydning i den praktiske dagligdag. I takt med, at informationssamfundet er vokset frem, er den almene betydning af også personrelateret information steget markant, og dermed har retlig regulering på dette område væsentlige praktiske konsekvenser.

Det er i denne henseende karakteristisk, at der i moderne tid er udviklet teknologier, som gør det muligt langt mere indgribende, end det hidtil har været tilfældet at trænge ind på privatlivets område og overvåge samt kontrollere dette område. Beskyttelsesbehovet har fået øget aktualitet. Det er ikke mindst den udbredte anvendelse af edbteknologien, der har sat fokus på behovet for beskyttelse af personlig information. Det er denne teknologi, der danner udgangspunktet for det moderne personværn, der omtales nærmere nedenfor.

Den stadige hurtige udvikling af edb-teknologien stiller nye udfordringer til retssystemet og rejser konstant spørgsmålet om, hvor intensivt den retlige regulering skal være, og om der er en tilstrækkelig tungtvejende begrundelse for beskyttelsesregler, hvis virkning er, at mulighederne for at nyttiggøre personlig information begrænses for andre. Det er denne problemstilling, der gennemsyrer store dele af denne bog. Der er tale om et dilemma, der gør det særdeles vanskeligt at fastlægge indholdet af de enkelte regler. Det-

te må ske ud fra en delikat afbalancering mellem informationsbeskyttelse og informationsanvendelse.

2 Menneskerettighedskonventionen

Som nævnt ovenfor findes der ikke i den danske grundlov en almindelig beskyttelse af privatlivets fred. En sådan regel findes derimod i den Europæiske Menneskerettighedskonvention 1950, artikel 8, der har følgende ordlyd:

»Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.

Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder«.

Efter at det i mange år havde været omdiskuteret, hvilken retskildemæssig status konventionen har i national ret, d.v.s. i forhold til borgerne, blev konventionen ved lov nr. 285 af 29.4.1992 utvivlsomt til en del af dansk ret. Konventionen må antages at have en særlig status, således at dens bestemmelser kun vil kunne fraviges, såfremt der er utvivlsom klar hjemmel hertil i en lov udstedt efter april 1992. På denne baggrund er det klart, at der i dansk ret er en forpligtelse til at yde en beskyttelse af privatlivets fred. Traditionelt er menneskerettighederne begrundet i et ønske om at beskytte det enkelte individ over for staten. For så vidt angår privatlivets fred, er dette dog et for snævert perspektiv, idet et beskyttelsesbehov med tilsvarende styrke foreligger i forhold til (store) private virksomheder. Det er ud fra denne antagelse, at menneskerettighedskonventionen i denne bog tillægges betydning, også i henseende til den retlige regulering i den private sektor.

Beskyttelsen af privatlivets fred er ikke absolut i den forstand, at

der kan være tilfælde, hvor der må ske en afvejning over for andre menneskerettigheder. Dette er i særlig grad tilfældet i forhold til informations- og kommunikationsfriheden, der på en mere omfattende måde end i grundlovens § 77 om ytringsfrihed ydes beskyttelse i artikel 10, der har følgende ordlyd:

»Stk. 1. Enhver har ret til ytringsfrihed. Denne ret omfatter meningsfrihed og frihed til at modtage eller meddele oplysninger eller tanker uden indblanding fra offentlig myndighed og uden hensyn til landegrænser. Denne artikel forhindrer ikke stater i at kræve, at radio-, fjernsyns- eller filmforetagender kun må drives i henhold til bevilling.

Stk. 2. Da udøvelsen af disse frihedsrettigheder medfører pligter og ansvar, kan den underkastes sådanne formaliteter, betingelser, restriktioner eller straffebestemmelser som er foreskrevet ved lov og er nødvendige i et demokratisk samfund af hensyn til den nationale sikkerhed, territorial integritet eller offentlighed tryghed for at forebygge uorden eller forbrydelse, for at beskytte sundheden eller sædeligheden, for at beskytte andres gode navn og rygte eller rettigheder for at forhindre udspredelse af fortrolige oplysninger, eller for at sikre domsmagtens autoritet og upartiskhed«.

Disse to menneskerettigheder er af forskellig karakter, idet artikel 8 tilvejebringer en individuelt orienteret beskyttelse, medens artikel 10 er en politisk baseret rettighed. Der er ikke nogen fast formel for, hvorledes afvejningen mellem modstridende menneskerettigheder skal ske, og det er ikke muligt generelt at fastslå, at en af rettighederne er den vigtigste. Der må således ske en konkret bedømmelse ud fra karakteren af det samfundsmæssige område, der reguleres. Af betydning ved en stillingtagen til de retlige problemer, der diskuteres fra kapitel 3, er, at den retspolitiske vurdering vedrører værdier af stor almen betydning. Denne iagttagelse er væsentlig at have i erindring, når de praktiske konsekvenser af de enkelte regler vurderes. Selv om menneskerettigheder ikke bør være dogmatiske trosartikler, der ureflekteret determinerer den praktiske retlige regulering, er der ikke destomindre tale om grundlæggende værdier, hvis realisering har betydning for det samfund, vi

lever i og den måde, vi forholder os til det enkelte individ i den stadigt mere komplekse og dynamiske samfundsmæssige udvikling, der kan være svær at overskue.

3 Det moderne personværn

I takt med den stadigt større udbredelse af edbteknologien blev det hurtigt klart, at denne teknologi etablerede nye muligheder for at håndtere alle former for information, herunder de data, der er relateret til enkeltpersoner. Disse muligheder, der i første række er knyttet til opbevaring af store informationsmængder, effektive og hurtige måder til at lokalisere og kombinere data, samt lettere måder til at videregive data, skaber også et potentiale, der kan føre til brug af persondata, som kan opleves som integritetstruende af det enkelte individ. Et forøget beskyttelsesbehov opstår, og dette følte nok mest markant på det tidspunkt, hvor edb for de fleste, herunder også for lovgiver, blev oplevet som noget fremmed og truende. George Orwells scenario 1984 kunne blive til virkelighed, og ved hjælp af edb-maskinen kunne Big Brother vise sig. Alt i alt opstod et behov for, hvad man med et dækkende norsk udtryk kan betegne et personværn.

3.1 National lovgivning

Juridisk har dette behov afsat flest spor i Vesteuropa, der har været foregangsområde for etableringen af en retlig regulering. Den første regulering blev skabt i den Vesttyske delstat Hessen, hvor der i 1970 blev indført en art dataombudsmandsinstitution. I 1973 fremkom den første nationale registerlov i Sverige (lov 1973:289), og i 1978 gennemførtes tilsvarende love i Norge (lov nr. 48 af 9.6.1978) og Danmark. I Frankrig (lov 78-17 af 6.1.1978) blev der lovgivet samme år. Danmark, Frankrig og Vesttyskland (lov 27.1.1977, ikrafttrådt 1.1.1978) er dermed de første EU-lande, der får denne type lovgivning. I disse lande har man flest erfaringer med denne form for lovgivning, hvilket kan anmærkes i forbindelse med de verserende overvejelser om en EU-retlig regulering, jfr.

nærmere herom nedenfor. Det er et fælles karakteristikon for udformningen af den nationale lovgivning, at udgangspunktet er, at der foreligger en risiko for, at persondata kan misbruges med heraf følgende integritetskrænkelser, og at der dermed er en række situationer, hvor anvendelsen af persondata alene bør ske i overensstemmelse med en fastsat retlig regulering.

Selv om der er store individuelle variationer, kan der skematisk udsondres i hvert fald tre forskellige måder, som en registerlovgivning kan struktureres ud fra. For det første love, der tilstræber detaljeret i selve loven at fastlægge reguleringen. De skandinaviske landes lovgivning falder ind under denne kategori. For det andet love, hvor der opstilles en række principper for persondataanvendelsen, der nærmere udmøntes i administrativ og judiciel praksis. Det primære eksempel her er den engelske Data Protection Act af 12.7.1984. For det tredje love, der alene fastlægger bestemte rammer og herefter i vidt omfang overlader det til selvregulering at fastlægge de konkrete retningslinier. Holland (lov 28.12.1988) har anvendt denne model. I alle tilfælde er det karakteristisk, at væsentlige reguleringsspørgsmål ikke lader sig beskrive med fuldstændig præcision i regelform, hvorfor de retshåndhævende organer i praksis får meget stor betydning. De tre reguleringsmetoder er vigtige, når det retspolitisk skal vurderes, hvorledes den fremtidige retlige ordning bør være. Selv om det kan forekomme at være et teknisk, juridisk problem, vil det senere blive illustreret, at valget af reguleringsmodel har overordentlig stor praktisk betydning ved en fastlæggelse af de dataanvendende instansers muligheder for at influere på reguleringens praktiske konsekvenser, jfr. især i kapitel 10.

3.2 International regulering

På internationalt niveau er der ligeledes opstået en vis regeldannelse. Det primære formål med denne er at fremme mulighederne for fri udveksling af persondata over grænserne. I takt med den stigende internationalisering og den stigende betydning, som persondata har fået, er der tale om en målsætning, hvis realisering er blevet stadig mere væsentlig. De eksisterende regelsæt er fra 1980 og er baseret på den grundantagelse, at forudsætningen for dataudveks-

lingen er, at der i de enkelte lande eksisterer et tilsvarende beskyttelsesniveau. I hvilken udstrækning ensartethed bør kræves, diskuteres nærmere i kapitel 9. I de eksisterende regelsæt opstilles en række regler og principper for persondataanvendelsen, der bør være opfyldt i national ret og som dermed danner basis for fri dataudveksling.

3.2.1 Europarådet

OECD udsendte i 1980 en henstilling, der indeholder en række principper for persondatabehandling.[2] Denne henstilling, der er tiltrådt af alle organisationens medlemslande, er ikke juridisk bindende for landene, men har haft en vis betydning, især uden for Europa. Vigtigst for danske forhold er Europarådets databeskyttelseskonvention 1981, der for vores vedkommende trådte i kraft 1. februar 1990.[3] Denne konvention er idag tiltrådt af 15 lande. I konventionen fastslås en række hovedprincipper for moderne persondatabeskyttelse. Ifølge disse skal det i national lovgivning sikres, at persondata kun kan behandles efter fastsatte kriterier, der for særlige kategorier af data kan være specielt restriktive, at der gennemføres sikkerhedsforanstaltninger, at høj datakvalitet sikres, herunder at de registrerede har ret til at få slettet eller korrigeret ukorrekte data, og at der gives enhver ret til registerindsigt. Der gives herudover de enkelte lande adgang til at fastsætte strengere regler end dem, der følger af konventionen. Inden for den fastsatte ramme skal der herefter frit kunne udveksles persondata mellem konventionsstaterne. Denne frihed til international dataoverførsel – transborder data flow – har ikke været nogen succes, hvilket skyldes, at konventionens regler er forholdsvis åbent formuleret og som nævnt kan fraviges i restriktiv retning. Forudsætningen om et tilsvarende beskyttelsesniveau er dermed sjældent opfyldt, jfr. nærmere hertil i kapitel 9.

Som nævnt er konventionen alment udformet, men det har fra starten være klart, at inden for bestemte sektorer og for bestemte dataanvendelsessituationer er det ønskeligt at udforme specielle

2. Guidelines governing the protection of privacy and transborder flows of personal data, OECD 23.9.1980.
3. Konvention af 28.1.1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger. Konventionen er optrykt i Lovtidende C 1991 p. 133.

regler inden for de almene rammer. På denne baggrund er der åbnet mulighed for, at der udstedes rekommandationer, hvilket er sket i en række tilfælde.[4] Disse rekommandationer er ikke som konventionen juridisk bindende for staterne, men ved at tiltræde deres udstedelse tilkendegiver staterne en intention om at ville opfylde dem. Rekommandationerne har da også haft en betydelig praktisk gennemslagskraft.

Reguleringsmodellen er interessant ved en vurdering af, hvorledes de retlige regler om databeskyttelse bedst udformes. En mulighed er således at have et alment udformet generelt regelsæt, der udbygges med en mere specificeret sektororienteret regulering. Det må indgå i de fremtidige overvejelser, om det kan være hensigtsmæssigt at overføre denne model til den nationale regulering. Modellen vil derfor indgå i diskussionen af reguleringsmetoder i kapitel 10.

3.2.2 EU

De internationale regelsæt er i dag, i betragtning af de hurtige teknologiske og samfundsmæssige innovationer, gamle og det er naturligt at overveje en revision. Disse overvejelser er indtil videre sat i bero, idet indholdet af den kommende EU-retlige regulering afventes. Elementer af denne vil blive inddraget i kapitel 3-10, idet der her blot skal gøres nogle bemærkninger om baggrunden for, at EU vil gennemføre en regulering af persondatabeskyttelsen, jfr. også i kapitel 9. Behovet for regulering knytter an til det indre marked, der ønskes udviklet til også at være et informationsmarked. Udfra en erkendelse af den betydning, som persondata for det private erhvervsliv, jfr. nærmere under 4, har Europakommissionen anset det for afgørende, at det indre marked også omfatter persondata. Dette antages at være en vigtig forudsætning for, at dette marked kan få markant betydning, også på globalt niveau. Ligeledes erkendes, at også for den offentlige sektor, og ikke mindst for det internationale samarbejde, spiller persondata en betydelig rolle. Formålet med et EU-direktiv er dermed at tilvejebringe grundlaget for fri datastrøm indenfor EU (og EØS), øg det har dermed

4. R(81)1: Automatiserede medicinske databanker, R(83)10: Data i forbindelse med forskning og statistik, R(85)20: Direkte markedsføring, R(86)1: Sociale data, R(87)15: Politidata, R(89)2: Arbejdsmarkedsdata, R(90)19: Betalingsdata, R(91)10: Videregivelse til private fra offentlige registre.

også haft betydning, at Europarådets konvention ikke har virket tilfredsstillende.

Et direktiv vil i sig selv være et mere virksomt juridisk instrument end en konvention. Dette beror på den almindelige retlige karakter af EU samarbejdet. Direktiver er bindende for medlemsstaterne og kan påberåbes af borgerne. De har således en ganske anden karakter end folkeretlige regler, der i princippet er intern national ret uvedkommende. Samtidigt er det væsentligt, at direktivregler kan håndhæves ved EF-domstolen. På denne baggrund er der stor sandsynlighed for, at direktivbestemt fri dataoverførsel vil blive til praktisk virkelighed.

Det foreliggende direktivudkast[5] er baseret på samme princip som de øvrige internationale regelsæt, idet der opstilles bestemmelser, der vil skabe et ensartet beskyttelsesniveau i de enkelte lande. På denne måde vil direktivet blive en af de mest ambitiøse reguleringer gennemført af EU. Dette skyldes, at persondatabeskyttelsesregler i national ret regulerer et meget bredt område og er udformet ud fra den i de enkelte stater herskende opfattelse af, hvorledes forholdet mellem stat og individ samt mellem private virksomheder og individet skal reguleres. Der er dermed tale om en regulering, der er tæt forbundet med den nationale retlige kultur og direktivet bliver således en harmonisering af disse kulturer.

Det høje ambitionsniveau er baggrunden for, at der ikke endnu er gennemført et direktiv. Første udkast til direktiv blev fremsat i 1990[6], og efter voldsom kritik blev et revideret udkast fremlagt i 1992. Om det lykkes i 1995 at få vedtaget et direktiv, er usikkert. Under alle omstændigheder vil der efter vedtagelsen være en frist for landene til at implementere det i national lovgivning, og en større retspolitisk diskussion vil herefter starte her i landet.

De problemområder, der vil blive aktualiseret af direktivet, er velkendte, selv om indholdet af den endelige direktivtekst for nærværende er usikkert. Det er forventeligt, at direktivet vil adskille sig en del fra det foreliggende udkast. På denne baggrund vil der kun i meget begrænset omfang i de følgende kapitler blive refereret

5. Ændret forslag til Rådets direktiv om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (KOM (92) 422 endelig udg. - Syn287, EFT C 311/30 af 27.11.1992.
6. KOM (90) 314 endelig udg. - SYN 287.

til specifikke regler i direktivudkastet, hvorimod en række af de principielle nydannelser, direktivet vil indebære, vil blive inddraget. De retspolitisk orienterede synspunkter i kapitel 3 til 10 udgør et bidrag til overvejelserne vedrørende implementeringen af direktivet og dermed den fremtidige retlige regulering af persondataanvendelsen i den private sektor.

4 Persondatas erhvervsmæssige betydning

På den ovenfor skitserede baggrund vil det herefter blive søgt indkredset, hvilken betydning persondata har for private virksomheder. Et behov for persondataanvendelse foreligger åbenbart hos offentlige myndigheder, men dette behov vil ikke blive drøftet nærmere her, da det er reguleringen af den private sektor, der sættes i centrum for denne fremstilling. Med andre ord er det den erhvervsmæssige eller kommercielle interesse i persondata, der søges indkredset.

Det kan være hensigtsmæssig indledningsvis at foretage en række opdelinger. Der må skelnes mellem en virksomheds interesse i internt i virksomheden at råde over persondata og heroverfor interessen i at anvende disse data i eksterne sammenhænge overfor andre. For det andet kan der skelnes mellem data, der er relateret til personer, som er ansat i virksomheden, og data, der vedrører udenforstående, f.eks. kunder og konkurrenter. Som det vil fremgå af de kommende kapitler, kan det have betydning at skelne mellem forskellige kategorier af data i forhold til deres følsomhed og ligeledes at skelne mellem forskellige formål for dataanvendelse, men disse distinktioner er det ikke nødvendigt at inddrage ved en belysning af de generelle erhvervsmæssige aspekter.

Intern anvendelse af persondata har betydning i en række relationer. Oplysninger om de ansatte er for det første nødvendige for, at virksomheden kan fungere lovligt. Hovedeksemplet er pligten til at indberette udbetalte lønninger til skattevæsenet, hvilket forudsætter, at virksomheden er bekendt med de ansattes privatadresse og deres personnummer. I relation til indgåede kollektive eller

individuelle arbejdsaftaler kan det også være legitimt for virksomheden at have bestemte oplysninger om de ansatte. Er der f.eks. adgang til frihed grundet barns 1. sygedag, vil det være berettiget for virksomheden at registrere, hvorvidt den enkelte har mindreårige hjemmeboende børn. I mange tilfælde vil det være hensigtsmæssigt at opbevare yderligere viden om de ansatte, f.eks. i henseende til disses kundskaber og erfaringsbaggrund. Sådanne oplysninger vil kunne være af stor betydning for virksomhedens muligheder for en optimal udnyttelse af sin arbejdskraft. I denne sammenhæng er der en forbindelseslinie til de oplysninger, en virksomhed kan have interesse i at opbevare vedrørende potentielle ansatte. Selv om oplysninger om faktisk ansatte i sagens natur har størst betydning, er der ikke tvivl om, at et grundlag for udvidelser/nyansættelser også er væsentligt for de fleste virksomheder.

Intern anvendelse af andre oplysningstyper kommer selvsagt også på tale. En væsentlig kategori er oplysning om kunder, d.v.s. aftagere af virksomhedens produkter m.v. Anvendelse af disse data har stor betydning også for den fremtidige profitabilitet, herunder for vurderinger af markedsandele og for tilrettelæggelse af produkterne således, at det etablerede kundegrundlag kan bevares. En anden kategori er data vedrørende potentielle kunder, der har betydning for mulighederne for udvidelse af den opnåede markedsandel. Det vil være væsentligt at kunne tilrettelægge virksomhedens drift på grundlag af denne form for oplysninger. For det tredje vil de fleste virksomheder have behov for at opbevare og anvende oplysninger om forretningsforbindelser, herunder underleverandører. Sådanne data har bl.a. betydning for virksomhedens evne til at opfylde de fastsatte produktionsmål inden for de aftalte tidsfrister. En fjerde kategori af data er oplysninger om konkurrenter, der vil være relevante i henseende til dels tilrettelæggelse af produktet, dels for fastholdelse og eventuel udvidelse af den opnåede markedsandel. Disse oplysninger spiller dermed en væsentlig rolle for en virksomheds strategiske planlægning.

Internt i virksomheden er der behov for anvendelse af data både om ansatte og om udenforstående. Forudsætningen for denne dataanvendelse er, at det juridisk er muligt at indsamle og opbevare disse oplysninger. Begrænsninger af disse muligheder forringer potentielt virksomhedernes indtjeningsevne. I hvilken udstræk-

ning dette faktisk er tilfældet, vil selvsagt afhænge af karakteren af den enkelte virksomhed. Generelt har det stor betydning, om der er sikkerhed for, at de begrænsninger, der bliver fastsat i lovgivningen ud fra hensynet til integritetsbeskyttelse, fungerer i forhold til alle virksomheder inden for en branche. Er dette tilfældet, vil reglernes økonomiske konsekvenser være begrænsede, da der vil gælde lige konkurrencebetingelser for alle virksomheder. Her vil effekten først og fremmest være en begrænsning af mulighederne for en samlet udvidelse af markedet. Disse bemærkninger om de juridiske reglers kommercielle betydning har også gyldighed i henseende til begrænsninger i den eksterne anvendelse af data.

Ekstern anvendelse af persondata vedrører oplysninger opbevaret i virksomheden og disses anvendelse uden for denne. Der vil være tale om samme type af data, som omtalt ovenfor, dog normalt med undtagelse af data om de ansatte. Oplysninger vedrørende aktuelle kunder kan være af betydning i en række henseender. Det kan være ønskeligt at foretage en markedsføringsindsats overfor disse med henblik på at motivere dem for virksomhedens samlede produktudbud. Det vil i denne sammenhæng være nyttigt at være i besiddelse af oplysninger, der belyser den enkelte kundes livsmønster og interesser, således at reklamering kan udføres specifikt på grundlag af denne profil, hvilket øger sandsynligheden for et positivt resultat, jfr. kapitel 5. I forhold til kunder er det endvidere vigtigt for virksomheden på et solidt grundlag at kunne vurdere disses betalingsevne, hvilket forudsætter adgang til kreditinformation, jfr. kapitel 7. Dette har særlig betydning i forbindelse med nye kunder, men spiller også en rolle i forhold til de, der tidligere har haft et kundeforhold. Det vil i praksis sjældent være nødvendigt for virksomheden selv at opbevare disse data, idet det er tilstrækkeligt at kunne søge denne information hos et kreditoplysningsbureau og have adgang til at anvende sådanne data.

Som allerede indiceret har virksomheden behov for at kunne anvende data om potentielle kunder i relation til markedsføring. Sådanne data vil kunne benyttes til direkte markedsføring, der har større gennemslagskraft end den brede uspecificerede markedsføring. Det vil her være hensigtsmæssigt at have adgang til oplysninger, der angiver interesseprofiler hos potentielle kunder, således at indsatsen kan målrettes. Registrering af oplysninger om po-

tentielle kunder med henblik på ekstern anvendelse vil for mange virksomheder have stor betydning, jfr. i kapitel 5.

Oplysninger om konkurrenter vil kunne have værdi anvendt eksternt, idet disse dels kan influere på den ovenfor omtalte markedsføring, dels kan benyttes i situationer, hvor der skal forhandles eller på anden måde være forbindelse med disse virksomheder. Viden om »fjenden« er væsentlig.

De her nævnte oplysningstyper vil udover at kunne indgå i virksomhedens egen eksterne anvendelse kunne videregives til andre, der enten udfører opgaver for virksomheden eller som indgår i en eller anden form for samarbejdsrelation med denne. I visse tilfælde vil det også kunne være relevant at kunne sælge sådanne data. I det elektroniserede miljø vil det udover videregivelse kunne komme på tale at gennemføre samkøringer, hvorved oplysninger fra to eller flere registre samles i et nyt register. Denne fremgangsmåde, der ofte vil være den teknologisk mest effektive, rejser særlige spørgsmål i henseende til databeskyttelse, hvilket vil blive belyst nærmere, især i kapitel 4. Det kan indtil videre konkluderes, at i henseende til ekstern anvendelse foreligger der en række forskellige datakategorier, der har væsentlig betydning for virksomhedernes erhvervsevne.

De foran anførte synspunkter har taget sigte på generelt at angive den erhvervsmæssige betydning, som persondata kan have, og dermed også den interesse, som en retlig regulering af dataanvendelsen må påkalde sig. De anførte behov vil kunne udspecificeres nærmere indenfor enkelte brancher og behovet for at råde over persondata vil variere i styrke, men i alle brancher/erhvervsområder vil et sådant behov foreligge. Som ligeledes nævnt tidligere vil der være forskelligartede anvendelsesformål, der rejser særlige spørgsmål i henseende til udformningen af den retlige regulering. En række af disse vil blive omtalt i de følgende kapitler.

Et generelt fænomen er, at behovet for anvendelse af personrelateret information er stærkt stigende i disse år, hvor informationssamfundet udvikles stadigt mere. Information er blevet en central erhvervsmæssig ressource, og i almindelighed tager den retlige regulering sigte på at fremme en samfundsmæssig acceptabel informationsanvendelse. Grundet den erhvervsmæssige betydning er udgangspunktet, at der skal skabes gode rammer for informa-

tionsanvendelsen, hvilket betyder, at der skal være klare begrundelser for begrænsninger. Hensynet til beskyttelse af den enkeltes integritet og privatliv er tungtvejende, men det må altid afbalanceres over for samfundsmæssige behov for persondataanvendelse. Dette grundsynspunkt danner udgangspunkt for de retspolitiske vurderinger, der er åbne overfor, at både integritetsorienterede og erhvervsmæssige hensyn må tages i betragtning.

5 Bogens opbygning

Den følgende fremstilling er primært af retspolitisk karakter. Dette betyder, at der ikke gives nogen detaljeret redegørelse for gældende ret. For en gennemgang af de enkelte bestemmelser i lov om private registre mv. henvises til Peter Blume: Personregistrering (2. udg. København 1992). I kapitel 2 gives dog en oversigt over den foreliggende lovgivning og de hovedsynspunkter, der fremgår af denne. Dette kapitel tjener således på samme måde som det foran anførte det formål at lægge en ramme omkring de retspolitiske drøftelser.

Bogen er begrænset til problemstillinger, der er relevante i den private sektor. Dette betinger i særlig grad udformningen af kapitel 3-8, hvor en række af de hovedspørgsmål, der foreligger i denne sektor, diskuteres. Disse angår både bestemte virksomhedsformer og anvendelsesformål, der særligt påkalder sig interesse ved udformningen af den retlige regulering. I kapitel 9 diskuteres specielt international dataudveksling, der må forventes at få stigende betydning i de kommende år. Kapitel 10 sætter fokus på, hvorledes den retlige regulering kan håndhæves i praksis, og herudfra hvorledes regelgrundlaget bedst kan tilrettelægges. Hovedtemaet er, hvorledes de retlige reglers overholdelse kan og bør kontrolleres. Med en anden formulering, hvorledes reglerne bliver til en praktisk realitet. Endelig fremhæves i en kort efterskrift en række almene konklusioner af betydning for den fremtidige regulering.

2 Oversigt over den retlige regulering

1 Registerlovgivningen

I modsætning til de fleste andre lande har Danmark valgt at have to registerlove. Den ene omfatter edb-registre ført for den offentlige forvaltning,[1] medens den anden, lovbekendtgørelse nr. 622 af 2.10.1987, angår private registre. Det er denne lov, der omtales nærmere i dette kapitel. Udenfor de to loves område falder Folketinget og institutioner under Folketinget, som f.eks. Ombudsmanden og Rigsrevisionen.[2] Domstolene er ligeledes ikke omfattet.

Årsagen til at der findes to love er, at der i henseende til legitimationsgrundlaget for persondataanvendelse principielt er forskelle mellem de to sektorer. I og med at offentlige myndigheder varetager lovpålagte opgaver, har de i en række henseender en mere naturlig adkomst til at opbevare og anvende persondata. Forskellen er f.eks. tydeligt markeret i de gældende betingelser for at registrere og videregive følsomme oplysninger, hvilket i den private sektor er underlagt en betydelig strengere regulering end i den offentlige sektor. Det har tillige spillet en rolle, at kontrolmekanismerne kan opbygges forskelligt, idet det særligt kan tillægges stor betydning, at den administrative struktur og tradition kan nyttiggøres ved lovens praktiske anvendelse i den offentlige sektor. Den offentlige registerlov indgår som en del af den almindelige forvaltningsprocessuelle regulering sammen med forvaltningsloven og offentlighedsloven. Opdelingen i to registerlove gør det som udgangspunkt lettere at beskrive retsgrundlaget i den private sektor.

1. Lovbekendtgørelse nr. 654 af 20.9.1991.
2. Ved lov 245 af 22.4.1991 blev Rigsrevisionens status ændret til at være en institution under Folketinget. I lovens § 18b fastsættes, at Rigsrevisionen fortsat skal være omfattet af de regler, der findes i offentlighedsloven og forvaltningsloven, jfr. bkg. 447 af 6.5.1992. Det er formodentlig en lapsus, at man glemte registerloven.

Forinden dette sker, er det nyttigt med et kort tilbageblik til lovgivningens start i 1978.[3] I kapitel 1 er der redegjort for de årsager, der begrundede lovgivningen, men her er det væsentligt at bemærke den virkelighed, der var reguleringens genstand. Den teknologiske infrastruktur var på dette tidspunkt karakteriseret ved centrale store edb-systemer, der fandtes få steder og som umiddelbart lod sig regulere. Idag er situationen som bekendt ganske anderledes, idet edbteknologien er blevet decentraliseret og spredt stort set alle steder. Den er ej heller længere stationær, idet bærbare computere er meget udbredte og sikkert inden længe i betydeligt omfang vil blive suppleret af mobile computere, som kan bæres på den enkelte person på samme måde som en lommeregner. Denne udvikling har medført en betydelig udvidelse af reguleringsområdet. Selvom en del af denne udvikling var kendt i 1987, hvor lovgivningen blev revideret, bærer denne fortsat præg af den infrastruktur, der fandtes i slutningen af 70'erne. Dette er nok især et problem for den offentlige registerlov, men spiller dog også en rolle for en række af reglerne vedrørende den private sektor.

I dag er selve registerbegrebet ved at være forældet. Den teknologiske udvikling med fænomener som netværk og relationsdatabaser betyder, at det opgavespecifikke register er ved at forsvinde. Det er da også karakteristisk, at man i mange lande taler om databeskyttelsesretlig frem for registerretlig regulering. Denne udvikling bør tages i betragtning ved kommende lovændringer, jfr. i øvrigt yderligere om udviklingstendenser i kapitel 6.

2 Lovens beskyttelsesobjekt

Registerlovens primære beskyttelsesobjekt er personoplysninger. Dette begreb defineres i § 1 stk. 2 og omfatter enhver oplysning, der direkte eller indirekte kan henføres til bestemte personer. Dette betyder, at selv om en oplysning er anonymiseret, vil den være omfattet af loven, såfremt oplysningen ved hjælp af en identifikationskode el.lign. kan gøres personrelateret. Uden for lovens område

3. Oversigt over lovhistorien findes i Peter Blume: Personregistrering (2. udg. 1992) p. 220.

falder således alene de fuldtud anonymiserede oplysninger.

Loven omfatter også oplysninger om virksomheder m.v., de såkaldte juridiske personer. Internationalt er dette usædvanligt, men beror på, at også denne form for oplysninger i visse tilfælde er beskyttelsesværdige. I denne bog behandles først og fremmest beskyttelsen af personoplysninger, men enkelte af de diskuterede problemstillinger har også relevans for virksomhedsoplysninger, jfr. særligt i kapitel 7.

3 Persondataanvendelse

Registerloven omfatter ikke alle faser i persondataanvendelsen. Dens regler gælder alene for registrering af oplysninger og videregivelse af registrerede oplysninger. Dette betyder især, at indsamling af oplysninger ikke er omfattet, men i visse tilfælde er reguleret af andre love, f.eks. markedsføringsloven, og ligeledes at intern anvendelse af registrerede data ej heller er reguleret. Sidstnævnte kræver en vis uddybning. Lovens regler angår, hvornår oplysninger må opbevares. Som det fremgår nedenfor, reguleres dette spørgsmål af en række retlige standarder. Ved bedømmelsen af, hvorvidt disse er opfyldt, vil det uundgåeligt indgå, hvad oplysningerne skal bruges til, idet dette naturligt vil udgøre begrundelsen for registreringsønsket. Betydningen af, at intern anvendelse ikke er reguleret, ligger således primært i, at anden form for benyttelse af de registrerede data ikke direkte reguleres. Er det således først accepteret, at oplysningerne kan registreres, kan de herefter frit benyttes, med mindre selvsagt særlige bestemmelser stiller sig hindrende i vejen herfor. I Europarådets databeskyttelseskonvention er fastsat et princip om, at registrerede data ikke må benyttes til andre formål end de, der begrundede deres registrering, men dette princip er ikke lovfæstet. I konkrete tilfælde kan det dog på denne baggrund spille en rolle, om det oprindelige formål med registreringen fortsat er til stede.

Ved en bedømmelse af, hvorvidt lovens betingelser for, at registrerede data kan videregives, gælder tilsvarende, at det vil blive taget i betragtning, hvad den modtagende virksomhed skal bruge

oplysningerne til, men at andre former for anvendelse principielt herefter er mulige, dog her forudsat, at den pågældende virksomhed har adkomst til at registrere oplysningerne. Som det fremgår, er det således ikke i denne relation helt enkelt at afgrænse lovens område.

Det må tilføjes, at det er sandsynligt, at den kommende EU-retlige regulering vil omfatte alle stadier af dataanvendelsen, d.v.s. hele spektret fra indsamling til videregivelse. Det forekommer umiddelbart hensigtsmæssigt at strukturere reguleringen på denne måde, jfr. også herom senere i bogen.

4 Elektroniske og manuelle registre

Registerloven omfatter både elektronisk og manuelt opbevarede oplysninger, idet dog sidstnævnte skal være underlagt en vis systematik for at være omfattet af loven (§ 1 stk. 1). Selv om der i det følgende primært lægges vægt på de elektronisk registrerede oplysninger, vil de omtalte bestemmelser for størstedelens vedkommende også gælde manuelt opbevarede oplysninger. Internationalt er der ikke konsensus om, at manuelle oplysninger skal ydes beskyttelse, hvorved kan bemærkes, at den i kapitel 1 omtalte Europarådskonvention alene omfatter elektroniske persondata. Medtagelsen af de manuelle oplysninger kan ses som en tilkendegivelse af en almindelig beskyttelse af privatlivets fred, hvilket f.eks. er baggrunden for, at manuelle oplysninger ikke beskyttes i engelsk ret, hvor common law ikke anerkender denne rettighed. Selv om der i denne bog fokuseres på elektroniske data, er der utvivlsomt behov for en generel databeskyttelse som fastlagt i gældende dansk ret.

5 Registrering

§ 3 indeholder de basale regler om registrering. Som en række af lovens andre bestemmelser tager § 3 udgangspunkt i en distinktion mellem almindelige oplysninger og oplysninger om rent private

forhold, der i daglig tale betegnes følsomme oplysninger. Da denne distinktion ikke blot er af betydning i gældende ret, men tillige spiller en væsentlig rolle for de retspolitiske overvejelser, er der god grund til at omtale denne opdeling noget nærmere, inden indholdet af § 3 beskrives.

Til grund for denne opdeling ligger den opfattelse, at der er visse oplysningstyper, der er specielt følsomme for det enkelte individ, og som det derfor er nødvendigt at give en særlig stærk beskyttelse. Disse oplysninger er opregnet i § 3, stk. 2, og er herefter »oplysninger om race, religion og hudfarve, om politiske, seksuelle og strafbare forhold samt oplysninger om helbredsforhold, væsentlige sociale problemer og misbrug af nydelsesmidler og lignende«. Denne opregning er ikke udtømmende og det er muligt for Registertilsynet i konkrete tilfælde at kategorisere andre oplysninger som følsomme. Det må endvidere tilføjes, at oplysninger om personnummer, der er undergivet en særlig regulering, jfr. nedenfor, også bliver betragtet som følsomme. Det er på basis af en politisk/ideologisk opfattelse, at det fastlægges, hvilke oplysninger der skal karakteriseres som følsomme. Herved fastlægges området for den egentlige privatsfære, og der kan her konstateres retskulturelle forskelle mellem de enkelte lande. Det er således interessant, at i det foreliggende udkast til EU direktiv er oplysninger om fagforeningsmæssige tilhørsforhold og moralske/etiske opfattelser rubriceret som følsomme.

Selv om det dermed er muligt at diskutere, hvilke oplysninger der er følsomme, og selv om dette kan variere i forhold til den samfundsmæssige udvikling, forekommer det velbegrundet at opstille en sådan kategori. Den omstændighed, at bestemte oplysningstyper underlægges strenge registreringsbetingelser, indebærer således, at reguleringen af de øvrige oplysningers beskyttelse kan være mindre indgribende. Det bør ligeledes fremhæves, at så længe man også fastsætter betingelser for, hvornår almindelige oplysninger må registreres, bliver det noget mindre afgørende, om de følsomme oplysninger er skarpt og præcist definerede. Dette skyldes, at alternativet til den særligt strenge regulering ikke er fri registreringsadgang, men blot at mere lempelige betingelser skal opfyldes. Det er dog et omdiskuteret spørgsmål, hvorvidt det er påkrævet at have en regulering af de almindelige oplysninger. Denne

problemstilling behandles nærmere senere, jfr. især kapitel 3 og 6.

Registrering af almindelige oplysninger kan ifølge § 3, stk. 1 ske, når det »er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art«. Denne bestemmelse er formuleret som en retlig standard, der nærmere fastlægges indholdsmæssigt i praksis. Udgangspunktet er en vurdering af formålet med erhvervsudøvelsen indenfor en bestemt branche i forhold til den type af oplysninger, der ønskes registreret, sammenholdt med det angivne formål med denne registrering. I denne vurdering indgår med stor vægt, hvorvidt registrering vil kunne medføre nævneværdig risiko for krænkelse af den personlige integritet. Afgørelsen af, om registrering kan ske, træffes af Registertilsynet, hvis afgørelse principielt kan indbringes for domstolene. Dette er der ikke nogen tradition for, hvorfor det reelt er Registertilsynet, der træffer den definitive afgørelse. Der gælder ikke noget krav om, at registre med almindelige oplysninger skal anmeldes eller om, at registrering ligefrem forudsætter en tilladelse. Dette betyder, at der enten må foreligge en klage til Registertilsynet, eller at tilsynet via pressen eller på anden måde bliver opmærksom på en konkret problemstilling. Uanset at langtfra alle registreringstilfælde bliver forelagt for Registertilsynet, er det med baggrund i dettes praksis, at gældende ret fastlægges.

§ 3, stk. 2, bestemmer, hvornår følsomme oplysninger kan registreres. Dette kræver opfyldelse af 3 betingelser. Oplysningen skal være afgivet af den pågældende eller indhentet med dennes samtykke og for det andet forudsættes, at den registrerede ved eller burde vide, at oplysningen registreres, og for det tredje, at det er nødvendigt for virksomheden at foretage registreringen. Disse strenge betingelser betyder, at det kun sjældent er muligt i den private sektor at registrere følsomme oplysninger, når man bortser fra særlige professioner som f.eks. læger. Sådanne edb-registre skal anmeldes til Registertilsynet, jfr. § 3, stk. 4, medmindre der er tale om foreningsregistre, der alene omfatter oplysninger om foreningens medlemmer. Med hjemmel i stk. 5 er der i bekendtgørelse nr. 121 af 11.3.1988 fastsat visse undtagelser fra anmeldelsespligten, idet disse bl.a. vedrører virksomhedsregistre med lovpligtig registrering af helbredsoplysninger eller med oplysninger, hvis registrering er nødvendig grundet kollektiv overenskomst, samt advo-

katers og revisorers klientregistre.

Hovedparten af de praktiske retspolitiske spørgsmål, der er aktuelle i forbindelse med en vurdering af udformningen af registerlovgivningen, vedrører de ikke-følsomme oplysninger, så selv om der er tale om en restriktiv regulering, er det forholdsvis sjældent, at disse regler har været udsat for seriøs kritik.

5.1 Advarselsregistre

En enkelt registertype er underlagt særlig regulering i § 3, stk. 6 og 7. Dette er de såkaldte advarselsregistre, hvis formål er at advare mod at have forretningsforbindelse eller ansættelsesforhold med de registrerede. For så vidt angår den førstnævnte situation bør det bemærkes, at sådanne registre adskiller sig fra kreditoplysningsregistre ved, at her registreres betalingsviljen fremfor betalingsevnen, jfr. nærmere i kapitel 7. Det er åbenbart, at det kan have umiddelbart indgribende konsekvenser for den enkelte at være optaget i et advarselsregister, og derfor kan sådanne kun oprettes efter tilladelse fra Registertilsynet, der kan knytte bestemte vilkår til tilladelsen. Disse vil bl.a. kunne fastslå, at bestemte oplysninger, f.eks. de følsomme, ikke må registreres, og kan bestemme, at de særlige regler for kreditoplysningsbureauer, jfr. nedenfor, helt eller delvis skal finde anvendelse. I Registertilsynets årsberetning offentliggøres en fortegnelse over tilladte advarselsregistre.

Det bør yderligere nævnes, at ifølge § 3, stk. 8, kan Justitsministeren fastsætte særlige regler for bestemte former for registre. Denne mulighed er udnyttet i forhold til headhunterfirmaer, der er underlagt bekendtgørelse nr. 523 af 11.8.1986, og ligeledes er pengeinstitutters muligheder for at videregive kreditoplysninger nærmere reguleret i bekendtgørelse nr. 122 af 11.3.1988. Det er ikke påkrævet nærmere at gennemgå de specielle regler i disse to bekendtgørelser, idet det blot kan bemærkes, at de i almindelighed indebærer en skærpelse i forhold til de almindelige regler i loven.

6 Videregivelse

§ 4 indeholder lovens hovedregler vedrørende videregivelse af registrerede oplysninger. For de almindelige oplysninger fastsættes i stk. 2, at videregivelse kan ske med samtykke eller når dette er et naturligt led i den normale drift af den pågældende virksomhed. Der er tale om den samme retlige standard, som er anvendt overfor registrering, men her er det altså videregivelsen, der skal ligge indenfor denne ramme. Er der tale om oplysninger, som er mere end 5 år gamle, er kravet til videregivelse skærpet, idet det her skal være åbenbart, at videregivelse er af afgørende betydning i forhold til det angivne formål. I denne forbindelse bør fremhæves, at statusoplysninger, f.eks. navn, adresse m.v., ikke er udsat for forældelse. For så vidt angår de følsomme oplysninger fastsætter stk. 1, at videregivelse uden samtykke alene kan ske, såfremt der er hjemmel hertil i anden lov. Som nævnt ovenfor er de følsomme oplysninger ikke normalt af stor betydning for almindelige erhvervsvirksomheder.

6.1 Samkøring

Stor praktisk betydning har den særlige videregivelsesform, der består i samkøring af oplysninger fra forskellige registre til et nyt register. Der er tale om en metode, som af mange betragtes som særlig farlig for personbeskyttelsen. Dette skyldes, at der ved samkøring kan tilvejebringes omfattende profiler af de registrerede med kontrol og overvågning til følge. Af betydning er yderligere, at der foreligger risiko for en ringe datakvalitet, dvs. vildledende eller ukorrekte oplysninger, ved at data fra forskellige registre oprettet på hver deres tidspunkt og til seperate formål sammenlægges.

På denne baggrund er der gennemført en speciel regulering i § 4, stk. 4. Efter denne er samkøring af forskellige virksomheders registre ikke tilladt, med mindre den alene foretages med henblik på ajourføring af oplysninger om navne, adresser og lignende. Der er tale om en ganske indgribende regel, hvis praktiske betydning især er mærkbar i koncerner, jfr. herom nærmere i kapitel 4, og i tilfælde, hvor der indgås strategiske samarbejdsaftaler. Forbudet

er ikke absolut, da der i stk. 5 er givet Registertilsynet adgang til at dispensere under forudsætning af, at de almindelige videregivelsesregler er opfyldt, og at årsagen til, at samkøring ønskes, klart overstiger hensynet til de registrerede. Disse skal i så fald informeres om, at samkøring kan finde sted, og tilsynet kan betinge en tilladelse af, at yderligere vilkår opfyldes. I almindelighed forudsætter en tilladelse, at der er et klart værdispring til fordel for samkøringen.

7 Personnummeret

I 1968 indførte Danmark personnummeret, der entydigt identificerer hver enkelt borger. Dette nummer er dermed velegnet, bl.a. i forbindelse med samkøringer, til at koble oplysninger fra forskellige registre. Dette forhold har betydet, at mange mennesker opfatter personnummeret som en fortrolig eller følsom oplysning og dermed lægger større vægt på de risici, der kan være forbundet med anvendelsen af personnummeret, end de fordele, der består i at forvekslinger undgås. Denne holdning er slået igennem i § 4a, hvorefter registrering ifølge stk. 1 forudsætter, at betingelserne for at registrere følsomme oplysninger er opfyldt. Videregivelse af registrerede personnumre kan efter stk. 2 ske, når betingelserne for at videregive almindelige oplysninger er opfyldt, og dette er af afgørende betydning for en entydig identifikation af den registrerede eller er krævet af en offentlig myndighed. Anvendelse af personnumre i den private sektor forudsætter således et særligt grundlag, og dette er i øvrigt et yderligere eksempel på den tidligere nævnte forskel mellem den private og den offentlige sektor i henseende til legitimationsgrundlag.

8 Markedsføringsdata

Visse dataanvendelsessituationer har påkaldt sig særlig interesse og har medført en speciel regulering. Dette gælder brug af regi-

strerede data til markedsføringsformål, jfr. nærmere herom i kapitel 5 og nedenfor vedrørende betalingskortloven. I § 4b fastslås, at videregivelse af oplysninger om forbrugere til andre virksomheder med henblik på markedsføring kun kan ske, når de almindelige videregivelsesbetingelser i § 4 er opfyldt, og når den registrerede har fået tydelig skriftlig meddelelse herom og har givet et udtrykkeligt samtykke. Den nævnte meddelelse skal angive, til hvilke typer virksomheder videregivelse vil kunne ske. Der er tale om en meget restriktiv regulering, der skaber store problemer for den direkte markedsføring, og som har været udsat for megen kritik fra erhvervslivets side.

9 Registrering af telefonopkald

I § 7f er der fastsat en særlig regulering med henblik på automatisk registrering af telefonnumre, hvortil der er ringet fra en virksomhed. En sådan registrering må virksomheden ikke foretage, med mindre der gives tilladelse hertil af Registertilsynet, hvilket skal være begrundet med afgørende private eller offentlige interesser. Tilladelse vil typisk blive givet, hvis registreringen har betydning for gennemførelsen af et kontraktforhold. Baggrunden for bestemmelsen er, at det opfattes som en uacceptabel overvågning af ansatte, såfremt sådan registrering finder sted. En række af de særlige spørgsmål, der foreligger i forbindelse med moderne telekommunikation drøftes iøvrigt nærmere i kapitel 8.

10 Datakvalitet og registerindsigt

Ved siden af regler om registrering og videregivelse er der fastsat en række bestemmelser for, hvorledes registrerede data skal behandles, og hvilke rettigheder registrerede personer har. I § 6 fastslås, at i edb-registre skal oplysningerne slettes, når de grundet alder eller andre forhold ikke har betydning længere, idet registre, der anvendes løbende, skal udformes således, at der kan ske den

fornødne ajourføring. Virksomhederne skal sikre, at der kun registreres korrekte oplysninger og foretage berigtigelse af fejl.

Virksomhederne skal endvidere træffe de nødvendige sikkerhedsforanstaltninger mod uautoriseret anvendelse. En række retningslinier omfattende sikkerhedskrav er opstillet af Registertilsynet, idet kravene er differentierede afhængig af, hvilke type oplysninger registeret omfatter. Det er ikke her påkrævet nærmere at uddybe, hvori disse krav består. De fastsatte sikkerhedskrav har ganske vist stor betydning for virksomhederne og de ressourcer, der må afsættes til at overholde registerloven, men desuagtet er der primært tale om en teknisk problemstilling, der kan udelades i den retspolitisk orienterede drøftelse i de følgende kapitler.

Registrerede personer har ret til at få korrigeret eller slettet urigtige og vildledende oplysninger, idet Registertilsynet efter § 5 er klageinstans, hvis virksomheden ikke vil medvirke hertil. Generelt gives der dermed den enkelte en adkomst til at sikre høj datakvalitet.

De registrerede har efter reglerne i lovens kapitel 2a ret til registerindsigt, idet denne ret som hovedregel kun kan udøves én gang om året. Oprindelig var der ikke givet en adgang til registerindsigt, da dette blev opfattet som en unødvendig økonomisk byrde for virksomhederne. Dette betød, at Danmark ikke kunne ratificere Europarådets databeskyttelseskonvention. Bl.a. derfor blev denne rettighed indført ved lovrevisionen i 1987.

Ved siden af de almindelige regler indeholder loven en særlig regulering af pressens informationsregistre (§§ 7g-7i), adresserings- og kuverteringsbureauer (§§ 17-19), kreditoplysningsbureauer (§§8-16) og edb-servicebureauer (§ 20).

11 Kreditoplysningsbureauer

Især kreditoplysningsbureauers vilkår har erhvervsmæssig interesse, og derfor omtales disse regler kort i det følgende, jfr. endvidere i kapitel 7.

Udgangspunktet for denne regulering er, at det kan have ganske indgribende betydning for den enkelte borger eller virksomhed at

blive registreret hos et kreditoplysningsbureau, hvorfor det er væsentligt, at der er sikkerhed for, at der kun registreres korrekte oplysninger, og at disse oplysninger er af en sådan karakter, at det er acceptabelt, at de tillægges betydning ved kreditbedømmelse. Dette udgangspunkt giver grobund for en ganske restriktiv regulering, der er baseret på, at forudsætningen for at drive et kreditoplysningsbureau er, at dette anmeldes til Registertilsynet (§ 8). I § 9 fastslås, at der kun må registreres oplysninger »af betydning for bedømmelse af økonomisk soliditet og kreditværdighed«, og yderligere bestemmes, at følsomme oplysninger ikke må registreres. Endvidere må oplysninger, der er mere end 5 år gamle, ikke registreres eller videregives, med mindre det er åbenbart, at de er af afgørende betydning. I praksis er det uhyre sjældent, at det accepteres, at sådanne oplysninger benyttes. Til § 9 er der udviklet en omfattende praksis, der tager sigte på at opfylde det ovenfor nævnte hovedprincip.

Den indgribende betydning, som optagelse i et bureaus registre kan indebære, er særligt udtalt i forbindelse med videregivelse af disse oplysninger, og i denne henseende er der fastsat yderligere begrænsninger. Disse er særligt relateret til videregivelse af summariske oplysninger, der adskilles fra de tilfælde, hvor bureauet udarbejder en større bedømmelse, der sædvanligvis kun vedrører virksomheder. Summariske oplysninger kan fremgå af publikationer eller af databaser, hvortil der er on-line adgang. Videregivelse kan alene ske til bureauets abonnenter, og det er dermed muligt for et bureau i abonnementskontrakten at foretage en vis yderligere regulering af, hvilke oplysningstyper der kan rekvireres.

To regler illustrerer særligt de begrænsninger, der er gennemført i videregivelsesmulighederne. I § 12, stk. 3, bestemmes, at videregivelse kun kan ske, når oplysningen enten stammer fra Statstidende eller vedrører et skyldforhold på over 1.000 kr. til samme kreditor, der skal kunne dokumentere, at der foreligger en forfalden gæld. Det er således politisk besluttet, at små-gæld ikke skal have betydning for kreditvurderingen. Betydningen af de politisk fastsatte begrænsninger fremgår nok endnu klarere af bestemmelsen i § 12, stk. 4. Her fastsættes, at videregivelse af kreditoplysninger ikke må ske på en sådan måde, at det giver grundlag for at vur-

dere andres kreditværdighed. Reglen betyder, at oplysninger ikke må være struktureret således, at adresser kan benyttes som søgekriterium, hvilket kan have den konsekvens, at den omstændighed, at man har bopæl i et område med mange dårlige betalere, medfører, at man selv ikke kan anses for kreditværdig.

Udover den beskrevne regulering af registrering og videregivelse er der ved siden af adgangen til registerindsigt (§11) fastsat yderligere bestemmelser til sikring af den enkelte. Så snart der registreres andre oplysninger end de, der er offentligt tilgængelige, skal den registrerede gives meddelelse om, at der er sket en registrering (§ 10), hvilket naturligt giver god grobund for udøvelse af registerindsigt. Forkerte oplysninger skal korrigeres, og er sådanne oplysninger videregivet, skal alle, der har modtaget dem inden for de sidste 6 måneder, have meddelelse om korrektionen, ligesom den registrerede skal have oplyst, hvem der har fået denne meddelelse, samt hvorfra de ukorrekte oplysninger stammer (§ 14). Bestemmelsen kan bl.a. have betydning, såfremt den registrerede har lidt et tab i forbindelse med, at kredit er nægtet, og på dette grundlag ønsker at gøre et erstatningskrav gældende.

Det bør afslutningsvis fremhæves, at de beskrevne bestemmelser – på samme måde som lovens andre regler – er minimumsregler i den forstand, at et bureau kan give den registrerede en større beskyttelse end den, der følger af loven. I praksis er dette ganske ofte tilfældet hos de større veletablerede bureauer, og alt i alt tilvejebringer praksis en betydelig beskyttelse. En væsentlig problemstilling, der drøftes i kapitel 7, er herefter, hvorvidt denne regulering tilstrækkeligt tager hensyn til, at kreditvurderinger kan finde sted på et seriøst grundlag.

12 Håndhævelse og kontrol

Håndhævelsen af registerlovens regler varetages af Registertilsynet, der er en fritstående myndighed under Justitsministeriet. Tilsynet træffer endelige administrative afgørelser på grundlag af sager, der enten indbringes for tilsynet som klage eller tages op af dette af egen drift. Principielt kan afgørelserne indbringes for dom-

stolene, men dette er kun sket i et enkelt tilfælde,[4] og reelt er det dermed tilsynet, der via sin praksis fastlægger gældende ret. Tilsynet består af et registerråd, der træffer afgørelse i større eller principielle sager, og et sekretariat, der træffer alle andre afgørelser samt forbereder sager til forelæggelse i rådet. Tilsynet har adgang til at kræve enhver oplysning, der har betydning for dets drift, og har adgang til udstede forbud og påbud.

En række af lovens bestemmelser er strafsanktionerede (§27), men sædvanligvis bliver der alene tale om bødestraf, og det kan konstateres, at det ikke er via strafferetlige sanktioner eller trusler herom, at det sikres, at loven bliver overholdt. En væsentlig faktor i denne sammenhæng er offentlig omtale, idet i hvert fald de større virksomheder er følsomme over for omtale af overtrædelser af loven, idet denne kan påvirke deres image negativt og derigennem indirekte kan have økonomisk betydning.

Der foreligger en lang række vanskelige spørgsmål i forbindelse med, hvorledes registerlovens overholdelse kan og bør kontrolleres, jfr. herom nærmere i kapitel 10.

13 Anden lovgivning

I en lang række andre love er der optaget bestemmelser, der tager sigte på at fremme persondatabeskyttelsen. I det følgende omtales alene de love, der har særlig betydning i den private sektor.[5] Den væsentligste af disse er utvivlsomt lov om betalingskort[6]. Denne lovs regler gælder forud for registerlovens, jfr. § 23, idet spørgsmål, der ikke er dækket af sådanne specialbestemmelser, reguleres af registerloven. I betalingskortloven har man været opmærksom på, at anvendelse af betalingssystemer, hvor man kan erhverve ydelser uden umiddelbart at skulle betale herfor, kan give anled-

4. Utrykt Østre Landsretsdom af 12.2.1987 (2. afd. nr. 492/1984) vedrørende nødvendighedskriteriet i § 3 stk. 2, der opretholdt tilsynets afgørelse, jfr. nærmere Peter Blume p. 44.
5. Regulering af beskyttelse af arkiverede persondata findes i lov nr. 337 af 14.5.1992 om offentlige arkiver mv., men disse regler er primært af betydning i den offentlige sektor. En omtale af disse bestemmelser findes i Peter Blume: Udviklingstræk i dansk databeskyttelsesret, Retsvidenskabeligt Institut B. Studier nr. 46/1992 p. 33-40.
6. Lovbekendtgørelse nr. 464 af 15.6.1992.

ning til specielle problemer, hvilket bl.a. skyldes, at denne form for betaling registreres, hvorved der dannes de såkaldte elektroniske spor, der kan benyttes til at profilere den enkelte forbruger. Det er særlig karakteristisk for bestemmelserne, at de i modsætning til registerloven også regulerer den interne anvendelse af registrerede oplysninger, jfr. nedenfor. Der skelnes mellem den situation, hvor kortet bruges som hævekort, hvor det jo er ubekendt, hvad de udbetalte penge skal anvendes til, og den situation, hvor kortet bruges som betalingskort. I forhold til sidstnævnte funktion fastsættes i § 24, stk. 1, at man kun må registrere sådanne oplysninger, der er nødvendige for gennemførelsen af en betalingstransaktion. Formålet med denne regel er at hindre, at disse oplysninger danner grundlag for markedsføring over for kortindehaver. Også i henseende til anvendelse og videregivelse af de registrerede oplysninger er det præciseret i § 24, stk. 2 og 3, at oplysningerne ikke må danne grundlag for markedsføring. Det er især væsentligt at gøre opmærksom på, at disse restriktioner også gælder for oplysninger om brug af betalingskortet hos kortudsteder eller betalingsmodtagere, hvorfor reguleringen er strengere end den ovenfor beskrevne regel i registerlovens § 4b.

Reglerne i betalingskortloven har været udsat for voldsom kritik fra erhvervslivets side, og som det fremgår, er deres primære virkning at begrænse mulighederne for direkte markedsføring. Dette er en almindelig tendens i lovgivningen. Eksempelvis blev der i 1992 gennemført en række ændringer i henseende til, hvilke oplysninger der kan fås udleveret fra det centrale erhvervsregister, men samtidig blev der fastsat en regulering, der begrænser muligheden for at benytte oplysningerne til direkte markedsføring[7] Denne problemstilling drøftes nærmere i kapitel 5.

I forbindelse med beslutningen om at elektronisere tinglysningsvæsenet blev der i 1992 indsat en række nye bestemmelser i tinglysningsloven med henblik på at sikre persondatabeskyttelsen.[8] Ved elektroniseringen skifter tinglysningssystemet karakter fra at være en samling af manuelle registre til at være et on line personregister af meget betydeligt omfang. Registeret indeholder en

7. Lovbekendtgørelse nr. 530 af 19.6.1992 om Det Centrale Erhvervsregister § 11 stk. 5-7.
8. Lov nr. 281 af 29.4.1992. Se også Bekendtgørelse nr. 326 af 24.5.1993 og nr. 327 af samme dato. En nærmere omtale af lovens regler findes hos Peter Blume, Studier 46/1992 p. 23-31.

lang række personoplysninger, hvoraf nogle kan indicere følsomme forhold. Den nye regulering opretholder princippet om, at tinglysningsoplysninger er offentligt tilgængelige, hvilket er selve rygraden i systemet, men begrænser adgangen til ekstern on line søgning i det elektroniske register til dem, der professionelt anvender tinglysningsoplysninger. Samtidig fastsættes, at de søgte oplysninger alene må benyttes til formål, der er forbundet med tinglysning, og ikke til andre formål, f.eks. markedsføring. Også med henblik på, hvilke oplysninger der må registreres, er tinglysningsformålet styrende. Da tinglysning betragtes som en judiciel opgave, er tilsynet med reglernes overholdelse placeret hos landsretspræsidenterne. Reglerne i tinglysningsloven har stor betydning for dele af den private sektor, men er desuagtet specielle, hvorfor de ikke yderligere inddrages i denne bog.

Udover de love, der er omtalt ovenfor, findes der enkelte regler spredt rundt i lovgivningen, og det er generelt let at konstatere, at der i almindelighed fra Folketingets side er stor opmærksomhed over for behovet for databeskyttelse, når ny lovgivning gennemføres.

3 Almindelige erhvervs-virksomheder

Som fremhævet i kapitel 2 er de væsentligste retspolitiske spørgsmål for den almindelige erhvervsvirksomhed relateret til mulighederne for at opbevare og anvende ikke-følsomme persondata. Hovedvægten i det følgende lægges derfor på disse data, idet der dog også angives nogle synspunkter vedrørende enkelte af de følsomme oplysninger, der kan være af særlig interesse for almindelige virksomheder.

1 Beskyttelse af ikke-følsomme data

Et grundlæggende spørgsmål ved en vurdering af, hvilke databeskyttelsesregler, der bør være gældende, er, om det er rimeligt at lægge bindinger på anvendelsen af ikke-følsomme persondata. Det kunne hævdes, at en sådan regulering er en form for »overkill« og udtryk for en overdreven og urealistisk frygt for, hvilke krænkelser af den personlige integritet en sådan dataanvendelse kan medføre. Idag hvor edb-anvendelse er blevet naturlig og computeren er på vej til at blive ligeså almindelig som telefonen, der også i sin barndom blev betragtet med frygt af mange, kan det hævdes, at den eksisterende lovgivning er baseret på en forældet teknologiskræk og på en unødvendig måde begrænser denne samfundsmæssigt vigtige teknologis anvendelsesmuligheder. Det kan ligeledes anføres at i og med, at teknologien er blevet så udbredt, er lovgivningens ambitionsniveau blevet urealistisk højt i den betydning, at det er blevet umuligt at kontrollere reglernes overholdelse, hvorfor det bliver ganske tilfældigt hvilke virksomheder, der konkret bliver påvirket af de fastsatte begrænsninger.

1.1 Befolkningens holdning

De her anførte synspunkter giver grobund for at overveje de fundamentale træk ved den eksisterende lovgivning og den ideologi, som registerloven er baseret på. Det centrale spørgsmål er, om de almindelige oplysninger med rimelighed kan siges at udgøre en del af privatsfæren og dermed være retligt beskyttelsesværdige. Dette er et spørgsmål, der i en vis forstand ikke lader sig besvare. Der findes ikke pålidelige undersøgelser, som kan belyse, hvilken opfattelse befolkningen har. Det kan konstateres, at de gange databeskyttelsesmæssige sager påkalder sig massemediernes opmærksomhed, er der næsten altid tale om følsomme oplysninger eller om særlige anvendelsessituationer, jfr. nærmere om disse i de kommende kapitler. Det nærmer sig reelt gætteri, hvis der gives et svar på, om befolkningen som sådan opfatter alle persondata som hørende til den beskyttelsesværdige privatsfære. Dette er ikke en situation, der er unik for dette retsområde. I det repræsentative demokrati vil det ikke mindst i moderne tid, hvor den lovgivningsmæssige regulering er meget omfattende og den samlede lovgivning særdeles kompleks, være usikkert, om befolkningens retsopfattelse harmonerer med de enkelte love. Det er muligt, at brug af moderne teknologi i fremtiden vil kunne udvikle demokratiet til en styreform, hvor befolkningen er mere aktivt deltagende, jfr. hertil kapitel 6, men i dag er det ikke reelt muligt at basere en retspolitisk vurdering på antagelser om befolkningens retsopfattelse. I Folketinget kan der i disse år spores en vis tendens til en mere liberal holdning til de almindelige data, men det er dog usikkert, om der vil være opbakning bag en total friholdelse af disse datatyper fra retlig regulering.

Uanset at det ikke er muligt at fastlægge befolkningens retsopfattelse, er der ikke tvivl om, at en del mennesker betragter alle deres persondata som private, og på denne baggrund er det ønskeligt, såfremt det enkelte individ sættes i centrum, at der opretholdes en vis beskyttelse også af de almindelige data. Selv når bortses fra den omstændighed, at Danmark som følge af internationale forpligtelser, jfr. Europarådets databeskyttelseskonvention som omtalt i kapitel 1, vil være forpligtet til at have en sådan beskyttelse, forekommer hensynet til erhvervsvirksomheders almindelige omdømme

også at tale herfor. Det er næppe tilstrækkeligt at overlade en sådan regulering til virksomhedernes interne regeldannelse, jfr. herom nærmere i kapitel 10. Overordnede hensyn taler dermed til fordel for en regulering, men andre momenter må også tages i betragtning.

1.2 Teknologisk proportionalitet

En regulering af brugen af alle persondata betyder, at der vil være situationer, hvor edb-teknologiens fulde potentiale ikke vil kunne udnyttes, hvilket ofte ses anført som basal kritik af registerlovgivningen. I sin rene form indebærer denne kritik, at der overhovedet ikke skulle være en sådan lovgivning, fordi det netop er dennes pointe, at de teknologiske muligheder begrænses, således at kun de anvendelsesområder, der politisk kan accepteres, udnyttes. Lovgivningen er således udtryk for den generelle opfattelse, at det skal være menneskene og ikke maskinerne, der skal bestemme udviklingen. Der skal ske en samfundsmæssig bevidst anvendelse af edb-teknologien.

Denne indfaldsvinkel betyder, at det ikke i sig selv er et argument imod en registerregel, at den begrænser teknologien, idet det derimod må vurderes, om der er tale om en begrænsning, der hviler på en hensigtsmæssig opfattelse af de vilkår, der skal gælde for anvendelsen af persondata, og endvidere, om de virkninger, som den pågældende regel har, står i et rimeligt forhold til de opnåede mål. Der kan således opstilles, hvad man kunne kalde en teknologisk proportionalitetssætning, der kan fungere som målestok for en vurdering af de enkelte bestemmelser.

Anvendes denne målestok i forhold til behandlingen af de almindelige persondata, fører dette til, at en regulering skal sikre en saglig dataanvendelse uden på indgribende måde at begrænse teknologianvendelsen og erhvervsudøvelsen samt uden at der påføres virksomhederne store omkostninger. Reguleringen skal så at sige sætte nogle ydre grænser for behandlingen af de almindelige persondata. Hvorvidt gældende ret lever op til en sådan norm, drøftes nærmere nedenfor.

1.3 Mild regulering

Udgangspunktet for en vurdering af, hvorledes den retlige regulering bedst udformes, er i overensstemmelse med det ovenfor anførte, at denne ikke må være af indgribende karakter, men i hovedsagen må bestå i en betoning af, at dataanvendelsen skal være sagligt begrundet. Kan det konstateres, at den eksisterende praksis er i overensstemmelse med dette udgangspunkt, er det nærliggende at konkludere, at den er så mild og dens skadevirkninger så begrænsede, at den gældende ordning uden betænkeligheder kan opretholdes.

Medtager man alle persondata i den retlige regulering, opnås den fordel, at en udtømmende og helt sikker opdeling af persondata i forskellige kategorier får noget mindre betydning. Som omtalt i kapitel 2 er en række datakategorier idag udskilt som særligt følsomme, jfr. §§ 3, stk. 2 og 4a, men opregningen i loven har karakter af en eksemplifikation, der ikke udelukker medtagelse af andre kategorier. Lovgiver har således ikke foretaget nogen fuldstændig binding af praksis. Dette kan ske fordi valget idag ikke består mellem regulering og frihed, men mellem mild og streng regulering. For Registertilsynet vil det være vanskeligere i førstnævnte situation at inddrage nye datatyper under den strenge regulering, da dette vil være et meget vidtgående skridt. Det vil være nødvendigt for lovgiver på en meget præcis måde at definere de følsomme data, hvilket i sig selv vil kræve betydelig omtanke. Samtidig opstår der en nærliggende risiko for, at gentagne lovændringer i takt med indvundne erfaringer vil være påkrævet. Under en teknisk juridisk synsvinkel er det derved hensigtsmæssigt, at alle persondata er omfattet af registerloven.

Valget mellem regulering eller frihed for de almindelige persondata er ikke afhængig af, om særlige dataanvendelsessituationer skal underlægges bestemte regler. Det er således muligt at forestille sig, at almindelige persondata ikke omfattes af loven, samtidig med at der fortsat gælder regler for markedsføring, oplysninger om telefonopkald etc. Behovet for en regulering af disse særlige situationer kan således ikke anføres som argument for opretholdelsen af en regulering af de almindelige persondata, men selvfølgelig ej heller for det modsatte. Ved en bedømmelse af den diskuterede

problemkreds er det dermed vigtigt at være opmærksom på, at særlige situationer som de nævnte, der iøvrigt drøftes nærmere i kapitel 5 og 8, ikke spiller nogen rolle.

1.4 Praksis

Det er i det foregående lagt til grund, at det er hensigtsmæssigt at regulere brugen af de almindelige persondata. Dette er ikke det samme som, at den eksisterende regulering er tilfredsstillende. Dette spørgsmål vurderes nærmere i det følgende. Som det fremgår af beskrivelsen i kapitel 2, er udgangspunktet i § 3, stk. 1, at registrering kan ske, når dette er et naturligt led i den normale drift af den enkelte virksomhedstype. Denne retlige standard indebærer, at afgørelsen af, om en registrering kan ske, afhænger af i hvilken branche, virksomheden befinder sig. Med andre ord er det erhvervsudøvelsen, der betinger registreringsadgangen. Dette forekommer for en umiddelbar betragtning tilfredsstillende. Det kunne anføres, at denne standard kan virke begrænsende overfor en virksomhed, der anlægger en innovativ fremgangsmåde indenfor en branche, og dermed har et konservativt præg, men heroverfor står, at standarden ved at lægge vægten på en gennemsnitsvurdering kan medvirke til at fremme lige konkurrencebetingelser for så vidt angår persondataanvendelse, hvilket i sig selv må betragtes som positivt. Det ville således ikke være ønskeligt, om der i denne henseende kunne konkurreres mellem virksomhederne, dels fordi dette kunne skade borgerne, dels fordi der er tale om et aspekt, der sædvanligvis ikke har implikationer for kvaliteten af det produkt, virksomheden producerer. Som udgangspunkt er den retlige standard derfor acceptabel.

En vurdering afhænger dog endvidere af, hvorledes det afgøres, om en bestemt situation er indenfor eller udenfor standarden. En stillingtagen hertil forudsætter kendskab til den enkelte branche, herunder forståelse af de betingelser, der har betydning for produktivitet og indtjeningsevne. Afgørelsen træffes af Registertilsynet, der ikke umiddelbart har et sådant kendskab, jfr. også iøvrigt i kapitel 10 om kontrolformer. Det er dermed nødvendigt, at tilsynet skaffer sig et sådant kendskab. Samtidig er bedømmelsen også betinget af, om det er samfundsmæssigt hensigtsmæssigt, at per-

sondata opbevares i den pågældende situation. Uden at det i og for sig fremgår af den nævnte standard, er en normering af brancherne indbygget. Dette skyldes, at ved en vurdering af de konkrete situationer vil og bør det blive taget i betragtning, om der er integritetsmæssige problemer. Bestemmelsens anvendelse sker naturligt indenfor en overordnet ramme, der sættes af loven og især dennes overordnede formål. Forstået på denne måde afhænger den egentlige bedømmelse af den opstillede retlige standard af tilsynsmyndighedens praksis. Det er på grundlag af praksis, at det kan afgøres, om der sker en urimelig intervention i virksomhedernes drift.

Ved vurderingen af praksis må det tages i betragtning, at registrering af almindelige personoplysninger ikke skal anmeldes til Registertilsynet, hvorfor tilsynets praksis ikke afspejler alle de tænkelige registreringssituationer. Desuagtet er praksis i forbindelse med § 3 stk. 1 generelt bedømt tilbageholdende, d.v.s. at det er forholdsvis sjældent, at bestemmelsen antages at stille sig hindrende i vejen for registrering. Dette kan dog være tilfældet, og til illustration af sådanne situationer kan det være hensigtsmæssigt først at omtale bestemmelsens anvendelse over for fagforeninger og arbejdsløshedskasser. Et væsentligt spørgsmål i denne sammenhæng har været, om disse instanser må registrere oplysninger om potentielle medlemmer. Dette har man ønsket, fordi en sådan registrering kan danne baggrund for hvervekampagner og lignende. For en umiddelbar betragtning kan dette fremstå som et sagligt og forståeligt formål, hvorfor det er accepteret, at fagforeninger foretager sådan registrering, så længe den kun omfatter identifikationsoplysninger. Derimod er det fast praksis, at en sådan registrering ikke kan foretages af arbejdsløshedskasser[1] og dermed falder uden for standarden i § 3, stk. 1. Baggrunden for denne praksis er bl.a. ønsket om at undgå, at der sker en for stor dataophobning i den private sektor samtidig med, at det kan spille en rolle, at der generelt er betænkeligheder forbundet med brug af persondata i reklamemæssige øjemed, jfr. nærmere herom i kapitel 5.

Denne praksis har interesse i forhold til almindelige virksomheders behov for at registrere data om potentielle kunder. Selv om der så vidt det ses ikke foreligger egentlige afgørelser herom, er ud-

1. Jfr. RÅ 1992 p. 73-75.

gangspunktet, at sådan registrering ikke kan finde sted, idet private virksomheder ellers vil kunne opbygge personregistre omfattende en meget stor del af befolkningen. Et af de almindelige formål med registerlovgivningen er at forebygge dataophobning. Accept af denne form for registrering ville indebære nærmest ubegrænset frihed for virksomhederne og dermed en nærliggende risiko for, at meget store personregistre blev opbygget. Selvom registrering af potentielle kunder kunne anses for naturligt for en virksomhed, er de modgående hensyn mere tungtvejende. For så vidt angår en registrering af en virksomheds konkurrenter, er hensynene derimod ikke af tilsvarende tyngde, hvorfor en sådan registrering som udgangspunkt vil være lovlig.[2]

Der har foreligget en række sager om, hvilke oplysninger der medtages i personaleregistre. Det er fundet acceptabelt at registrere, om de ansatte er medlemmer af en fagforening, og tillids- og bestyrelsesposter, de pågældende måtte have.[3] Derimod er det ikke i de fleste virksomhedstyper lovligt at registrere oplysninger om de ansattes privatøkonomi eller andre private forhold.[4] Som et specielt tilfælde fra praksis kan nævnes, at det er anset for lovligt, at en bank registrerer, hvilke forpligtelser personalet har i forbindelse med værnepligt for at kunne vurdere, hvorledes banken er stillet i en krigssituation.[5]

Gennemgående indicerer praksis, at der lægges meget stor vægt på formålet med den ønskede registrering, og at dette formål i en vis udstrækning relateres til branchetypen. Den konkrete vurdering kan føre til afgørelser, der forbyder en registrering, som ganske vist kan være erhvervsmæssigt relevant, men hvor de integritetsmæssige hensyn betragtes som mere tungtvejende. I denne forstand giver den fastsatte standard en form for carte blanche til Registertilsynet til at fastsætte niveauet for acceptabel registrering i de enkelte brancher. På denne baggrund bør § 3 stk. 1 anvendes med stor forsigtighed. Bestemmelsens elasticitet understreger betydningen af, at der i Registertilsynet, både i sekretariatet og i Registerrådet, er repræsenteret tilstrækkelig viden om erhvervslivets

2. Dette fremhæves i lovens forarbejder, jfr. Folketingstidende 1977/78 Tillæg A sp. 625.
3. Jfr. RÅ 1984 p. 54-55.
4. Jfr. RÅ 1992 p. 79-80.
5. Jfr. RÅ 1979 p. 203-204.

arbejdsvilkår, således at den ønskelige afbalancering over for integritetsbeskyttelseshensynet gennemføres, jfr. nærmere i kapitel 10.

1.5 Konklusion

Uanset at praksis på enkelte punkter kan virke begrænsende på erhvervsudøvelsen, er der gennemgående tale om marginalsituationer. Reguleringen anfægter ikke de centrale dele af virksomhedernes erhvervsudøvelse, og gennemgående må det konstateres, at den retlige standard i § 3 stk. 1 anvendes med passende forsigtighed og forståelse af de erhvervsmæssige forhold.

På baggrund af de ovenfor anførte synspunkter konkluderes det herefter, at den gældende regulering af almindelige oplysningers registrering ikke behøves ændret, idet det blot til stadighed må sikres, at erhvervsmæssige synspunkter bliver taget i betragtning ved udfyldningen af den retlige standard.

2 Følsomme oplysninger

Som fremhævet i kapitel 2, indebærer § 3, stk. 2, at private virksomheder kun i sjældne tilfælde har mulighed for at registrere de følsomme personoplysninger. Der er grund til at overveje, hvorvidt denne regulering er for streng.

Det kunne anføres, at virksomheder har behov for at være i besiddelse af helbredsoplysninger om personalet, både før og efter ansættelse, og at kendskab til oplysninger om strafbare forhold, både om personale og for kunder, vil være relevant, idet disse vil kunne indgå som et bidrag til bedømmelsen af, hvorvidt der vil kunne gives kredit og lignende. Der er ikke tvivl om, at der kan peges på anvendelsesmuligheder for de følsomme oplysninger, og at den gældende strenge regulering i visse tilfælde virker begrænsende på erhversudøvelsen, jfr. nærmere om disse særlige oplysningstyper under 2.2.

2.1 Almindelig vurdering

Det er et vanskeligt retspolitisk spørgsmål, om det vil være ønskeligt at gennemføre en liberalisering af de gældende regler om registrering af følsomme oplysninger. Forskellige typer af hensyn må tages i betragtning. Først må det fremhæves, at de følsomme oplysninger ligger i centrum for borgernes privatsfære, d.v.s. at det særligt er disse oplysninger, som beskyttelsen af privatlivets fred tager sigte på at værne. Tungtvejende ideologiske synspunkter taler derfor for, at der lovgivningsmæssigt må være faste regler for, hvornår sådanne oplysninger kan registreres. En streng regulering er udfra denne synsvinkel nødvendig. En generel lempelse af adgangen til at registrere følsomme oplysninger vil indebære en reel svækkelse af beskyttelsen af privatlivets fred. Det er der hverken politisk eller ideologisk basis for.

En sådan udvikling ville iøvrigt næppe være i overensstemmelse med erhvervslivets overordnede behov. For den enkelte erhvervsvirksomhed er et godt omdømme hos forbrugerne af stor betydning for afsætning og markedsandele. Hvor stor en betydning omdømmet har, vil variere fra virksomhed til virksomhed og bl.a. afhænge af produktionens karakter og konkurrenceforholdene. Der er næppe tvivl om, at håndteringen af de følsomme oplysninger har betydning for omdømmet, samtidig med at der i almindelighed er tale om en faktor, der ikke snævert er forbundet med de produkter/ydelser, der ønskes afsat. Der er dermed tale om et område, der er egnet til en retlig regulering med den funktion at skabe lige konkurrencebetingelser. En regulering på linie med den gældende har en sådan funktion, og under forudsætning af dens overholdelse i praksis stilles virksomhederne lige og er fritaget for at inddrage dette spørgsmål ved fastlæggelsen af deres interne politik. I betragtning af den imagemæssige betydning, som de følsomme persondata har, foreligger der en formodning om, at i hvert fald de større virksomheder vil overholde de fastsatte regler.

På den herved skitserede baggrund er udgangspunktet, at en regulering svarende til den gældende bør opretholdes. Afgørende idag er, at den enkelte borger er bekendt med, at følsomme data registreres, og at dette må anses for nødvendigt for virksomheden. Det er ikke nødvendigt at stramme denne regulering yderligere, og

om der i praksis bør ske en vis afsvækkelse, afhænger primært af, hvad der skal forstås ved nødvendighedskravet. Dette lægger op til en branchespecifik bedømmelse, hvor det ud fra formålet med den ønskede registrering vurderes, om denne er af så tvingende karakter, at det er acceptabelt, at virksomheden gennemfører denne. Med udgangspunkt i den generelle forsigtighed overfor registrering af følsomme oplysninger i den private sektor må det være åbenbart, at registrering er nødvendig. Praksis er således restriktiv, og en fastholdelse heraf må anses for ønskelig. Det kan derfor konkluderes, at generelt bør gældende ret forblive uforandret.

2.2 Helbred, straf

Som nævnt ovenfor er det særligt visse af de følsomme oplysningstyper, hvis registrering kunne være af erhvervsmæssig interesse. Dette taler for, at det overvejes, om det er hensigtsmæssigt ved specialregler at åbne for en sådan registrering, hvilket har den funktion, at det almindelige udgangspunkt ikke berøres. Sådanne specialregler kunne komme på tale i forhold til helbredsoplysninger og oplysninger om strafbare forhold.

Særligt for helbredsoplysninger er det et omdiskuteret spørgsmål, om den almindelige ret, enhver patient har til at få udleveret sådanne oplysninger fra autoriserede sundhedspersoner[6] bør føre til en situation, hvor det er normal praksis, at arbejdsgivere får adgang til disse oplysninger. Dette kan ske ved, at patienten, den ansatte eller stillingsansøgeren, videregiver de oplysninger, de ved brug af deres ret til aktindsigt har fået udleveret. I mange tilfælde vil denne videregivelse ikke være frivillig, men være udløst af et pres fra arbejdsgiverens side. Efter min opfattelse er det uden for virksomhedstyper, hvor særlige forhold gør sig gældende, ikke ønskeligt, at ofte ganske følsomme helbredsoplysninger bliver spredt på denne måde. De strenge registreringsbetingelser bør derfor opretholdes, og der bør yderligere, jfr. nedenfor, gennem-

6. Jfr. Lov nr. 504 af 30.6.1993 om aktindsigt i helbredsoplysninger samt lov om offentlige myndigheders registre § 13. De særlige spørgsmål om forsikringsselskabers adgang til helbredsoplysninger udelades her.

   Se iøvrigt nærmere om lovgivningen, Peter Blume, Retsvidenskabeligt Institut B, Studier nr. 54/1994 p.25-36.

føres regler, der begrænser risikoen for spredning af helbredsoplysninger.

Tilsvarende gør sig gældende for oplysninger om strafbare forhold. I den almindelige virksomhed er der ikke et tungtvejende behov for adgang til disse oplysninger. Det er i strid med dansk mentalitet, at der i alle mulige situationer skal produceres en ren straffeattest. Dette vil være et skråplan, som retssystemet bør træffe foranstaltninger imod.

Disse faktisk foreliggende problemer bør ikke løses ved, at den enkeltes adgang til registerindsigt begrænses. Denne rettighed er en fundamental del af individets selvbestemmelsesret. I den databeskyttelsesretlige lovgivning bør gennemføres en almindelig regel, hvorefter enhver har ret til at afvise krav fra udenforstående om, at indsigtsretten skal benyttes.[7] Herudover bør det i speciallovgivning fastsættes, at en arbejdsgiver ikke i almindelighed har ret til at kræve denne form for oplysninger, idet undtagelser kan tillades i tilfælde, hvor en virksomheds særlige beskaffenhed gør dette sagligt velbegrundet. I betragtning af den imagemæssige betydning de følsomme oplysninger har, vil en sådan regulering reelt også være i erhvervslivets interesse.

3 Reguleringsområdet

I henseende til erhvervsvirksomheders generelle adgang til persondataanvendelse tilbagestår herefter at vurdere reguleringens omfang. Som fremhævet i kapitel 2 er den gældende registerlov begrænset til at vedrøre registrering og videregivelse af registrerede oplysninger. Dette betyder, at indsamling af oplysninger og disses anvendelse internt i virksomheden ikke reguleres. For disse to faser gælder der i nogle tilfælde andre lovregler. I betalingskortloven er den interne anvendelse omfattet, og markedsføringslovens § 1 med generalklausulen om god markedsføring vil have betydning for, hvilke oplysninger der kan indsamles. Det må dog overvejes, om en generel regulering af disse spørgsmål bør gennemføres.

7. I udkastet til EU direktiv 1992 er en regel af denne karakter fastsat i artikel 13 stk. 2.

Denne problemstilling er aktualiseret af, at det er sandsynligt, at den kommende EU-retlige regulering vil omfatte disse faser.

3.1 Indsamling af oplysninger

Et rimeligt udgangspunkt ved vurderingen af, om indsamlingsfasen generelt bør reguleres, er, at forudsætningen for oplysningers registrering er, at de er kommet virksomheden i hænde. Dette kan selvsagt ske på mange måder, men en af disse vil være, at den pågældende person selv afgiver oplysningerne. I dette tilfælde kan det være velbegrundet at antage, at den integritetsorienterede beskyttelse allerede bør virke ved indhentelse af oplysningerne. Behovet foreligger, fordi det langtfra altid er frivilligt, at oplysninger afgives og yderligere, fordi det ofte kan forekomme, at den pågældende ikke er klar over, at oplysninger undergives fortsat databehandling. I disse to situationer kunne en retlig regulering være relevant.

Udover hvad der allerede idag kan udledes af markedsføringslovens § 1, er der ikke behov for egentlige forbud, men snarere for information. I udkastet til EU-retlig regulering fastsættes, at der skal gives information om, hvorvidt afgivelse af oplysninger er frivillig, og om der kan være negative konsekvenser forbundet med ikke at afgive oplysninger. I mange tilfælde vil dette følge af selve afgivelsessituationens karakter, men der vil kunne forekomme situationer, hvor der er berettiget uklarhed, og hvor information af denne karakter vil være hensigtsmæssig. Denne vil normalt kunne afgives, uden at der dermed opstår nogen større ressourcebelastning af virksomhederne.

3.2 Intern anvendelse

Information om den databehandling, der finder sted i virksomheden , er det vanskeligere at bedømme betimeligheden af. Det vil ikke altid være fuldtud klart for virksomheden, hvilken brug der vil blive gjort af de pågældende data, og i hvilket omfang data vil blive givet videre. Det vil derfor være svært at opfylde en informationsforpligtelse fuldtud. Det forekommer tilstrækkeligt, at borgerne ved hjælp af registerindsigt og eventuelle særregler for spe-

cielle anvendelsessituationer, jfr. herom i de kommende kapitler, kan skaffe sig denne form for information. Det vil i denne forbindelse være hensigtsmæssigt, om retten til registerindsigt blev udvidet til at omfatte information om, i hvilket omfang registrerede data er blevet videregivet. En sådan udvidelse af indsigtsretten vil kunne imødekomme informationsbehovet og kunne skabe en tillidsfremmende åbenhed omkring dataanvendelsen.

For så vidt angår intern anvendelse af registrerede persondata kunne det anføres, at en regulering ikke vil tilføje noget nyt, idet en adgang til at registrere implicit angiver adgang til at anvende de pågældende oplysninger. Som anført i kapitel 2 vil mange former for intern anvendelse reelt være omfattet af registreringsreglerne, ligesom der gælder et almindeligt databeskyttelsesprincip om, at oplysningerne ikke må anvendes til andre formål end de, der begrundede deres registrering. Det må erkendes, at en fuldstændig gennemførelse af princippet medfører for stor infleksibilitet i virksomhederne. Uanset dette forbehold lægger de almindelige regler om registrering en ramme omkring den interne anvendelse.

På denne baggrund konkluderes, at en regulering, der fastslår informationsforpligtelser for virksomheden, er tilstrækkelig. Anden form for regulering af den interne persondataanvendelse er ikke i almindelighed påkrævet. I særlige dataanvendelsessituationer kan der være behov for yderligere regler, jfr. herved især i kapitel 6. I sådanne tilfælde må det selvstændigt vurderes, om særlige hensyn har en sådan styrke, at det her angivne almindelige udgangspunkt bør fraviges.

4 Koncerner

1 Koncernen som en flerhed af selskaber

Koncerndannelser er meget udbredte i erhvervslivet. Der er tale om en forholdsvis dominerende selskabsform. Selv efter at den store fusionsbølge er ophørt, dannes der stadig nye koncerner. Ved en vurdering af de erhvervsmæssige konsekvenser forbundet med registerlovgivningen er det dermed af central betydning at inddrage koncerner som en særlig virksomhedstype. Til grund for den gældende regulering af koncerners persondataanvendelse er den almindelige opfattelse i dansk ret af, hvad en koncern er. Her lægges til grund, at koncerner er sammenslutninger af flere selvstændige virksomheder, der således f.eks. skatteretligt og selskabsretligt både behandles som fritstående med egne forpligtelser og som enheder, der er relateret til hinanden i en mere eller mindre kompleks hierarkisk struktur som moder- og datterselskaber. Afgørende er opfattelsen af koncernen som en flerhed af selskaber fremfor som et enhedsselskab.

Dette udgangspunkt tages også i registerlovgivningen med en række diskutable konsekvenser i henseende til mulighederne for dataanvendelse. Disse konsekvenser opstår som følge af den eksisterende regulering af intern anvendelse, registrering og videregivelse af persondata. I enhedsselskabet indebærer registrering i princippet fri intern anvendelse, medens i koncernen vil dette kun være tilfældet indenfor det selskab, der har registreret de pågældende data, medens overførsel af disse data til andre selskaber i koncernen vurderes under videregivelsesreglerne.

I det følgende belyses først hvilken betydning denne retstilstand har, hvorefter det drøftes om der bør ske ændringer enten i form af specialregler eller ved at den generelle opfattelse af en koncerns ka-

rakter fraviges på registerlovens område.[1] Det bør indledningsvist understreges, at disse spørgsmål er særligt væsentlige, fordi det tit er en del af begrundelsen for en koncerndannelse, at der herved kan ske en udvidet anvendelse af den samlede mængde af persondata. Som det fremgår af det følgende er dette en forudsætning, som ikke i alle henseender holder stik.

2 Videregivelse

Ved overførsel af almindelige persondata mellem koncernforbundne selskaber indebærer § 4, stk. 2, at videregivelsen skal være et naturligt led i den normale drift af den afgivende virksomhed, medmindre, hvilket kun sjældent i praksis vil forekomme, der foreligger et samtykke fra den registrerede. Dette er ikke strengt krav, men desuagtet vil der være tilfælde, hvor denne retlige standard ikke anses for opfyldt og videregivelse altså ikke kan finde sted. Det må derfor vurderes, om der er grundlag for en særlig anvendelse af standarden i koncernforhold. Det kunne hævdes, at det altid vil være naturligt for en koncernvirksomhed, at overdrage oplysninger til en anden koncernvirksomhed. Under en rent erhvervsmæssig betragtningsmåde vil dette synspunkt have meget for sig, men fuldt gennemført vil det være i modstrid med den gældende regulering. Antages det, at koncerner bør gives en særlig retsposition, kan en retspolitisk konklusion være, at der blev indsat en tilføjelse til § 4, stk. 2, hvorefter bestemmelsen ikke finder anvendelse i koncernforhold.

Forinden en sådan konklusion drages, er det dog nødvendigt dels at overveje, om en mindre radikal løsning er mulig dels om der er tungtvejende grunde, der kan tale imod et sådant resultat. Ved vurderingen heraf må det tillægges betydning, hvorvidt der kan opstilles retningslinier for Registertilsynets praksis i henseende til § 4, stk. 2, der tager særlige hensyn til koncerner, uden en ændring af lovgrundlaget.

Udgangspunktet for en sådan løsningsmodel er, at koncerner

1. Jfr. også om problemstillingen Peter Blume, UfR 1993 p 392-98.

kan bestå af mange forskellige typer af virksomheder og at disse kan ligge tættere eller fjernere på hinanden. Dette hænger sammen med, at så mange forskelligartede hensyn kan begrunde oprettelsen af en koncern. Denne konstatering kan føre videre til den antagelse, at det har betydning for anvendelsen af den retlige standard i § 4, stk. 2, om der er en produktionsmæssig sammenhæng mellem de pågældende virksomheder eller dette ikke er tilfældet. Der kunne på dette grundlag opstilles den retningslinie, at jo nærmere to koncernselskaber ligger i funktioner og erhvervsobjekt, i jo større udstrækning vil videregivelse af data kunne finde sted. Med andre ord en gradueret skala over de forskellige virksomheder strækkende sig fra sammenfald til ingen lighed.

En sådan model vil kunne få erhvervsmæssige konsekvenser for den enkelte koncern. I nogle koncerner vil der kunne opstå en registerretligt orienteret divisionering, hvor data frit kan udveksles mellem nogle af selskaberne, men ikke mellem andre. En sådan situation vil, uanset at den vil kunne opleves som noget kunstigt, være praktisabel. Den er en god illustration af de undertiden ganske intensive virkninger, som registerlovgivningen har i det private erhvervsliv. Det bør tilføjes, at virkningerne af den nævnte divisionering vil variere i den enkelte koncern, men at denne model må anses for gennemførlig i alle tilfælde. En praktisk udfyldning af § 4, stk. 2, som den her skitserede, vil være i overensstemmelse med princippet om, at registrerede data alene må anvendes til de formål, der har begrundet deres registrering.

Valget mellem de to løsningsmodeller afhænger af, om en fuldstændig undtagelse af koncerner fra den almindelige videregivelsesregel vil have integritetsbeskyttelsesmæssige skadevirkninger. Det kunne anføres, at en sådan regel kunne friste til at bruge koncernmodellen som en metode til at omgå registerloven, men dette forekommer ikke sandsynligt, eftersom der er andre og reelt mere tungtvejende, retlige konsekvenser forbundet med oprettelsen af en koncern. Det er ikke ud fra databeskyttelsesretlige hensyn det afgøres, om en koncern skal dannes. En omgåelsesrisiko synes dermed ikke at foreligge. Når vægten lægges på, at der alene er tale om almindelige persondata og at det fortsat vil være muligt, jfr. nærmere i det følgende, at have særregler for specielle dataanvendelsessituationer og når det yderligere tages i betragtning, at kontrol-

mulighederne er særligt ringe indenfor koncerner, der udefra kan være svært gennemskuelige, bliver konklusionen, at den mest enkle regel er en fuldstændigt undtagelse af koncerner. Dette betyder, at har et koncernselskab lovligt registreret en oplysning, kan denne uden yderligere formaliteter overføres til andre selskaber i koncernen. I forhold til selskaber udenfor koncernen finder de almindelige videregivelsesregler anvendelse. Indtil en sådan ordning lovgivningsmæssigt måtte være gennemført bør praksis indrettes i overensstemmelse med den ovenfor angivne retningslinie.

2.1 Følsomme oplysninger

For så vidt angår de følsomme persondata, medfører den omstændighed, at videregivelsesreglerne finder anvendelse, en betydelig begrænsning i adgangen til udveksling af sådanne data mellem koncernselskaber. Som omtalt i kapitel 2 er registreringsadgangen efter § 3, stk. 2, restriktiv, men efter § 4, stk. 1, er videregivelse uden samtykke ganske enkelt udelukket, medmindre der er særlig lovhjemmel hertil. De væsentlige forskelle mellem registrerings- og videregivelsesbetingelserne indebærer, at det ikke er muligt i dette tilfælde at angive en retningslinie for praksis, hvorefter der kan tages særligt hensyn til koncerner. Her foreligger alene den mulighed, at gennemføre en lovændring. Det vil være forholdsvist sjældent, at et behov for udveksling af følsomme oplysninger mellem koncernforbundne selskaber vil foreligge, men et eksempel herpå er en koncern af forsikringsselskaber, hvor der er registreret helbredsoplysninger om forsikringstagerne.

I koncerntilfælde kunne det overvejes at opstille en regel, der på samme måde som lovens system for de almindelige oplysninger paralleliserede betingelserne for registrering og videregivelse. En sådan regel ville betyde, at videregivelse kunne ske, når de registrerede blev informeret herom og når dette måtte anses for nødvendigt for driften af det pågældende selskab. Der ville fortsat være tale om en restriktiv regulering, men videregivelse uden egentligt samtykke ville ikke være udelukket. Informationskravet ville ofte kunne opfyldes ved hjælp af en standardskrivelse, således at det reelt afgørende ville være, om nødvendighedskravet, der altså er relateret til videregivelsen, er opfyldt. Dette spørgsmål måtte vur-

deres på sædvanlig måde, idet afgørelsen heraf relateres til den pågældende virksomhedstype, de implicerede datatyper og dataomfanget samt formålet med videregivelsen. På dette grundlag ville der være enkelte situationer, hvor videregivelse kunne ske, men under så strenge betingelser som angivet ville disse ikke indebære integritetsrisici for de registrerede. På den således skitserede baggrund og under hensyn til de ovenfor nævnte særlige momenter, der gør sig gældende i koncernforholdet, konkluderes, at en sådan regel bør gennemføres.

2.2 Personnumre

Oplysninger om personnumre er som nævnt i kapitel 2 undergivet en særlig regulering i § 4a og disse er af særlig interesse i henseende til udveksling af personaledata mellem koncernselskaber. Udveksling, herunder samkøring, af personaledata vil ofte være meget nærliggende og indebære en ressourcemæssig rationalisering i koncernen. Personaledata vil normalt ikke være følsomme med undtagelse af personnumre, der vil være registreret bl.a. grundet pligten til at indberette lønudbetaling til skattemyndighederne. Efter den gældende regel må personnumre videregives, når dette er et naturligt led i den normale drift af virksomheden og videregivelsen er nødvendig for en entydig identifikation af den pågældende. Netop i personaleadministrative sammenhænge kan det hævdes, at disse betingelser vil være opfyldt. Lægges det altså til grund, at koordineret personaleadministration er naturlig i koncerner vil § 4a så vidt det kan bedømmes ikke udgøre et problem for koncerner, hvorved det er forudsat, at oplysningerne alene anvendes til personaleadministrative formål. Under alle omstændigheder bør det ved anvendelsen af § 4a tages i betragtning, at der er tale om en koncern og en liberal fortolkning af bestemmelsen bør dermed lægges til grund i disse tilfælde.

3 Samkøring

I koncernforhold vil det være særligt udbredt, at videregivelse sker i form af samkøring. Medens det vil være forholdsvist atypisk, at der mellem forskellige fritstående private virksomheder gennemføres samkøringer, vil dette være normalt i koncerner. Dette betyder, at § 4, stk. 4, der som hovedregel forbyder samkøring, som sit hovedområde har koncerner. Denne konstatering, der ikke kan antages at have stået fuldstændig klart for lovgiver, må tillægges en vis betydning ved en vurdering af, hvorledes samkøringsforbudet praktiseres og i henseende til en bedømmelse af, om der retspolitisk er behov for ændringer. Det kan ligeledes indledningsvist noteres, at medens forbudet i det lovforslag, der førte frem til de gældende regler, alene omfattede edb-registre med følsomme data, blev det under forslagets behandling i Folketinget udvidet til at omfatte alle elektroniske registre. På dette tidspunkt (1987) var der dermed en betydelig uvilje mod samkøring i Folketinget.

Selvom holdningen idag næppe er så restriktiv, er der fortsat ikke tvivl om, at netop samkøring af mange betragtes som en særlig farlig fremgangsmåde. Et rationelt grundlag for disse betænkeligheder er, at der ved samkøring, hvor data hentes fra forskellige registre med hver deres formål og tidsafgrænsning, er en særlig risiko for en lav datakvalitet, d.v.s. at der kan opstå vildledende eller ukorrekte data. Det er ligeledes klart, at ved samkøring kan der ske en sådan kobling af data, at der etableres intensiverede profiler af de registrerede personer. Herudover er det væsentligt, at netop restriktioner overfor samkøring indebærer et indgreb overfor den moderne teknologis muligheder, hvorfor der må være en særlig sikkerhed for, at disse regler medfører en reel integritetsbeskyttelse. Dette skyldes især, at samkøringsforbudet udgør et alvorligt indgreb i koncerners erhvervsmæssige udfoldelsesmuligheder.

Ved en vurdering af konsekvenserne af det gældende forbud er det hensigtsmæssigt at se på, hvorledes dispensationsadgangen i § 4, stk. 5, praktiseres. Først kan det fremhæves, at tillades samkøring, er det et vilkår, at de registrerede skal informeres herom. Denne ressourcebelastning vil således altid foreligge i modsætning til ved almindelig videregivelse. Det kan i almindelighed

konstateres, at er der en naturlig erhvervsmæssig sammenhæng mellem to virksomheder og er samkøringsformålet fornuftigt, vil tilladelse blive givet, men at dette dog også forudsætter, at virksomhederne faktisk har det samme erhverv, f.eks. to forsikringsselskaber.[2] Et klart sagligt formål med samkøringen skal foreligge, men er denne forudsætning opfyldt, er praksis rimelig.

3.1 Den finansielle sektor

For den finansielle sektor er der opstillet særlige retningslinier.[3] Udgangspunktet i disse retningslinier tages i de regler om tavshedspligt, der gælder i denne sektor.[4] På dette grundlag vil der kunne samkøres oplysninger om kundeforhold, låntageres og forsikringstageres forhold. Oplysninger, der ikke er omfattet af bestemmelser om tavshedspligt, vil ikke kunne samkøres eller videregives, da dette ikke antages at være et naturligt led i driften af en koncern (§ 4, stk. 2). I disse tilfælde vil samkøring dog kunne ske, hvis de registrerede på informeret grundlag giver et samtykke, hvorved bemærkes, at samtykket kan gives forudgående og generelt. Omfattet af samkøring kan være kunder i de koncernselskaber, der er underlagt lovbestemt tavshedspligt. Andre selskaber kan også være omfattet, når de indgår i en sammenhæng[5] med de øvrige koncernselskaber og et samtykke foreligger. Samkøring vil kunne omfatte personnummeret, da selskaberne for egne kunders vedkommende allerede har denne oplysning, der sikrer entydig identifikation. Som et særligt tilfælde på retningsliniernes anvendelse kan nævnes, at et moderpengeinstitut vil kunne få samkøringstilladelse for datterselskabernes engagementsoversigter med det formål at sikre, at lovgivningens regler om størrelsen af det samlede engagement med en enkelt kunde overholdes. Generelt anføres endvidere, at samkøring ikke kan ske med henblik på markedsføring, jfr. § 4b og nedenfor samt i kapitel 5. I konkrete sager

2. Jfr. lovens forarbejder, Folketingstidende 1986/87 Tillæg A sp. 511. – Som et illustrerende eksempel se RÅ1992 p 99-101 om SAS' Euro-bonusordning.
3. Jfr. hertil RÅ1992 p 94-96 samt RÅ1993 p 102-04.
4. Se i denne forbindelse Lars Hedegaard Kristensen, Juristen 1993 p 224-234, hvor forholdet mellem tavshedspligtregler og videregivelsesregler i den selskabsretlige og registerretlige lovgivning behandles.
5. Denne formulering er et citat fra retningslinierne. Den er ikke særlig oplysende, men angiver vel, at der skal være tale om tilknyttede funktioner.

vil Registertilsynet ofte konsultere Finanstilsynet, inden der træffes en afgørelse.

Det afgørende fikspunkt i denne praksis er antagelsen af, at tavshedspligtsregler lægger en ramme for omfanget af samkøringen. Tankegangen må være, at disse regler indebærer, at de enkeltselskaber, der får adgang til nye oplysninger, ikke formidler disse videre til andre, da tavshedspligten begrænser råderummet for videregivelse af de pågældende oplysninger. I den almindelige virksomhed indebærer en samkøring, at der bliver adgang til en række nye oplysninger, som de pågældende virksomheder frit kan anvende internt, men selvsagt kun yderligere kan videregive, såfremt betingelserne herfor er til stede. Er de pågældende oplysninger underlagt tavshedspligt, indebærer dette en vis begrænsning af den interne anvendelse, men det er ikke uden videre åbenbart, at sådanne regler bør være afgørende for i hvilket omfang samkøring kan accepteres. § 4, stk. 4 og 5 er ikke baseret på en sådan betragtning. Overført til andre områder kan der opstå en ganske restriktiv praksis, såfremt det generelt skulle være udslagsgivende for adgangen til samkøring, om der er tale om tavshedsbelagte oplysninger.

Tilsvarende kan det i denne sammenhæng forekomme lidt problematisk at acceptere samkøring, såfremt et samtykke foreligger. Det må erkendes, at det vil være meget svært for den enkelte at overskue, hvad der gives samtykke til og at der dermed må stilles meget store krav til den information, der ligger til grund for samtykket. På dette grundlag er denne praksis, selvom dens intention er at åbne op for visse samkøringer i koncernforhold, noget problematisk.

Det vil være bedre i al almindelighed at erkende, at der i koncernforhold foreligger en sådan forbindelse mellem de enkelte selskaber, at det ikke er hensigtsmæssigt, at samkøring er forbudt. Snarere bør denne videregivelsesform behandles på samme måde som andre former for videregivelse og dermed i almindelighed accepteres, når den fremtræder som naturlig ud fra det pågældende koncernforhold. Det er muligt at en sådan liberalisering er for vidtgående i henseende til de følsomme data. Her kunne retsstillingen være den, at samkøring uanset de ovenfor fremhævede forhold forudsatte et samtykke fra de registrerede samt at samkøring er nødvendigt for virksomhedernes drift. I betragtning af, hvor

ringe en betydning de følsomme data har i de fleste erhvervsvirksomheder, vil en sådan særregel ikke have den store erhvervsmæssige betydning samtidig med, at den vil sikre en forholdsvis fast regulering af den form for samkøring, der reelt kan føre til integritetskrænkelser.

3.2 Generelle overvejelser

I henseende til samkøring kan der være grund til at overveje betydningen af det almindelige databeskyttelsesprincip om, at registrerede data ikke må anvendes til andre formål end de, der begrundede deres registrering. Man kan rejse det spørgsmål, om der er harmoni mellem dette princip og den regulering, der ovenfor er blevet foreslået. Ved samkøring sættes de registrerede data ind i en ny kontekst, der ofte ikke vil være medtænkt på det tidspunkt, hvor registreringen fandt sted. Besvarelsen heraf afhænger af, hvorledes man skal forstå begrebet formål i denne sammenhæng. Anlægges en meget snæver forståelse, ville dette udelukke stort set alle former for videregivelse. Tager man derimod det udgangspunkt, at kravet om tilsvarende formål angiver, hvorledes de registrerede data anvendes, hvorved det ikke tillægges selvstændig betydning, hvem der faktisk realiserer denne anvendelse, indebærer dette dels, at videregivelse af data bliver muligt, dels at regler om samkøring, der lægger vægten på korrespondens mellem erhvervsudøvelsen i de enkelte selskaber, harmonerer med princippet.

For at der skal være tale om et meningsfuldt princip, må et sådant udgangspunkt tages og det betyder følgeligt, at de ovenfor anførte retspolitiske forslag antages at falde indenfor de internationalt anerkendte normer på området.

4 Markedsføring

Den sidste særlige problemstilling i forbindelse med koncerner angår adgangen til at videregive data med henblik på markedsføring, hvilket som nævnt i kapitel 2 alvorligt begrænses af § 4b, der iøvrigt mere uddybende drøftes i næste kapitel. Anvendelsen af

denne regel viser med særlig styrke de erhvervsmæssige konsekvenser, der er forbundet med antagelsen af, at spredning af oplysninger indenfor en koncern skal betragtes som en videregivelse.

En del af det økonomiske rationale bag koncerndannelser er, at der herved bliver mulighed for en bred anvendelse af de enkelte selskabers kundedata og dermed forbedrede muligheder for at øge selskabernes markedsandele. Det må konstateres, at § 4b effektivt udelukker disse muligheder ved kravet om skriftlig specificeret samtykke fra hver enkelt kunde, såfremt disse er forbrugere. I praksis er der ikke nogen mulighed for at komme udenom bestemmelsen, da ingen dispensationsadgang er optaget i loven.

Selvom den nærmere drøftelse af persondataanvendelse til markedsføringsformål sker i næste kapitel, kan der være grund til at overveje, hvorvidt der kunne opstilles en særregel for koncerner i den situation, hvor § 4b iøvrigt blev opretholdt uændret. Det må her erkendes, at selve den omstændighed, at der foreligger en koncern ikke understøtter en undtagelse fra markedsføringsforbudet. Om markedsføring foretages af et selvstændigt selskab eller af et koncernselskab, må anses for ligegyldigt set fra forbrugerens perspektiv og denne forskel kan ikke indenfor en sådan tankegang begrunde en undtagelse. Grundlaget for en sådan, der kunne opretholde informationsforpligtelsen, men fjerne samtykkekravet, kan alene være den omstændighed, at reglen har særligt skadelige erhvervsmæssige konsekvenser for koncerner, da selve grundlaget for koncerndannelsen berøres.

Det er et rent politisk spørgsmål, om en sådan argumentation virker overbevisende og det er derfor ikke nødvendigt her at forfølge spørgsmålet nærmere. Det kan blot forudskikkes, at i næste kapitel vil der blive argumenteret for en generel ændring af reguleringen af dataanvendelse til markedsføringsformål og bliver dette resultatet, vil koncerners erhvervsmæssige situation automatisk blive forbedret.

5 Koncernbegrebet

Til grund for den retspolitiske drøftelse i de forrige afsnit har ligget en implicit accept af, at koncerner opfattes som en flerhed af selskaber fremfor ét selskab. Det falder udenfor denne bogs rammer i almindelighed at vurdere, hvorvidt denne grundopfattelse er hensigtsmæssig på andre retsområder. Derimod er det værd at overveje, om synspunktet bør opretholdes på databeskyttelsesrettens område, hvorved det lægges til grund, at det ikke er nødvendigt, at koncerner opfattes på samme måde på alle områder. Det er i hvert fald svært at se en tvingende argumentation for en sådan enhedstankegang og en varierende betragtningsmåde skønnes ikke at åbne for omgåelsesmuligheder og lignende.

Det er derfor en mulighed at opfatte koncerner som enhedsselskaber, hvorved de foran behandlede problemstillinger uden videre ville være løst. Når det lægges til grund, at det uanset den økonomiske betydning, som persondata har, ikke er dataorienterede hensyn, der er afgørende for, om en koncern dannes, forekommer det nærliggende på databeskyttelsesrettens område at revidere opfattelsen af koncernbegrebet. De almindelige beskyttelsesregler, der er anvendelige i forhold til fritstående virksomheder, yder den tilstrækkelige garanti for værnet af den personlige integritet og privatlivet.

En sådan revision af selve koncernbegrebet kan det dog være vanskeligt at få gennemført.[6] Dette er baggrunden for, at den mindre radikale retspolitiske model er tillagt størst betydning i dette kapitel. En gennemførelse af de stillede forslag udelukker dog ikke, at man på et senere tidspunkt vælger en mere »ren« løsning og beslutter at betragte en koncern som et enhedsselskab fremfor som en flerhed af selskaber.

6. I bemærkningerne til artikel 2f i EU direktivforslaget 1992, hvor begrebet tredjemand defineres, lægges til grund, at en koncern er en flerhed af selskaber.

5 | Markedsføring

Et væsentligt erhvervsmæssigt spørgsmål er i hvilket omfang persondata kan benyttes med henblik på markedsføring. I takt med udviklingen af informationssamfundet, internationaliseringen og nye teknologier, der kan understøtte salg af produkter og tjenesteydelser, er betydningen af markedsføring vokset betragteligt, og der investeres betydelige beløb i denne aktivitet. Mange virksomheder har selvstændige markedsføringsafdelinger og yderligere er der en række virksomheder, der lever af at informere og formidle reklame for andre virksomheder. Forinden de egentlige databeskyttelsesretlige spørgsmål behandles, kan det være hensigtsmæssigt at indkredse problemstillingen nærmere ved at kategorisere forskellige former for markedsføring.

1 Direkte markedsføring

Det er nødvendigt at skelne mellem direkte markedsføring og uadresseret markedsføring. Ved direkte markedsføring forstås i det følgende en reklameindsats rettet til en specificeret del af befolkningen, hvor det er karakteristisk, at reklamen henvender sig personligt til den potentielle køber. I modsætning hertil indebærer den uadresserede markedsføring, at reklamen rettes bredt mod hele aftagerkredsen og ikke specifikt mod hver enkelt køber. Det er ved den direkte markedsføring, at der er behov for et persondatagrundlag, hvorudfra adressaterne for reklamen kan udvælges. Uden en adgang til persondata, hvorudfra modtagerkredsen kan segmenteres, er det ikke muligt at gennemføre denne form for markedsføring. På denne baggrund er det den direkte markedsføring, der er emnet for dette kapitel.

2 Adressater

Der kan skelnes mellem 3 adressatgrupper for direkte markedsføring. For det første forbrugere, der karakteriseres ved, at de ikke erhvervsmæssigt skal benytte de pågældende produkter eller tjenesteydelser. Det er en udbredt opfattelse, at forbrugere er svagere udrustede end erhvervslivet, hvorfor der er behov for en retlig regulering, som giver disse en særlig retsbeskyttelse. Det er denne grundlæggende antagelse, der begrunder den forbrugerretlige lovgivning. I databeskyttelsesmæssig sammenhæng er det særligt væsentligt, at forbrugere er enkeltpersoner, og at datagrundlaget i forhold til disse dermed udgøres af personoplysninger.

For det andet er andre erhvervsdrivende adressat for markedsføring. I forhold til disse foreligger der ikke et særligt civilretligt beskyttelsesbehov, men de falder dog indenfor databeskyttelsesrettens område. Registerloven gælder som nævnt i kapitel 2 også for oplysninger om juridiske personer, og selvom integritetsbeskyttelsesbehovet ikke er så tungtvejende som ved enkeltpersoner, kan der muligvis være tilfælde, hvor det er rimeligt også at beskytte virksomhedsdata i forhold til markedsføring, jfr. den i kapitel 2 omtalte lov om det centrale erhvervsregister. Denne problemstilling behandles dog ikke her, eftersom den ikke giver anledning til samme vanskelige retspolitiske afvejningsspørgsmål som markedsføring i forhold til forbrugere.

For det tredje kan adressaten være offentlige myndigheder, der sædvanligvis hverken i forbrugerretten eller i databeskyttelsesretten antages at have et beskyttelsesbehov i forhold til markedsføring. Denne antagelse synes i almindelighed at være velbegrundet, hvorfor denne form for markedsføring ikke inddrages i det følgende.

3 Anvendte medier

I retspolitisk sammenhæng kan det være væsentligt at skelne mellem de forskellige medier, der benyttes til markedsføring. De an-

vendte medier har nok størst betydning forbrugerretligt, men kan dog også spille en rolle ved fastlæggelsen af den databeskyttelsesretlige regulering. Markedsføring kan ske ved personlig henvendelse til adressaten, ved telefonisk henvendelse, ved fremsendelse af skriftligt materiale, ved brug af moderne medier som telefax, elektronisk post, og inden længe interaktivt fjernsyn.

Disse forskellige formidlingsmetoder kan kategoriseres på forskellige måder. Der kan skelnes mellem de metoder, hvor der er umiddelbar kontakt mellem markedsfører og forbruger og andre former, hvor en sådan umiddelbar kontakt ikke foreligger. Der kan også ske en graduering ud fra, hvor »pressende« anvendelse af de forskellige medier kan opleves. Sådanne opdelinger kan have betydning ved vurderingen af i hvilken udstrækning, det er acceptabelt, at benytte persondata som grundlag for markedsføring.

4 Produkterne

Det kan endelig komme på tale at inddrage karakteren af det produkt eller tjenesteydelse, der formidles. Det kunne tænkes, at gøre en forskel, om varen er almindelig eller følsom i den forstand, at den indicerer et behov hos forbrugeren, der kan sættes i relation til de rent private oplysningstyper. Sidstnævnte kunne tænkes at foreligge bl.a. indenfor det seksuelle og det helbredsmæssige område. Det kan overvejes, om der bør gælde strengere regler for dataanvendelsen i henseende til formidlingen af sådanne reklamer.

5 Elektroniske spor

Det databeskyttelsesretlige problemkompleks angår i hvilket omfang og under hvilke betingelser det skal være muligt at benytte persondata som grundlag for direkte markedsføring. De gældende hovedbestemmelser herom findes i registerlovens § 4b og kapitel 4 samt i betalingskortloven.

I betydeligt omfang angår problemstillingen det, som er blevet

betegnet elektroniske spor. Herved forstås det forhold, at forbrugerne ikke mindst ved anvendelsen af forskellige former for elektroniske betalingsformer efterlader sig et spor, der samlet angiver deres behov og interesser. Samlingen af de mange i sig selv sædvanligvis trivielle enkeltoplysninger tegner en profil over den enkelte forbruger. Spørgsmålet er herefter om sådanne spor skal kunne benyttes. Det må i almindelighed tages i betragtning, at de kan give en viden om den enkelte person, som kan betragtes som beskyttelsesværdig og dermed illustrerer, at selv meget trivielle oplysninger i visse relationer kan indgå i en sammenhæng, hvor risiko for integritetskrænkelser kan opstå., jfr. iøvrigt foran i kapitel 3.

Bedømmelsen af disse risici må afhænge af, hvem der benytter det elektroniske spor og til hvilke formål, jfr. nærmere i næste kapitel. Medens det er åbenbart, at de pågældende data har stor nytteværdi i forbindelse med beslutninger om markedsføring, er dette selvsagt ikke ensbetydende med, at en sådan brug udgør en potentiel integritetskrænkelse. Den omstændighed, at en person modtager personligt orienteret reklame, kan efter min opfattelse ikke generelt antages at være integritetskrænkende. Dette betyder, at en retlig regulering, der ud fra en sådan synsvinkel i almindelighed begrænser direkte markedsføring ikke er påkrævet. Derimod kan det ikke afvises, at nogle mennesker opfatter denne form for markedsføring som krænkende, hvilket taler for en regulering, som giver den enkelte mulighed for at undgå markedsføring.

Hermed er en af de centrale retspolitiske brudflader, der vil gennemsyre den følgende fremstilling, antydet. Der går således en skillelinie mellem ordninger, der er baseret på, at den registrerede skal samtykke til dataanvendelsen og ordninger, hvor den registrerede har mulighed for at modsætte sig en sådan dataanvendelse. I den internationale debat skelnes mellem opt in og opt out regulering.

6 Fordele ved direkte markedsføring

Forinden de enkelte retspolitiske spørgsmål underkastes drøftelse, kan det være nyttigt med nogle enkelte bemærkninger om de forde-

le, som anvendelsen af direkte markedsføring medfører. Disse er først og fremmest af ressourcemæssig karakter. Formålet med markedsføring er selvsagt at få afsat det reklamerede produkt og et rationelt mål er, at de midler, der afsættes til markedsføring, står i et fornuftigt forhold til antallet af afsatte produkter. Markedsføringsinvesteringen bør i så ringe omfang som muligt belaste prisen på det enkelte produkt. Ud fra denne synsvinkel er markedsføring rettet til den del af befolkningen, der med størst sandsynlighed er interesseret i produktet, og dermed er potentielle købere, mere effektiv end den brede markedsføring, der også kommer ud til personer, der ingen interesse har i produktet. Det er ikke overraskende, at direkte markedsføring opfattes som den bedste form for markedsføring.

Ses der alene på markedsføring ved anvendelse af trykte publikationer, taler økologiske hensyn også for den direkte markedsføring. I og med at markedsføring er målrettet, vil antallet af trykte reklamer være mindre end ved den uadresserede forsendelse, ofte betegnet som junk mail, og dermed er papirforbruget tilsvarende mindre. Et ikke uvæsentligt moment.

På denne baggrund er det erhvervsmæssigt ønskeligt, at der juridisk er gode vilkår for gennemførelsen af direkte markedsføring og et udgangspunkt for de følgende betragtninger er dermed, at – medmindre databeskyttelsesmæssige hensyn klart indicerer andet – bør der være frihed til at anvende persondata som grundlag for markedsføringen.

7 Anvendelse af egne data

Som den første juridiske problemstilling behandles i det følgende virksomhedens anvendelse af egne data til markedsføring af egne produkter.[1] Det lægges til grund, at der er tale om lovligt registrerede data. Der findes ikke i registerloven specialregler om denne situation, hvorfor det alene kan overvejes, hvorvidt det ikke lovfæstede princip om, at registrerede data alene må anvendes til de for-

1. Se generelt til de følgende afsnit Peter Blume, UfR 1994 p 163-69.

mål, der begrundede deres registrering, skulle skabe vanskeligheder. I mange tilfælde vil et af formålene med registrering af kundedata være anvendelse til senere markedsføring og her er der selvsagt ikke problemer. Også i andre tilfælde er det fast antaget, at virksomheder kan bruge egne data til markedsføring overfor kunder og personale. Dette er en del af den interne anvendelse, der ikke omfattes af registerloven.

Tages der hensyn til, at nogle mennesker som anført ovenfor opfatter modtagelse af personligt adresseret reklamemateriale som privatlivskrænkende, bør dette havde den konsekvens, at den frie interne anvendelse begrænses. Det bør således være muligt for kunder (og ansatte) at meddele virksomheden, at de ikke ønsker at modtage sådant reklamemateriale. I de følgende afsnit lægges det som et almindeligt synspunkt til grund, at en sådan nægtelsesret (»opt out«) bør anerkendes. Dette bør derfor også gælde for de internt anvendte data.

7.1 Betalingskortdata

Er de pågældende data registreret som følge af den registreredes brug af et betalingskort, er situationen en anden. I disse tilfælde er det betalingskortlovens § 24, der regulerer dataanvendelsen. Ifølge denne bestemmelse må data opstået som følge af kortets brug alene benyttes i det omfang, det er nødvendigt af hensyn til gennemførelsen af betalingstransaktioner. I bestemmelsens forarbejder gøres det klart, at reglen er til hinder for, at der opbygges forbrugsprofiler og er til hinder for at data benyttes med henblik på markedsføring. I forbindelse med senere ændringer af betalingskortloven er dette synspunkt blevet konfirmeret og underbygget.[2] Det særlige ved § 24 er, at bestemmelsen også omfatter kortudsteders og betalingsmodtagers interne anvendelse. Der er således tale om en meget virkningsfuld begrænsning i mulighederne for dataanvendelse til markedsføringsformål og bestemmelsen tilkendegiver den grundopfattelse, at genererede elektroniske spor ikke må benyttes til dette formål.

I lyset af de ovenfor anførte synspunkter vedrørende den er-

2. Se hertil Peter Blume, Retsvidenskabeligt Institut B. Studier nr. 46/1992 p 18.

hvervsmæssige betydning af direkte markedsføring er det naturligt at overveje, hvorvidt § 24 bør ændres, således at anvendelse af data til markedsføringsformål bliver muligt. En sådan ændring bør efter min opfattelse gennemføres. Direkte markedsføring er ikke i almindelighed integritetstruende eller privatlivskrænkende. Ses der bort fra særlige former, hvor specielt må nævnes personlig henvendelse på forbrugerens bopæl eller lignende, der kan reguleres i den forbrugerretlige lovgivning,[3] er det svært at se, at markedsføring i almindelighed skulle kunne være krænkende. Der kan forekomme særlige tilfælde, hvor en sådan krænkelse kan fremtræde som mere nærliggende, men disse kan, hvilket der redegøres nærmere nedenfor, reguleres i specielle bestemmelser. Det bør tilføjes, at der kan være andre anvendelsesområder for de elektroniske spor, hvor det med rette kan antages, at der foreligger en risiko for integritetskrænkelser, jfr. kapitel 6, men dette gælder altså ikke i almindelighed for markedsføring.

Det kan derimod ikke afvises, at enkelte personer kan opfatte direkte markedsføring som privatlivskrænkende. Der bør derfor være en mulighed for, at en sådan dataanvendelse kan undgås. En registreret bør således ved en simpel meddelelse til den registeransvarlige virksomhed kunne tilkendegive, at den pågældende ikke ønsker markedsføringsmateriale og det skal herefter være en pligt at respektere en sådan meddelelse. Som konsekvens af en sådan regulering skal virksomheden føre et register over modtagne anmodninger, således at det sikres, at de pågældende ikke senere modtager reklamer.

8 Andre virksomheders data

De kundedata, en virksomhed er i besiddelse af, kan også være af interesse for andre virksomheders markedsføring. De registrerede data udgør dermed en værdi og den registrerende virksomhed kan have interesse i at sælge disse data. Ved bedømmelsen heraf lægges det i det følgende til grund, at det er uden betydning for den retlige

3. Jfr. § 2, stk. 1 i lovbekendtgørelse nr. 886 af 23/12 1987 om visse forbrugeraftaler.

regulering, om de pågældende data videregives til en anden virksomhed, der herefter foretager sin markedsføring, eller om den registrerende virksomhed foretager markedsføring på vegne af andre virksomheder. Selvom det ikke er sikkert, at gældende ret regulerer disse to situationer på samme måde, lægges det her til grund, at der i begge tilfælde reelt sker en videregivelse. Det lægges dermed også til grund, at når data videregives, sker det i form af en aftale, hvori det sikres, at de pågældende data ikke benyttes til andre formål end markedsføring. En regel, der forudsætter en sådan kontraktregulering, bør dermed medtages i forbindelse med den regulering, der retspolitisk foreslås nedenfor.

Som det fremgik af beskrivelsen i kapitel 2, indebærer registerlovens § 4b en meget restriktiv regulering af adgangen til sådan datavideregivelse, da denne forudsætter at forbrugeren har givet et skriftligt specificeret samtykke på informeret grundlag. Baggrunden for bestemmelsen er en af Europarådet udstedt rekommandation med udgangspunkt i Rådets databeskyttelseskonvention.[4] Som det angives nedenfor, er § 4b på enkelte punkter mere restriktiv en rekommandationen.

I det følgende overvejes, om denne strenge regel, der ofte er blevet kritiseret fra erhvervslivets side, bør opretholdes eller modificeres. For at forebygge misforståelser præciseres, at diskussionen alene angår videregivelse til markedsføringsformål, og at der dermed ikke tages stilling til videregivelse af købsoplysninger med henblik på andre formål. Det er således fortsat en begrænset anvendelse af de elektroniske spor, der diskuteres her.

Problemstillingen angår herefter, om markedsføring fra andre virksomheder end den virksomhed, hvori et køb er foretaget, indebærer en særlig krænkelsesrisiko, der forudsætter et specielt retsværn. Hertil kan anføres, at der hos den enkelte kan opstå en vis tvivl, ja endda uro, overfor det forhold, at en fremmed virksomhed fremsender markedsføringsmateriale. Dette forhold indicerer et behov for information, således at denne form for markedsføring ikke kommer som en overraskelse. Selve modtagelsen af markedsføringmaterialet adskiller sig derimod ikke fra den situation, hvor det er virksomheden selv, der markedsfører. Der sker hverken no-

4. Recommendation no R (85) 20 on the protection of personal data used for the purposes of direct marketing.

gen mindre eller større integritetskrænkelse eller privatlivsindtrængen.

På dette grundlag forekommer der ikke at være behov for en så indgribende regulering som i § 4b, der iøvrigt er indispensabel.[5] Det er tilstrækkeligt, at der informeres om, at oplysninger kan blive videregivet til markedsføringsformål og at der gives forbrugerne en ret til at nægte en sådan videregivelse. På denne måde vil man kunne imødekomme hensynet til de personer, der opfatter direkte markedsføring som generende og samtidig fjerne en unødvendig hindring for virksomhedernes erhvervsudøvelse. En sådan ordning vil fortsat være i overensstemmelse med Europarådets rekommandation, der netop forudsætter en nægtelsesadgang og alene for de følsomme data, jfr. om disse nedenfor, kræver, at der skal foreligge et egentligt samtykke fra forbrugeren. Danmark vil således fortsat med en ordning som den skitserede opfylde sine internationale forpligtelser.

9 Kuverterings- og adresseringsbureauer

En virksomhed kan opnå det fornødne datagrundlag for markedsføring ved at erhverve fortegnelser over adressater fra kuverterings- og adresseringsbureauer, der er underlagt en særlig regulering i registerlovens kapitel 4. Der er tale om bureauer, som bl.a. lever af, at sælge adresser til andre. Inden lovrevisionen i 1987 var det tilladt for disse bureauer at registrere oplysninger om fritidsinteresser, således at det var muligt at foretage en vis segmentering, men denne adgang blev ophævet, således at bureauerne idag kun har ret til at registrere offentligt tilgængelige oplysninger som navn og adresse, herunder oplysninger, der kan fås fra erhvervsregisteret. På dette grundlag vil der kunne fås en bopælsorienteret afgrænsning af forbrugerne, men altså ikke mere end dette.

Enhver kan købe sådanne lister eller benytte bureauet til at formidle markedsføring. En registreret har ret til at kræve sig slettet af så-

5. Registertilsynet fremhæver den manglende dispensationsmulighed i sin afgørelse i RÅ 1991 p 117-19.

danne bureauers fortegnelser og denne adgang (opt out) er i overensstemmelse med de ovenfor advokerede retspolitiske synspunkter.

Der forekommer ikke at være noget egentligt behov for at gennemføre ændringer af reglerne i kapitel 4. Selvom den almindelige holdning til mulighederne for markedsføring skulle blive liberaliseret og det i en sådan situation kunne overvejes igen at tillade segmentering udfra fritidsinteresser, er dette dog næppe ønskeligt. Det kan til støtte herfor anføres, at der er en vis forskel på at tillade virksomheder at anvende oplysninger om foretagne køb som grundlag for direkte markedsføring og mere fritstående at acceptere registrering af interesser m.v. Under et overordnet databeskyttelsesperspektiv kan sådanne registre forekomme mere betænkelige, fordi de medfører en form for dataophobning, som sædvanligvis bør undgås. Konklusionen er derfor, at reglerne i registerlovens kapitel 4 ikke bør ændres.

10 Markedsføring fra udlandet

En særlig problemstilling angår markedsføring fra udlandet overfor danske forbrugere. I det omfang datagrundlaget herfor udgøres af almindelige oplysninger indebærer § 21, at der ikke er nogen begrænsning heri under forudsætning af, at de almindelige videregivelsesregler er opfyldt. Dette betyder, at gennemføres de ændringer af retstilstanden, som er anført tidligere, vil der ligeledes opstå forbedrede muligheder for markedsføring fra udlandet. Særligt kan der være grund til at pege på, at det vil være muligt at videregive sådanne oplysninger til udenlandske virksomheder indenfor rammerne af en liberaliseret udgave af § 4b. Det må derfor overvejes, om dette er en acceptabel retsudvikling, hvorved det generelt forudsættes, at den information, som gives til forbrugerne vedrørende videregivelse til markedsføringsformål, skal omfatte, at dette også kan ske til udenlandske virksomheder.

Det er i almindelighed lagt til grund, at de videregivne oplysninger alene anvendes til markedsføringsformål, og denne forudsætning implicerer, at der eksisterer et generelt retligt miljø til sikring heraf. Dette kunne tale for, at fri overførsel af data alene bør ske til

de lande, der har en acceptabel databeskyttelseslovgivning, jfr. nærmere i kapitel 9. Overførsel af data til virksomheder i lande, der ikke opfylder denne forudsætning, bør således forudsætte et samtykke fra forbrugeren (opt in). På denne måde vil man kunne fastholde, at andre former for anvendelse af de elektroniske spor ikke umiddelbart er acceptabel, jfr. hertil i kapitel 6. En regel af denne karakter synes også at være i overensstemmelse med de generelle betænkeligheder, der ofte høres fra forbrugere netop i forbindelse med markedsføring fra udlandet. Der er dermed tale om en begrænsning, der vil gøre det lettere, at få gennemført den generelle liberalisering af dataanvendelsesmulighederne.

11 Telemarkedsføring

De ovenfor anførte synspunkter har taget sigte på direkte markedsføring i almindelighed og kan uden videre lægges til grund for så vidt angår markedsføring i form af postbesørgede forsendelser. Der er derimod behov for at overveje, om der er særlige forhold forbundet med andre former for markedsføring, der kan gøre det berettiget at have specielle databeskyttelsesbestemmelser.

Først og fremmest er der grund til at behandle persondatanvendelse til brug for telemarkedsføring. I forbrugeraftalelovens § 2 findes et almindeligt forbud mod denne form for markedsføring, når den finder sted uden opfordring fra forbrugeren. Denne regel er betinget af forbrugerretlige overvejelser, som særligt er baseret på den iagttagelse, at der ved telefonisk henvendelse sker en direkte konfrontation mellem forbruger og markedsfører, der tit kan føre til, at en forbruger presses eller lokkes til at foretage en disposition, som vedkommende efterfølgende fortryder.

Under en privatlivssynsvinkel er det antageligt, at denne form for henvendelse kan opfattes som en indtrængning. Det følger af markedsføringslovens § 1, at sådanne henvendelser på de områder, hvor de iøvrigt er lovlige ikke må ske på et for forbrugeren generende tidspunkt. I norsk ret har Datatilsynet bestemt, at telefonisk henvendelse alene må ske mellem kl. 09.00 og 21.00 og ikke på søn- og helligdage. Tilsvarende bestemmelser findes også i andre

lande. I udkastet til direktiv om databeskyttelse i forbindelse med telekommunikation fremlagt i 1990[6] er det bestemt, at forbrugeren kan anmode teleselskabet om at stoppe uopfordrede henvendelser, hvilket teknisk forekommer lidt problematisk. En sådan regel forudsætter tilsyneladende, at teleselskabet skal skaffe sig kendskab til indholdet af førte samtaler, hvilket ikke kan anses for acceptabelt. I et revideret udkast til dette direktiv[7] er bestemmelsen (artikel 13) ændret således at det blot pålægges medlemslandene at sikre at sådanne opkald ikke finder sted.

I forhold til telemarkedsføring, hvis gennemførsel kan være vanskelig at kontrollere og som direkte intervenerer i privatsfæren, bør der gives adressaterne en særlig beskyttelse. Den gældende ordning i forbrugeraftaleloven, hvorefter et samtykke er påkrævet (opt in), bør derfor opretholdes. I henseende til fremskaffelse af datagrundlaget er der ikke behov for særregler, men ønsker virksomheden at markedsføre via telefon, må den opnå et forudgående samtykke hertil. Med en ordning som denne er der i og for sig ikke behov for regler om telefontid, men det bør være normalt, at markedsføringen foretages på acceptable tidspunkter.

12 Fax, elektronisk post m.m.

Yderligere er der grund til at overveje, hvorvidt markedsføring ved brug af moderne medier som telefax og elektronisk post gør en særlig regulering påkrævet. For en bedømmelse heraf er det nødvendigt at overveje karakteren af den kommunikation, der sker ved disse medier. Det er karakteristisk, at disse kommunikationsformer er hurtige og i en række tilfælde kan skabe en forventning/pres for et hurtigt svar. På denne måde ligner de den telefoniske henvendelse. Det er dog også karakteristisk, at der ikke er nogen umiddelbar konfrontation mellem afsender og modtager, idet sidstnævnte ikke sættes i en situation, hvor et øjeblikkeligt svar skal gives. Herved adskiller disse kommunikationsformer sig afgørende

6. KOM(90)314-Syn288. Det er sandsynligt, at der vil gå nogle år inden dette direktiv gennemføres, jfr. iøvrigt nærmere i kapitel 8.
7. KOM(94)128-Syn288, EFT C 200/4 af 22.7.1994.

fra den telefoniske henvendelse. Dette betyder, at der ikke er tilstrækkeligt behov for at forbyde eller generelt begrænse adgangen til direkte markedsføring ved hjælp af disse medier.[8] Der sker ikke en potentiel privatlivskrænkelse, der kan berettige til denne form for regulering.

Generelt er det væsentligt fremover, hvor nye former for kommunikationskanaler vil opstå, internaktivt fjernsyn og i almindelighed »informationslandeveje« (information super highways) at være opmærksom på, at det alene er i de tilfælde, hvor der kommer til at foreligge en umiddelbar konfrontationssituation, at det vil være berettiget af integritetsorienterede grunde at begrænse eller ligefrem forbyde uopfordret direkte markedsføring.

13 Følsomme produkter

Særlige forhold foreligger i de tilfælde, hvor markedsføringsgenstanden er produkter eller tjenesteydelser, hvis udbud indicerer oplysninger af følsom karakter om adressaterne. Der vil nok primært være tale om varer indenfor det helbredsmæssige og seksuelle område, men andre felter vil også kunne være aktuelle. Hvis det til grund liggende datamateriale i sig selv er følsomt, følger det af de gældende regler, der ikke på dette punkt behøves ændret, at det vil være særdeles sjældent, at sådanne data lovligt vil være i virksomhedens besiddelse. I sådanne situationer bør der kræves et samtykke (opt in) til, at direkte markedsføring kan foretages. Formålet med den foretagne registrering vil normalt ikke være relateret til muligheden for markedsføring og risikoen for integritetskrænkelser vil være betydelig.

Der kan også være tilfælde, hvor de anvendte data ikke i sig selv kan karakteriseres som følsomme, men hvor karakteren af det udsendte medfører, at modtagelsen opfattes som privatlivskrænkende. Et eksempel herpå kan være fremsendelse af reklamer for pornografi. Selvom man i disse tilfælde, der i praksis vil kunne indkredses ved en listning af særlige produkter m.v., kan stille krav om

8. I udkastet til direktiv om fjernsalg, KOM(93)396 endelig udg.-Syn 411 af 7/10 1993, kræves samtykke til denne form for markedsføring. Ej heller forbrugerretligt forekommer dette påkrævet.

neutral kuvertering etc., vil modtagelsen i sig selv alligevel ofte opleves som krænkende. Det kan derfor overvejes, om man for sådanne særlige produktkategorier ligeledes bør have en mere stram regulering, hvor et samtykke til dataanvendelse forudsættes. En sådan ordning vil være ønskelig og samtidig have den positive sideeffekt, at den samlede regulering yderligere afbalanceres og dermed fremmer en generelt mere afslappet holdning til den direkte markedsføring.

14 Sammenfatning

Sammenfattende foreligger der et behov for en retspolitisk reform af mulighederne for persondataanvendelse til markedsføringsformål. Denne reform vil opretholde en mulighed for den enkelte borger til at udøve kontrol med denne form for dataanvendelse, men samtidig styrke erhvervslivets muligheder for at benytte direkte markedsføring, der økonomisk, afsætningsmæssigt og samfundsmæssigt er den mest rationelle form for markedsføring.

6 | Elektroniske spor

1 Intensiveret elektronisering

Den stadig mere intensive elektronisering af samfundet medfører en synliggørelse af de enkelte individer. Brug af edb-teknologi til alle former for kommunikation, økonomisk som ikke økonomisk, offentlig som privat, skaber et miljø, der i princippet er åbent og gennemskueligt. Et miljø, hvor det bliver stadig sværere for den enkelte at være sig selv, at være privat. Denne udvikling, der i mange henseender er fordelagtig ved at tilvejebringe nye udfoldelsesmuligheder for borgerne, skaber dog samtidig en potentiel mulighed for et overvågnings- og kontrolsamfund. Det er dermed en udvikling, der bør styres via en gennemtænkt og forudseende retlig regulering. Det er en udvikling, der vil kunne være farlig, hvis den får lov til at ske frit, og selv om de retlige virkemidler ikke er perfekte i den forstand, at de i alle henseender vil være i stand til at kontrollere udviklingen, kan de dog i betydeligt omfang fastlægge grænser for teknologien.

Den retlige regulering er påkrævet både i den offentlige og i den private sektor. Under det klassiske Big Brother perspektiv er det den offentlige sektors teknologianvendelse, der er i centrum, men dette er en alt for begrænset synsvinkel. Det elektroniserede samfund skaber i særdeleshed nye muligheder for private virksomheder og fører let til en situation, hvor afstanden mellem det enkelte individ og store ressourcestærke virksomheder, der opleves som fremmede og anonyme, bliver større end tilfældet er idag. Den private sektor er et vigtigt reguleringsområde, såfremt det udfoldede informationssamfund skal være et civiliseret samfund med en acceptabel persondatabeskyttelse.

2 Beskyttelse af almindelige persondata

Det er hensigtsmæssigt til en begyndelse kort at repetere nogle af de observationer, der er gjort i de tidligere kapitler. Først og fremmest er det blevet lagt til grund, at selv om privatlivsbeskyttelsens kerneområde udgøres af de følsomme persondata, er der behov for en retlig regulering, der også yder en vis beskyttelse af de øvrige personoplysninger. Det er blevet anført, at det vil være en uheldig udvikling, såfremt reguleringen blev indsnævret til alene at angå bestemte persondatatyper. Den følgende drøftelse af de elektroniske spor udgør en uddybning og underbygning af dette almindelige synspunkt. Det er yderligere blevet fremhævet, at der kan være dataanvendelsessituationer, hvor brug af elektroniske spor kan være uproblematisk, og dette synspunkt er – måske lidt paradoksalt – i forhold til gældende ret særligt blevet pointeret i relation til direkte markedsføring. Det er således vigtigt at fremhæve, at selv om alle persondata som udgangspunkt bør ydes en vis beskyttelse, er dette ikke en dogmatisk opfattelse, der udelukker en fleksibel regulering med hensyntagen til samfundsmæssige interesser, der motiverer anvendelsen af persondata.

Sammenfattende udgør de følgende betragtninger især en underbygning af, hvorfor almindelige persondata bør beskyttes, og er samtidig et forsøg på en til en vis grad fremtidsorienteret beskrivelse af den betydning, som de elektroniske spor vil få.

3 Informationslandeveje

I den teknologiske udbygning af samfundet spiller visionen om og planlægningen af informationslandeveje en fremtrædende rolle. De såkaldte information super highways er et kerneområde i den nuværende amerikanske regerings politik, der har den generelle målsætning at etablere en national informationsstruktur. På disse highways vil der blive genereret og anvendt elektroniske spor i en helt ny målestok. Grundlaget for udvikling af informationslandeveje, der af mange forventes at blive afgørende for de fremtidige

magtforhold mellem de økonomiske kraftcentre i verden, er foreningen af de forskellige former for moderne teknologi, d.v.s. en systematisk og omfattende anvendelse af multimedier. Kernen udgøres af computerteknologi, videoteknologi og telekommunikationsteknologi.[1] Selve landevejene består af lysledernet med optiske fibre, der ideelt forbinder alle erhvervsvirksomheder og private hjem i samfundet, samtidig med at der er porte ud til det globale informationssamfund. Et umiddelbart betragtet storslået projekt, der skulle kunne danne basis for endnu en »industriel revolution«.

I det følgende beskrives nogle af de anvendelsesmuligheder, man ser for disse landeveje, idet det ikke er påkrævet inden for denne bogs rammer at gå nærmere ind på de teknologiske detaljer i forbindelse med landevejenes konstruktion.

Forinden denne omtale af potentielle anvendelsesmuligheder indledes, er der grund til nogle enkelte bemærkninger om det ideologiske koncept for disse landeveje, hvor det er naturligt i et vist omfang at modstille USA og Europa. Begge steder er udgangspunktet, at denne nye informationsmæssige infrastruktur kræver en så voldsom investering med en trods alt noget usikker og under alle omstændigheder langsom omslagstid, at det offentlige må være drivkraften bag etableringen af denne infrastruktur. I USA er det derfor den federale regering og i Europa EU, der via medlemslandsfinansiering søger at skabe denne informationsmæssige infrastruktur. Begge steder er man dog samtidig afhængig af betydelige private investeringer.

Herfra skilles den politiske filosofi bag projektet. I USA har regeringen ganske vist nogle ideer om, hvorledes disse landeveje kan forbedre uddannelsesniveauet, det medicinske behandlingsniveau og deltagelsen i de demokratiske processer, jfr. også nedenfor, men primært er det op til markedet, hvorledes denne informationsstruktur skal benyttes, d.v.s. hvilke tjenesteydelser mv. der skal formidles. I Europa er det tanken at styre informationsstrukturen mere systematisk. Det offentlige vil således sikre sig betydelig indflydelse på, hvad de nye informationslandeveje skal benyttes til, og hvilke generelle samfundsmæssige målsætninger de skal medvirke til at realisere. Selv om man også i Europa vil være afhængig af pri-

1. Internettet, der idag bl.a. bruges til elektronisk post, er således kun en spæd begyndelse.

vate investeringer til at supplere de offentlige midler, vil informationsstrukturen ikke her blive et tag-selv-bord for det kommercielle marked. Det er dog samtidig naturligvis væsentligt, at markedet benytter strukturen, og at den har den ønskede betydning for samfundsøkonomien og den europæiske industris konkurrencedygtighed på det globale marked. Det offentlige vil på denne baggrund tilskynde til anvendelse af strukturen og være bevidst om, at retlig regulering skal lægge så få bånd som muligt. Desuagtet vil der blive reguleret for at sikre mod misbrug, og det vil utvivlsomt blive et centralt felt for fremtidig retlig regulering, hvorledes trafikreglerne på disse nye informationslandeveje skal udformes. Inden for rammerne af denne bog er det kun de databeskyttelsesmæssige aspekter, der tages op til drøftelse i det følgende.

3.1 Anvendelsesmuligheder

Der vil være mange forskellige former for anvendelsesmuligheder for de kommende informationslandeveje. I de forskellige visioner satses der på at tilgodese overordnede samfundsmæssige formål. Disse angår bl.a. forbedring af det generelle uddannelsesniveau ved en systematisk distribution af fjernundervisning, der modtages i private hjem, arbejdspladser mv., og en ny dimensionering af det politiske system via former for elektronisk demokrati.[2] Herudover kan man forestille sig visse serviceydelser såsom lægebehandling i et vist omfang formidlet via landevejene.[3] Opfyldelsen af sådanne offentlige formål vil generere en mængde persondata og afføde et reguleringsbehov, der dog i tråd med bogens afgrænsning ikke vil blive nærmere uddybet.

For den private sektor er der ligeledes mange anvendelsesmuligheder. Nærliggende er selvsagt formidling af varer og tjenesteydelser. Især for sidstnævntes vedkommende vil der kunne ske et kvali-

2. I denne sammenhæng kan bl.a. nævnes muligheden for elektroniske afstemninger, der sætter fokus på om det repræsentative parlamentariske demokrati bør fornys, og muligheden for en kvalitativ forbedring af offentlighedens adgang til forvaltningens dokumenter. Se om problemstillingen Marcus Schmidt: Direkte demokrati i Danmark (København 1993) og Jakob Sand og Jens Engbjerg: Teledemokrati (Teknologinævnet, København 1993).
3. Eksempelvis vil lægen via videoforbindelse kunne samtale med patienten og gennemføre behandling af sådanne sygdomme, der ikke nødvendiggør personlig konsultation. Dette vil kunne ske i betydeligt større omfang end ved de velkendte telefonkonsultationer.

tativt spring i forhold til i dag. Underholdning og kursustilbud af enhver karakter vil blive formidlet, og inden for de enkelte brancheområder vil der kunne tilbydes en lang række nye valgmuligheder for borgerne. Den omstændighed, at netværkene vil kunne anvendes interaktivt, d.v.s. med umiddelbar dialog mellem individ og virksomhed, betyder, at en række nye indtjeningsfelter vil blive etableret i den private sektor med en voldsomt stigende datatrafik til følge. Denne udvikling, der må forventes realiseret i nær fremtid, skaber nye udfordringer for persondatabeskyttelsen og sætter ikke mindst focus på behovet for beskyttelse af almindelige persondata.

3.2 Dataophobning

Informationslandevejene betyder en åbning af de markedsmæssige relationer, ved at alle former for transaktioner bliver synlige og ikke mindst genererer data. Dette gælder også for andre relationer end de rent markedsmæssige og rejser bl.a. problemer i henseende til, hvorledes en form for posthemmelighed skal sikres. Midlet hertil kan være kryptografering, der rejser en række interessante principielle spørgsmål, som det dog falder uden for denne bogs rammer at behandle.[4]

Af central betydning er, at der bliver et stort, ja nærmest overvældende potentiale for at indsamle og ophobe data, hvorved de nye netværk udgør en risiko for privatlivsbeskyttelsen. Denne dataophobning sker, fordi der etableres stadig tydeligere elektroniske spor, hvis eksterne anvendelighed ligger langt udover det snævert markedsføringsmæssige. Selv om brug af informationslandeveje principielt vil være frivillig, vil der blive tale om en så udtalt kommunikationsform, at den i mange tilfælde reelt vil være nødvendig at anvende. Det må forventes, at det på nogle områder vil blive den eneste kommunikationsform, hvorfor en valgmulighed ikke foreligger. Det er dermed ikke en realistisk mulighed at beskytte pri-

4. Ved kryptografering kodes afsendte meddelelser, hvilket kan ske således, at alene den autoriserede modtager er i stand til at dekode meddelelsen. Dette skaber problemer for polities muligheder for at efterforskning af bl.a. økonomisk kriminalitet. Den amerikanske regering ønsker at undgå den situation, at ubrydelige koder benyttes ved at lovbestemme anvendelsen af en bestemt standard, krypteringschippen Clipper, hvilket har givet anledning til en meget ophidset debat i USA.

vatlivet ved at modarbejde eller fraråde brug af landevejene.

De data, der ophobes, vil i betydeligt omfang være almindelige, d.v.s. ikke følsomme data. Disse data vil ikke blot reflektere, hvilke køb den enkelte foretager, men tillige hvilke serviceydelser der benyttes. Meget nøjagtige profiler af den enkelte borger vil kunne dannes. Blandt serviceydelser vil være, hvilke videoer der ses, hvilke TV-kanaler der benyttes, hvilke programmer den enkelte og dennes husstand faktisk ser, etc. etc. Det er uden videre klart, at disse profiler indebærer risici for privatlivsbeskyttelsen, der rækker langt videre end benyttelse af data til markedsføring, der i kapitel 5 er drøftet med den konklusion, at det i modsætning til eksisterende lovgivning ikke er på dette punkt, de reelle risici for integritetskrænkelser foreligger.

Det bliver af nærmest vital betydning, at der oparbejdes en retlig regulering, der sikrer mod etableringen af et overvågningssamfund med de potentielle risici for styring af borgernes liv, som et sådant samfund indebærer. Denne aspiration understreger betydningen af at regulere anvendelse, opbevaring og videregivelse af almindelige persondata, og den betoner ikke mindst de voldsomme teknologiske udfordringer, som en sådan retspolitisk ambition konfronteres med.

4 Intern dataanvendelse

På denne baggrund er det af central betydning, at den databeskyttelsesmæssige lovgivning også regulerer den interne anvendelse af de persondata, en virksomhed er i besiddelse af, jfr. kapitel 3. Der bør i modsætning til registerloven, men i overensstemmelse med det kommende EU-direktiv således som det kendes idag, fastslås nogle principper for, hvad oplysninger kan anvendes til af den databesiddende virksomhed. Disse regler må først og fremmest have som målsætning at sikre åbenhed, d.v.s. at det skal være klart, hvad data anvendes til, og yderligere at denne dataanvendelse har en saglig klar forbindelse til den pågældende virksomheds erhvervsformål. Disse krav bør i særdeleshed gælde i henseende til profilering, der skal være saglig, hvilket indebærer, at interne samkørin-

ger etc. ikke bør kunne ske frit. Ved siden af den traditionelle adgang til registerindsigt bør borgerne i overensstemmelse hermed have ret til at få beskrevet, i et forståeligt og klart sprog, virksomhedens dataanvendelsespolitik, herunder konkret, hvorledes den enkeltes data bliver benyttet. Enhver virksomhed bør dermed pålægges at udarbejde en redegørelse for, hvorledes persondata behandles i virksomheden, herunder til hvilke formål data opbevares. Denne generelle virksomhedspolitik bør være offentligt tilgængelig og konkret overfor den enkelte borger suppleres med specifikke oplysninger om dennes data. En sådan regulering vil udover at styrke borgernes retssikkerhed bidrage til at løse de vanskelige kontrolproblemer, jfr. om disse nedenfor samt senere i kapitel 10.

5 Dataopbevaring

I henseende til opbevaring angiver de anførte synspunkter vedr. samkøring det udgangspunkt, at reglerne bør omfatte ikke blot betingelser for opbevaring, men i særdeleshed opbevaringsmåden. Her bør der tages særligt hensyn til profileringsaspektet. Denne hensyntagen peger mod ønskværdigheden af, at der anvendes registre, der kan karakteriseres som opgavespecifikke. Problemet i denne forbindelse er først og fremmest, at en sådan reguleringsmetode vil være baseret på en dataorganiseringsmodel, der er og især vil blive mere og mere teknologisk forældet ved anvendelse af relationsdatabaser og netværk m.v. og dermed vil blive stadig mere indgribende over for virksomhedernes teknologianvendelse.

Under dette perspektiv vil det let blive for vidtgående og samtidig i praksis urealistisk at kræve anvendelse af registre i traditionel forstand. Reguleringen bør derfor snarere satse på en begrænsning af de søgemuligheder, en virksomhed kan applicere i forhold til sin samlede datamasse. Oplysninger om disse anvendte søgemuligheder kunne indgå i den information, der stilles til rådighed for indsigtssøgende borgere. En regulering af denne karakter vil, så vidt det kan bedømmes, være den mest effektive måde at påvirke dataophobningen bort fra en for vidtgående profilering.

6 Samkøring/videregivelse

Data, der skabes ved anvendelsen af de moderne informationslandeveje, genereres selvsagt af mange forskellige virksomheder, og det er derfor ikke mindst videregivelse af data mellem virksomheder, der har interesse for den retlige regulering. Her må det vurderes, hvorvidt de eksisterende principper er tilstrækkelige, idet der i denne forbindelse bortses fra, at registerbegrebet som beskrevet ovenfor er ved at blive forældet. Som udgangspunkt kan det konstateres, at forbudet mod samkøring af forskellige virksomheders registre i § 4 stk. 4 med dispensationsmuligheden i stk. 5 ikke kan være strengere. Bortses fra de særlige forhold i koncerner, som blev drøftet tidligere i kapitel 4, er det hensigtsmæssigt at opretholde dette forbud, idet det blot må konstateres, at samkøringsmodellen bør opdateres. En mulighed kunne være en regel, der som hovedregel forbød dannelse af personprofiler baseret på data fra forskellige virksomheder. I de tilfælde, hvor samkøring accepteres, bør denne ikke kunne anvendelse til etablering af vidtgående personprofiler. En sådan regel kunne indbygges i § 4, stk. 5, som et lovbestemt vilkår, der skal medtages i de tilfælde, hvor Registertilsynet giver tilladelse til samkøring. Denne ordning vil være teknologisk neutral og ville således ikke være så påvirkelig af teknologiske innovationer, der i sagen natur er vanskelige at forudberegne.

Fulgtes denne vej, ville man samtidig have imødekommet de problemer, der kan foreligge i forbindelse med den almindelige videregivelsesregel i § 4 stk. 2. Den retlige standard i denne bestemmelse er som påpeget i kapitel 2 ganske vag, men dog også – hvilket i denne sammenhæng er væsentligt – teknologineutral. Det vil være vanskeligt at stramme denne regel uden at skabe en retlig regulering, der enten er overdrevent bureaukratisk eller bliver for indgribende over for erhvervslivets udfoldelsesmuligheder. Det må derfor konkluderes, at det vil være tilstrækkeligt at gennemføre en regulering, der begrænser de profileringsmuligheder, som videregivelse af data giver så store muligheder for i fremtiden.

7 En realistisk retlig regulering

Et væsentligt problem tilbagestår. Det vedrører, hvorvidt den teknologiske udvikling skaber en virkelighed, hvorindenfor den databeskyttelsesretlige regulering ikke lader sig kontrollere. I kapitel 10 drøftes kontrolproblemerne generelt, hvorfor de følgende bemærkninger alene tager sigte på informationslandevejene. Hovedproblemet er her, at de nye multimedieorienterede, sammenhængende netværk er uden en overordnet struktur og organisering i traditionel forstand. Der vil blive tale om en konstant cirkulation af uoverskuelige mængder af data med et tilsvarende uoverskueligt antal aktører. Datacirkulationen vil være ubundet af traditionelle grænser, jfr. hertil nærmere i kapitel 9. Disse forhold betyder, at kontrol gennemført af offentlige myndigheder vil blive udøvet under meget vanskelige vilkår med den konsekvens, at databeskyttelsen i endnu mere udtalt grad end i dag ikke udelukkende kan være afhængig af denne kontrol.

Udviklingen vil således utvivlsomt understrege betydningen af, at den databeskyttelsesretlige regulering udformes og praktiseres på en måde, der virker rimelig og rigtig for de virksomheder, der anvender persondata. Med et udtryk hentet fra Alf Ross er det påkrævet, at lovgivningen efterfølges ud fra en uinteresseret respekt for retten.[5] Dette betyder ikke, at reguleringen udelukkende kan overlades til markedet og til normer fastsat af den enkelte virksomhed. Databeskyttelseshensynene har ikke en sådan udtalt økonomisk betydning, at et selvregulerende system vil virke tilfredsstillende. Derimod må de retlige regler skabes i en dialog med bl.a. virksomhederne og selvregulerende normer bør opfattes som et integreret supplement til de af lovgivningsmagten fastsatte regler. Alene ud fra en sådan reguleringsmodel vil det være muligt i praksis at sikre databeskyttelsen i multimedievirkeligheden.

5. Jfr. Alf Ross: Om ret og retfærdighed (København 1953) p 68.

8 Konstante innovationer

Sammenfattende indebærer den teknologiske udvikling en lang række perspektiver og udfordringer til den retlige regulering af databeskyttelsen. Et velkendt træk i moderne tid er, at den teknologiske innovation er meget hurtig og tit under en retrospektiv synsvinkel er overraskende. Det er langt fra alle fremtidsvisioner, fremsat de sidste 30 år, der er blevet til noget. Det forekommer desuagtet meget sandsynligt, at informationslandevejene vil blive bygget og vil blive en central bestanddel af det fremtidige samfundsmæssige liv. Det er derfor påkrævet til stadighed at vurdere miljøet for databeskyttelsen og i videst muligt omfang at fremtidssikre den retlige regulering, således at den hurtigt og fleksibelt kan tilpasses de teknologiske innovationer.

7 Kreditoplysning

1 Kreditsystemets samfundsmæssige betydning

Den form for persondataanvendelse, der mest klart kan få skadelige og tabsudløsende konsekvenser for den person, som oplysningerne angår, er benyttelse af data som kreditinformation. Formålet med denne dataanvendelse er at skabe et grundlag for, at der kan træffes en afgørelse om, hvorvidt den pågældende person kan modtage kredit, eller om dette vil være risikabelt for kreditgiver. I et samfund med en hurtig økonomi, hvor langsigtede dispositioner med stor afstand mellem investering og udbytte ligeledes er fremtrædende, er der tale om betydningsfulde afgørelser, ikke blot for den enkelte, men herudover tillige under et samfundsøkonomisk perspektiv.

Kreditafgørelser træffes også i forhold til virksomheder og juridiske personer, og en række af de regler og de hensyn, der drøftes i det følgende, er dermed også relevante for virksomheder som kreditmodtagere. På dette område har det væsentlig betydning, at registerloven ikke blot har den fysiske, men også den juridiske person som beskyttelsesobjekt. Selv om der i det følgende tales om personer, angår dermed en stor del af de diskuterede problemstillinger også virksomheder. Der er dermed tale om et område, der i alle henseender har betydelig erhvervsmæssig interesse.

Som allerede indiceret har det væsentlig samfundsmæssig og økonomisk betydning, at kreditsystemet fungerer. Hermed forstås i denne sammenhæng, at kredit bliver ydet i optimalt omfang, d.v.s. at enhver har mulighed for at opnå kredit til finansiering af personlige og erhvervsmæssige formål, og at denne kreditgivning ikke påfører de virksomheder, der yder kredit, en urimelig eller stor risiko. Alle økonomiske dispositioner indebærer en vis risiko,

men tilbøjeligheden til at foretage de pågældende dispositioner øges, i det omfang risikoen minimeres, og selvsagt i det omfang det økonomisk for kreditgivere er fordelagtigt. Sidstnævnte aspekt falder uden for denne fremstilling, medens minimering af risikoen er et centralt tema ved bedømmelse af de persondataanvendelsesregler, der fastsættes i lovgivningen og herfra udsprunget praksis.

Problemstillingen i dette kapitel kan følgelig formuleres således, at den angår, hvorledes der fastlægges den rette balance mellem de betingelser, der angiver, hvornår persondata kan anvendes som kreditinformation, overfor hensynet til at sikre, at risikoen ved i konkrete tilfælde at yde kredit er så lav som muligt. Den retspolitiske vurdering tager dermed udgangspunkt i det ønskværdige i et generelt fornuftigt kreditmiljø, der er udformet under hensyntagen til beskyttelsen af den personlige integritet.

2 Fælles interesse i et godt kreditmiljø

Det er væsentligt indledningsvist at tilkendegive, at muligheden for kredit som udgangspunkt må betragtes som god og fornuftig. Det er dermed en fælles interesse for kreditgiver og kreditmodtager, at de lovgivningsmæssige rammer tilvejebringer et godt kreditmiljø. Ved at tale om fælles interesser peges der på, at de relevante aktører, hvis interesser bør tages i betragtning ved udformningen af de juridiske regler, må karakteriseres på en bestemt måde. Med en velkendt juridisk terminologi tages udgangspunkt i en bonus pater kreditgiver og kreditmodtager.

For en sådan kreditgiver gælder, at vedkommende ikke vil udnytte sin kreditgivningsmulighed til på uberettiget måde at diskriminere mellem de potentielle modtagere og ej heller vil lægge usaglige data til grund for sin kreditbeslutning. Ingen har pligt til at yde kredit, men når det sker, er kreditgivers legitime interesse adgang til den information, der giver et sagligt grundlag for et økonomisk/kommercielt rigtigt valg. En sådan kreditmodtager kan karakteriseres som personer/virksomheder, der som intention har at benytte den givne kredit til finansiering, og hvis intention er at tilbagebetale den ydede kredit og ligeledes besidder økonomisk evne

til at opfylde denne intention. Denne kreditmodtager har dermed ikke interesse i at skjule data, der med rimelighed kan dokumentere, hvorvidt vedkommende lever op til disse krav. Det er centralt at fremhæve, at det ikke kan være lovgivningens formål at beskytte kreditmodtagere, der ikke har intention om eller evne til at tilbagebetale ydet kredit, »den dårlige betaler«.

Ved siden af de umiddelbare interesser, som kreditgiver og kreditmodtager har, er der en almindelig samfundsmæssig interesse i at sikre, at overordnede hensyn af ikke økonomisk karakter til privatlivsbeskyttelse og værn af personlig integritet varetages. Det må afgøres, hvad der samfundsmæssigt skal anses for et rigtigt grundlag for kreditafgørelser og dermed være rammen for kreditmiljøet. Dette udgør kernen for de retspolitiske overvejelser.

Endeligt bør det eksplicit fastslås, at der ikke er et fornuftigt grundlag for en generel modvilje mod kreditinformation. Dette fremhæves, fordi der ofte spores tendenser til en sådan uvilje, der altså her betegnes som uigennemtænkt og uden et rationelt grundlag. Det er vigtigt, at den retlige regulering ikke præges af sådanne opfattelser.

3 Kreditoplysningsdata

De data, der danner grundlaget for kreditafgørelser, kan stamme fra forskellige kilder. Der kan være tale om data vedrørende kundeforhold, der allerede er i virksomhedens besiddelse. Her foreligger ikke særlige problemer, og efter gældende ret står det virksomheden frit for at benytte registrerede oplysninger til dette formål. Der kan for det andet være tale om data, der er videregivet fra andre virksomheder. Er der ikke tale om systematisk videregivelse af kreditoplysninger, behandles denne situation i gældende ret efter de almindelige videregivelsesregler i § 4,[1] og det er ikke påkrævet nærmere at diskutere denne form for videregivelse i dette kapitel. For det tredje kan data blive videregivet fra virksomheder, der erhvervsmæssigt har til formål at producere kreditinformation. Dis-

1. Jfr. RÅ1992 p 107-08 vedrørende videregivelse fra et inkassobureau. Det fremhæves, at lejlighedsvis videregivelse af kreditoplysninger omfattes af § 4.

se kreditoplysningsbureauer skal efter § 8 anmeldes til Registertilsynet, og det er i forhold til disse, at de indledningsvis skitserede problemstillinger er særlig aktuelle.

På denne baggrund tager den følgende diskussion sigte på kreditoplysningsbureauer. De gældende regler i registerlovens kapitel 3 er omtalt foran i kapitel 2. Selv om der her i landet findes et dominerende bureau, RKI Kreditinformation, tager fremstillingen sigte på kreditoplysningsbureauer som sådan, og der findes da også flere, hvorved bemærkes, at i Registertilsynets årsberetning listes de bureauer, der er anmeldt.[2]

4 Grundlaget for den retspolitiske vurdering

Måske i større udstrækning end på noget andet område er der i Registertilsynets praksis udviklet en meget detaljeret regulering, hvorom der henvises til Peter Blume: Personregistrering, side 86-105, og senere udgivne Registertilsynsårsberetninger. I det følgende inddrages denne praksis ikke i synderligt omfang, da fremstillingen tager sigte på at diskutere det almindelige retlige grundlag for kreditoplysning, og en sådan fremstilling kan nemt blive uoverskuelig og unødig kompleks ved inddragelse af den detaljerede praksis, der ud fra det anlagte perspektiv er af mindre interesse. De retspolitiske brudflader og afvejningsproblemer tydeliggøres bedre uden inddragelse af praksis.

5 Anvendelige persondata

Centralt ved drøftelse af kreditinformation står en indkredsning af de data, der må betragtes som relevante. Den gældende regulering angiver i § 9 stk. 1 den almindelige karakteristik, at der er tale om oplysninger, som skal være relateret til den pågældendes »økono-

2. Med udgangen af 1993 var der anmeldt 20 kreditoplysningsbureauer.

miske soliditet og kreditværdighed«. Som et udgangspunkt forekommer denne karakteristik dækkende og kan for så vidt uden videre benyttes i fremtidig regulering, uden at dette som nævnt implicerer, at den eksisterende praksis hermed i alle henseender tiltrædes. Det er en rigtig prøvesten, om en datatype tilfredsstiller den angivne karakteristik, og det er hensigtsmæssigt, at denne vurdering foretages ud fra en afvejning mellem erhvervsmæssige og integritetsmæssige hensyn.

I betragtning af de betydelige konsekvenser, der er forbundet med kreditoplysning, er det ønskeligt at kræve stor sikkerhed for oplysningernes korrekthed og ligeledes for, at de falder ind under den angivne ramme. Er disse krav opfyldt, bør det lægges til grund, at der skal være klare integritetsorienterede modhensyn for, at en oplysningstype desuagtet ikke kan benyttes til kreditoplysning. Herved er der således opstillet en retningslinie for en udfyldende praksis, der, så vidt det kan bedømmes, til en vis udstrækning er mere positiv over for kreditoplysningsformålet, end tilfældet er i eksisterende praksis.

5.1 Betalingsevne og betalingsvilje

Ved anvendelsen af registerlovens regelsæt skelnes idag mellem tilfælde, hvor en oplysning angår betalingsevne, hvor reglerne om kreditoplysning finder anvendelse, og på den anden side oplysninger om betalingsvilje, hvor reglerne i §§ 3, stk. 6 og 7 om advarselsregistre benyttes. Sædvanligvis stilles der vilkår til advarselsregistre, der svarer til kreditoplysningsbestemmelserne, og i den forstand er distinktionen mere teoretisk end praktisk. Opdelingen har dog den betydning, at advarselsregistres oprettelse kræver tilladelse af Registertilsynet, medens kreditoplysningsbureauer som nævnt blot skal anmeldes.

Det bør derfor overvejes, om sondringen mellem evne og vilje bør opretholdes, hvorved det også kan tages i betragtning, at kreditoplysning må betragtes som en advarsel om ikke at give kredit. Ses der på formålet med kreditinformation, der består i at danne grundlag for en prognose over, hvorvidt en ydet kredit vil blive tilbagebetalt, er det svært at se en rationel begrundelse for at skelne mellem betalingsevne og betalingsvilje. Udgangspunktet må være,

at begge fænomener er relevante for kreditafgørelser, og dermed at oplysninger om betalingsvilje også må kunne indgå i det datagrundlag, et kreditoplysningsbureau kan stille til rådighed. Det er klart, at oplysninger om betalingsvilje i en række tilfælde vil være mere vurderingsprægede end betalingsevneoplysninger, men dette betyder blot, at de praktiske krav til oplysningernes korrekthed må være særlig strenge i disse tilfælde.

Opdelingen foreslås derfor ophævet i henseende til kreditinformation med den konsekvens, at de særlige regler om advarselsregistre herefter alene finder anvendelse på andre typer oplysninger end de økonomiske og på registre med økonomiorienterede oplysninger, der ikke tager sigte på at fungere som kreditinformation.

5.2 Følsomme oplysninger

En særlig problemstilling vedrører, hvorvidt de følsomme oplysningstyper skal kunne indgå som kreditoplysninger, hvilket efter § 9 stk. 2 i dag er udelukket. Dette betyder, at selv om en oplysning må karakteriseres som relevant kreditoplysning og ligger inden for den ovenfor beskrevne ramme, kan den ikke benyttes, når den er rubriceret som følsom efter § 3 stk. 2. Denne begrænsning har primært betydning i forhold til oplysninger om visse former for strafbare forhold, f.eks. checkbedrageri. Som tidligere fremhævet er det særligt de følsomme oplysninger, hvis beskyttelse angår centrale dele af privatlivets fred, og på denne baggrund er det berettiget at fastsætte restriktive betingelser for sådanne oplysningers registrering og videregivelse. Sidstnævnte, der er særlig relevant for kreditoplysningsbureauer, kan i almindelighed efter § 4 stk. 1 ske med samtykke, der jo ikke vil være praktisk i forhold til potentielle dårlige betalere, eller med hjemmel i anden lov. Reelt er § 9 stk. 2 for så vidt angår videregivelse således ikke strengere end § 4 stk. 1.

Det er dog ikke uden videre fornuftigt totalt at udelukke følsomme data fra kreditinformation, idet det for god ordens skyld pointeres, at oplysningernes korrekthed forudsættes sikret. Bruges eksemplet med checkbedrageri, forekommer det nærliggende, at en oplysning herom er relevant for en beslutning om kreditgivning, og at der dermed sagligt bør kunne ske anvendelse af sådanne op-

lysninger. Et nærliggende retspolitisk synspunkt er dermed, at også følsomme data af betydning for vurderingen af økonomisk soliditet og kreditværdighed bør kunne benyttes. På denne baggrund kan det konstateres, at det er et egentligt politisk spørgsmål, om følsomme data skal indgå i kreditoplysninger, og at besvarelsen af dette spørgsmål afhænger af en stillingtagen til, hvilke data der med rimelighed bør have betydning for kreditgivningen. Herved ligner problemstillingen en række af de spørgsmål, der drøftes i de følgende afsnit.

5.3 Gamle oplysninger

Efter § 9 stk. 3 må negative oplysninger, der er mere end 5 år gamle, normalt ikke benyttes i kreditoplysning, medmindre det konkret er åbenbart, at de er af afgørende betydning for vurderingen af soliditet og kreditværdighed. Det er således kun i sjældne situationer, at gamle oplysninger kan inddrages.[3] 5-årsgrænsen er sædvanligvis absolut, og i praksis er der for en række specifikke oplysningstyper fastsat kortere frister.[4]

Den almene problemstilling er, hvorvidt en oplysnings alder skal udelukke den fra beslutningsgrundlaget i henseende til kreditgivning, idet det herved forudsættes, at oplysningen fortsat er korrekt og ikke vildledende. Den tankegang, at alder ændrer den retlige betydning af et forhold, kendes i andre dele af retssystemet og i særdeleshed i regler om forældelse, der på det privatretlige område særligt indebærer, at når en fordring har en vis alder, kan den ikke inddrives, medmindre retlige skridt er iværksat inden den fastsatte skæringslinie. Den ovenfor nævnte 5-årsfrist genfindes i den almindelige lov om forældelse fra 1908.[5] En aldersbegrænsning er således ikke noget unikt og er i almindelighed udtryk for, at der må være grænser for, hvor længe fortidens synder skal forfølge nogen. Efter min opfattelse er denne tankegang rigtig i sine grundtræk. På kreditområdet virker det fornuftigt, at den omstændighed, at en person for flere år siden har en ubetalt gæld, ikke i sig

3. Registertilsynet har tilkendegivet, at der ikke kan opstilles generelle retningslinier for, hvornår ekstraordinære omstændigheder begrunder fravigelse fra 5-års fristen, jfr. RÅ1992 p 113.
4. Eksempelvis 2 år for oplysninger om tvangsauktion, der er aflyst.
5. Lov nr. 274 af 22/9 1908 om forældelse af visse fordringer.

selv bør udelukke vedkommende fra i dag at opnå kredit. Man kan naturligvis altid diskutere, hvor tidsgrænsen skal sættes, og den vil altid i betydeligt omfang være arbitrær, men udelukkelsen af gamle oplysninger fra kreditbeslutningsgrundlaget, medmindre særlige grunde ekstraordinært taler for det modsatte, kan tiltrædes. På dette punkt er der derfor ikke grundlag for at ændre de gældende regler.

6 Videregivelse

Af størst interesse i forbindelse med kreditoplysningsbureauer er ikke så meget hvilke oplysninger, disse bureauer må registrere, men derimod hvilke data der kan videregives. Det er ved videregivelsen til den virksomhed, der skal træffe en kreditbeslutning, at de særlige beskyttelseshensyn aktualiseres, og hvor den retlige regulering determinerer kreditgivningsmiljøet.

6.1 Summariske oplysninger og bedømmelser

Ved den følgende diskussion af videregivelsesmulighederne er det værd at være opmærksom på, at der traditionelt i praksis skelnes mellem to former for videregivelse. For det første videregivelse af enkeltstående oplysninger – i den gældende lovs terminologi »summariske oplysninger« (§ 12 stk. 1) – hvor der på grundlag af en forespørgsel gives oplysninger om en identificeret person. Den gældende regulering tager især sigte på denne form for videregivelse, der er den mest udbredte og dagligt forekommende. For det andet findes bedømmelser, hvor bureauet leverer en rapport, der, på grundlag af de oplysninger bureauet har registreret og eventuelt indhentede supplerende oplysninger i forhold til den konkrete sag, tegner et samlet billede af den bedømtes kreditværdighed. Sådanne bedømmelser vil som altovervejende hovedregel angå virksomheder og ikke enkeltpersoner. De forekommer mere sjældent, da de selvsagt ikke kan leveres fra dag til dag, er dyre og dermed forudsætter, at der foreligger en kreditsituation af et vist omfang og af længere tidsmæssig udstrækning.

Spørgsmålet om videregivelse af data er naturligvis også relevant i forhold til bedømmelser, men det er ikke så fremtrædende som ved de enkeltstående oplysninger. Da bedømmelser som nævnt næsten altid angår virksomheder, koncentreres også af denne grund opmærksomheden i det følgende om de enkeltstående oplysninger.

6.2 Videregivelsesmåden

Et væsentligt problem i henseende til videregivelse af enkeltstående oplysninger vedrører, på hvilken måde videregivelse bør kunne ske. Baggrunden for denne problemstilling er, at der må etableres en vis sikkerhed for, at formålet med indhentelsen af oplysningerne faktisk er kreditinformation og ikke andre uvedkommende formål, og at det er væsentligt at kunne dokumentere, hvilke oplysninger der er videregivet til hvem i de tilfælde, hvor det efterfølgende viser sig, at oplysningerne ikke er korrekte, og en erstatningsansvarssituation måtte opstå. En kontrolleret form for videregivelse kan medføre den fordel for reguleringens effektivitet, at kreditoplysningsbureauet gives en aktiv rolle med henblik på at sikre, at oplysningerne indgår i et acceptabelt kreditinformationsmiljø.

På denne baggrund kræver de gældende regler, at enkeltstående oplysninger alene må videregives til abonnenter hos bureauet, hvilket indebærer, at der foreligger et kontraktforhold mellem bureauet og den modtagende virksomhed. Denne kontrakt kan således benyttes til den regulering, som loven forudsætter, at bureauet foretager. I almindelighed bør det her fremhæves, at kreditoplysningsbureauet må kunne dokumentere, at loven og Registertilsynets retningslinier overholdes.[6]

Videregivelsesformen må således sikre, at det ovenfor nævnte dokumentationskrav kan opfyldes. Skriftlig videregivelse kan selvsagt ske, men for andre former er det nødvendigt med særlige regler eller i hvert fald en styring af videregivelsen. For så vidt angår mundtlig – d.v.s. i praksis telefonisk – videregivelse, bestemmer § 12 stk. 1, at modtagerens navn og adresse skal noteres og op-

6. Jfr. hertil RÅ1992 p 108-09.

bevares i 6 måneder. Dette er en enkel måde at opfylde dokumentationskravet på.

Større problemer foreligger i forbindelse med moderne elektronisk formidling, der har vundet stadig større udbredelse grundet dens effektivitet. Videregivelse vil kunne ske via elektronisk post, og her er forholdet ret enkelt, idet de afsendte breve, der vil omfatte modtagerens identitet, vil kunne udskrives og opbevares. Vanskeligere er videregivelse via online databaser, hvor der gives adgang til fri søgning. Her er det praktisk ikke muligt at fastslå, hvem der konkret har søgt hvilke oplysninger. Der er dog tradition for, at det er tilladt for kreditoplysningsbureauer at udsende publikationer med masseoplysninger til deres abonnenter (§ 12 stk. 2), og her foreligger den samme situation.[7] Online databasen bør derfor principielt reguleres på samme måde som publikationer og rejser kun særlige spørgsmål i relation til, hvilke oplysninger der skal kunne bruges som søgeord, hvilket indgår i det tema, der drøftes i de følgende afsnit.

På denne baggrund kan det konstateres, at alle former for videregivelse vil kunne ske på en måde, der lader sig kontrollere, og at der derfor ikke er behov for bestemmelser, der udelukker særlige videregivelsesformer.

6.3 Smågæld

Selv om en oplysning giver viden om økonomisk soliditet og kreditværdighed, kan der være almene samfundsmæssige hensyn, der medfører, at den ikke bør kunne videregives for at indgå i beslutningsgrundlaget for kreditgivning. En regel af denne type findes i dag i § 12 stk. 3, hvorefter der ikke må videregives oplysninger om skyldforhold under 1.000 kr. til samme kreditor, medmindre oplysningerne stammer fra Statstidende, eller retlige skridt er indledt mod den pågældende. Denne beløbsgrænse, der omfatter både forbrugsmæssig og erhvervsmæssig gæld, angiver det synspunkt, at

7. For små virksomheder kan on line adgang være for dyr, hvorfor det er anset acceptabelt, at sådanne abonnenter modtager udskrevne printerlister, jfr. RÅ1991 p 131-33, hvor det bemærkes, at disse lister skal udformes således, at det ikke er muligt at kopiere dem.
8. Det præciseres, at reglen kun gælder for videregivelse af summariske oplysninger og at smågæld altså kan registreres med henblik på bedømmelser, såkaldt »lukket registrering«. Kravet om, at oplysningerne skal være korrekte, gælder selvsagt også her, jfr. RÅ1992 p 110.

smågæld ikke bør påvirke mulighederne for kredit. Det forhold, at en person kan have sådan smågæld til mange forskellige kreditorer, blev taget i betragtning ved bestemmelsens gennemførelse og antoges ikke at kunne tillægges betydning.

Det må erkendes, at der databeskyttelsesretligt ikke er noget »rigtigt« svar på, om smågældsoplysninger bør kunne videregives fra kreditoplysningsbureauer. Dette er et rent politisk spørgsmål, men det er værd at bemærke, at reglens eksistens indicerer, at kreditorer anser sådanne oplysninger som relevante. Smågæld indicerer da også, at der er en vis risiko forbundet med kreditgivningen, men heroverfor står, at når kreditadgangens store betydning for den enkelte tages i betragtning, er det måske ikke rimeligt, at smågæld, hvor beløbsgrænsen jo er arbitrær, skal have den indgribende betydning, at kredit nægtes. Jeg har en vis sympati for denne opfattelse, men konstaterer som allerede nævnt, at en stillingtagen er rent politisk, og at det i en vis forstand er en smagssag, om gældsforhold under en bestemt beløbsgrænse skal kunne oplyses over for potentielle kreditorer.

6.4 Oplysninger om mange personer

Ikke mindst i forhold til de forbedrede søgemuligheder, som online kreditoplysning indebærer, men også i forhold til traditionel kreditoplysning via publikationer, foreligger spørgsmålet om, hvorvidt oplysninger kan struktureres eller gøres søgbare på måder, der giver grundlag for kreditbedømmelse af andre end den person, der aktuelt vurderes. En sådan form for videregivelse udelukkes i § 12 stk. 4, for så vidt der er tale om enkeltpersoner, hvorimod den i forhold til erhvervsvirksomheder er tilladt.

Det mest nærliggende eksempel på en sådan form for kreditbedømmelse er anvendelse af et bopælskriterium. Den omstændighed, at mange dårlige betalere er bosat et bestemt sted, får den konsekvens, at andre personer bosat samme sted ikke anses for kreditværdige. En sådan vurdering fremtræder umiddelbart ikke på overbevisende måde som saglig og bør derfor vanskeliggøres ved, at adressesøgning og lign. ikke tillades hos kreditoplysningsbureauer. En sådan regel har et integritetsbeskyttelsesmæssigt grundlag, og den gældende regulering kan for så vidt opretholdes.

Det må dog tilføjes, dels at der faktisk ofte er en sammenhæng mellem bopæl og betalingsevne, hvorfor en sådan søgningsmulighed i og for sig kan være relevant, dels at den manglende videregivelsesmulighed selvsagt ikke udelukker, at et bopælskriterium kan inddrages af den enkelte kreditgiver, idet reglen blot kan gøre det vanskeligere at indkredse de lokaliteter, der kreditmæssigt er relevante. Uanset disse forbehold konkluderes, at bestemmelsen i § 12 stk. 4 bør opretholdes.

7 Åbenhed

I betragtning af den betydning, som kreditvurdering har, og den almindelige forsigtighed over for dataanvendelse til dette formål, er det væsentligt, at der er betydelig åbenhed og indsigt omkring kreditoplysningsbureauers praksis. Denne målsætning opfyldes i betydeligt omfang af de gældende regler. Den registrerede skal, så snart ikke offentligt tilgængelige oplysninger registreres, have meddelelse om, at data om vedkommende befinder sig i et kreditoplysningsbureaus register (§ 10) og har herefter adgang til registerindsigt, der dog ikke omfatter, hvorfra de registrerede oplysninger stammer (§ 11), jfr. herom nedenfor. I det omfang videregivne oplysninger viser sig ukorrekte/vildledende, skal de berigtiges over for dem, der inden for de sidste 6 måneder har modtaget oplysningerne, og den registrerede skal have meddelelse om, hvem der har modtaget denne berigtigelse, og hvorfra de forkerte oplysninger stammer (§ 14).

7.1 Identifikationsoplysninger

I forhold til disse bestemmelser kan det drøftes, hvorvidt den registrerede under alle omstændigheder i forbindelse med indsigtsbegæringen skal have oplysning om, hvorfra de enkelte data hidrører, og om til hvem de er videregivet. Umiddelbart ville disse yderligere rettigheder styrke databeskyttelsen, omend de selvsagt vil indebære en vis ressourcebelastning for kreditoplysningsbureauerne. Dette er ikke afgørende, da ressourcebelastningen ikke kan

anses for særlig omfattende, hvis oplysningspligten begrænses til videregivelse inden for de sidste 6 måneder, der i forvejen skal registreres af bureauet. Derimod må det overvejes, om kreditgivningsmiljøet vil blive forringet. Ved vurderingen heraf må der skelnes mellem de to situationer.

Information om, hvem der har indhentet kreditoplysninger, kan ikke antages at ville forringe mulighederne for kreditvurdering og vil samtidig skabe større åbenhed og dermed bedre muligheder for, at konkrete kreditafgørelser kan forstås. Der eksisterer ikke nogen legitim interesse i at skjule, at kreditoplysninger indhentes[9] og andre afgørende modhensyn ses ej heller at foreligge. Indsigtsadgangen bør derfor omfatte information om til hvem, oplysninger er blevet videregivet også i de tilfælde, hvor oplysningerne er korrekte.

For så vidt angår oplysning om kilden, er det vanskeligere at vurdere konsekvenserne af en sådan regel, der ville udelukke anonymitet. Umiddelbart lyder dette sympatisk, da overdragelse af kreditoplysninger til et bureau kan opfattes som en form for angiveri, der ikke bør ske anonymt. Heroverfor står det forhold, at manglende anonymitet vil kunne medføre, at bureauerne modtager færre oplysninger, uanset at mange erhvervsdrivende i dag åbent tilkendegiver, at sådanne indberetninger sker. Det kan ikke afvises, at den samlede mængde kreditoplysninger ville blive reduceret, og det kunne anses for tilstrækkeligt, at kilden til ukorrekte oplysninger som i dag oplyses. Uanset disse modhensyn er det min opfattelse, at der også i forhold til korrekte data bør være almindelig åbenhed, og at denne oplysning dermed bør gives i forbindelse med en indsigtsbegæring. Disse to udvidede rettigheder vil yderligere styrke retssikkerheden omkring kreditoplysning og bør derfor gennemføres i forbindelse med ny regulering.

8 Erstatningsansvar

Bureauerne har efter § 13 en almindelig pligt til at sikre, at der kun registreres og videregives korrekte data. Desuagtet kan der være til-

9. Der bortses her fra situationer, hvor der eksisterer en personlig relation mellem kreditgiver og kreditmodtager og hvor denne information kan være pinlig.

fælde, hvor forkerte oplysninger videregives med den konsekvens, at kredit nægtes, og at den registrerede lider et tab. Forudsættes, at bureauet har gjort, hvad der må anses for rimeligt for at sikre korrektheden af de pågældende data, er det den, der har afgivet oplysningerne, som har forårsaget kreditnægtelsen, og som angivet vil den registrerede allerede idag efter § 14 blive bekendt med den pågældendes identitet.

I en sådan situation aktualiseres spørgsmålet om, hvorvidt et erstatningsansvar vil kunne gøres gældende. Under behandlingen i Folketinget i 1987 af forslaget til registerlov blev et forslag om en erstatningsregel med objektivt ansvar overvejet, men et flertal fandt en sådan bestemmelse alt for vidtgående,[10] og ingen erstatningsregel findes i dag i registerloven med den konsekvens, at dansk rets almindelige erstatningsregler finder anvendelse. Dette betyder, at den, der har overdraget en ukorrekt oplysning til bureauet, skal have handlet culpøst, d.v.s. at det skal kunne bebrejdes vedkommende, at oplysningen ikke er korrekt eller vildledende. Herudover skal der være årsagssammenhæng mellem den forkerte oplysning og den nægtede kredit, der endvidere skal være påregnelig for oplysningsafgiveren (adæquans). Endelig skal der være lidt et tab, der kan henføres til den manglende kredit. Det er skadelidte, der har bevisbyrden for, at disse betingelser er opfyldt. En vanskelig, men ikke uopfyldelig bevisbyrde.

I forhold til gældende ret kan det overvejes, om ansvarsgrundlaget skal gøres objektivt, eller om bevisbyrden skal vendes. Traditionelt kræves, at der skal foreligge særlige omstændigheder for at et objektivt ansvar gennemføres. Efter mit skøn er et sådant ansvar ikke tilstrækkeligt indiceret i dette tilfælde. De strenge regler for kreditoplysningsbureauer, der udøver kontrol med oplysningers korrekthed, taler for, at det ikke er vanskeligt i sager af denne karakter at påvise en culpøs adfærd fra oplysningsafgiveren. Denne kender via kontrakten med bureauet reglerne for, hvornår oplysninger kan indberettes og bør af denne grund udvise agtpågivenhed. Yderligere bør antages, at det er forholdsvis let at bevise, at der foreligger såvel årssagssammenhæng som adæquans. Hvorvidt den manglende kredit har medført et tab, der bør erstattes, kan

10. Jfr. Personregistrering p 102.

derimod være vanskeligere at bevise, men her forekommer det mest rimeligt, at det er skadelidte, der skal bevise et sådant tab, og ligeledes vil en omvendt bevisbyrde i denne henseende ikke være rimelig. Konklusionen er følgelig, at det fortsat bør være dansk rets almindelige erstatningsregler, der finder anvendelse, og at der ikke er behov for på dette område at indføre særlige erstatningsregler i registerloven.[11]

9 Sammenfatning

Sammenfattende kan det konkluderes, at med de ændringer af de gældende regler, der er foreslået i det foregående, vil der foreligge en lovgivningsmæssig regulering, der sikrer, at kreditvurdering kan foregå på et databeskyttelsesmæssigt forsvarligt grundlag. Tages der i praksis hensyn både til integritetsbeskyttelsen og kreditmiljøets samfundsmæssige betydning, vil der foreligge en god retlig ramme.

Det vil ligeledes være en ramme, der vil være anvendelig også for gæld til offentlige myndigheder, der indberettes til private kreditoplysningsbureauer. Dette kan ikke ske i dag grundet bestemmelser i loven om offentlige myndigheders registre[12] med den konsekvens, at der er en naturlig tilbøjelighed til at prioritere betalingen af privat gæld frem for offentlig gæld. Dette er tilfældet selvom mange offentlige myndigheder, især kommuner, de senere år har strammet kursen overfor borgere og virksomheder, der ikke betaler deres gæld til det offentlige.[13] Denne uheldige situation vil ikke på tilfredsstillende måde kunne løses af et gældsregister placeret i den offentlige forvaltning, medmindre private gives søgeadgang heri, og så kan man lige så godt benytte de etablerede kreditoplysningsbureauer, der har erfaringer med at formidle kreditop-

11. Som angivet foran er det lagt til grund, at et objektivt erstatningsansvar for kreditoplysningsbureauet ej heller bør komme på tale.
12. Lovbekendtgørelse nr. 654 af 20/9 1991 §§ 16, stk. 1, 17 og 21, stk. 1-3.
13. Det bemærkes, at det er et selvstændigt spørgsmål, hvad konsekvensen i forhold til offentlige myndigheder skal være af, at gæld ikke betales. Pointen her er, at information om manglende betaling af sådan gæld vil påvirke kreditmulighederne i den private sektor og i og for sig også er en relevant oplysning for private kreditgivere.

lysning. Behovet for inddragelse af den offentlige gæld demonstrerer endnu en gang den store samfundsmæssige betydning, som kreditoplysning og kreditvurdering har.[14]

14. 23.11.1994 er fremsat lovforslag 64 om begrænsning af skyldneres muligheder for at deltage i offentlige udbudsforretninger og om ændring af visse andre love. Ifølge forslaget indsættes et nyt kapitel 5a i lov om offentlige myndigheders registre, hvorefter gæld over 25.000 kr. under bestemte fastsatte betingelser kan indberettes til et kreditoplysningsbureau.

8 Tele-kommunikation

1 Moderne telefoni

Elektroniseringen har betydet fornyelse og forbedringer i mulighederne for telekommunikation, herunder ikke mindst telefoni. Denne er i disse år ved at blive digitaliseret ved implementeringen af det såkaldte ISDN-netværk.[1] Denne teknologi giver bl.a. muligheder for nye former for telefoni til gavn for både forbrugere og erhvervsliv. Samtidig giver den dog også nye muligheder for behandling af persondata og rejser nye former for risici i forhold til privatlivets fred. Det er derfor nødvendigt at overveje, i hvilken udstrækning det er påkrævet at gennemføre retlig regulering, og hvorledes balancepunktet mellem databeskyttelse og dataanvendelse skal placeres på dette område.

Det er forventeligt, at der vil blive udstedt et EU-direktiv omfattende denne særlige problemstilling. Et første udkast blev fremsat i 1990 og et revideret udkast i 1994[2], men afgørelsen af denne sag afventer vedtagelsen af det almindelige direktiv om databeskyttelse omtalt i kapitel 1. Der vil således gå nogle år, inden et direktiv vil blive vedtaget, og dets indhold vil sikkert adskille sig en del fra 1994-udkastet, hvorfor der ikke direkte tages hensyn til dette i det følgende. Udkastet har dog haft den betydning, at dets bestemmelser indkredser en del af de problemstillinger, der må tages i betragtning, og dermed har det medvirket til at strukturere afsnittet.

Udgangspunktet for de følgende betragtninger er på samme

1. ISDN står for Integrated Services Digital Network. Teknologien integrerer tale(telefoni), tekst, data og billeder, jfr. herved også de i kapitel 6 omtalte informationslandeveje.
2. Forslag til Rådets direktiv om beskyttelse af personoplysninger og kommunikationshemmeligheden i forbindelse med offentlige digitale telenet, herunder det tjenesteintegrerede digitalnet (ISDN) og offentlige digitale mobilnet, KOM(90)314 endelig udg.-Syn288 af 24/9 1990, og revideret forslag, KOM(94)128 endelig udg.-Syn288 af 14/6 1994.

måde som på andre områder, at en retlig regulering skal sikre en rimelig beskyttelse af privatlivet, på samme tidspunkt som erhvervsliv og forbrugere skal kunne drage nytte af de teknologiske forbedringer, der generelt styrker og differentierer de samfundsmæssige kommunikationsmuligheder.

2 Registrering af foretagne telefonopkald

Som den første problemstilling behandles i det følgende virksomheders registrering af foretagen telefoni, som er det eneste af de i dette kapitel behandlede spørgsmål, der i dag er underlagt lovregulering. Ifølge § 7f er det forbudt for virksomheder at foretage automatisk registrering af telefonnumre, hvortil der er sket opkald fra virksomhedens telefoner.[3] Registertilsynet kan dispensere herfra, hvilket bl.a. kan ske, såfremt en sådan registrering er nødvendig ved gennemførelsen af en kontrakt, hvor virksomhedens medkontrahent er forpligtet til at dække foretagne telefonsamtaler. I praksis er der kun blevet givet få dispensationer fra forbudet, der blev indført ved lovrevisionen i 1987. Formålet med bestemmelsen er først og fremmest at beskytte de ansatte, da registrering af opkald antages at have karakter af en overvågning, der er for vidtgående i forhold til at hindre, at en virksomheds telefoner misbruges til private opkald. Det spiller her en rolle, at en virksomhed vil kunne sikre sig over for store telefonudgifter ved f.eks. at bestemme, at udenbys og internationale samtaler alene kan ske via et omstillingsbord.

Under en hensyntagen til de arbejdsmæssige forhold, der er sædvanlige på danske virksomheder, er den gældende bestemmelse hensigtsmæssig, så længe de klart erhvervsmæssigt begrundede tilladelser bliver givet. Registrering af opkaldte numre vil være uheldig for arbejdsmiljøet, og da virksomheder som nævnt kan sikre sig mod for store telefonudgifter på anden måde, er der ikke behov for at lempe den gældende ordning. Det vil være i strid med dansk mentalitet at tillade denne form for registrering.

3. Det bemærkes, at automatiserede opkaldt i forbindelse med kontrol af edb-systemers brug ikke er omfattet af bestemmelsen, jfr RÅ1988 p 90-91.

I denne sammenhæng må det anmærkes, at en konsekvens af § 7f er, at virksomheder ikke kan modtage fuldt ud specificerede telefonregninger, jfr. hertil også nedenfor, men dette forhold kan ikke i sig selv medføre en revision af den angivne konklusion.

De gældende regler udelukker ikke registrering af opkald foretaget til virksomheden, hvilket skyldes, at teknologien ikke i 1987 muliggjorde en sådan registrering. I dag kræves således blot, at de almindelige registreringsbestemmelser i § 3 skal være opfyldt. Det kan overvejes, hvorvidt denne form for registrering også bør forbydes med en tilføjet dispensationsmulighed for Registertilsynet. Så vidt det kan bedømmes, gør der sig et tilsvarende beskyttelseshensyn gældende som ved registrering af opkaldte numre. Der vil også her være tale om en vidtgående kontrol med de ansattes tidsanvendelse og yderligere med de personer, der foretager de pågældende opkald. Udover denne kontrolfunktion er det vanskeligt at se et tungtvejende erhvervsmæssigt formål, der kan begrunde en sådan form for registrering, som jo ikke belaster telefonbudgettet. Hensynet til et acceptabelt arbejdsmiljø taler på denne baggrund for, at § 7f udvides til også at omfatte automatisk registrering af opkald foretaget til virksomheder.

2.1 Opkald fra private hjem

Som det fremgår, tager den eksisterende lovgivning alene sigte på virksomhedernes registrering og ikke på privatpersoners, hvilket til dels skyldes, at det følger af § 1, at det ikke er tilladt for privatpersoner at have edb-registre med persondata. Denne regel er i dag absurd og selvsagt både upraktisk og ukontrollabel. Det er derfor nødvendigt på områder, hvor det er relevant at overveje retsstillingen også for private, at foretage en retspolitisk vurdering. Regulering af, hvilke registre private til personlige formål må opbygge, er normalt ikke ønskelig og støder an på det almindelige juridiske hensyn, at retsregler ikke bør være programerklæringer, men må have et indhold, der lader sig håndhæve. Da offentlig kontrol i private hjem som alt overvejende hovedregel er uønskelig og i sig selv krænkende for privatlivets fred, er der retspolitisk ikke grundlag for at foreslå sådanne registerregler.[4]

4. I udkastet til almindeligt persondatabeskyttelsesdirektiv oktober 1992, artikel 3, stk. 2, undtages registre til personligt brug fra reguleringen.

Anderledes stiller sagen sig i situationer, hvor udenforstående på vegne af privatpersoner foretager registrering. Her kan en regulering være meningsfuld, og en sådan situation foreligger i henseende til spørgsmålet om, hvorvidt privatpersoner skal kunne modtage specificerede telefonregninger, hvoraf det fremgår, til hvilke numre der er foretaget opkald fra abonnentens telefon. Under en forbrugersynsvinkel er sådanne regninger fordelagtige, fordi de tilvejebringer forbedrede muligheder for at kontrollere regningens korrekthed. Det er velkendt, at det ofte er vanskeligt for en abonnent at dokumentere en indsigelse over en telefonregnings størrelse, og en specificeret regning vil selvsagt skabe bedre muligheder herfor.

I mange tilfælde vil regningen dog ikke kun angå en enkelt persons telefonbrug, men derimod en husstands. Det betyder, at en specificeret regning reducerer de enkelte husstandsmedlemmers selvstændige privatliv og forstærker husstanden som et kollektiv. Under dette perspektiv foreligger et integritetsproblem i forhold til sådanne regninger. Det kunne derfor overvejes, hvorvidt specificerede regninger skulle forudsætte en anmodning til teleselskabet fra alle (myndige) medlemmer af husstanden, således ikke blot fra den, der mere eller mindre tilfældigt, formelt er abonnent. Selv om man kan nære en vis sympati for en sådan ordning, vil en regel herom nok for udtalt regulere husstandens private liv og bør derfor næppe gennemføres. Det må dog erkendes, at der er tale om en vanskelig afvejning af ligeværdige hensyn, hvorfor spørgsmålet grundigt bør overvejes i forbindelse med den kommende lovrevision. Indtil videre er resultatet med en vis tvivl, at det må være frit for teleselskaber at tilbyde og give deres private abonnenter specificerede regninger, men at det dog skal være muligt for den enkelte fortsat at modtage uspecificerede regninger, som de kendes i dag. På baggrund af ovenstående bør ordningen udformes således, at en specificeret regning alene udstedes efter anmodning fra abonnenten.[5]

5. Se hertil RÅ1993 p 108-09, hvor det forudsættes at abonnenten samtidig er bruger.

3 Identificerbar telefoni

En væsentlig nyskabelse i den moderne telefoni er, at anonymiteten ophæves. I dag ved man ikke, når telefonen ringer, hvem den kaldende er, forinden opkaldet besvares. Fremover vil et display på telefonen kunne angive, fra hvilket nummer opkaldet stammer (»caller identification«). Den omstændighed, at anonymiteten på denne måde ophæves, rejser en række privatlivsorienterede spørgsmål, som behandles nærmere i det følgende.

Først anskues spørgsmålet fra den ringendes synsvinkel, og her kan det overvejes, i hvilket omfang det skal være muligt at blokere identifikationsfunktionen, således at anonymiteten fastholdes, hvorved bemærkes, at dette teknisk er muligt. Bør det være en ret at være anonym ved brug af telefoni? I en række tilfælde, hvor særligt må nævnes brug af rådgivningslinier etc., vil det være ønskeligt, at anonymiteten kan fastholdes. Brug af denne form for service vil ofte i praksis forudsætte, at den anvendes anonymt. Det bør derfor være muligt at kunne blokere identifikationsfunktionen, hvorved bemærkes, at politiet i konkrete situationer til gengæld må have mulighed for at suspendere blokeringen, når konkrete retshåndhævelsesformål tilsiger dette. Det kan diskuteres, hvorvidt det er nødvendigt retligt at regulere adgangen til at blokere identifikationsfunktionen, men skønnes dette påkrævet, bør ordningen være som her skitseret.

Større interesse er knyttet til den opkaldtes situation. Det er ved modtagelse af telefonopringninger, at der foreligger hensyn, der klart er relateret til privatlivet. Her er identifikationsfunktionen en tydelig fordel. Selv om den naturligvis alene viser det nummer, hvorfra der ringes, og ikke angiver den person, der faktisk ringer, giver den en forbedret mulighed for at vurdere, hvorvidt et foretaget opkald skal modtages. I særdeleshed vil denne funktion indebære en mulighed for at begrænse generne ved chikanøse opkald. Disse forhold betyder, at der bør være en adgang til at bestemme, at alene identificerede opkald vil modtages, hvilket teknisk vil være muligt. Dette betyder, at opringninger, hvor identificeringsfunktionen er blokeret, ikke bliver modtaget. Denne mulighed må betragtes som meget væsentlig og vil generelt betyde en styrkelse

af privatlivets fred. Der er således tale om en teknologisk innovation, der må bedømmes som entydigt positiv.

4 Viderestilling

Den nye teknologi giver forbedrede muligheder for, at modtagne opkald umiddelbart kan viderestilles til en anden person end den umiddelbart opkaldte. Viderestilling til trediemand er normalt uproblematisk, men det vil være ønskeligt, at der gives den kaldende information om, at en sådan viderestilling finder sted. Sådan information sikrer, at der fortsat er mulighed for en vis individuel kontrol med den telefoni, den enkelte foretager. Samtidig er det ønskeligt, at den, der modtager viderestillede opkald, er klar over, at der er tale om en sådan opringning, og ligeledes har den ovenfor beskrevne ret til alene at modtage identificerede opkald.

Omtalen af denne problemstilling indicerer, at de udvidede telefonimuligheder bør praktiseres i overensstemmelse med normer, der er udtryk for en respekt for de medvirkendes integritet.

5 Telefonetik

Sådanne normer vil undertiden mere være etiske end i egentlig forstand retlige. Dette gælder således særlig i henseende til anvendelsen af medhør, hvor andre gives adgang til at lytte med på en samtale. Her bør den kaldende informeres om, at der sættes medhør på, og således have indflydelse på, hvem der deltager i samtalen. En sådan norm tager sigte på at opretholde udgangspunktet om, at en telefonsamtale principielt er en fortrolig samtale mellem to parter. Tilsvarende bør der altid gives information, såfremt en af parterne ønsker at båndoptage en foretaget samtale.

Sådanne normer bør næppe indgå i en retlig regulering, men snarere som en del af en almindelig adfærdskodeks for god telefoni. Det er ikke ønskeligt, at retssystemet belastes med regler, der tilkendegiver normer for almindelig høflighed, hvortil kommer, at

regler af denne karakter sjældent vil kunne håndhæves ved brug af retlige virkemidler. En adfærdskodeks er derfor en mere fornuftig metode at anvende.

6 Sammenfatning

Sammenfattende tilvejebringer moderne telekommunikation en række nye og forbedrede muligheder for brug af telefoni. Den etablerer en mere åben og gennemskuelig kommunikation, hvorfor det i en række henseender er påkrævet at gennemføre en retlig regulering, der sikrer opretholdelsen af en rimelig beskyttelse af privatlivets fred. Det forekommer forholdsvis enkelt at udforme disse regler, og det er således næppe de teknologiske innovationer på dette område, der i fremtiden vil indebære en trussel mod privatlivets fred.

9 International dataoverførsel

1 Dataanvendelsesbehovet

Internationaliseringen af de erhvervsmæssige og mere generelt de samfundsmæssige relationer sætter fokus på behovet for at kunne formidle persondata over grænserne. I takt med, at personrelateret information har fået stadig større kommerciel betydning, opstår der et stigende pres for at de nationale grænser ikke skal medføre begrænsninger i mulighederne for at anvende sådanne data. Imødekommelse af dette behov forudsætter som udgangspunkt, at den internationale anvendelse af persondata kan ske på en sådan måde, at borgernes integritet og privatliv er undergivet en acceptabel beskyttelse. Anerkendelse af dette behov er ligeledes som det uddybes nærmere nedenfor en forudsætning for, at international distribution af data vinder bred anerkendelse. Der opstår i denne forbindelse en række vanskelige retlige problemer, hvis drøftelse er formålet med dette kapitel.

2 Borgernes perspektiv

For at trænge ind i denne besværlige problemstilling kan det være hensigtsmæssigt indledningsvist at belyse den under borgernes synsvinkel. De databeskyttelsesretlige regler tager sigte på at beskytte borgerne og de er hovedsageligt begrundet med den opfattelse, at der foreligger en række risici for, at personlige oplysninger bliver misbrugt eller behandlet på en ukorrekt måde. Reglernes virkning eller formål er bl.a., at borgerne får større tillid til de dataanvendende virksomheder og således har færre betænkeligheder ved at overdrage personinformation til disse. Denne tillid er her i

landet baseret på, at registerloven er velindarbejdet i praksis og at Registertilsynet fører tilsyn med lovens overholdelse. Selvom loven ikke virker perfekt eller altid overholdes, har den bevirket, at egentlige skandaler, d.v.s. store og omfattende misbrug af persondata ikke er forekommet i det private erhvervsliv. På det nationale niveau har det endvidere betydning, at borgeren har en vis viden om, hvor deres data befinder sig og under alle omstændigheder ved, at der foreligger en i hovedtræk acceptabel retlig regulering af databehandlingen.

På denne baggrund kan internationalisering i sig selv opfattes som en trussel. Når persondata overføres til andre lande, opstår der hos den enkelte større usikkerhed om, hvor dennes data egentlig befinder sig og til hvilke formål, de bliver benyttet. Risikoen for misbrug af oplysninger vil forekomme meget større. Samtidig bliver det vanskeligere at bedømme, endsige forstå, hvilke retlige regler, de udenlandske virksomheder er underlagt og det kan i praksis bliver nærmest umuligt for den enkelte borger at kontrollere eller få kontrolleret, hvorvidt sådanne regler faktisk bliver overholdt. Disse forhold, der bevidst er trukket noget skarpt op, bevirker, at der foreligger et betydeligt behov for en retlig regulering af international dataoverførsel og at en sådan regulering ikke mindst er påkrævet for at sikre den nødvendigt tillid til persondataanvendelsen.

3 Reguleringsproblemer

Udformningen af en sådan retlig regulering er meget vanskelig og det kan være hensigtsmæssigt allerede her at indkredse disse vanskeligheder nærmere, jfr. herved også de almindelige synspunkter i kapitel 1. Regler om persondatabeskyttelse udtrykker i vidt omfang, hvilke generelle ideologiske holdninger, der gør sig gældende i de enkelte samfund. I den offentlige sektor dækker reglerne over opfattelsen af forholdet mellem borger og stat, medens reguleringen i den private sektor angiver holdningen til forholdet mellem borgerne og de private virksomheder. Reguleringen berører således centrale træk ved et samfunds retlige kultur og tradition.

Særligt i den private sektor er reglerne ligeledes betegnende for, hvor intensivt staten søger at regulere det private erhvervsliv. Med en anden formulering kan persondatabeskyttelsesområdet betegnes som meget nationalt. Dette udgangspunkt klargør, at det er ambitiøs opgave at ville samordne forskellige landes regulering på dette område. En sådan samordning kan blive opfattet som meget indgribende uanset de stærkt motiverende behov for at få skabt rammer for international dataoverførsel.

Udover disse generelle træk foreligger den situation, at der eksisterer meget forskellige traditioner for national regulering af området. Nogle lande startende med Sverige (1973) efterfulgt af bl.a. Danmark, Frankrig og Vesttyskland (1978) har lange traditioner for lovgivning på området, medens en række andre lande, f.eks. Belgien og Spanien, først for nylig har fået gennemført registerlove. Hertil kommer en meget stor gruppe lande, der ikke har en almindeligt dækkende national lovgivning. Indenfor EU gælder dette for Grækenland og Italien. Det samme er tilfældet for de fleste østeuropæiske lande samt for USA og Canada. I en række af disse lande med svage reguleringstraditioner er dette træk særlig udtalt for så vidt angår den private sektor. Dette skyldes, at data- eller privatlivsbeskyttelsen er blevet opfattet som et menneskerettighedsspørgsmål og ud fra traditionel opfattelse angår sådanne spørgsmål forholdet mellem stat og borger, medens de ikke er aktuelle i den private sektor, jfr. også foran i kapitel 1. Det er således et meget uensartet retligt miljø, der præsenteres for transnationale dataoverførsler. Dette kombineret med de grundlæggende forskelle i henseende til retlig kultur betyder, at reguleringsopgaven er meget vanskelig.

4 International regulering

Det er efterhånden en gammel målsætning, at der skal etableres retlige rammer for, at international dataoverførsel kan finde sted og at denne principielt skal kunne ske frit. Dette er hovedformålet i de internationale reguleringer, der idag eksisterer. Der er tale om retningslinier udstedt af OECD i 1980 og Europarådets Databe-

skyttelseskonvention (108/81) fra 1981. Sidstnævnte er ratificeret af Danmark og for vores vedkommende trådt i kraft 1990. Danmark har også tiltrådt OECDs retningslinier.

Indholdet af disse to dokumenter er forholdsvist ens, jfr. nærmere i kapitel 1. Der opstilles en række hovedprincipper for databeskyttelsen, der skal implementeres i national lovgivning. Når dette er sket, fastsættes, at data mellem disse lande frit skal kunne overføres, eftersom der nu foreligger et tilsvarende beskyttelsesniveau, jfr. nærmere herom nedenfor. Det er dog samtidig karakteristisk især for konventionen, at den åbner mulighed for, at de enkelte lande kan tildele deres borgere en højere beskyttelse end de fastsatte principper forudsætter. Dette forhold kombineret med, at principperne for det meste er forholdsvist åbent formuleret med den konsekvens, at de kan implementeres på forskellig måde, betyder, at der kan opstå betydelige afvigelser mellem de enkelte lande. Dette medfører, at forudsætningen om et tilsvarende beskyttelsesniveau ikke opfyldes og at den frie internationale dataoverførsel dermed ikke realiseres. Dette er også blevet det faktiske resultat, idet der har været en række tilfælde bl.a. angående overførsel af kreditoplysninger mellem Tyskland og Frankrig, hvor dataoverførsel ikke er blevet tilladt af den nationale tilsynsmyndighed grundet et afvigende og ringere beskyttelsesniveau i den anden konventionsstat. I forhold til dette afgørende punkt i de internationale dokumenter kan det således konstateres, at de ikke har virket efter deres hensigt.

5 EU

Det er denne konstatering af, at databeskyttelseskonventionen ikke har fungeret, der har været hovedårsagen til, at Europakommissionen har taget initiativ til, at der skal udstedes et direktiv om databeskyttelse, der for så vidt angår den private sektor entydigt er begrundet med etableringen af det indre marked, der for at fungere

optimalt også må omfatte persondata.[1] I det foreliggende direktivudkast fastslås i artikel 1, stk. 2, at medlemslandene ikke kan begrænse eller lægge hindringer i vejen for den frie udveksling af persondata begrundet i hensynet til privatlivets fred, og hovedparten af de øvrige regler tager sigte på at samordne landenes bestemmelser, således at ens beskyttelsesniveau opstår, jfr. videre herom nedenfor.

Forslaget til direktiv blev oprindeligt fremsat i 1990[2] og var udformet på en sådan måde, at der blev fastlagt et meget højt beskyttelsesniveau og reglerne var dermed på mange måder ganske indgribende overfor private virksomheder, der samtidig blev pålagt omfattende anmeldelses- og informationsforpligtelser med et heraf afledt ressourceforbrug. Direktivudkastet blev mødt med en voldsom kritik fra alle medlemslande og fra en lang række brancheorganisationer og lignende. Europaparlamentet var ligeledes særdeles kritisk og vedtog (11/3 1992), efter at have været udsat for den mest intensive lobbyvirksomhed i Parlamentets historie, et større antal ændringsforslag til direktivet. Det stod herefter klart, at direktivet skulle omarbejdes ganske betydeligt også i lyset af det subsidaritetsprincip, der efter Maastricht-traktatens gennemførelse var blevet en del af den almindelige EU-ret.

På denne baggrund blev et nyt revideret udkast forelagt af Kommissionen i oktober 1992[3]. Dette udkast adskiller sig på en række punkter fra det første og er især karakteriseret ved, at der er givet en større frihed til medlemslandene med hensyn til, hvorledes de enkelte regler implementeres.

Siden forelæggelsen af 2. udkast er der blevet forhandlet om dette på arbejdsgruppeniveau under ministerrådet og det forventes for tiden, at et direktiv vil kunne udstedes i 1995, hvorefter der vil være nogle års frist for landene til at implementere dette i national lovgivning. Forhandlingerne i arbejdsgruppen, der er fortrolige,

1. I andre henseender søges også etableret rammer for international dataoverførsel. Dette gælder således på toldområdet, hvor et omfattende informationssystem, CIS, er under opbygning, jfr. RÅ1991 p 20-23. Særligt bør fremhæves det store informationssystem, SIS, der skal etableres indenfor Schengen-samarbejdet, der vedrører fjernelse af enhver form for grænsekontrol indenfor EU, jfr. herom Peter Blume, Social Kritik nr. 22/23 (1992) p 64-71. – Danmark deltager nu som observatør i Schengen-samarbejdet, jfr. forespørgselsdebat herom, Folketingstidende 1994-95, Forhandlinger sp. 217-241 (25.10.1994).
2. KOM(90)314endelig udg.-Syn287 af 24/9 1990.
3. KOM(92)422endelig udg.-Syn287 af 15/10 1992.

er vanskelige og det må forventes, at det endelige direktiv vil adskille sig en del fra det foreliggende udkast. Det er derfor af mindre interesse nærmere at omtale enkeltheder i direktivudkastet, hvorfor alene de bestemmelser, der direkte vedrører dataeksport i det følgende inddrages.

5.1 Harmonisering eller subsidaritet

Et centralt spørgsmål er, hvorvidt persondatabeskyttelse er et egnet område til at blive reguleret ud fra subsidaritetsprincippet eller om en egentlig harmonisering er påkrævet. Udfra de historiske erfaringer forbundet med de gældende internationale reguleringer, især Europarådets konvention, kunne det umiddelbart set være klart, at en egentlig harmonisering er nødvendig. Netop de afvigende beskyttelsesniveauer i de enkelte lande foranlediget af friheden til at implementere brede principper og adgangen til at fastsætte afvigende bestemmelser har medført, at den frie internationale datatrafik ikke er etableret. Årsagen er således en manglende harmonisering.

Når spørgsmålet ikke hermed er uddebatteret, hænger det sammen med den forskelligartede juridiske status, som en folkeretlig konvention og et EU-retligt direktiv har. Medens førstnævnte alene forpligter staterne og principielt ikke kan påberåbes af borgerne, er et direktiv ganske anderledes forpligtende, idet det kan påberåbes af borgere og virksomheder ved de nationale domstole og overfor staten ved EF-domstolen, der utvivlsomt vil anvende direktivet i overensstemmelse med dets formål, der som nævnt er etableringen af det indre informationsmarked. Domstolen har således tit anlagt en aktivistisk linie, hvor de overordenede formål bag EUsamarbejdet betinger fortolkningen af de konkrete retsforskrifter. Selvom direktivet er implementeret på forskellig måde i de enkelte medlemslande og selvom der i overensstemmelse med dette ligefrem skulle være fastsat afvigende nationale regler, vil bestemmelsen om fri dataoverførsel gælde for alle lande og skal fuldt ud respekteres. Målsætningen om fri dataoverførsel bliver opfyldt uanset om subsidaritetsprincippet bliver dominerende.

Problemstillingen er dermed snarere knyttet til de substantielle årsager til at kræve et reelt ens beskyttelsesniveau og dermed i be-

tydelig grad til de risici under den enkelte borgers synsvinkel, som internationaliseringen på dette område medfører. Disse risici angår overførsel af data til lande, der ikke har samme beskyttelsesniveau som i den nationale ret og det uønskelige i, at en sådan overførsel i sig selv skal betyde en forringelse af den retsbeskyttelse, der ydes den enkelte borger. Udfra denne synsvinkel er anvendelse af subsidaritetsprincippet på dette område uheldigt og kan medføre en underminering af den enkelte borgers retssikkerhed. Dette er en situation, der også set fra erhvervslivets synsvinkel er uheldig, fordi den svækker tilliden til dataanvendelsen og kan bevirke mistro til den internationalisering, som under et kommercielt perspektiv bør fremmes.

Som den altovervejende hovedregel er det på denne baggrund ønskeligt, at harmonisering bliver ledestjernen for de kommende direktivbestemmelser og at subsidaritetsprincippet reserveres til andre områder. Det forekommer desværre ikke sandsynligt, at det endeligt vedtagne direktiv vil modsvare dette synspunkt. Dette skyldes de ovenfor nævnte retskulturelle forskelle i medlemslandene, der skaber så store politiske vanskeligheder, at subsidaritetsprincippet bliver det middel, der skal gøre det muligt, at landene i det hele taget kan blive enige om en udformning af direktivet, i hvis udstedelse der efterhånden er investeret ganske betydelige ressourcer. Netop ved at tillade nationale frihedsgrader kan det nødvendige politiske kompromis opnås.

Den nærliggende risiko er, at direktivet fra at skulle være et retsværn for de europæiske borgere i henseende til international dataoverførsel tværtimod kommer til at undergrave dette retsværn og endog kan betyde, at de enkelte lande i større udstrækning, end det er muligt idag, kan benytte beskyttelsesniveauet som konkurrenceparameter, hvilket set under en virksomhedssynsvinkel er særdeles uheldigt. Det kan tilføjes, at disse problemer generelt illustrerer de svagheder, der for tiden kan konstateres i det EU-retlige samarbejde, hvor medlemslandene ikke kan bestemme sig for, om de vil prioritere nationalstaten eller den europæiske integration.

5.2 Forholdet til tredjelande

Medens direktivet i sig selv vil medføre, at persondata frit kan overføres indenfor EU (og EØS) vil der fortsat foreligge et særligt reguleringsspørgsmål i henseende til overførsel af data til tredjelande. Til belysning af denne problemstilling og som optakt til de generelle drøftelser nedenfor kan det være belysende kort at omtale den ordning, der fastsættes i det foreliggende direktivudkast.

Ifølge artikel 26 kan overførsel af data til tredjelande som hovedregel kun ske, såfremt »det pågældende tredjeland sikrer et passende beskyttelsesniveau«. Vurderingen af, hvorvidt denne norm er opfyldt, skal ske ud fra den konkrete videregivelsessituation sammenholdt med de foreliggende retlige regler i tredjelandet samt eventuelle bestemmelser om god forretningsskik.

Selvom denne bedømmelse falder negativt ud, åbnes der mulighed for, at dataeksport desuagtet kan ske i en række tilfælde. Disse omfatter situationer, hvor den registrerede giver sit samtykke i forbindelse med en kontraktindgåelse, videregivelse er nødvendig for opfyldelsen af en kontrakt mellem den registrerede og den registeransvarlige og at der er informeret herom, samt de tilfælde, hvor videregivelse »er nødvendig af hensyn til beskyttelse af en vigtig samfundsinteresse« og endelig, hvor den er nødvendig for at beskytte »den registreredes vitale interesser«.[4] Herudover giver artikel 27 mulighed for, at videregivelse konkret kan accepteres, hvis den registeransvarlige dokumenterer, at f.eks. kontraktbestemmelser sikrer beskyttelsen af den registrerede, idet Kommissionen og de andre medlemslande i disse tilfælde skal orienteres med en adgang til at fremsætte indsigelser.[5]

Samlet giver denne regulering ganske vide muligheder for dataeksport, men er dog ikke destomindre baseret på den naturlige opfattelse, at bedømmelseskriteriet for tilladeligheden af dataeksport til tredjelande er det beskyttelsesniveau, der er fastlagt i EU. På denne baggrund åbnes for angreb for, at man vil etablere et Fort

4. Denne bestemmelse tager særligt hensyn til organisationer som Amnesty International, idet politiske fanger m.fl. selvsagt ikke har mulighed for at give et samtykke, jfr. tilsvarende registerlovens § 4, stk. 1, 2. pkt.
5. Registertilsynet har i almindelighed tilkendegivet, at kontrakter alene bør opfattes som et supplement ikke et alternativ til national lovgivning, jfr. RÅ1991 p 32-34.

Europa og påtvinge den øvrige verden sin retsopfattelse. Denne kritik må ganske vist anses for overdreven, men er ikke uden en vis berettigelse. Den peger frem mod behovet for en global konsensus omkring persondatabeskyttelsen. Denne problemstilling tages op i slutningen af dette kapitel.

6 Registerloven

Registerlovens § 21 fastslår, at oplysninger, hvis registrering her i landet forudsætter anmeldelse eller tilladelse fra Registertilsynet, kun kan overføres til udlandet med tilladelse af Registertilsynet. Herudover kan registre med følsomme data kun overføres til udlandet med tilladelse. Sådanne oplysningers overførsel til udlandet med henblik på elektronisk databehandling kræver ligeledes tilladelse.[6] I stk. 3 fastsættes som retningslinie, at tilladelse forudsætter, at dataeksport »ikke vil medføre en væsentlig forringelse af den beskyttelse af den eksisterende, loven tilsigter at sikre«. Endvidere kan generelt bestemmes, at overførsel kan ske til bestemte lande, der generelt antages at opfylde denne retningslinie.

Der er særlig grund til at fremhæve, at alle persondata ikke er omfattet af de særlige dataeksportregler. Almindelige persondata, der ikke registreres med henblik på de formål, som forudsætter anmeldelse eller tilladelse, kan frit registreres i eller videregives til udlandet, når blot de almindeligt nationalt orienterede betingelser er opfyldt, jfr. også foran i kapitel 5 om international markedsføring.

Anmærkes kan endvidere, at kriteriet for dataoverførsel er negativt formuleret og åbner for, at beskyttelsesniveauet i det importerende land ikke behøver at være fuldt på højde med niveauet her i landet. Desuagtet er reguleringen baseret på det sædvanlige koncept, hvorefter bedømmelseskriteriet er den nationale lovgivning og det forudsættes, at der foreligger en form for korrespondens mellem denne og den udenlandske regulering. På denne måde er dansk ret idag i overensstemmelse med den internationale opfattelse.

6. Et eksempel på en sådan tilladelse er omtalt i RÅ1991 p 136-38 om overførsel af oplysninger fra udfyldte spørgeskemaer i et kontaktformidlingsbureau til edb-behandling i Norge.

7 Almindelige synspunkter

På baggrund af ovenstående er det væsentligt at starte den almindelige drøftelse med en konstatering. Registerlove eller andre former for databeskyttelsesretlig regulering udgør ikke nogen barriere, men er derimod forudsætningen for, at international dataoverførsel kan finde sted. Under et samfundsmæssigt perspektiv illustrerer de omtalte regelsæt og den tankegang, der ligger bag disse, at dataoverførsel uden national regulering ikke vil blive accepteret. En sådan situation vil blive betragtet som alt for risikabel for integritetsbeskyttelsen og som en undergravning af borgernes retsposition. Dette fundamentale udgangspunkt lægges også til grund her. Det er nødvendigt, at der foreligger en vis parallelitet mellem de nationale regler for, at dataeksport og -import kan ske i et retligt miljø, hvor integritetsbeskyttelsen kan sikres.

Dette synspunkt fremhæves også for at dokumentere, at de erhvervsvirksomheder, der har en kommerciel interesse i transnational dataoverførsel dermed også har en interesse i, at der i de enkelte lande etableres en tilsvarende lovgivning. Dette er væsentligt, fordi det umiddelbart kunne fremtræde således, at en retlig regulering begrænser erhvervsudøvelsen, men denne opfattelse er altså misvisende og uden forståelse for de politiske realiteter. Den fører til, at den nødvendige dialog mellem erhvervsliv og lovgivningsmagt bliver ufrugtbar og føres fra bastioner, der ikke reelt udtrykker de interesser, der bør varetages. Diskussionen angår dermed ikke, om der skal være en retlig regulering, men derimod hvad indholdet af denne bør være, hvorunder især falder, hvilken form for parallelitet mellem de nationale regler, der skal give grundlag for fri dataoverførsel. Det er denne problemstilling, der behandles i det følgende.

7.1 Et ens beskyttelsesniveau

Det centrale og vanskelige spørgsmål er, hvor høj grad af lighed mellem forskellige landes databeskyttelseslovgivning, der skal foreligge, for at fri dataoverførsel kan finde sted, d.v.s. overførsel, som ikke forudsætter anmeldelse til eller tilladelse fra den nationa-

le tilsynsmyndighed. Mulige normer er, at beskyttelsesniveauerne skal være tilsvarende, adæquate eller ækvivalente. Sidstnævnte er det strengeste krav, der indebærer, at der på ingen områder af nogen form for signifikans må være afvigelser mellem de nationale regler. En sådan retsstilling ville yde den største sikkerhed for, at borgernes retssikkerhed ikke påvirkes af overførsel af data til udlandet og dermed skabe det ideelle internationale miljø for dataoverførsler. Det er imod realiseringen af denne målsætning, at reguleringen bør udformes.

Det må dog konstateres, at en norm om ækvivalens er ideel og ikke har mulighed for at vinde genklang i den politiske virkelighed, hvorfor en ubetinget fastholdelse af denne reelt ville være ensbetydende med, at international dataoverførsel i store træk ville være udelukket. Under hensyntagen til det samfundsmæssige pres for at fremme disse overførsler, ville det være urealistisk at fastholde et krav om ækvivalens.

Opgaven er dermed, at fastlægge i hvilket omfang nationale afvigelser har en sådan karakter, at de kan accepteres uden, at integritetsbeskyttelsen falder til et uacceptabelt niveau. Udgangspunktet for denne vurdering bør være, at reglerne om, hvornår persondata kan registreres og videregives (samkøres), bør være ens, ligesom den registrerede bør have samme rettigheder i de enkelte lande. Herudover bør der fastlægges et fælles edb-teknisk sikkerhedsniveau. Afvigelser vil herefter være tilladelige i henseende til de bureaukratiske rammer, d.v.s. forholdet mellem den registeransvarlige og tilsynsmyndigheden. Dette gælder eksempelvis for regler om, hvornår databehandling skal anmeldes eller have tilladelse fra den nationale tilsynsmyndighed. Det er de indholdsmæssige regler for databeskyttelse, der må være ens med den konsekvens, at det bliver berettiget at tale om et fælles beskyttelsesniveau.

De regler, der herefter bør gælde i alle lande, skal være fastsat ved lovgivning. Dette betyder, at etableringen af et fælles niveau ikke kan overlades til markedet, der ganske vist vil kunne yde et værdifuldt bidrag ved at supplere den formelle regulering via udstedte kontraktbestemmelser og konkret fastsatte branchenormer, men som ikke på egen hånd har et tilstrækkeligt incitament til at fastlægge reguleringen, jfr. mere generelt herom i næste kapitel. Med

dette udgangspunkt kan der skabes en retlig ramme, der kan sikre en betryggende international dataoverførsel.

7.2 Samarbejde

Der er dog en achilleshæl, der underminerer den skitserede regulering. I henseende til beskrivelsen af de indholdsmæssige regler for databehandling (registrering/videregivelse m.v.) må det konstateres, at det ikke er muligt i regelsprog, at opnå nogen tilfredsstillende grad af præcision. Disse regler får, uanset om de er generelle eller sektorspecifikke, i mange tilfælde karakter af standarder, hvis implementering er afhængig af den nationale tilsynsmyndigheds praksis og retshåndhævelsesmidler, jfr. nærmere herom i kapitel 10.

Dette er så vidt det kan bedømmes et uafvendeligt træk ved databeskyttelsen og det betoner, at det er afgørende for betryggende international dataoverførsel, at der sker en systematisk udbygning af det internationale tilsynsmyndighedssamarbejde og at der i alle lande er stor åbenhed omkring praksis. Samarbejde og åbenhed udgør centrale forudsætninger for, at databeskyttelsens internationalisering sikrer integritetsbeskyttelse og retssikkerhed. Det er ligeledes forudsætningen for, at databehandlingsniveauet ikke de facto benyttes som konkurrenceparameter mellem virksomheder og at reguleringen i praksis tilvejebringer lige konkurrencebetingelser på dette område.

7.3 Alle persondata

Det bør endvidere præciseres, at den skitserede regulering må omfatte alle persondata og således ikke som i gældende dansk ret undtage de almindelige persondata. Som der er redegjort for i kapitel 3 og i kapitel 6 om de elektroniske spor, foreligger der et reguleringsbehov også i forhold til persondata, der isoleret bedømt kan fremtræde som trivielle og ligegyldige. Det vil derfor ikke være acceptabelt, at sådanne data kan overføres til lande enten uden nogen form for beskyttelse eller med et for lavt beskyttelsesniveau. Det er derfor positivt, at det foran omtalte direktivudkast ikke i sin regulering af adgangen til dataoverførsel gør forskel mellem de forskel-

lige datatyper. Dette udgangspunkt bør fastholdes som en væsentlig retspolitisk ledetråd.

7.4 Bistand til borgerne

Selvom der etableres en regulering, der i videst muligt omfang sikrer ens nationale databeskyttelsesniveauer, foreligger der som allerede indiceret vanskelige retshåndshævelsesproblemer. Dette er ikke mindst tilfældet, når problemstillingen anskues ud fra den enkelte borgers synsvinkel. Det kan let fremtræde som en ganske uoverskuelig opgave at skulle gøre sine rettigheder gældende i et fremmed land hvis sprog, man ofte ikke forstår og som har anderledes juridiske traditioner og bureaukratiske ordninger.

Det er derfor påkrævet, at der i en regulering indbygges en procedure, der gør det praktisk muligt for borgerne at få håndhævet deres rettigheder. Denne ordning kan bestå i, at borgerens egen tilsynsmyndighed forpligtes til at varetage borgernes interesse. Dette betyder, at borgeren kan indbringe en klage for denne myndighed, der herefter skal foranstalte den undersøgt og afgjort af den relevante udenlandske tilsynsmyndighed i forhold til hvilken, borgerens myndighed må virke som advokat for denne. På denne måde vil der være etableret en procedurel ramme, der kan medvirke til at sikre en betryggende international dataanvendelse.

8 Global regulering

Som det er fremgået er international dataoverførsel en meget vanskelig problemstilling og den foreliggende internationale regulering er ikke endnu tilfredsstillende. Der er fortsat en betydelig risiko for, at udenlandske virksomheder for borgerne vil fremtræde som en art Superbrother. Det kommende EU-direktiv vil forhåbentlig udgøre et fremskridt, men vil selvsagt ikke være tilstrækkeligt. Når dette direktiv er gennemført, vil næste opgave være at starte arbejdet for, at der udformes en globalt dækkende konvention, hvilket kunne ske i FN-regi. En mulighed kunne måske også være WTO (World Trade Organization), såfremt dette nye organ

etableret indenfor GATT-samarbejdet viser sig arbejdsdygtigt.

Vesteuropa, der indenfor databeskyttelsesretten er et foregangsområde, bør tage initiativ til en sådan konvention i bevidstheden om, at det globale informationssamfund er i kraftig fremvækst og den globale informationslandsby kommer stadigt nærmere. Gennemførelsen af en sådan konvention vil ikke være nogen nem opgave, men først når denne foreligger og er ratificeret af et tilstrækkeligt antal lande, vil der for alvor være skabt en forsvarlig retlig ramme for international dataoverførsel.

10 | Regulering og kontrol

1 Problemstilling

Et tilfredsstillende databeskyttelsesniveau forudsætter, at de fastsatte regler bliver overholdt i praksis, og at der er rimelige muligheder for at kontrollere og håndhæve reglerne. Det er naturligvis afgørende, at databeskyttelsesretten ikke blot består af en række fine ord, der kan hyldes ved festlige lejligheder, men faktisk tilvejebringer et beskyttelsesniveau, der sikrer borgerne den integritetsbeskyttelse og det privatliv, som reglerne tilkendegiver.

Der foreligger en lang række problemer i henseende til sikring heraf. Disse er i betydeligt omfang knyttet til denne retlige reguleringens særlige karakter. Den er meget omfattende og vedrører således alle dele af den private sektor og skal på denne måde fungere i mange forskellige brancher med hver deres erhvervsmæssige særtræk. Reguleringen er under en umiddelbar betragtningsmåde indgribende over for erhvervsudøvelsen, og derfor vil der let foreligge situationer, hvor den mødes af et fjendtligt miljø, i hvilket de fastsatte regler søges omgået.

Samtidig er det karakteristisk for en række databeskyttelsesnormer, at de ikke lader sig omsætte præcist i regelsproget. Selv om alle juridiske regler i større eller mindre udstrækning er åbne for fortolkning, er dette forhold særlig udtalt for mange af de fundamentale bestemmelser i databeskyttelsesretten. Det er derfor særdeles væsentligt, hvorledes regelværket fortolkes og praktiseres. Dermed har det stor betydning, hvorledes myndighedsstrukturen er opbygget.

De praktiske vanskeligheder hænger selvsagt også sammen med edb-teknologien, der er i konstant udvikling, og som medfører, at det er nødvendigt, at kontrollerende myndigheder har et højt teknologisk beredskab. Samtidig betyder de teknologiske innovatio-

ner, at der konstant opstår nye reguleringsspørgsmål, og at det derved hele tiden er nødvendigt at sikre, at beskyttelsesniveauet er tilfredsstillende.

Disse problemstillinger giver anledning til at overveje en række spørgsmål. Disse omfatter, hvilke former for håndhævelses- og kontrolmidler der bør være til rådighed. Centralt er spørgsmålet om, hvilken reguleringsmetode der er mest effektiv på dette område, hvilket inkluderer en vurdering af alternativer til lovgivning og andre former for traditionel regulering. Tilknyttet hertil er spørgsmålet om betydningen af intern virksomhedsregulering og dermed også betydningen af andre virkemidler end de rent retlige. I denne sammenhæng er det endvidere naturligt at inddrage den rolle, som etiske normer kan spille. Det er i hovedsagen disse problemstillinger, der drøftes i dette kapitel.

2 Virksomhedernes interesse

Indledningsvis kan der være grund til at fremhæve, at det ikke blot er borgerne, der har en interesse i, at de databeskyttelsesretlige regler bliver overholdt. Dette er også en virksomhedsinteresse. De databeskyttelsesretlige regler angiver på samme måde, som det er tilfældet indenfor andre retsområder, betingelser for, hvorledes erhvervsudøvelsen kan praktiseres og fastsætter derved vilkår for konkurrencen mellem virksomhederne. Reguleringen begrænser den i en vis forstand anarkistiske frihed, som markedet er udtryk for. Med en anden formulering betyder reguleringen, at persondatabehandling ikke kan indgå som en faktor af betydning for konkurrenceforholdene i den forstand, at de retlige rammer for denne er ens. Den retlige regulering medfører, at der på dette felt skabes lige konkurrencebetingelser.

Denne virkning forudsætter selvsagt, at reglerne faktisk overholdes, og at der ikke er virksomheder, der »snyder« og dermed opnår en uberettiget fordel. Da det må lægges til grund, at en retlig regulering af persondatabeskyttelsen er en samfundsmæssig realitet, bliver det på denne baggrund en almen erhvervsinteresse, at det beskyttelsesniveau, der fastlægges, rent faktisk generelt etable-

res, og at de lige konkurrencemuligheder dermed bliver en realitet. På denne baggrund har kontrol- og retshåndhævelsesspørgsmålene betydelig erhvervsmæssig interesse.

3 Registertilsynet

På samme måde som i mange andre lande er der i dansk ret etableret en særlig myndighed, Registertilsynet, der har til opgave at overvåge, at registerlovgivningen bliver overholdt. Registertilsynet er en selvstændig myndighed i den forstand, at dets afgørelser ikke kan påklages til andre administrative myndigheder, men alene indbringes for domstolene, hvilket der ikke er tradition for. Organisatorisk og personelt hører Registertilsynet dog under Justitsministeriet. Det er således fra ministeriet, at tilsynet får sin bevilling, og personalet i sekretariatet kommer fra ministeriet og indgår i dettes personalepolitik.

Ved siden af sekretariatet med direktøren i spidsen findes et registerråd, bestående af 7 medlemmer udpeget af justitsministeren ud fra en vurdering af deres sagkundskab. I store og principielle sager træffer rådet afgørelse på grundlag af sagsforelæggelse fra sekretariatet.

Årsagen til, at denne særlige myndighed er oprettet, er den velbegrundede antagelse, at der er tale om et retsområde, der forudsætter en særlig viden og sagkundskab, og at denne bedst opbygges i en selvstændig myndighed frem for i et departement eller i en styrelse. Kvalitativt tilfredsstillende afgørelse af mange databeskyttelsesretlige spørgsmål forudsætter en indlevelse i og en dyb forståelse af de hensyn, der skal afbalanceres og de regler, der danner udgangspunkt for denne afbalancering. Denne opgave håndteres bedst i en specialiseret myndighed.

Registertilsynets placering under Justitsministeriet er ikke uproblematisk. I praksis medfører den en meget høj grad af personalemobilitet, der svækker muligheden for at oparbejde den tilstrækkelige sagkundskab.[1] Selv om afgørelser ikke kan påklages,

1. Se hertil Peter Blume, Juristen 1993 p 345-46. Se ligeledes kritik af tilsynets placering og rolle i Teknologinævnets rapport »Hvem ved hvad – og bør de det?« (København 1993) p 19.

er personalets karriereforløb knyttet til ministeriet,[2] og dette forhold er måske en del af forklaringen på, at Registertilsynet ofte er ret tilbageholdende – nogle ville polemisk sige usynlig – i den offentlige debat og normalt ikke selv tager initiativ til at få undersøgt nye reguleringsspørgsmål, inden konkrete sager forelægges.

Det er vanskeligt at finde den rette personalemæssige balance mellem kontinuitet og fornyelse. Som anført, bør det lægges til grund, at databeskyttelsesretten er et vanskeligt tilgængeligt retsområde og at det derfor tager nogen tid inden en sagsbehandler kan håndtere dette på kvalificeret måde. Dette forhold taler for kontinuitet. Heroverfor står det ønskelige i undertiden at lade nye øjne se på problemerne. Tilsynsmyndigheden bør ikke stivne i en bestemt opfattelse. En vis løbende fornyelse, der også må omfatte Registerrådets sammensætning, bør dermed også tilstræbes. Idag må det dog konstateres, at mobiliteten især på sekretariatsniveau er alt for udtalt.

Som nævnt er det ønskeligt, at Registertilsynet spiller en aktiv rolle i den offentlige debat og her henleder opmærksomheden på nye databeskyttelsesretlige spørgsmål. Samtidig bør tilsynet selvstændigt tage initiativ til at lade sådanne spørgsmål undersøge også før de politisk aktualiseres. På denne baggrund er det nødvendigt fremover at styrke tilsynets position ved at omdanne dette til en helt selvstændig myndighed, eventuelt placeret direkte under Folketinget.[3] Uanset organisatorisk placering er det af afgørende betydning, at Registertilsynet tager selvstændige initiativer og har en sådan sagkundskab, at det kan indgå i en meningsfuld dialog med erhvervslivet.

4 Håndhævelse

Registerlovens håndhævelsessystem er baseret på, at Registertilsynet har en almindelig ret til at kræve alle oplysninger, der har be-

2. For en god ordens skyld bemærkes, at der ikke er nogen tendens til, at Justitsministeriets egne registre gives nogen uberettiget favorabel behandling.
3. Så vidt det kan bedømmes vil der ikke forfatningsretligt være problemer forbundet med en sådan placering.

tydning for de afgørelser, tilsynet skal træffe (§ 22 stk. 2). Dette er en meget væsentlig beføjelse, og det er berettiget, at undladelse af at udlevere oplysninger er strafsanktioneret (§ 27 stk. 1 nr. 3). Bestemmelsen forudsætter, at udleverede oplysninger i videst muligt omfang behandles fortroligt, men den omstændighed, at der kan være tale om erhvervshemmeligheder, kan ikke påberåbes som en legitim grund til ikke at udlevere oplysninger.

Ved siden af en adgang til at udstede påbud og forbud samt den omstændighed, at overtrædelse af en række af lovens regler er strafsanktioneret, er den klart vigtigste beføjelse adgangen til inspektion, der omfatter de anmeldelsespligtige registre, advarselsregistre og de tilfælde, hvor data overføres til udlandet (§ 22 stk. 3). Inspektion indebærer, at tilsynet uden retskendelse og principielt, men sjældent i praksis, uden varsel har adgang til alle lokaliteter i virksomheden, der anvendes i forhold til de omfattede registre. Det er en udbredt erfaring, at disse inspektioner altid afslører større eller mindre overtrædelser af loven og de i praksis fastsatte retningslinier. Inspektioner er ressourcekrævende, og der gennemføres kun et forholdsvis begrænset antal af disse hvert år, men selv om der derfor bliver tale om stikprøver, har selve den omstændighed, at denne mulighed foreligger, en vis præventiv virkning.

Af størst betydning er dog ikke, at der ved inspektioner kan afsløres fejl, men derimod at disse kan fungere som rammen for en dialog med virksomhederne. Som det nærmere uddybes senere i kapitlet, er dialog mellem tilsynsmyndigheden og virksomhederne afgørende for den generelle realisering af det databeskyttelsesniveau, som lovgivningen tager sigte på at opretholde. Det må således antages, at de sanktionsmuligheder, loven indeholder, ikke har større alment adfærdsdirigerende betydning. Strafniveauet kan ikke gøre indtryk på nogen virksomhed, og en forøgelse af dette vil næppe have nogen signifikant betydning. I henseende til advarselsregistre, kreditoplysningsbureauer og servicebureauer er der, som supplement til de almindelige regler i straffelovens § 79, adgang til dom for rettighedsfortabelse (§28), men dette radikale skridt er ikke anvendt i praksis og vil da også meget sjældent kunne forekomme. Det er ikke ved hjælp af sanktioner, at databeskyttelsesretten skal gennemføres, hvilket også harmonerer med, at det må betragtes som umuligt for tilsynsmyndigheden i praksis på ef-

fektiv måde at kontrollere reglernes overholdelse.

Dette betyder, at tilsynsmyndighedens opgave i første række er pædagogisk opdragende. Gennem dialog må tilsynet så at sige overbevise virksomhederne om, at de fastsatte regler er fornuftige, og at det er i den enkelte virksomheds interesse at overholde dem. Det primære krav til myndigheden er dermed, at den besidder en saglig kompetence, der giver den mulighed for at indgå i en frugtbar dialog. Ved siden af juridisk viden forudsættes derfor teknisk og erhvervsmæssig viden. Det er først og fremmest via dialog, at de databeskyttelsesretlige regler skal blive til virkelighed.

5 Offentlighed

Forinden der ses nærmere på de forskellige reguleringsmodeller, der kan danne udgangspunkt for den her skitserede håndhævelse og kontrol, er der grund til at pege på den betydning, som offentligheden, repræsenteret af massemedierne, har i denne sammenhæng. Det er velkendt, at persondatabeskyttelse ikke er et område, der konstant har mediernes bevågenhed som f.eks. miljøspørgsmål, men også at konkret foreliggende sager ofte får ganske betydelig omtale og tit afføder en kritisk offentlig debat. Dette indebærer, at der på dette område foreligger en risiko for dårlig omtale, der kan påvirke det renommé, den enkelte virksomhed har, med en heraf affødt negativ indvirkning på dennes placering på markedet. Det kan få økonomisk betydning, at en virksomhed bliver kendt for at have en kritisabel databeskyttelsespraksis. Dette forhold har betydning for de virksomheder, der er synlige som selvstændige enheder på markedet, dvs. store eller fremtrædende virksomheder inden for en branche. På denne måde foreligger der for større virksomheder et konkurrenceorienteret incitament til at have en god databeskyttelsespraksis.

På denne baggrund er det væsentligt, at offentligheden inddrages aktivt i sikringen af det beskyttelsesniveau, der er fastlagt i den databeskyttelsesretlige regulering. I det omfang dette efter en konkret vurdering er hensigtsmæssigt bør dialogen om udmøntningen af beskyttelsesniveauet indenfor forskellige brancheområder lige-

ledes foregå åbent.

For mindre eller små virksomheder, der ikke er fremtrædende i en branches erhvervsprofil, spiller offentlig omtale en mindre rolle, og det er på mange måder disse virksomheder, der udgør det store problem i den faktiske databeskyttelsesret. Dette skyldes selvsagt også, at mere aktiv kontrol af disse er så ressourcekrævende, at det ikke er praktisk muligt at gennemføre denne. Som det omtales nærmere nedenfor, er det i forhold til disse virksomheder i særlig grad brancheorganisationer og lign., der må være »sparringspartner« i den praktiske udvikling af databeskyttelsesretten.

6 Lovgivning

Blandt de anvendelige reguleringsmetoder er det naturligt at starte med at omtale lovgivning og andre former for formelt nedskrevne regler, udstedt af offentlige myndigheder. Som det er indiceret forskellige steder i denne bog, er det på den ene side væsentligt, at sådanne regler udstedes, idet de udgør det naturlige udgangspunkt for databeskyttelsesretten, men på den anden side må det konstateres, at denne form for »black letter law« ikke er tilstrækkelig til at sikre det tilsigtede databeskyttelsesniveau.

Dette skyldes ikke blot det brede reguleringsområde med heraf affødte retshåndhævelsesproblemer, men tillige at en række af de fundamentale felter i databeskyttelsesretten ikke lader sig formidle på en tilstrækkeligt præcis måde ved hjælp af det juridiske regelsprog. I forhold til især regler om registrering og videregivelse vil det ofte være nødvendigt at benytte sig af retlige standarder. Der lægges herved til grund, at det ikke er hensigtsmæssigt eller ønskeligt at gøre alle former for databehandling afhængig af samtykke, og at det ikke er muligt ved anvendelse af en kasuistisk lovform, dvs. en opregning af samtlige legitime situationer, at indkredse hele området, hvorfor anvendelsen af standarder bliver nødvendig.

Disse forhold indebærer, at lovgivningen ikke kan stå alene, og at der overlades et relativt stort frirum til praksis. Dette er som nævnt uundgåeligt, men bør ikke misforstås således, at lovgivning

dermed bliver overflødig. Det er fortsat væsentligt, at lovgivningsmagten ud fra en samlet bedømmelse af de involverede interesser fastlægger det basale grundlag for databeskyttelsesretten, og at dette grundlag således danner udgangspunkt for den øvrige regulering, hvis funktion er at supplere og berige reguleringen med henblik på at forbedre dennes effektivitet.

Det bør tilføjes, at disse antagelser om anvendeligheden af lovgivning på dette område gælder, uanset om der anvendes almindelige, generelt dækkende regler eller bestemmelser, der er orienteret mod særlige sektorer og brancher. I de sidstnævnte situationer kan der på nogle punkter opnås en højere grad af præcision, men ej heller her kommer man uden om de retlige standarder. Dette eksemplificeres i øvrigt både af den sektororienterede lovgivning, der findes her i landet, og af de rekommandationer, der over årene er udstedt i Europarådets regie på grundlag af den generelle databeskyttelseskonvention. Det konstateres derfor, at ej heller sektororienteret lovgivning kan stå alene, men som skitseret ovenfor må suppleres med andre former for regler.

7 Markedet

I den private sektor er alternativet til lovregulering at overlade fastlæggelsen af beskyttelsesniveauet til markedet og de normsæt, som konkurrenceforholdene driver frem. Som allerede tidligere angivet, er dette ikke nogen farbar vej, men dette synspunkt fortjener en vis uddybning. Den frie markedsregulering er på mange måder et forældet udgangspunkt, idet det er en alment accepteret erkendelse, at denne regulering fører til uligheder og uretfærdigheder, der ikke er acceptable i et moderne civiliseret samfund. Uanset at grundsætningen om kontraktfrihed stadig er et accepteret udgangspunkt for privatretlig regulering, er der i nutiden tale om en grundsætning, der er underlagt mange modifikationer. Det er almindeligt anerkendt, at en lovregulering er påkrævet for at undgå, at der opstår uligheder og misbrug af økonomiske magtpositioner på markedet.

De områder, hvor markedets egne reguleringsmekanismer kan

spille en rolle, karakteriseres ved, at konkurrenceforholdene i sig selv tilsiger en vis orden og en koordineret praksis. Uanset den øgede økonomiske betydning, som persondata har, kan databeskyttelsen ikke henføres til det område, som markedet frit kan regulere. Det forekommer derfor ikke betryggende eller i og for sig hensigtsmæssigt at lade markedet være det styrende element i reguleringen. Som der redegøres nærmere for nedenfor, er dette ikke ensbetydende med, at den private sektor ikke har en selvstændig rolle i reguleringen, blot at den ikke fuldstændigt kan overlades til denne sektor.

8 Selvregulering

Særligt i Holland er den databeskyttelsesretlige regulering opbygget således, at der i lovgivningen er fastsat en række hovedprincipper, hvorefter disse udmøntes i regelsæt udformet af de enkelte brancher i samarbejde med tilsynsmyndigheden og så vidt muligt repræsentanter for de registrerede, dvs. forbrugerorganisationer og lign. En form for selvregulering indgår således som en integreret del af den samlede regulering, hvilket kan begrundes med, at der dels dermed kan opbygges en sektororienteret regulering, dels at regler, som de dataansvarlige virksomheder selv har været med til at udforme, med større grad af sandsynlighed vil blive overholdt af disse. Modellen indebærer endvidere, at særlige forhold eller hensyn, som det kan være vanskeligt for lovgivningsmagten at indkredse fuldt ud eller at integrere i en almindelig lovgivning, kan blive inddraget.

Det forekommer umiddelbart at være fornuftigt at inddrage de implicerede parter i regelfastsættelsen, eftersom dette styrker sandsynligheden for dennes effektivitet. Afklares må derfor, hvorledes dette gøres på den mest adæquate måde. Udgangspunktet bør være, at der i den almindelige lovgivning først gives en så udtømmende regulering som muligt, idet denne regulering udformes under inddragelse af alle interesserede brancher. I loven gives der hjemmel til, at udfyldende brancheorienterede normer kan udstedes, og staten stiller en offentliggørelsesprocedure til rådighed for disse normer.

På dette grundlag, der nok vil komme til at svare til det kommende EU-direktiv,[4] er det tilsynsmyndighedens opgave at tilskynde de enkelte brancher til at udforme regelsæt, herunder codes of conduct, og til at medvirke til etableringen af rammer, hvorindenfor alle interesserede parter kan indgå i en dialog omkring normernes udformning. Det er i denne forbindelse væsentligt, at alle betydende virksomheder på det pågældende område bliver aktivt inddraget. Det er afgørende, at der bliver bred enighed og forståelse for det regelsæt, der bliver udformet.

Gennemføres en sådan proces, vil der være etableret et regelsæt, der på en produktiv måde vil kunne indgå i den samlede regulering af persondatabeskyttelsen, og som kan danne grundlag for yderligere virksomhedsorienteret regulering, jfr. nærmere hertil nedenfor. Som også fremhævet tidligere, vil inddragelse af denne form for regulering stille store krav til tilsynsmyndighedens kompetence og fleksibilitet, hvorfor der yderligere er grund til fremover meget nøje at overveje og vurdere denne myndigheds organisering i bred forstand.

9 Dataetik

Ved siden af de egentlige retlige regler vil normer af moralsk og etisk karakter også kunne spille en rolle i den samlede regulering. Databeskyttelsesretten formidler en opfattelse af det enkelte menneskes position i samfundet og gør det bl.a. som tidligere fremhævet ved hjælp af retlige standarder. Disses nærmere fastlæggelse og dermed præciseringen af gældende ret er et juridisk anliggende, men i forhold til praktiseringen af de fastlagte regler er der ikke tvivl om, at holdningen til de grundlæggende ideologiske normer har betydning. Dette er ligeledes tilfældet i de situationer, hvor der foreligger flere praktiske valgmuligheder i henseende til realiseringen af de gældende regler. Et eksempel herpå kan være bestemmelser om datakvalitet.

En dataetisk holdning er ikke noget, man kan fastsætte ensidigt.

4. I direktivudkastet 1992 fastlægger artikel 28 og 29 en ramme for branchenormer både på nationalt og på EU niveau.

Tværtimod må sådanne normer vokse frem via diskussion og dialog med udgangspunkt i relationen virksomhed og menneske. Der er i en vis forstand tale om en uddannelsesmæssigt orienteret proces. Denne proces fører ideelt frem til en dataetisk bevidsthed med et øget opmærksomhedsniveau i de dag-til-dag situationer, hvor databeskyttelsesmæssige spørgsmål opstår.

Det er ønskeligt, at en sådan proces igangsættes og vedligeholdes. Dette kan ske på branche- eller virksomhedsniveau og understreger betydningen af, at der udarbejdes materiale, der kan danne grundlag for denne diskussion. Dette betyder ikke, at indoktrinering anbefales som middel, men derimod at åben debat og refleksion, relateret til praktisk orienterede situationer, må anses for at være et væsentligt middel i den samlede reguleringsvifte. I et samarbejde mellem brancheorganisation og tilsynsmyndighed vil et grundlag for oparbejdelsen af en dataetik kunne etableres. En væsentlig og central opgave i henseende til sikringen af det faktiske beskyttelsesniveau.

10 Virksomhedsinterne regler

Disse betragtninger fører frem til en fremhævelse af betydningen af virksomhedsinterne regler. Disse regler, der skal tjene som vejledning for de ansatte, bør regulere den persondatabehandling, der konkret skal praktiseres i den pågældende virksomhed. Reglerne har dermed til formål at udmønte den øvrige regulering i bestemmelser, der er udformet ud fra en viden om virksomhedens aktiviteter. Et sådant regelsæt kan betragtes som et ledelsesinstrument, der skal sikre, at virksomheden faktisk har en forsvarlig praksis, der værner det renommé og den position, virksomheden har på markedet. Regelsættet fastlægger således de ansattes forpligtelser på dette område og kan på dette grundlag indgå i den virksomhedsinterne uddannelse af de ansatte.

Det vil afhænge af reglernes specifikationsgrad, sammenholdt med produktionens følsomhed, herunder forholdet til konkurrerende virksomheder, i hvilket omfang disse regler kan gøres offentligt tilgængelige. Dette vil være ønskeligt, men er dog ikke påkræ-

vet for, at reglerne kan opfylde deres funktion. Som påpeget i kapitel 6 er der behov for en offentlig tilgængelig databehandlingspolitik på virksomhedsniveau, men det er ikke absolut ønskeligt, at denne omfatter alle de interne regler. I relationen offentlighed og virksomhed er det ønskeligt at være åben overfor en vis fleksibilitet og ikke indtage firkantede holdninger.

I forbindelse med udformningen af de interne regler kan det være hensigtsmæssigt at etablere en dialog med tilsynsmyndigheden, der ikke har til formål, at myndigheden skal godkende reglerne, men kan medvirke til, at de udformes bedst muligt i overensstemmelse med de intentioner, der har været motiverende for den øvrige regulering. Tilsynsmyndigheden må derfor være gearet til at kunne indgå i en sådan dialog og selvsagt tildeles ressourcer, der gør en sådan funktion praktisk mulig. I denne sammenhæng bør ligeledes fremhæves, at de enkelte brancheorganisationer har en vigtig opgave i at formidle det ønskelige i intern regulering til deres medlemsvirksomheder.

10.1 Organisering

På virksomhedsniveau er det ønskeligt, at det nævnte regelsæt kobles til en organisering af området. Der bør således være opbygget en struktur med ansvar for virksomhedens databeskyttelsespolitik. Den nærmere udformning af denne struktur vil variere fra virksomhed til virksomhed, men en vigtig ingrediens er, at en person er udpeget som persondataansvarlig. Denne bør være placeret på et forholdsvis højt niveau i virksomheden og under alle omstændigheder have reference direkte til ledelsen. Denne person vil være ansvarlig for, at de virksomhedsinterne regler bliver implementeret, og vil yderligere kunne varetage virksomhedens interesser eksternt i forhold til myndigheder og offentlighed.

Med baggrund i denne strukturs store praktiske betydning bør det i lovreguleringen fastsættes, at der i virksomheder, i det mindste af en vis størrelse, skal være en persondataansvarlig, der naturligvis godt kan have andre arbejdsopgaver ved siden af. En sådan regel kan ikke betragtes som en unødvendig eller intensiv indtrængen i virksomhedernes interne drift. På andre områder, f.eks. indenfor arbejdsmiljøretten, findes tilsvarende ordninger.

11 Reguleringsvifte

Samlet kan det på baggrund af de gjorte bemærkninger fastslås, at det er et bredt spektrum af reguleringsmidler, der er påkrævet for, at databeskyttelsesretten skal blive en succes forstået på den måde, at et acceptabelt databeskyttelsesniveau faktisk eksisterer. Det er væsentligt, at denne regulering bliver til i åbenhed og med inddragelse af alle de aktører, der har interesser på området. Det er derfor en krævende regulering, der ikke overstås ved ensidig regelfastsættelse. Et væsentligt budskab er således, at flotte ord og formuleringer ikke er tilstrækkelige, men at det kræver hårdt og vedvarende arbejde at sikre databeskyttelsen.

Oparbejdelsen af en forståelse for beskyttelsesorienterede rammer for databehandlingen er en central målsætning. Som tidligere påpeget er det vigtigt, at denne forståelse er nuanceret og ikke ensidigt fokuserer hverken på det enkelte menneske eller på de databehandlende virksomheder. Ved aktiv inddragelse af alle aktører er der mulighed for at opnå den afbalancering af den samlede regulering, der i sidste instans betinger dennes succes. Selv om dette måske kan forekomme banalt, er det denne afbalancering, der i alle de forskellige dele af databeskyttelsesretten må være i centrum og være styrende for den regulering, der gennemføres.

Databeskyttelsen er afhængig af den samfundsmæssige og teknologiske udvikling. Reguleringsmiljøet er derfor under stadig forandring. Der er til stadighed behov for justeringer og tilpasninger, ligesom nye reguleringsspørgsmål opstår. I denne fortsatte udvikling af databeskyttelsen er det væsentligt, at hele reguleringsviften og alle implicerede aktører inddrages. De løsninger, der nås, må være fastsat ud fra denne totalitet, og det er derfor særlig vigtigt at undgå hurtige og ikke tilstrækkeligt gennemtænkte regler. Alene ved en sådan omhyggelighed er det muligt konstant at fastholde en forsvarlig og realistisk persondatabeskyttelse.

Efterskrift

Den retspolitisk orienterede gennemgang af persondatabeskyttelsen i den private sektor i de forrige kapitler illustrerer, at problemstillingerne har en betydelig bredde og omfatter meget varierede situationer. Retsområdet omfatter hele den private sektor og har mere eller mindre følelig betydning for alle former for virksomheder. Det er dermed et reguleringsområde, der er relateret til erhvervsudøvelsen i bred forstand. Samtidig er der tale om en regulering, der har været i fremmarch siden den første registerlov i 1978 og især siden den vidtgående lovrevision i 1987 har fået stadig større betydning for erhvervslivet.

Det er karakteristisk, at denne fremmarch i betydeligt omfang er sket uformidlet i den forstand, at der ikke er gjort nogen tilstrækkelig systematisk indsats for at formidle de grundlæggende hensyn, der ligger bag den gennemførte regulering. Denne opfattes da også fortsat af mange i den private sektor som uberettiget og som et unødvendigt snærende bånd på erhvervsudøvelsen. Konsekvensen heraf er, at der på mange områder foreligger et ufrugtbart miljø for den databeskyttelsesretlige diskussion.

Dette er i sig selv uheldigt, men er særlig problematisk i lyset af den forestående retspolitiske debat om fremtidens lovgivning, der inden længe må forventes at blive udløst af implementeringen af det EU-direktiv, hvis vedtagelse nærmer sig. Uanset udfaldet af den politiske diskussion omkring direktivet og uanset, om dette ender med at prioritere harmonisering eller subsidiaritet, vil det grundet karakteren af den databeskyttelsesretlige reguleringsgenstand i et vist omfang betjene sig af retlige standarder. Der vil dermed være åbnet for en implementeringsfrihed, der indebærer, at det ikke bliver en instrumentel, mekanisk opgave at omsætte direktivet til dansk ret, men at dette, omend med et bundet udgangspunkt, bliver en selvstændig retspolitisk opgave.

Dette retspolitiske projekt er vidtspændende og omfatter ikke blot selve registerloven, men tillige den øvrige lovgivning, hvori databeskyttelsesretlig regulering indgår. I den private sektor vil betalingskortloven særligt være i fokus. Der vil blive tale om en bred retspolitisk debat, hvor det gælder om »at holde tungen lige i munden«. Det vil blive en debat, hvor der kræves et højt opmærksomhedsniveau fra brancheorganisationer og andre interessenter i den private sektor.

Med henblik på, at der i den kommende lovgivning fastlægges et databeskyttelsesniveau, der både er betryggende for det enkelte menneske og er afbalanceret over for de erhvervsmæssige og hertil knyttede samfundsmæssige interesser, er det ønskeligt, at den retspolitiske afklaring kan ske i et miljø, der ikke præges af positioner, der forsvares bag bastioner og skyttegrave, uden at en egentlig dialog foregår. En sådan situation vil på sigt i sig selv undergrave det beskyttelsesniveau, der fastsættes.

Det ønskværdige i, at der eksisterer rammer, der fremmer muligheden for en frugtbar dialog, har været baggrunden for den måde, den retspolitiske drøftelse i denne bog har været tilrettelagt på. Det er blevet set som centralt at fremhæve, at de databeskyttelsesretlige regler ikke med nogen nødvendighed er ensidige, og at de ikke per se er vendt mod erhvervslivet eller er erhvervsfjendske. Tværtimod er der i betydeligt omfang tale om en regulering, der kan have en positiv erhvervsmæssig betydning ved at fremme lige konkurrencebetingelser på et område, der ikke direkte er forbundet med den enkelte virksomheds produktion. Samtidig kan reguleringen medføre, eller måske mere moderat og realistisk fremme et miljø, der ved at styrke de enkelte virksomheders renommé og status på markedet er præget af tillid mellem erhvervsliv og forbrugere. Som udgangspunkt er generel erhvervsmæssig modstand mod denne regulering dermed uigennemtænkt og ufornuftig.

Den anden side af denne mønt har været en stadig betoning af nødvendigheden af afbalancering. Det er ikke hensigtsmæssigt eller ønskeligt, at reguleringen udformes på en måde, der ensidigt anskuer reglerne som beskyttelsesorienterede og ikke tager hensyn til de berettigede interesser, som de persondataanvendende virksomheder har. Det må tages alvorligt, at persondata har en økonomisk, kommerciel og erhvervsmæssig betydning. Det må reelt ta-

ges i betragtning, at der er en selvstændig samfundsmæssig interesse i, at erhvervslivet kan integrere persondata i sin kommercielle profil. Dette har en overordnet økonomisk betydning for danske virksomheders konkurrenceevne og har dermed samfundsøkonomisk betydning. Dette udgangspunkt betyder, at det ved udformningen af de enkelte regler må tages i betragtning, hvorvidt den risiko for integritetskrænkelser og privatlivsindtrængning, som reguleringen skal forebygge, er reel, og om de midler til forebyggelse, der tages i anvendelse, er adæquate i forhold hertil og udformes med reel hensyntagen til legitime behov for persondataanvendelse. Afbalancering er således en afgørende kvalitet ved den fremtidige databeskyttelsesret.

Disse bemærkninger skal ikke misforstås således, at beskyttelsen af det enkelte menneskes integritet nedprioriteres. Denne beskyttelse er fortsat det overordnede formål med reguleringen og er også hovedårsagen til, at der overhovedet lovgives. Det er nødvendigt at have et klart blik for, at integritetsbeskyttende regler er nødvendige, såfremt informationssamfundet skal være et civiliseret samfund baseret på respekt for det enkelte menneske. Det må erkendes, at regulering er nødvendig, og at beskyttelse ikke kommer af sig selv eller med nogen nødvendighed følger af de almindelige markedsmekanismer. Det er ikke hensigten her at antaste dette udgangspunkt. Det, der advokeres, er blot en kølig og velovervejet implementering med stor vægt på, at reguleringen bliver realistisk og dermed ikke bliver til flotte programerklæringer, der ikke kan blive til praktisk virkelighed.

Den retlige regulering må nødvendigvis føre til begrænsninger i den frie erhvervsudøvelse og til, at enhver form for teknologisk innovation ikke kan appliceres. Sådanne virkninger er i en vis forstand uundgåelige, og det er netop derfor, at det altid meget nøje må overvejes, om de konkrete begrænsninger, når alle aspekter er analyseret, er påkrævede for at opnå den nødvendige integritetsbeskyttelse. En sådan velovervejet regulering kræver imødekommenhed fra alle parter i den retspolitiske proces og kan opfattes som en beskrivelse af en idealtilstand, der ikke er helt realistisk. Dette må erkendes, også fordi retspolitik ikke blot er teknik, men netop er politik, der ikke er objektiv, men udtrykker valg mellem divergerende muligheder, der ikke i sig selv er rigtige.

Selv om det derfor ikke kan forventes, at den retspolitiske proces vil leve op til den idealtilstand, der er beskrevet her, er det ud fra erkendelsen af de vanskeligheder, som databeskyttelsen i praksis konfronteres med, jfr. kapitel 10, at den er fremhævet. Det er henimod åbenhed og eftersøgning af holdbare, afbalancerede løsninger, at den retspolitiske proces må søge. Det er nødvendigt at indgå kompromiser, men samtidig må det sikres, at disse ikke bliver forfladigelser, således at der fortsat er tale om en klar og sammenhængende regulering.

Den retspolitiske debat om implementeringen af EU-direktivet i dansk ret vil være af særlig betydning, fordi det er sandsynligt, at der vil gå lang tid, inden Pandoras æske pány åbnes. Det har været ekstraordinært besværligt at få gennemført direktivet, og det er naturligt, at der efter at dette er lykkedes vil være en betydelig træthed og en betydelig uvilje mod at foretage ændringer i dette. I mange år fremover vil denne sag være lukket, og det tilsvarende vil være tilfældet på det nationale plan. Selv om den teknologiske udvikling vil sætte nye spørgsmål på dagsordenen, vil det almindelige grundlag for databeskyttelsesretten være fastlagt i mange år. Dette er en yderligere grund til, at de forskellige brancher i de nærmest liggende år bør være særligt opmærksomme på de databeskyttelsesretlige spørgsmål og være bevidste om, at brug af ressourcer på dette område er en god investering. Den nye databeskyttelsesretlige lovgivning vil gælde i mange år og lægge en forholdsvis vedvarende ramme om den øvrige regulering og den udfyldende praksis. Fremtiden er tæt på, og i de nærmeste år fastlægges den grundlæggende databeskyttelsesret ind i det næste årtusind.

Selv om det almindelige grundlag for databeskyttelsesretten således vil blive lagt fast, er dette ikke ensbetydende med, at nye reguleringsspørgsmål ikke vil opstå. Den informationsteknologiske udvikling er meget hurtig og innovativ. Der opstår til stadighed nye muligheder for persondatabehandling, og nye udfordringer til retssystemet præsenteres. Der kan kun gisnes om denne udvikling, og det er velkendt, at forudsigelser på dette område er endog meget usikre. Der vil fremkomme overraskelser og teknologiske muligheder, vi ikke i dag kan forudse. Selv om et kapitel lukkes, vil mange nye fremover blive påbegyndt. Databeskyttelsesretten vil være i fortsat udvikling, og nye retspolitiske spørgsmål i forhold til

lovgivning eller praksis vil opstå.

På denne baggrund er det sandsynligt, at databeskyttelsesretten fortsat vil være i centrum for styringen af informationssamfundet, og at et konstant opmærksomhedsniveau vil være påkrævet. Det vil til stadighed være nødvendigt at sikre, at retssystemet er på højde med udviklingen, og at der gennem alle omskifteligheder fortsat findes et retsværn, der sikrer en betryggende beskyttelse af det enkelte menneskes integritet og privatliv.

Forkortelser

EFT = EF-Tidende

RÅ = Registertilsynets Årsberetning

UfR = Ugeskrift for Retsvæsen

Lovfortegnelse

Lov nr. 274 af 22.9.1908 om forældelse af visse fordringer
Lovbekendtgørelse nr. 622 af 2.10.1987 om private registre m.v.
Lovbekendtgørelse nr. 886 af 23.12.1987 om visse forbrugeraftaler
Lov nr. 245 af 22.4.1991 om ændring af lov om revisionen af statens regnskaber m.m.
Lovbekendtgørelse nr. 654 af 20.9.1991 om offentlige myndigheders registre
Lov nr. 281 af 29.4.1992 om ændring af tinglysningsloven og retsafgiftsloven m.v.
Lov nr. 285 af 29.4.1992 om Den Europæiske Menneskerettighedskonvention
Lov nr. 337 af 14.5.1992 om offentlige arkiver m.v.
Lovbekendtgørelse nr. 464 af 15.6.1992 om betalingskort m.v.
Lovbekendtgørelse nr. 530 af 19.6.1992 om Det Centrale Erhvervsregister
Lov nr. 504 af 30.6.1993 om aktindsigt i helbredsoplysninger

Litteratur

Peter Blume:
Personregistrering (2. udg. Akademisk Forlag, København 1992)
Udviklingstræk i dansk databeskyttelsesret, Retsvidenskabeligt Institut B. Studier nr. 45 (København 1992)
Schengen og persondatabeskyttelsen, Social Kritik nr. 22/23 (1992) p 64-71.
Koncerner i registerretlig belysning, Ugeskrift for Retsvæsen 1993 p 392-98.
Den interne regulering af databeskyttelsen, Juristen 1993 p 337-46.
Adgang til helbredsoplysninger, Retsvidenskabeligt Institut B. Studier nr. 54 (København 1994) p 25-36.
Direkte markedsføring og integritetsbeskyttelse, Ugeskrift for Retsvæsen 1994 p 163-69.

Lars Hedegaard Kristiansen:
Tavshedspligt og koncerndannelser i den finansielle sektor, Juristen 1993 p 224-34.

Alf Ross:
Om ret og retfærdighed (København 1953)

Jakob Sand, Jens Engbjerg:
Teledemokrati (Teknologinævnet, København 1993)

Marcus Schmidt:
Direkte demokrati i Danmark (København 1993)

Teknologinævnet:
Hvem ved hvad – og bør de det? (København 1993)

Samuel D. Warren, Louis D. Brandeis:
The right to privacy, Harvard Law Review 1890 p 193-200.