driver og justerer resultatet på grunnlag av 15 andre kostnadsdrivere. Andre eksempler er SLIM – se Putnam (1978), COPMO – se Conte et al. (1986) og Function Point – se Garmus & Herron (2000). Se Walkerden & Jeffery (1997) for en oversikt over kalkylemodeller.

På 1980-tallet ble mange av de da tilgjengelige metodene bygd inn i kommersielt tilgjengelige estimeringsverktøy. Samtidig viste det seg at de ulike modellene ga svært sprikende resultater og ikke kunne brukes rått utenfor de miljøene de opprinnelig var kalibrert for.

Følgen var at vi på 90-tallet fikk en rekke forslag til metoder basert på andre prinsipper enn kalkylemodeller. Et eksempel er lærende estimeringssystemer – se Jørgensen (1995), Srinivasan & Fisher (1995), Finnie et al. (1997). Et annet eksempel er analogimodeller – se Shepperd & Schofield (1997) og Walkerden & Jeffery (1999). Et eksempel på en analogibasert modell er ANGEL – se Shepperd, Chofield et al. (1996).

I tillegg har det vært forsket på effekten av å kombinere historiske data og ekspertvurderinger – se Höst & Wohlin (1998), Stensrud & Myrtveit (1998) og Chulani et al. (1999), og på hvordan eksperter egentlig tenker – se Briand et al. (1998). Disse forskningsretningene vil trolig få stor betydning for estimeringsfaget i årene som kommer.

Kapittel 17

Jus og etikk

Av Dag Wiese Schartum[58] (jus, avsnitt 17.1 til 17.6)
og Gerhard Skagestein (etikk, avsnitt 17.7)

I dette kapitlet skal vi se på skrevne og uskrevne regler som virker inn på systemutviklingen. Vi begynner med rettsreglene, dvs. lovverket, og fortsetter med de etiske reglene.

Kapitlet gir ingen uttømmende oversikt – vi har tatt med det vi mener er viktigst for en systemutvikler å kjenne til. Målet er å sette deg i stand til å kjenne igjen situasjoner det kan være knyttet rettsspørsmål eller etiske spørsmål til. Den konkrete analysen og løsningen av rettsspørsmålene må vi imidlertid ofte overlate til juristene.

17.1 Rettsregler som innhold og ramme

Rettsregler kan virke inn på utvikling av informasjonssystemer i hovedsak på to måter.

Rettsregler kan virke inn på utvikling av informasjonssystemer på to ulike måter: Et informasjonssystem kan inneholde representasjoner av rettsregler, og rettsregler kan sette krav til hvordan utviklingsarbeidet skal gjennomføres.

For det første kan informasjonssystemet inneholde *representasjoner av rettsregler.* Dette er for eksempel tilfellet dersom vi skal lage en database med informasjon vi trenger for å treffe vedtak i henhold til et regelverk. Tilsvarende er situasjonen dersom vi programmerer rettsregler slik at vedtak kan automatiseres. I slike tilfeller er det i stor grad rettsreglene som bestemmer innholdet av datamodeller, programkode mv. De fleste regler har bare interesse for bestemte informasjonssystemer. For eksempel har lov og forskrift vedrørende lån og stipend fra Lånekassen primært interesse for de som skal utvikle systemløsninger for Lånekassen. Noen rettsregler har et mye bredere virkeområde: For eksempel gjelder personopplysningsloven for alle systemer som behandler "personopplysninger", og forvaltningsloven gjelder for alle forvaltnings-

58. Avdeling for forvaltningsinformatikk, Universitetet i Oslo

organer. Det er imidlertid ikke så vanlig å automatisere slike generelle regler.

For det andre kan det være gitt regler som setter krav til de prosedyrer og arbeidsmåter, aktiviteter mv. som må følges når informasjonssystemer skal utvikles, og som setter rammer for hvilke valg utviklere kan gjøre. I noen tilfeller må vi for eksempel ha tillatelse før vi kan etablere en persondatabase, eller følge visse fremgangsmåter som åpner for arbeidstakeres medvirkning, eller avstå fra å bruke et materiale fordi det er opphavsrettigheter knyttet til det.

I dette kapitlet vil vi først og fremst være opptatt av rettsregler som rammer for utviklingsarbeider, men også enkelte krav til rettslig innhold i informasjonssystemer vil bli tatt med.

17.2 Behandling av personopplysninger

17.2.1 Når gjelder personopplysningsloven for utviklingsarbeidet?

Personopplysningsloven gjelder for alle informasjonssystemer som omfatter opplysninger som kan føres tilbake til enkeltindivider.

Dersom det planlagte informasjonssystemet skal inneholde personopplysninger, gjelder bestemmelsene i *personopplysningsloven*[59]. "Personopplysninger" er opplysninger som direkte eller indirekte kan knyttes til en fysisk person. Opplysninger om navn, adresse mv. er klare eksempler på personopplysninger. En opplysning om at brukeren av en maskin med et bestemt IP-nummer har benyttet en nettjeneste, eller at føreren av en bil med et bestemt registreringsnummer har passert et trafikkovervåkningskamera, vil imidlertid ofte også være en personopplysning fordi det er mulig å knytte Internett-bruken og bilen til en eller flere bestemte personer. En opplysning kan altså være "personopplysning" selv om det er flere ledd mellom opplysningen og personen(e).

Personopplysningsloven regulerer "*behandling*" av personopplysninger. All elektronisk behandling er omfattet, også dersom den er bare delvis elektronisk. Videre gjelder loven for alle personopplysninger som er ført inn eller skal føres inn i et "register", dvs. i en systematisk lagret fortegnelse. Det spiller ingen rolle om personopplysningen fremkommer som

59. En mer inngående forklaring av personopplysningsloven er gitt i Schartum og Bygrave; "Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger", Fagbokforlaget 2004, s. 101–181.

skrift, bilde, lyd eller på annen måte; hele loven gjelder uansett dersom behandlingen er elektronisk eller gjelder et register. For videoovervåking (eksempelvis med web-kamera) gjelder egne supplerende regler.

Begrepet "behandling" er viktig i mange av lovens bestemmelser, og kan ofte oversettes til "et sammenhengende behandlingsopplegg", med andre ord et informasjonssystem. En behandling refererer altså ikke til hver gang det blir behandlet konkrete personopplysninger, men til et generelt opplegg for behandlingen. Således vil for eksempel all behandling av personopplysninger knyttet til et lønns- og personalsystem være "en behandling", mens all behandling av personopplysninger som er knyttet til et nettsted, vil være en annen behandling osv.

Kort sagt vil enhver utvikling av informasjonssystemer som inneholder personopplysninger, komme inn under personopplysningsloven, som dermed blir en viktig ramme for utviklingen av mange systemer. Uansett hva slags manipulering av slike data som skal skje i systemet, vil det være tale om "behandling" av personopplysninger i lovens forstand. Dersom bestemmelsene ikke følges, kan det innebære erstatningsansvar og kostbare krav til endring av en eksisterende systemløsning.

Loven gjør viktige unntak for behandling av personopplysninger for rent private eller personlige formål og for behandling der formålet utelukkende er kunstnerisk, litterært eller journalistisk, herunder opinionsdannende. For det første unntaket er tommelfingerregelen at dersom du behandler personopplysninger i samband med en jobb eller et verv, må du ta hensyn til loven. Men selv i privatlivet kan loven komme til anvendelse; for eksempel dersom du åpent legger ut private personbilder på nettet. Det andre unntaket gjelder for eksempel systemløsninger der folk slipper til med sine meninger i et nettbasert debattforum. I slike unntakstilfelle er det store deler av loven som ikke gjelder.

17.2.2 Krav til rettslig grunnlag for å behandle personopplysninger

For at det skal være lovlig å ta i bruk en informasjonssamling (database, register) som inneholder personopplysninger, må den som er *"behandlingsansvarlig"* for denne personinformasjonen, sørge for at visse grunnkrav er oppfylt. Med "behandlingsansvarlig" sikter loven til den som har rett til å bestemme hva opplysningene skal brukes til og hvilke hjelpemidler som skal benyttes. Det er primært den behandlingsansvar-

lige som har plikter etter loven. I et systemutviklingsprosjekt vil det være oppdragsgiver eller systemeier som har denne rollen.

Loven stiller opp tre grunnkrav som alle informasjonssystemer der personopplysninger inngår, må etterleve:

Tre grunnkrav for informasjonssystemer som omfatter personopplysninger: Et rettslig grunnlag for behandlingen, et formål med behandlingen, og tilfredsstillende kvalitet på opplysningene.

- Det må være et *rettslig grunnlag* for behandling av personopplysningene
- Det må være fastsatt et *formål* for behandling av personopplysningene
- Personopplysningene må tilfredsstille visse grunnleggende krav til *kvalitet*

Kravet til rettslig grunnlag innebærer at personopplysningene må kunne behandles på grunnlag av:

Det rettslige grunnlaget kan være basert på lovhjemmel, samtykke eller nødvendighetsgrunner.

- *lovhjemmel* eller
- *samtykke* eller
- en av de *nødvendighetsgrunner* som er regnet opp i loven (§ 8 og § 9)

At det eksisterer en lovhjemmel for å behandle personopplysninger betyr at det står i en lov eller forskrift at det skal/kan samles inn personopplysninger. Sentrale eksempler her er lover om folkeregistrering, strafferegistrering, krav til rapportering ved mistanke om hvitvasking mv. Poenget er at lovgiver har bestemt at personopplysninger skal samles inn og behandles. Mange systemløsninger innen offentlig sektor vil helt eller delvis ha et slikt grunnlag i lov eller forskrift.

Dersom lovhjemmel mangler, kan personopplysninger behandles forutsatt at hver og en av de det skal behandles opplysninger om, har gitt sitt *samtykke* til behandlingen.

> Universitetet ønsker for eksempel å legge ut informasjon på nettet om studenter som deltar i et kurs. Dersom universitetet mangler lovhjemmel, må det spørre hver enkelt student. Hver student må i så fall kunne nekte universitetet å legge ut bestemte opplysninger. Universitetet bør derfor være forsiktige med å planlegge obligatorisk bruk av personopplysninger i et kurs (noen studenter vil for eksempel nekte å la seg avbilde på en nettside som skal opprettes som del av et kurs i webdesign).

For at et samtykke skal være gyldig, må visse krav etterkommes. Samtykket må være:

- frivillig (ikke et resultat av tvang eller press) og
- informert (det må gis full informasjon om den planlagte bruken av opplysningene), og
- uttrykkelig (det må være klart at samtykket er gitt, dvs. det må foreligge en underskrift, opplysninger i en logg eller liknende som viser at vedkommende har godtatt behandlingen)

Dersom det verken foreligger lovhjemmel eller samtykke (pga. motstand, praktiske vanskeligheter mv.), er den siste muligheten å hevde at behandlingen av personopplysninger faller inn under ett av de tilfellene der loven tillater behandling fordi den må anses å være "nødvendig". Det mest aktuelle her er tilfeller der behandling av personopplysninger er nødvendig for å oppfylle eller forberede en avtale med den registrerte. Den som utvikler en rutine for bestilling av varer eller tjenester over nettet, kan altså gjøre bruk av alle opplysningstyper som er nødvendige for å gjennomføre handelen. Dersom andre opplysninger som ikke er nødvendige, skal med, (kjønn, alder, interesser mv.), må dette derimot være basert på samtykke fra den enkelte. Den som gir samtykke, kan når som helst fritt trekke samtykket tilbake. Derfor bør informasjonssystemet lages slik at opplysninger om hver person lett kan spores og slettes, og at opplysninger som er "nødvendige", kan behandles atskilt fra de opplysningene som er basert på samtykke.

For lovlig å kunne behandle personopplysninger som loven definerer som "sensitive", må det gjennomføres separate vurderinger av det rettslige grunnlaget for å behandle slike opplysninger. Det betyr for eksempel at det må innhentes samtykke som spesielt gjelder de sensitive opplysningene. Hva som regnes som sensitivt, framgår av loven og omfatter for eksempel opplysninger om straff, rase, etnisitet, helse, seksuelle forhold og religion. Det er nok at én opplysningstype er sensitiv for at særreglene om sensitive opplysninger skal komme til anvendelse.

Vanligvis må det søkes konsesjon fra Datatilsynet før sensitive opplysninger kan behandles. Det kan innebære en stor risiko å påbegynne et slikt utviklingsarbeid dersom det er tvilsomt om slik konsesjon vil bli gitt, og dersom det er ukjent hvilke vilkår som eventuelt vil bli stilt.

17.2.3 Krav til angivelse av formål for behandling av personopplysninger

Tidlig i utviklingsarbeidet, og senest 30 dager før systemet er ferdig utviklet og behandling av personopplysninger begynner, må det være fast-

satt ett eller flere formål for behandlingen. Vi må altså beskrive hva opplysningene skal brukes til. Slike formål spiller en avgjørende rolle ved innhenting av samtykke (fordi den enkelte skal informeres) og ved vurdering av hvilke krav til kvalitet som må stilles til personopplysningene, jf. neste avsnitt.

Et formål kan endres, men endringsadgangen er begrenset. Forenklet kan vi si at dersom et informasjonssystem er laget for å samle inn opplysninger om personer for å tilby dem fordeler eller tjenester, kan ikke de samme opplysningene senere benyttes til å kontrollere de samme personene. Det er derfor alltid betydelig enklere og billigere å tenke nøye igjennom formålet tidlig i utviklingsarbeidet istedenfor å redefinere formålet senere.

Formålet må være saklig begrunnet ut ifra virksomheten. Det betyr at et idrettslag for eksempel ikke kan behandle andre opplysningstyper enn det lagets virksomhet gir grunnlag for, slik dette framgår av vedtekter eller liknende. Dersom fotballklubben legger opp til en systemløsning som omfatter registrering av medlemmenes kjøpevaner på sportsmarkedet, eksempelvis for å selge disse opplysningene videre til leverandører av sportsartikler, vil dette trolig være et ulovlig formål fordi saklighetskravet ikke er tilfredsstilt. Denne delen av informasjonssystemet vil derfor være ulovlig og kan ikke brukes, med mindre idrettslagets vedtekter blir endret i tråd med formålet.

17.2.4 Krav til kvaliteten av personopplysningene

Alle personopplysninger må som et minimum tilfredsstille krav til:

- Fullstendighet
- Relevans
- Korrekthet
- Ajourhold
- Begrenset lagring

Alle disse kravene må sees i forhold til formålet med behandlingen, jf. forrige avsnitt. Det betyr for eksempel at opplysninger ikke kan lagres lenger enn det formålet tilsier. Også kravet til korrekthet vil variere avhengig av formålet. Kravet øker for eksempel dersom formålet eller bruken kan gi virkninger som alvorlig kan skade personvernet.

Kvalitetskravene til personopplysninger kan gjøre det nødvendig med særlige rutiner for å sikre at kravene etterkommes, for eksempel rutiner for samkjøring av opplysninger fra ulike kilder, kontroll av at opplysninger er konsistente, sikring av dataintegritet mv. Vi kommer nærmere tilbake til spørsmålet om hvorledes arbeidet for å sikre opplysningskvalitet mv. skal skje, jf. neste avsnitt om sikring og internkontroll.

17.2.5 Krav til sikring og internkontroll

Den behandlingsansvarlige har et stort ansvar.

Loven stiller krav om at den behandlingsansvarlige gjennomfører tiltak for å sikre tilfredsstillende ivaretakelse av:

- konfidensialitet, dvs. at ikke uvedkommende får tilgang til opplysningene,
- informasjonsintegritet, dvs. at opplysningene ikke endres på uautorisert måte, og
- tilgjengelighet, dvs. at opplysningene er tilgjengelige for de angitte formålene[60].

I tillegg stiller loven krav om at den behandlingsansvarlige har rutiner for internkontroll. Internkontrollen skal sikre at kravene i lov, forskrift, konsesjon og andre eventuelle enkeltvedtak (pålegg fra Datatilsynet om å endre systemet mv.) blir etterlevd. Bestemmelsen innebærer en plikt til å gå gjennom alle aktuelle bestemmelser og vurdere hvilke tiltak som er nødvendige for å sikre slik etterlevelse.

Sikringstiltak og internkontrolltiltak skal være planlagte, systematiske og dokumenterte. I praksis innebærer det at analysen og vurderingen av sikkerhetstrusler og behov for tiltak ellers må skje som ledd i systemutviklingen. Kravet til planlegging innebærer bl.a. at arbeidet må skje etter en fremgangsmåte som er fastsatt på forhånd. Kravet til systematikk betyr at arbeidet må skje på grunnlag av helhetlige forståelser.

Sikrings- og kontrolltiltak skal dokumenteres.

Både sikrings- og kontrolltiltakene skal være dokumenterte. Det er ikke spesielle krav til hvorledes dokumentasjonen av sikrings- og kontrolltiltakene skal utformes, poenget er at tilsynsmyndigheter og andre lett skal kunne få kunnskap om hvilke tiltak som er iverksatt. Dokumentasjonen skal være tilgjengelig for alle som arbeider med opplysningene,

60. Oppdragsforhold mv. holder vi altså utenfor her.

for Datatilsynet og for klageorganet Personvernnemnda. Dokumentasjonen vil trolig spille en stor rolle ved stedlige kontroller og i tilfelle det reises erstatningskrav etter § 49 i loven. I de fleste erstatningssaker krever loven at den behandlingsansvarlige må kunne vise at vedkommende ikke har vært uaktsom. Dette vil være vanskelig uten at det foreligger tilstrekkelig dokumentasjon av tiltakene.

17.2.6 Sletting og retting mv. av personopplysninger

Dersom personopplysninger er uriktige, ufullstendige e.l., plikter den behandlingsansvarlige å rette på forholdet. Dette skal skje av eget tiltak og så snart forholdet er oppdaget. Om mulig skal den behandlingsansvarlige også sørge for at feilen ikke får betydning for vedkommende person, eller at skadevirkningene blir så små som mulig. Korrigerende tiltak som er aktuelle, er bl.a. retting, sletting, sperring og supplering av opplysningene.

Dersom lagring av personopplysninger ikke lenger er nødvendig for å gjennomføre formålet med behandlingen, skal opplysningene i utgangspunktet slettes. Merk likevel at enkelte lover kan pålegge lengre lagring. Visse opplysninger kan fortsatt lagres for historiske, statistiske eller vitenskapelige formål. Også for slike opplysninger kan en imidlertid kreve sletting i spesielle enkelttilfeller.

Reguleringen av sletting mv. av personopplysninger er forholdsvis komplisert, og vi skal ikke gå nærmere inn i detaljspørsmål her. Et generelt poeng er likevel at kravene til retting, sperring og supplering mv. kan stille bestemte krav til systemløsningen. For eksempel vil det kunne være et krav at systemet gjør det mulig å korrigere opplysninger og samtidig ta vare på historikk (dvs. uriktige opplysninger) som da må bli tilstrekkelig skjermet.

17.2.7 Regler om innsyn og åpenhet

Alle har krav på å få vite om det skjer behandling av personopplysninger i en virksomhet, og hva denne behandlingen går ut på.

Alle har krav på å få vite om det skjer behandling av personopplysninger i en virksomhet, og hva denne behandlingen nærmere bestemt går ut på[61]. Dette gjelder spesielt:

- Hvem som er ansvarlig for behandlingen av personopplysninger

61. På http://www.saftonline.no/ finner du en tjeneste som hjelper deg med å finne ut hvilke innsynsrettigheter du har og som bistår med å sette opp innsynsbegjæringer.

- Hvilken person som har det daglige ansvaret
- Hva formålet med behandlingen er
- Hvilke opplysningstyper som behandles
- Hvor opplysningene hentes fra (hvilke kilder)
- Hvem opplysningene blir utlevert til

Alle har dessuten rett til å få vite om det er registrert opplysninger om dem selv. Dersom slike opplysninger finnes, har de rett til innsyn i disse personopplysningene. I den grad det ikke svekker sikkerheten, har de dessuten krav på å få informasjon om hvorledes opplysningene er sikret. De har også krav på å få utdypende informasjon om de forhold som alle har innsynsrett i, jf. ovenfor.

I tillegg til innsynsretten har den ansvarlige også plikt til å gi visse informasjoner når personopplysninger blir samlet inn. Dette gjelder både når opplysninger samles inn direkte fra den registrerte og når de innhentes fra andre. Den informasjon som i slike situasjoner skal gis, er i stor grad de samme opplysninger som de som inngår i den generelle innsynsretten, jf. ovenfor. Kravene til informasjon kan gjøre det vel begrunnet å utvikle systemløsninger som genererer automatiske varsler til de aktuelle personene.

Loven har i tillegg en særlig bestemmelse om varsling ved bruk av "personprofiler", dvs. ved bruk av "informasjonsmønstre" der en har knyttet antagelser om hvilke evner, behov mv. som mennesker som passer inn i mønsteret, har.

Innsyns- og åpenhetsbestemmelsene i personopplysningsloven kan i noen tilfeller få direkte innvirkning på utviklingsarbeidet. Dersom det oppstår en varslingsplikt i tilknytning til bruk av personprofiler, kan dette for eksempel tenkes å ha slike konsekvenser for driftskostnader mv. at det kan være grunn til å vurdere om bruk av slike profiler skal unngås. Bestemmelsene kan også få konsekvenser for systemdokumentasjon mv., for eksempel ved at man må dokumentere de systemaspektene som alle har krav på informasjon om. Den individuelle innsynsretten kan videre tenkes å få innvirkning på hvilke spørrerutiner mot databasen det er aktuelt å velge.

17.2.8 Meldeplikt, konsesjon og klage

I utgangspunktet er alle behandlinger av personopplysninger *meldepliktige*, noe som innebærer at den ansvarlige skal sende inn til Datatilsynet visse opplysninger om vedkommende systemløsning minst 30 dager før systemet tas i bruk, noe som enkelt kan gjøres fra Datatilsynets hjemmeside (se www.datatilsynet.no). De opplysningene som skal sendes inn, er i stor grad de samme som alle har innsynsrett i, jf. forrige avsnitt. Dersom det er endringer i opplysningene, må ny melding sendes. Alle meldinger må uansett fornyes hvert tredje år.

I forskriften til loven gjøres det imidlertid en rekke unntak fra meldeplikten. For eksempel er det gjort unntak for begrenset bruk av enkle aktivitetslogger og for enkelte andre former for vanlig og "triviell" behandling av personopplysninger.

Dersom én eller flere av de opplysningstyper som skal behandles i informasjonssystemet, er å anse som "sensitive" (se avsnitt 17.2.2), må behandlingen normalt konsesjonsbehandles. Datatilsynet kan sette vilkår for konsesjon. Er den som er ansvarlig for systemet, i tvil om konsesjon er nødvendig eller ikke, kan han kreve at Datatilsynet avgjør spørsmålet før konsesjonssøknad eventuelt sendes.

Datatilsynet har generell myndighet til å treffe enkeltvedtak med slike pålegg som er nødvendig for å sikre etterlevelse av loven, og kan herunder ilegge tvangsmulkt. Vedtak som Datatilsynet treffer, kan påklages til Personvernnemnda.

17.3 Rettslige krav til elektronisk kommunikasjon

En rekke lover og forskrifter inneholder nærmere regler om elektronisk kommunikasjon/datautveksling. Slike bestemmelser gjelder for eksempel om slik kommunikasjon overhodet er tillatt, hvilke vilkår som gjelder for kommunikasjonen, og om de nærmere kravene til kommunikasjonen med hensyn til signering, autentisering, sikring av integritet og konfidensialitet og annet. For offentlig forvaltning er den såkalte e-forvaltningsforskriften av sentral betydning.

Kravene til kommunikasjon gjelder i stor grad krav til sikkerhet, og overlapper derfor delvis med de sikringsbestemmelsene mv. i personopplysningsloven som vi tidligere har gjort rede for, se avsnitt 17.2.5[62]. Vi skal ikke her gå inn på særlovgivning innen dette området, men nøyer oss med å nevne at sentrale lover som forvaltningsloven, sikkerhetsloven, tolloven, aksjeloven og regnskapsloven har slike bestemmelser. Hvor detaljerte kravene til kommunikasjonen er varierer imidlertid sterkt fra forholdsvis spesifikke angivelser til generelle krav om at kommunikasjonen skal være "betryggende". Konkret innebærer dette at det ved utvikling av rutiner for elektronisk kommunikasjon/dataoverføring alltid bør undersøkes om det gjelder særskilte rettslige krav og hvilke dette eventuelt er. Dersom det er tale om elektronisk kommunikasjon mellom forvaltningsorganer eller mellom et forvaltningsorgan og enkeltpersoner, vil de forholdsvis omfattende bestemmelsene i forvaltningsloven § 15a med forskrifter komme til anvendelse.

Ved utvikling av rutiner for elektronisk kommunikasjon/dataoverføring, bør vi alltid undersøke om det gjelder særskilte rettslige krav for dataoverføringen.

17.4 Opphavsrett

17.4.1 Generelt

Også opphavsrettslige spørsmål kan melde seg i tilknytning til systemutviklingsarbeider. Med *"opphavsrett"* sikter vi til den rett forfattere, programmerere og andre opphavsmenn har til å disponere over sine åndsverk. Opphavsretten tilkommer som hovedregel de fysiske personer som skaper verket, men retten er ikke sjelden overdratt til en juridisk person, for eksempel til en arbeids- eller oppdragsgiver.

Opphavsrett er den rett forfattere, programmerere og andre opphavsmenn har til å disponere over sine verk.

Opphavsretten omfatter dels økonomiske og dels ideelle rettigheter. De økonomiske rettighetene gjelder bl.a. en enerett til å framstille eksemplarer av verket, spredning og offentlig visning. De ideelle rettighetene omfatter retten til å bli navngitt og retten til respektfull behandling av verket.

For at opphavsrett skal oppstå, må frambringelsen ha såkalt *verkshøyde*. Det vil si at arbeidet må være et resultat av en selvstendig og original skapelsesprosess. Ikke enhver formgivning, tekst, ethvert bilde eller enhver lyd har verkshøyde. Den nærmere diskusjonen om hvor grensen for verkshøyde går kommer vi ikke inn på her.

For at opphavsrett skal oppstå, må frambringelsen ha verkshøyde.

62. De praktisk viktigste bestemmelsene om informasjonssikkerhet er gjennomgått på en lettfattelig måte i Jansen og Schartum; "Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT", Fagbokforlaget 2005.

Noen kategorier av verk oppnår beskyttelse selv om det ikke er snakk om åndsverk. Det gjelder for eksempel kataloger – jf. avsnitt 17.4.4 – og fotografiske bilder.

17.4.2 Materiale som fritt kan brukes

Noe materiale kan benyttes fordi det ikke er omfattet av det opphavsrettslige vernet. I utgangspunktet vil det således ikke være knyttet opphavsrett til offentlige saksdokumenter, herunder rettslig materiale. Det innebærer bl.a. at lovgivning, lovforarbeider, rettsavgjørelser og forvaltningsavgjørelser fritt kan benyttes. Likevel kan tilføyelser til slikt materiale være undergitt opphavsrett. Dette gjelder for eksempel bearbeidelse av lover mv. i form av noteverk, henvisningsstrukturer og annet. I Lovdatas tekstbaser finnes det flere eksempler på vernede tekster og strukturer som er føyd til tekster som ikke er vernet.

Sitatretten.

Selv om et materiale i utgangspunktet er vernet, kan det være anledning til fritt å bruke utdrag av verket (dokumentet, bildet, lydopptaket mv.) i form av *sitater*. Forutsetningen er at verket er offentliggjort, og at sitering skjer i samsvar med god skikk og i den utstrekning formålet betinger. Dette innebærer at sitatet må settes inn i en relevant sammenheng og brukes for å illustrere forhold som blir fremhevet i det siterende verket. Dersom en for eksempel ønsker å beskrive oppsettet av en programkode, kan det gjengis illustrerende utsnitt av koden, selv om andre har opphavsrett til denne. Det må imidlertid alltid opplyses om hvem som er opphavsmannen, jf. de ideelle rettighetene.

Noen verk har vært opphavsrettsbeskyttet, men de økonomiske rettighetene er ikke lenger i behold pga. den tiden som har gått. Vernet opphører vanligvis 70 år etter at opphavsmannen døde. Det innebærer for eksempel at en rekke klassiske kunstverk (bilder, musikk mv.) kan benyttes til å pynte opp et nettsted, som skjermsparer mv. De ideelle rettigheter er likevel i behold, noe som innebærer at opphavsmannen alltid skal angis og verket skal behandles på respektfull måte.

17.4.3 Spesielt om opphavsrett til datamaskinprogrammer

For opphavsrett til datamaskinprogrammer gjelder særskilte regler.

Opphavsrett til datamaskinprogrammer er spesielt regulert i *åndsverkloven*. Lovens generelle prinsipp for tildeling av opphavsrett er at det er den eller de personer som har frambrakt verket, som får retten. For

datamaskinprogrammer som er skrevet av en ansatt innenfor rammene av et arbeidsforhold, er utgangspunktet motsatt. Dersom programmeringen skjer som en del av jobben eller etter arbeidsgivers anvisning, er det i utgangspunktet arbeidsgiveren som får opphavsretten til programmet. For at programmereren likevel skal få opphavsrett, må dette avtales særskilt.

Den som har rett til å bruke et datamaskinprogram, kan kopiere, endre, bearbeide og rette feil i programmet dersom dette er nødvendig for å bruke programmet i samsvar med programmets formål. Bearbeidelse av programmer for å bruke det til andre formål enn det er skrevet for, er med andre ord ikke tillatt. Det er også lov å undersøke eller prøve ut hvordan programmet virker for på den måten å finne fram til de ideer og prinsipper som programmet bygger på. Videre er det på visse vilkår anledning til å dekompilere et datamaskinprogram (dvs. å gjenvinne programteksten fra det kompilerte programmet). En forutsetning er at det må være nødvendig å dekompilere for å skaffe opplysninger om hvordan programmet funksjonelt kan virke sammen med andre programmer. For eksempel kan vi ønske å ta data fra et lagerstyringssystem inn i et økonomisystem, og trenger å dekompilere koden for å forstå hvorledes dette eventuelt kan gjøres.

17.4.4 Vern av databaser

Databaser kan ha tilstrekkelig verkshøyde til å være beskyttet som åndsverk, hvis dette ikke er tilfelle, kan de likevel falle inn under katalogregelen.

Åndsverkloven inneholder et spesielt vern for "kataloger" mv., herunder databaser, den såkalte *katalogregelen*. Årsaken er primært at disse ikke alltid tilfredsstiller kravet til verkshøyde (jf. avsnitt 17.4.1) og derfor ikke er beskyttet som åndsverk. I enkelte tilfeller vil imidlertid deler av en database være beskyttet av opphavsrett, mens andre deler kun er beskyttet av katalogregelen.

Hovedvilkåret for å få vern etter katalogregelen er at katalogen eller databasen sammenstiller et større antall opplysninger. Selv om antallet opplysninger ikke er stort, kan vern oppnås dersom databasen er resultatet av en vesentlig investering. I begge tilfeller vil opphavsmannen ha enerett til å framstille eksemplarer av databasen og til å vise den fram for allmennheten.

Andre kan normalt råde over "uvesentlige deler" av kataloger og databaser mv., dvs. det er mulig å kopiere eller gjøre offentlig mindre deler av materialet. Dette gjelder likevel ikke dersom slik bruk skjer gjentatt

og systematisk. Uten avtale vil det for eksempel ikke være anledning til å inkorporere en "fremmed" databasetjeneste i egne tjenester, selv om oppslagene ved hver enkelt bruk kun gjelder en uvesentlig del av basen. Sporadisk og begrenset bruk vil derimot være tillatt. Jeg kan for eksempel ta kopi av enkeltstående søkeresultater fra katalogtjenester mv. på nettet.

Katalogregelen gir kun vern i 15 år regnet fra det året da katalogen eller databasen ble fremstilt eller offentliggjort. Katalogvernet er en økonomisk rettighet, og det er ikke knyttet noen ideelle rettigheter til katalogvernet. Offentlige saksdokumenter er dessuten ikke vernet etter åndsverkloven og nyter derfor heller ikke noe "katalogvern".

17.5 Bortsetting av utvikling og drift av informasjonssystemer

Bortsetting av utvikling og drift fritar ikke virksomheten fra det juridiske ansvaret.

Dersom utviklings- og/eller driftsoppgaver i tilknytning til et informasjonssystem settes bort til andre (såkalt *"outsourcing"*), oppstår det enkelte interessante rettsspørsmål. For det første melder spørsmålet seg om det alltid er tillatt å sette bort slike oppgaver til andre. I noen tilfeller vil det i lover mv. være forutsatt at myndighet skal utøves av bestemte instanser. Særlig gjelder dette innen offentlig sektor, der det for eksempel er fastlagt at ligningsetaten skal fastsette hva den enkelte skal betale i skatt. Når ligningsetatens og andre offentlige myndigheters informasjonssystemer blir utviklet, vil viktige deler av arbeidet gå ut på å ta stilling til hva som er en riktig fortolkning og representasjon av skatteregler mv. Den offentlige myndigheten kan derfor ikke overlate slike avgjørelser til andre, men må selv eksplisitt ta stilling til de mange fortolkningsspørsmål som aktualiseres som ledd i utviklingsarbeidet. Selvsagt kan forvaltningen benytte eksterne konsulenter til å utarbeide løsningsforslag, men den reelle beslutningen om hva som er rettslig korrekt innhold av programmene, eksempelvis for skatteberegning, er det vedkommende myndighet selv som må treffe.

Rene driftsoppgaver gir ikke behov for å treffe bestemmelser som innebærer utøvelse av offentlig myndighet. Likevel kan det være forbudt å overlate driftsoppgavene til en annen virksomhet. Dette gjelder for eksempel dersom oppdragstakeren ikke kan etterleve de sikkerhetskrav som gjelder for systemet. Dersom en virksomhet har funnet ut at de vil sette bort driften av et informasjonssystem, må de sikkerhetskrav som gjelder for systemet, også etterleves etter at bortsetting av driften har

skjedd. Det vil således ikke være anledning til å "forhandle ned" sikkerhetskravene for å oppnå en akseptabel pris fra oppdragstaker.

Dersom bortsetting av utvikling- eller drift kan skje, er oppdragstakeren bundet av de samme bestemmelsene som gjelder for oppdragsgiver. Dette gjelder for eksempel taushetsplikt for person- og forretningsopplysninger. Når det gjelder personopplysninger stiller personopplysningsloven § 15 i tillegg opp et krav om skriftlig avtale mellom oppdragsgiver og oppdragstaker. Avtalen skal regulere hvorledes oppdragstaker skal behandle personopplysningene. Liknende krav gjelder etter den såkalt IKT-forskriften for finansforetak (bank, forsikring mv).

17.6 Medbestemmelse og brukermedvirkning

17.6.1 Noen generelle utgangspunkter

I det følgende bruker vi *"medvirkning"* og *"medbestemmelse"* som stikkord for rettigheter som ansatte har til å ha innflytelse på egen arbeidssituasjon. Slike rettigheter har bl.a. betydning når informasjonssystemer og tilhørende arbeidsprosesser skal utformes.

Den situasjonen vi går ut fra, er at det foreligger ansettelsesforhold, dvs. at det foreligger en arbeidsgiver med arbeidstakere som arbeider mot godtgjørelse.[63] Det rettslige utgangspunktet er da at arbeidsgiveren har en "styringsrett", dvs. en rett til å bestemme over innholdet og utførelsen av arbeidet. Retten omfatter bl.a. informasjonssystemer, organisering og arbeidsdeling. Styringsretten er imidlertid ikke ubegrenset. Den avgrenses bl.a. av en rekke bestemmelser i lov og avtale, som for eksempel bestemmelser om de ansattes medbestemmelse og medvirkning.

Reglene om "arbeidstakerdemokrati" kan sies å gjelde to aspekter. For det første er det etablert et bedriftsdemokrati som gir ansatte rett til med*bestemmelse* ved å være representert i virksomhetenes styrende organer. Tillitsvalgte deltar på styrebehandling av saker om innføring av informasjonssystemer mv. Dette aspektet kommer vi ikke nærmere inn på her. Det andre aspektet gjelder med*virkning* gjennom det daglige arbeidet i virksomheten, for eksempel i tilknytning til planlegging og utvikling av informasjonssystemer. Vi bruker benevnelsen *med*virkning,

63. Oppdragsforhold mv. holder vi altså utenfor her.

og forstavelsen i ordet understreker at det her ikke er tale om en rett for ansatte til å bestemme alene, men til å påvirke avgjørelser i virksomhetens styrende organer.

17.6.2 Hvor finner vi regler om ansattes medvirkning?

Medbestemmelsesretten for ansatte og bedriftsdemokrati er nedfelt i Grunnloven § 110 annet ledd, der det står at nærmere regler skal gis i lov.

Regler om arbeidstakeres rett til medvirkning finnes primært i arbeidsmiljøloven.

Medbestemmelsesretten for ansatte og kravet om bedriftsdemokrati er nedfelt i Grunnloven § 110 annet ledd, der det står at nærmere regler skal gis i lov. Regler om arbeidstakeres rett til medvirkning finnes primært i arbeidsmiljøloven. Denne loven gjelder i utgangspunktet for alle arbeidstakere, dvs. for folk som utfører arbeidsoppgaver for en arbeidsgiver mot vederlag og derved underlegger seg arbeidsgiverens ledelse og kontroll. Arbeidsmiljøloven gjelder med andre ord for alle virksomheter som ansetter noen i sin tjeneste (arbeidstakere), dvs. i så vel offentlig som i privat sektor.

I tillegg til lovbestemmelsene finnes det regler om medbestemmelse i avtaler mellom arbeidsgiver og arbeidstaker ("tariffavtaler"). Slike avtaler finnes i minst to "lag". For det første er det inngått sentrale avtaler som gjelder alle arbeidsgivere og arbeidstakere som er organisert hos de aktuelle organisasjonene. Slike "hovedavtaler" og "rammeavtaler" finnes både i privat og offentlig sektor. LO og NHO har for eksempel inngått "Rammeavtale om teknologisk utvikling og datamaskinbaserte systemer", som er en tilleggsavtale til hovedavtalen. På liknende måte har Hovedavtalen i staten en egen bestemmelse om informasjonsteknologi. I tillegg finnes det i varierende grad lokale avtaler for enkelte virksomheter.

I tillegg til lovbestemmelsene finnes det regler om medbestemmelse i avtaler mellom arbeidsgiver og arbeidstaker ("tariffavtaler").

Visse bestemmelser i lov- og avtaleverket kan ha direkte betydning for medbestemmelse ved utvikling av informasjonssystemer. Her skal vi nevne de viktigste. Vi velger å ta utgangspunkt i reglene for privat sektor for deretter å angi noen spesielle trekk ved Hovedavtalen i staten. Samtidig gjør vi oppmerksom på at det kan være flere forskjeller mellom offentlig og privat sektor enn det vi direkte kan formidle her.

17.6.3 Hvordan medvirkning skjer i privat sektor (LO–NHO)

I skandinavisk systemutviklingsteori legges det ofte vekt på "brukermedvirkning". Dersom vi ser på den rettslige reguleringen, kan imidlertid brukerrepresentasjon og -medvirkning bety minst to ting. Dels kan

medvirkning skje via tillitsvalgte, og dels medvirker arbeidstakere ellers på relevante måter.

I hver virksomhet skal det være minst to tillitsvalgte, og antallet tillitsvalgte kan være høyere avhengig av bedriftens størrelse. I bedrifter med mer enn 20 ansatte kan arbeidstakerne kreve arbeidsmiljøutvalg, og er det mer enn 50 ansatte, *skal* virksomheten ha et slikt utvalg. Der deltar de tillitsvalgte sammen med arbeidsgivers representanter med like mange representanter. I arbeidsmiljøutvalgene sitter bl.a. verneombudene, som er de ansattes representant. Arbeidsmiljøutvalgene skal behandle planer som kan få vesentlig betydning for arbeidsmiljøet, så som planer om rasjonalisering, endring av arbeidsprosesser og vesentlige endringer i arbeidsmetoder og drift. Utvalgene kan således behandle planer om vesentlig utvikling, tilpassing og endring av bedriftens informasjonssystemer og tilknyttede rutiner. Utvalgets oppgave er å sørge for et fullt ut forsvarlig arbeidsmiljø. Planer om informasjonssystemer som kan innebære stress, ensformig arbeid mv., vil altså kunne møte motbør i arbeidsmiljøutvalgene.

"Dataavtalen" mellom LO og NHO (og dessuten Hovedavtalen i staten) åpner for at det i den enkelte virksomhet kan velges en "datatillitsvalgt" (eventuelt flere). Det er en forutsetning at de datatillitsvalgte skal gis anledning til å sette seg inn i generelle spørsmål om hvordan ny teknologi kan påvirke de ansatte. De skal dessuten ha tilgang til all dokumentasjon, utstyr og programmer som gjelder teknologi og systemer som angår planlegging og gjennomføring av arbeid i virksomheten. Dette innbefatter også systemer for lagring og bruk av persondata.

Arbeidsmiljøloven § 12 nr. 3 bestemmer at arbeidstakerne og deres tillitsvalgte skal være med på å utforme systemer som nyttes ved gjennomføring av arbeidet. I tillegg legger rammeavtalen om teknologisk utvikling og datamaskinbaserte systemer opp til å sikre reell innflytelse for "alle ansatte som blir direkte berørt". Avtalen sier ingen ting om hvorledes dette skal oppnås, men foruten informasjon og alminnelig lydhørhet, er det nærliggende å delvis arbeide med prototyper av informasjonssystemer.

Som oftest kommer initiativet til nye eller endrede informasjonssystemer fra ledelsen i virksomheten. Bedriften skal drøfte med de tillitsvalgte viktige omlegginger, herunder endringer i produksjonsopplegg og metoder. Slike drøftinger skal skje så tidlig som mulig. Nye eller

endrede informasjonssystemer vil således ofte være gjenstand for slik drøftingsplikt. Bedriften skal også holde de tillitsvalgte løpende informert om planene/arbeidet.

Informasjonen til ansatte og tillitsvalgte skal gis slik at de ansatte kan legge fram sine synspunkter så tidlig som mulig og før bedriften har iverksatt sin beslutning. Lovens krav er som nevnt at de ansatte skal være med på å utforme systemer som benyttes i arbeidet. Informasjon som kommer så sent at slik innflytelse er umulig, representerer derfor normalt en ulovlig praksis. Retten til å være med på å utforme slike systemer innebærer imidlertid ingen rett til å bestemme på tross av arbeidsgivers synspunkter. Bedriftsledelsen kan således nekte å ta hensyn til de ansattes innvendinger og forslag, men i så fall må bedriften begrunne sitt syn.

Rammeavtalen fastsetter at alle ansatte som deltar i konkrete prosjekter, skal ha tilgang til all nødvendig dokumentasjon. Begrunnelsen for den nevnte brede deltakelsen i utviklingsarbeidet er ikke bare hensynet til medbestemmelse. I avtalen sies det at siktemålet også er å dra nytte av de kunnskaper som finnes i alle ledd i bedriftsorganisasjonen.

Rammeavtalen legger opp til at de tillitsvalgte i rimelig grad skal kunne benytte bedriftens ekspertise. Tillitsvalgte på sin side skal stå til disposisjon for de andre ansatte. På den måten vil mange spørsmål fra ansatte sluses via de datatillitsvalgte.

17.6.4 Medvirkning innen statlig sektor

Den situasjonen for medvirkning ved systemutvikling som vi har skissert ovenfor innen LO–NHO-området, er langt på vei også illustrerende for situasjonen innen statlig forvaltning. Vi skal her nøye oss med å presisere enkelte forhold nærmere.

Medbestemmelsesordningene innen statlig sektor er basert på forhandlinger, drøftinger og informasjon. Det er særlig forhandlingssystemet som er spesielt, fordi det innebærer at arbeidsgiver og arbeidstaker i visse tilfeller skal forhandle seg fram til avgjørelse, dvs. at arbeidsgiveren (staten) ikke ensidig kan treffe en avgjørelse. Dersom partene i forhandlingssaker ikke blir enige, gir hovedavtalen i staten anvisning på mekling og behandling i partssammensatt nemnd med nøytral leder hvis mekling ikke fører fram.

Blant de saker som kan være gjenstand for forhandlinger, er "rasjonalisering, innføring eller endring av teknologi som har vesentlig innvirkning på de tilsattes arbeidssituasjon" (§ 13 bokstav a). Forhandlingene må imidlertid alltid skje innenfor de rammene som er trukket opp i Stortingets budsjettvedtak og -fullmakter. Partene kan følgelig ikke forhandle seg fram til IKT-løsninger som innebærer at slike budsjettrammer sprenges. Forhandlingene må dessuten forholde seg til arbeidsgiverens myndighetsområde. I trygdeetaten kan man altså ikke forhandle seg fram til en systemarkitektur som innebærer at arbeidsdelingen mellom trygde- og skatteetaten må endres. Forhandlingsresultater må dessuten ligge innenfor de instrukser og prioriteringer som vedkommende departement har gitt, eller som en underordnet instans har gitt etter fullmakt fra departementet. Disse tre elementene i rammen for forhandlingsløsninger kan sees som en grenseoppgang mellom det representative demokratiet og demokrati på arbeidsplassen.

Forhold som gjelder informasjonsteknologi, er spesielt regulert i Hovedavtalens § 14. Vi skal her nevne de vesentligste punktene. For det første er det eksplisitt fastsatt at arbeidsgiver skal informere om all planlegging og bruk, anskaffelse av utstyr og programvare og utvikling/etablering eller endringer av datasystemer. Dersom det skal utvikles egne systemer eller gjøres betydelige endringer i slike, skal det avtales hvorledes de ansatte skal medvirke, for eksempel innenfor rammene av en prosjektorganisasjon. Avtalen gir også tillitsvalgte rett til nødvendig innføring og opplæring i virksomhetens datasystemer.

Dersom et nytt eller endret datasystem får omfattende konsekvenser for de ansattes arbeidssituasjon, skal det gjennomføres konsekvensanalyser. Dette skal skje før arbeidet igangsettes. Ved større utviklingsarbeider bør det også gjennomføres resultatanalyser, dvs. etterfølgende analyser av hvilke resultater arbeidet brakte.

17.7 Moral og etikk

Bruk av informasjonsteknologi kan ha stor innvirkning både på samfunnet og på enkeltindivider. Teknologien i seg selv har få føringer med hensyn til på hvilken måte den blir brukt, og den kan derfor like gjerne bli utnyttet for gode som for onde formål. Vi som deltar i systemutviklingsprosesser, må være bevisste på at våre valg og våre handlinger kan få store konsekvenser, og etter beste evne handle i overensstemmelse med høyverdige moralske prinsipper.

17.7.1 Hva er moral?

Moral er skrevne eller uskrevne regler for hvordan en bør handle.

Moral er skrevne eller uskrevne regler for hvordan en bør handle. Helt siden Platon og Aristoteles har filosofene beskjeftiget seg mye med hvordan man fastlegger hva som er god moral. Et eksempel er utilitarismen, som sier at "god moral er det som gir mest mulig lykke", et annet er Kants moralfilosofi, som sier at fornuften er autoritet i moralske spørsmål. I praksis er man vel enig om at "god moral" er allment aksepterte, omforente normer og regler i et samfunn eller en kultur om hvordan man bør oppføre seg. Noen av disse reglene er nedfelt i lover og forskrifter, slik som vi har sett eksempler på tidligere i dette kapitlet.

Er "Computer Ethics" noe spesielt?

Hvorfor skal vi så diskutere "Computer Ethics" som noe spesielt? Gjelder ikke de vanlige moralnormene også i kontakt med datamaskinen? Forholdet er at datateknologien er så allsidig anvendelig og åpner for så mange helt nye muligheter at vi i mange situasjoner rett og slett ikke har noen erfaring å bygge på og dermed heller ingen retningslinjer med hensyn til hva som er riktige og gale handlinger. Vi mangler rett og slett "moralsk kompetanse". Et konkret utslag av mangelen på retningslinjer er at det har vært nødvendig å endre, utvide og tilpasse lovverket som følge av informasjonsteknologiens innmarsj i samfunnet, slik vi har sett mange eksempler på tidligere i dette kapitlet. Trendsettende forskere spår imidlertid at i løpet av noen år vil samfunnet være så gjennomsyret av informasjonsteknologi og teknologien så alminneliggjort at "Computer Ethics" igjen vil smelte sammen med den vanlige, generelle etikken.[64]

Uansett hvilket syn man har på dette er det behov for retningslinjer som kan hjelpe oss i de daglige avgjørelser som profesjonelle systemutviklere og brukere av informasjonsteknologien.[65]

17.7.2 ACM Code of Ethics and Professional Conduct

Det mest kjente eksemplet på slike retningslinjer er ACM Code of Ethics and Professional Conduct.[66] ACM ("Association of Computing Machinery") er en medlemsorganisasjon for "computer professionals", og det

64. Se Gorniac-Koscikowsak, Krystyna (1996), Deborah Johnson (1999).
65. Se Gotterbarn (1999).
66. Se http://www.acm.org/constitution/code.html

forutsettes at alle medlemmer handler i samsvar med "Code of Ethics". Retningslinjene gjelder både systemutviklere og brukere generelt.

Retningslinjene er delt i tre grupper: Generelle moralske absolutter, mer spesifikt profesjonsansvar og organisasjonsmessig lederskap.

Generelle moralske absolutter

Disse reglene gjelder selvsagt ikke bare for systemutviklere og brukere av datamaskiner!

Du skal

- bidra til samfunnets og individets livskvalitet (en viktig del av dette er spørsmål rundt klodens miljø)
- ikke skade andre
- være ærlig og troverdig
- være rettferdig og ikke diskriminere
- respektere rettigheter, copyrights og patenter
- gi korrekt kreditering til intellektuell eiendom
- respektere personvernet
- respektere taushetsplikten

Mer spesifikt profesjonsansvar

Som profesjonell systemutvikler eller bruker av datamaskin har du et mer spesifikt ansvar. Du skal

- søke å oppnå best mulig kvalitet, virkning og verdighet i både produkt og prosess
- bygge opp og vedlikeholde profesjonell kompetanse
- kjenne til og respektere lover som er relevante for ditt profesjonelle virke
- motta og gi profesjonell kritikk
- gi helhetlige og grundige evalueringer av datamaskinsystemer og deres virkninger, inkludert en analyse av mulige risiki
- respektere kontrakter, avtaler og ansvar
- bidra til allmennhetens forståelse av databehandling og dens konsekvenser
- bruke datamaskinutstyr og kommunikasjonsutstyr bare når du er autorisert til det

Organisjonsmessig lederskap

Ledere har større muligheter for å påvirke enn andre. Derfor har vi noen regler spesielt for dem.

Du skal

- gi tydelig utrykk for det sosiale ansvar som medlemmene i en organisasjonsenhet har, og oppmuntre til full aksept av dette ansvaret
- bruke personale og ressurser til å utforme og bygge informasjonssystemer som øker kvaliteten på arbeidslivet (arbeidsmiljøet)
- erkjenne og understøtte riktig og autorisert bruk av en organisasjons databehandlings- og kommunikasjonsressurser
- forsikre deg om at brukere og andre som vil bli berørt av et system, har fått uttrykt sine behov under vurdering og utforming av krav; senere må systemet valideres med hensyn til disse kravene
- gi uttrykk for og understøtte en politikk som ivaretar verdigheten til brukere og andre berørt av et datasystem
- gi muligheter for medlemmer i organisasjonen til å lære prinsippene og begrensningene i et datamaskinsystem

17.7.3 Moralske dilemmaer

Det er systemutviklernes ansvar å lage systemene slik at de ikke så lett kan bli misbrukt.

Disse retningslinjene er for så vidt greie nok. Problemet er at de bare delvis kan hjelpe oss i moralske og etiske dilemmaer – dilemmaer som blir forsterket gjennom informasjonsteknologiens enorme påvirkningskraft. Er det for eksempel moralsk riktig å delta i utviklingen av et prosesstyringssystem for et gasskraftverk hvis man er overbevist om at gasskraftverk er en katastrofe for miljøet på jorda? Er det moralsk riktig å være med på å utvikle internasjonale betalingssystemer som vil bidra til å gjøre internasjonale handelskonserner enda mektigere, mens fattige land i den tredje verden blir skjøvet enda mer ut over sidelinjen fordi de ikke har like god tilgang til teknologien? Er det riktig å lage systemer som bryter kopieringsbeskyttelsen på musikkfiler, ut fra en overbevisning om at plateindustrien beriker seg på de utøvende kunstnernes bekostning?

Problemet er at det som er bra for noen, kan være negativt for andre. Dersom automatisering ved hjelp av informasjonsteknologi gjør at vi

kan redusere arbeidsstokken til det halve, vil dette formodentlig glede aksjonærene og skape fortvilelse hos de ansatte.

Hva som er rett og galt, er ofte et politisk spørsmål.

Vi ser at i mange tilfeller vil spørsmålet om hva som er rett og galt, bare kunne besvares ut fra ens politiske holdninger. Det spesielle med systemutviklingsprofesjonen er at de valg man gjør i yrkeslivet, er mer politisert enn hva som er tilfellet i mange andre profesjoner.

> Personlig synes jeg ikke at man skal "melde seg ut av" systemutviklingsprosesser hvis mål man er politisk uenig i. Man gjør verden en større tjeneste ved å bli på sin post og ved klar tale og gode argumenter forsøke å påvirke prosessen og de artefakter som kommer ut av den i den retningen man synes er best.

Så kan man spekulere på om den "globalisering av informasjon" som informasjonsteknologien bringer med seg, vil føre til større forståelse mellom ulike kulturer, større enighet om hva som er rett og galt, og en gunstigere utvikling av verdenssamfunnet ...

17.8 Oppsummering

"God moral" er samfunnets omforente, allment aksepterte retningslinjer for hvordan vi bør oppføre oss. Mange av disse retningslinjene er uskrevne, andre er skrevet ned i form av avtaler, lover eller forskrifter. I dette kapitlet har vi sett på noen av de viktigste lovene og avtalene: Personopplysningsloven, Arbeidsmiljøloven, Åndsverksloven, rettslige krav til elektronisk kommunikasjon og avtaler om medbestemmelse og brukermedvirkning i arbeidslivet. I situasjoner der slike skriftlige lover og avtaler ikke er relevante, må vi falle tilbake på vår evne til å vurdere hva som er rett og galt. Etiske retningslinjer som "ACM Code of Ethics and Professional Conduct" kan da være til hjelp.

Generelt må også informasjonssystemer oppføre seg i samsvar med den "gode moral". Konkret har vi sett eksempler på at rettsregler bygges inn i informasjonssystemer.

17.9 Historikk og bibliografi

Norbert Wiener var den første som publiserte tanker om informasjonsteknologiens enorme påvirkningskraft – i boken "The Human use of Human Beings" (Wiener 1950). Dessverre gikk hans tanker stort sett upåaktet hen i mange år. I 1960-årene begynte Donn Parker fra Software Research Institute å undre seg over den uetiske oppførselen han

kunne observere hos mange utviklere og brukere, og publiserte som konsekvens av dette "Rule of Ethics in Information Processing" (Parker 1968). I 1970-årene gjorde Walter Maner en stor innsats for å få "Computer Ethics" inn i utdanningsprogrammene ved amerikanske universiteter. I 1980-årene ble "Computer Ethics" etablert som en teoretisk fundert, akademisk disiplin, bl.a. gjennom innsatsen fra sentrale forskere som James Moor (1985), Deborah Johnson (1985), Terrell W. Bynum (1985), Donald Gotterbarn (1991) og Simon Rogerson (1996).

I boken "Etikk og informasjonsteknologi" (G. Hartvigsen, D. Johansen, A. Måseide 2000) gir forfatterne først en oversikt over generell moralfilosofi, og belyser deretter moralfilosofiske aspekter ved bruk av informasjonsteknologi ved hjelp av utvalgte eksempler.

Den sosiotekniske tankegangen har et sterkt innslag av etiske diskusjoner. Den har preget det norske arbeidslivet helt siden tidlig på 1970-tallet, selv om det har tatt tid å få gjennomført reformene. En sentral person i utvikling var Einar Thorsrud, leder for Institutt for industriell miljøforskning ved Norges Tekniske høgskole. Han tok initiativ til forskning og prøveprosjekter rundt bedriftsorganisering på 1950- og 60-tallet – se E. Thorsrud, F. Emery (1970). I England arbeidet Enid Mumford ved Manchester Business School med liknende ideer – se Mumford (1983). I Norge fulgte Jern- og metallarbeiderprosjektet i 1970–73 under ledelse av Kristen Nygaard med flere. Dette førte til de første avtalene mellom Norges Arbeidsgiverforening (nå NHO) og LO i 1975 – se Nygaard & Bergo (1974).

Videre var den sosiotekniske tankegangen sentral i utformingen av Lov om arbeidsmiljø fra 1977 (med senere endinger), som også skal sikre arbeidstakernes rett til å ha innflytelse på innføring og bruk av ny teknologi.

Kapittel 18

Sikkerhet i informasjonssystemer

Verden hadde vært et bedre sted å være hvis alle hadde oppført seg i samsvar med høyverdige moralske normer. Dessverre gjør ikke alle det – det finnes nok av eksempler på økonomisk datakriminalitet, innbruddsforsøk i datamaskinbaserte systemer og virusplager.

Derfor hører det også til systemutviklerens ansvarsområde å påse at de systemene som blir utviklet, ikke så lett kan misbrukes. Dette er noe vi må ha i tankene under utformingsarbeidet. For det første må vi bygge på plattformer som tilbyr en rimelig grad av sikkerhet. For det andre må de systemene vi bygger på plattformene, ha sin egen sikkerhet, fordi disse systemene nødvendigvis må ha visse privilegier overfor plattformen.

En systemutvikler må alltid ha i tankene at samtidig som det systemet han utvikler skal være lett tilgjengelig og lett å bruke for rette vedkommende, må han i størst mulig grad forhindre at uvedkommende slipper til og bruker eller misbruker systemet, eller får urettmessig tilgang til data. Dette er blitt et stadig viktigere moment i systemutviklingsarbeidet etter som stadig flere systemer koples sammen i et verdensomspennende datanett, der ikke alle brukere nødvendigvis har ærlige hensikter.

Vi skal i dette kapitlet ikke gå inn på sikkerhetstiltak som ligger utenfor systemutviklerens normale ansvarsområde, som for eksempel fysisk sikring av bygninger og maskininstallasjoner, oppsett av brannmurer, driftsmessig sikring av data med sikringskopiering og utforming av sikre dataoverføringsprotokoller.