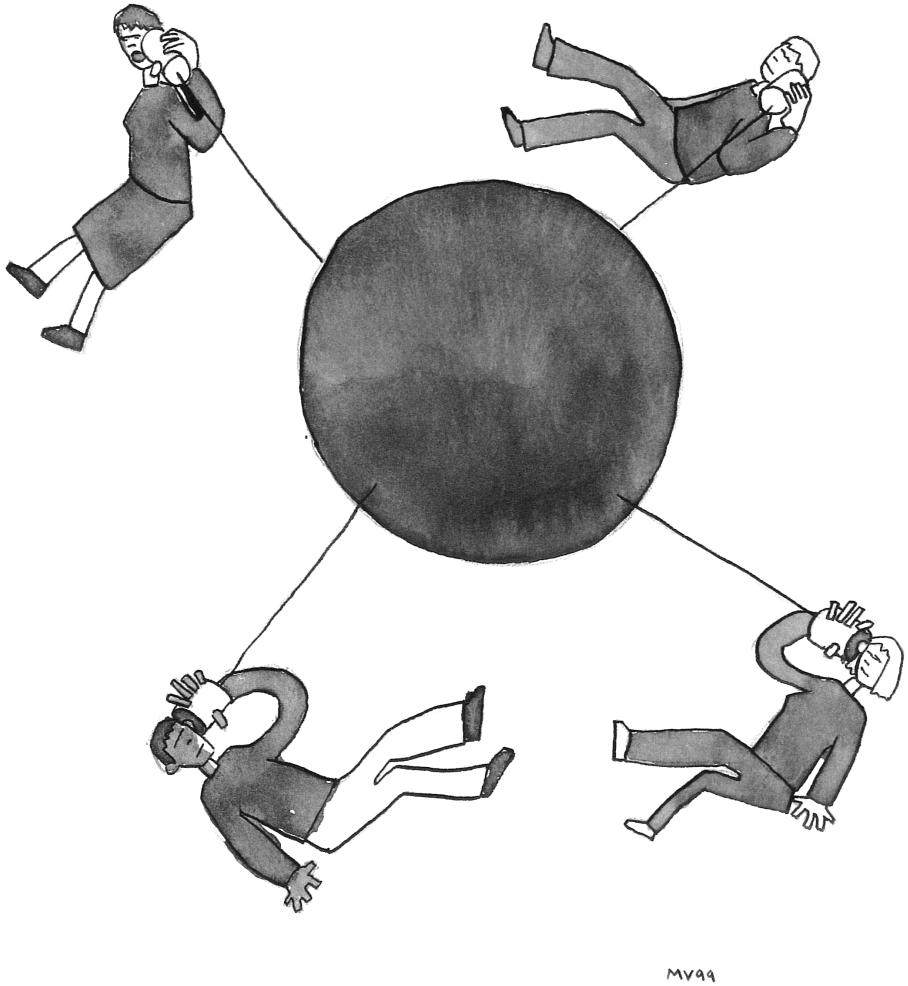
Del 2: IT, organisasjon og samfunn



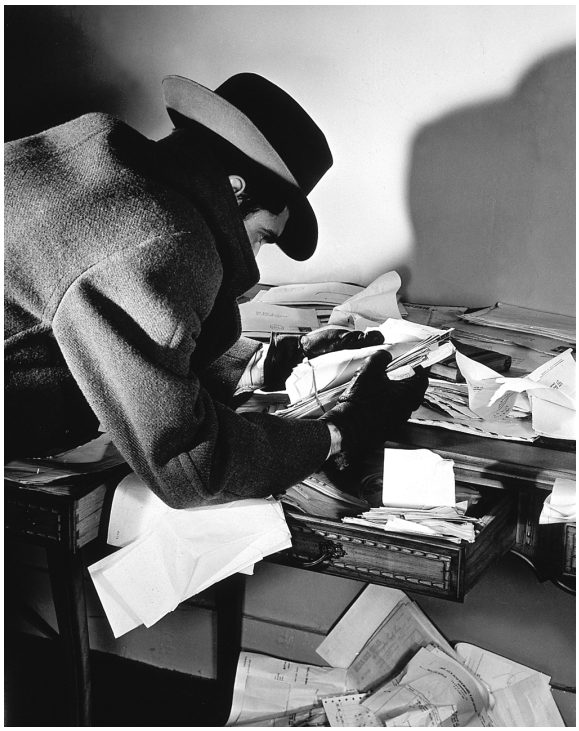


Foto: Scanpix/Superstock

4 IT, samfunnet og Lovverket

Som borger i et demokratisk land er det din soleklare rett å ha meninger om bruken av IT i samfunnet. Du har også rett til å beskytte deg mot negative virkninger av IT. For å kunne benytte deg av disse rettighetene må du ha kunnskap. Denne boka er et verktøy i din jakt på kunnskap om IT.

Så langt har du lest om tekniske definisjoner og verktøy. I delkapittel 1.3.3 leste du at programvare er delt inn i tre hovedtyper, men visste du at det er lovbrudd å bruke kopiert programvare? I kapittel 3.6.11 lærte du at e-brev i utgangspunktet kan leses av "alle", men tenkte du over at dette kan være en trussel mot ditt personvern?

Dette kapittelet skal gi deg et innblikk i, og en forståelse av, at IT ikke er løsrevet fra det juridiske regelverk som styrer samfunnet. Du skal også tenke over at IT er politikk. For Informasjonsteknologi er også det. Det er politikk at de ansatte har krav på opplæring og medvirkning når nye IT-systemer skal innføres i en

virksomhet. Det er politikk at det ikke uten videre er lov til å lagre opplysninger om din helsetilstand eller seksuelle legning.

Målet med dette kapittelet er ikke å gi deg en fullstendig innføring i IT og juss. Det er heller ikke meningen å gi en total oversikt over ulike samfunnsproblemer som kan knyttes til IT. Målet er å gi deg nok kunnskap til å tenke selv.

Hvis vi skal gi en kort oversikt over de viktigste lover og regler som gir deg rettigheter og plikter i forhold til IT, så kan vi liste dem opp som følger:

- *Straffeloven*: Forbyr endring og ødeleggelse av data, urettmessig innsyn i og bruk av data og ulovlig bruk av datautstyr.
- *Personopplysningsloven*: Regulerer retten til å opprette arkiv med personopplysninger, hvilke opplysninger som kan lagres og gir deg innsyn i hva som er lagret om deg.
- *Arbeidsmiljøloven*: Gir blant annet arbeidsgiver plikt til å gi arbeidstakerne relevant og forståelig informasjon.
- *Forvaltningsloven*: Gir rett til innsyn i offentlig saksbehandling.
- *Lov om opphavsrett*: Regulerer bruken av andres åndsverk, så som bilder, dataprogram etc.
- *Aksjeloven og Regnskapsloven:* Setter krav til økonomisk informasjon.
- *Lov om forebyggende sikkerhetstjeneste*: Gir blant annet adgang til monitoring og inntrenging i informasjonssystemer. Erstatter det tidligere *Datasikkerhetsdirektivet.*

Du som leser denne boka skal kanskje en dag ut i en bedrift for å utvikle et nytt informasjonssystem eller utbedre et eksisterende. Som systemutvikler vil du først og fremst måtte ta hensyn til Arbeidsmiljøloven med forskrifter, dataavtalen mellom LO og NHO, og Personopplysningsloven. I tillegg kan du få bruk for å ha kjennskap til Straffeloven, Lov om opphavsrett, Forvaltningsloven og Offentlighetsloven. De to siste lovene skal vi ikke behandle her, og det samme gjelder for Aksje- og Regnskapsloven. Lov om forebyggende sikkerhetstjeneste vil bli nevnt i delkapittel 4.3.3 der vi skal se litt på interessene til personvernet kontra andre interesser.

4.1 Informasjonsteknologi og straffeloven

Dersom du etter studiet får deg jobb som IT-ansvarlig ved en virksomhet, vil en del av arbeidet ditt gå ut på å kjenne til hvilke lover som beskytter de datasystemer din virksomhet benytter seg av. Du skal også vite litt om hvordan du skal gå frem dersom du oppdager innbrudd eller angrep på det datasystemet du har ansvaret for, hvem i politiet som skal etterforske det og litt om hvordan man går frem ved etterforskning og sikring av bevis i saker som involverer datamaskiner.

Men la oss først se på det lovmessige.

4.1.1 Uberettiget adgang til datasystemer

Den loven som først og fremst er av interesse her er Straffelovens §§ 145 og 393. La oss først se på § 145.

> ***§ 145**. Den som uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder.*
>
> *Det samme gjelder den som ved å bryte en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske midler.*
>
> *Voldes skade ved erverv eller bruk av slik uberettiget kunnskap, eller er forbrytelsen forøvet i hensikt å skaffe noen en uberettiget vinning, kan fengsel inntil 2 år anvendes.*
>
> *Medvirkning straffes på samme måte.*
>
> *Offentlig påtale finner bare sted når allmenne hensyn krever det.*

Som vi ser er det § 145 annet ledd som direkte henviser til IT, og det straffbare er her beskrevet som det å bryte en beskyttelse eller på lignende måte uberettiget skaffe seg adgang til data eller programutrustning.

Case 1: Inntrenging i SAMSON

Peder Ås er informatikkstudent ved Høgskolen i Lillevik. Han er en ivrig student og levende interessert i alt som har med UNIX, Internett og IRC å gjøre. Høgskolen i Lillevik benytter en HP-UNIX maskin, kalt SAMSON, som e-postserver, og studentene har tilgang til sine kontoer på maskinen via telnet. De ansatte har også sine e-postkontoer på denne maskinen.

Peder Ås har kontakt med andre som deler hans interesser i både Norge, USA og Canada og sammen planlegger de å benytte de ulike brukerkontoene på SAMSON som områder for IRC-servere og lagringsplass for piratkopiert programvare.

Peder Ås vet at i denne type datasystem er passordfilen åpen tilgjengelig. Han finner fila og kjører et passord-knekker program på den og får således tilgang til de ulike brukernes passord. Peder Ås distribuerer disse passordene til sine kontakter og sammen bryter de seg inn i en rekke brukerkontoer, for å installere IRC-servere og lagre piratkopiert programvare. SAMSON klarer ikke å håndtere den økte belastningen som IRC og nedlastning/lagring av piratprogram medfører, og går ned. Samtlige brukerkonti går tapt.

IT-avdelingen ved Høgskolen i Lillevik bruker en måned, med intensiv jobbing både morgen og kveld, for å restaurere kontoene og sette nye passord på hver enkelt av de 107 ansattekontoene og ca 100 studentkontoer. Flere av studentkontoene går tapt for alltid, fordi disse ikke blir tatt backup av like ofte som de ansattes konti.

Som vi ser i dette caset forbryter Peder Ås seg mot straffelovens § 145, 2. ledd. Han bryter beskyttelsen på brukerkontiene ved å knekke passordene i passordfilen, og får dermed uberettiget adgang til kontiene. Selv om Peder Ås ikke gjør seg kjent med hva som ligger på den enkelte konto, har han likevel forbrutt seg mot straffelovens § 145, 2. ledd, fordi det som loven regner som straffbart selve det å skaffe seg uberettiget innsyn.

Det er altså ikke nødvendig at inntrengningen har ført til skade eller at den har gitt noen en uberettiget vinning. Dersom en slik skade skjer eller noen får en uberettiget vinning av innbruddet, øker strafferammen fra 6 måneder til to års fengsel.

For at Peder Ås skal bli straffet må Høgskolen i Lillevik anmelde forholdet til politiet, jamfør siste ledd i paragrafen. Problemet i slike tilfeller er at svært få institusjoner anmelder forholdet, enten fordi de ikke vil offentliggjøre det at noen har klart å bryte seg inn datasystemet eller fordi de ikke har noen tro på at anmeldelse vil føre til noe.

Det er § 145 som er selve hovedparagrafen og som ved lov av 12. juni 1987 fikk sin nåværende form nettopp som et ledd i kampen mot datakriminalitet. Men straffeloven har enda en paragraf som er interessant i forbindelse med uberettiget adgang til datasystemer, nemlig § 393.

> ***§ 393****. Med Bøder straffes den, som retsstridig bruger eller forføier over Løsøregjenstand, der tilhører en anden, saaledes at den berettigede derved paaføres Tab eller Uleilighed, eller som medvirker hertil.*

I det foregående caset så vi at Peder Ås og hans medhackere benyttet SAMSON til IRC-servere og lagringsplass for piratkopiert programvare. I dette tilfellet var det et helt klart brudd på straffelovens § 393, særlig fordi det ikke bare var rettsstridig men også fordi det påførte Høgskolen i Lillevik skade ved at maskinen gikk ned og brukerkonti gikk tapt.

Men ikke alle tilfeller er like klare.

Case 2: Ulovlig bruk av datamaskiner , jfr straffelovens § 393. Høyesterettsdom av 1998-0083 B, snr 26/1998 (Svært forkortet utdrag)

A var tiltalt for brudd på straffelovens § 145, annet ledd og straffelovens § 393, i forbindelse med en test av datasikkerheten ved Universitetet i Oslo.

A benyttet seg av IP-adressen til UiOs WWW-server for å få opplysninger om to andre maskiner i nettverket. Ved bruk av finger mot en av disse maskinene fikk han ytterligere opplysninger om en arbeidsstasjon i nettet. Lagmannsretten mente at siden både WWW-serveren og den ene av de andre maskinene hadde vært i aktivitet som en følge av de kommandoer A gav og at det dermed kunne sies å være en overtredelse av straffelovens § 393 om ulovlig bruk av datamaskiner.

I denne saken kom flertallet i høyesterett frem til at dette ikke kunne ansees å være uberettiget bruk iht § 393. Flertallet mente at den som har koblet sin datamaskin til Internett, og har valgt å la den svare på forespørsler, må ansees å ha gjort maskinen til en del av det informasjonssystem som Internett representerer. Følgelig har datamaskineier akseptert at det blir rettet forespørsler til maskinen om hvilken informasjon den har å tilby, og den aktivitet som forekommer når maskinen svarer på en slik henvendelse kan ikke defineres som uberettiget bruk av maskinen.

A ble frifunnet for brudd på straffelovens § 393.

Mindretallet mente at A hadde gjort seg skyldig i brudd på § 393.

Hvem er du enig med - flertallet eller mindretallet?

I de andre kapitlene vil du finne tilnærmet faktaopplistinger og momenter som du helt klart kan se at "sånn er det". Som du kanskje allerede har fått en mistanke om er dette nesten umulig i jussen. Her er det meste basert på skjønn og fortolkninger, som vist i det siste caset. Du synes kanskje at det første caset var klart? Javel, men hva nå om Høgskolen i Lillevik hadde valgt dårlige passord, for eksempel fornavnet på den enkelte bruker, for de ulike kontoene? Kan slik passordbeskyttelse kalles en rimelig foranstaltning? Eller er en slik passordbeskyttelse så utilstrekkelig at man må anse maskinene som ubeskyttet og åpne mot nettet? Vil i såfall det ha betydning for hvorvidt en inntrenging er uberettiget?

Klare svar på dette kan kun domstolene gi.

Hva synes du?

4.1.2 Andre lovbrudd

Vi har nå snakket om uberettiget adgang til datasystemer, men dette er bare en type lovbrudd, som sammen med en rekke andre utgjør det vi kaller IT-kriminalitet. Men hva ligger egentlig i dette begrepet? Tradisjonelt kan vi si at IT-kriminalitet er når du:

- Bruker et datasystem for å svindle folk, tjene penger ved hjelp av bedrageri, eller for å begå tyveri som for eksempel å piratkopiere programvare.
- Forandrer eller ødelegger et datasystem uten å være autorisert for det, det vil si at du er ansatt som IT-ansvarlig og har lov til å forandre eller slette datasystemer.
- Gir deg selv tilgang til et datasystem eller datafiler uten å ha tillatelse til det, eller forsøker å skaffe deg slik tilgang.

Ut fra dette ser vi at handlinger som det å distribuere barnepornografi, hvitvaske narkotikapenger eller drive ulovlig spillevirksomhet ved hjelp av IT ikke kan kalles IT-kriminalitet ut fra en tradisjonell forståelse.

I dag er det imidlertid mest vanlig å definere alle straffbare handlinger som begås ved utnyttelse av informasjonsteknologi som IT-kriminalitet, selv om vi fortsatt skiller mellom IT-kriminalitet og bruk av IT i tradisjonell kriminalitet.

De viktigste former for IT-kriminalitet er:

- datainnbrudd
- databedrageri
- informasjonsheleri
- skadeverk
- ulovlig bruk av datakraft
- dokumentfalsk
- piratkopiering
- beskyttelsesbrudd – TV- og radiosignaler

Du har kanskje hørt om noe som kalles *"Distributed Denial-of-Service attack" (DDoS-angrep)*? Et DdoS-angrep er når noen bruker flere kraftige datamaskiner til samtidig å sende store mengder forespørsler en datamaskinen de ønsker å angripe. Dette kan føre til at den angrepne datamaskinen bryter sammen.

Et eksempel på et slikt angrep skjedde den 8. februar 2000, da noen gikk til angrep på nettstedet Yahoo! Tusenvis av brukere ble sannsynligvis omfattet av

angrepet da de plutselig ikke kunne bruke Yahoo! sine tjenester fordi belastningen fra angrepet ble for stort for Yahoo! sin server. Vi har også eksempler på at enkeltpersoner blir utsatt for slike angrep nesten hver gang de er ute på Internett. Mens tjenestetilbydere har avanserte logger og utstyr for sporing av trafikk har den vanlige hjemmebruker ingen slik beskyttelse. Og uten skikkelige logger og sporingsverktøy som viser hvem som utførte angrepet hjelper det ikke å anmelde forholdet til politiet. Du kan imidlertid beskytte deg selv ved å installere såkalte brannmurprogram. Et eksempel på et slikt program er ZoneAlarm, som du kan laste ned gratis fra Internett.

I følge politiet er IT-kriminaliteten sterkt økende.

4.1.3 Politiets oppgave

I Norge er det ØKOKRIM som står for etterforskning av IT-kriminalitet. Den enheten innenfor ØKOKRIM som har ansvaret for slik etterforskning kalles IKT- eller Datakrimteamet. Teamet består av både jurister og datafolk. Lederen for teamet er en jurist (førstestatsadvokat). ØKOKRIM behandler selv bare et begrenset antall saker og flesteparten av sakene behandles av lokale politidistrikter. ØKOKRIM tar først og fremst saker som er alvorlige eller komplekse eller har forgreninger til utlandet. Dersom en sak har prinsipiell betydning, hender det at ØKOKRIM tar den for å få avklart rettsspørsmålet eller straffenivået for politiets håndtering av lignende saker.[1]

Når politiet har avdekket et lovbrudd, slått fast hvilken rolle IT-utstyr har spilt i saken og fått de nødvendige hjemler til å aksjonere, blir det viktig å sikre åstedet. Dersom lovbryterne får tid på seg kan viktige bevis slettes med et tastetrykk.

Tenk deg at du er politimann. Du og dine kolleger er i ferd med å komme på sporet av en barnepornoring som benytter seg av Internett for å spre sine bilder.

Pedofile kan benytte seg av Internett på ulike måter, men oppslagstavler og diskusjonsgrupper er nok det vanligste. Se kapittel 3.2.2, 3.7 og 3.8 for nærmere informasjon om hva oppslagstavler og diskusjonsgrupper er for noe. For en politimann vil det være viktig å orienterer seg på Internett om hvilke diskusjonsgrupper som finnes og hvilke samtaler som foregår der.

Når så du og dine kolleger er klare til å gå til aksjon, gjelder det å sikre alt elektronisk utstyr som kan inneholde bevis i saken. Da må du straks sikre åstedet ved å bevare områder der det kan være fingeravtrykk, samt stanse all tilgang til datamaskiner. Videre må du koble datamaskinen(e) fra eventuelle nettverk eller modem. Når du har gjort dette, kan du begynne å undersøke datamaskinen(e), koble dem fra strøm etc, notere hva du kan finne på skjermen, osv.

I tillegg kan faksmaskiner, personsøkere, mobiltelefoner og håndholdte datamaskiner (Palm Pilot) inneholde informasjon som kan være vesentlig for saken. Du

[1] www.okokrim.no

må aldri slå på elektronisk utstyr du finner på et åsted. Dersom du av en eller annen grunn er helt nødt til å gjøre det, så pass på at du noterer deg hva du har gjort.[2]

Det å finne frem til bevis er alltid en utfordring, men det vil være særlig utfordrende i saker der datamaskiner er involvert. Du må ha gode datakunnskaper for å finne og ta vare på bevis i slike saker. Og det kreves forsiktighet i behandling og transport av elektroniske bevis. Vær også oppmerksom på at datamaskin-genererte bevis kan forfalskes og endres uten at det finnes spor etter dette. Det er derfor svært viktig at du hindrer muligheten for slike endringer straks du har sikret bevisene.

Når du nå har tatt beslag i datautstyret til den/de mistenkte må du være klar over at viktige filer kan være kryptert. Innholdet av en kryptert fil vil vises som en meningsløs samling med karakterer. Hvis vi åpner en fil som er kryptert med PGP i Notepad vil et lite utsnitt av den se slik ut:

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.3 for non-commercial use http://www.pgp.com

qANQR1DBwnMDXbpSDDwOpY4QDJEBS5lnqcHQjpZMZR/O8H3bKZMebJB0mlh6
1PLE6gInw9BznthJQXB0ls4o79ZFUcMk1DWBoynIGVVFc4xue5L4FN/xKqsZFEZYk
plZwSnKecBPKRC2uCVz3w0SYwAwRyroXJbKCKFE4OAvR7Tc+h08xc3a6vTUlaHy
of83IO472IhMHWHnTeAiYhag6KYtBL/a6VyYjv32oo2b9qHRO6/2EC/2Ey2xA5omUZ
D+E5hkTxSd5AWDar7EHpAmK9XRSrNX7T44o6gXr+rsLXem8IGOqqQ1SMlf9F9tLq
XrUKSHlPKQ5+BNnqTu3OnjHaqOHFWfjioTbH3MoAWFNUo4j27z8MUtgRArsY1xe
Hb+XrZPGrZBbQL2mLF9YUVKT0X6GCtFzWSdeeCFcnCRurkEiU427umvKPPwpp4
x8epMJ1kH7d8O1+Sr43vlmtJSgO8flCUmezctvUBxiypS4HMN95tJMz+qiBRZf4SsS/
GEQFcgwaV4/sFBrlBbeuxXvns6O4MTYL1s9XtHqQtcAzUvIi7UgvnwDJCS+KhiB3P
BUk0ZLFI74Igl4eb+/up3LaO2I11S4FlucelioWssHKkNoGGXPmFHuCe/YE8YTjYQo
g+hRq6DDMrKmjx6pYhPl1ofdUDUQwhfRWrDq1/4BVwqAYasUDdtOF6t9fdVozTyrU
EYA76o3ghIrQLVIIIYEZYGQ/4HNYeiue+tbEQu5G4tJ353SSk4fj2MD10rMRr7M9j8P/
H4Vp5hmDP2vm59KTb7OySadzti5+3GSi4PqNtLoqiD5NKinTFvPq9ECDZDPEuDdz
uXDjzVMNpJiYbE/7m0lPoO+XHNU5tHm9DA37SI0mq1Puwo5ZwIHijXNR5LouP4LP
IAET66gwuvZJTh5FoAEl+Q8B4tb88w00JHj1YAmKRzOe+XMpUWdQ9SAdxla9TtD4
ATJ43OMOe9UhlffAQUNQSEfzquCAFoN3Zjn4OQlwf3m5gkqNtzh2B2dTi/2Ze30EO
gVTUzOT12vn7Vk3Yl5eITqaqV9o+mUJwlQLm/PKMRoPCKjkWW4dSBjiINVVNx3Jy
2SWvMAg3J7OXpuU7KoDHvVX2GTUk5mRK0jIXPWHEaP7gkZO7ZlWjfeSng
```

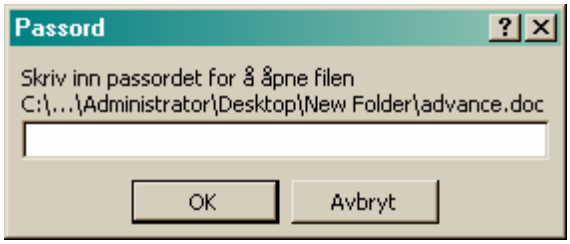
Hvis du finner krypterte filer så se om du finner krypteringsprogrammet som er brukt, eller om maskinen har et krypteringskort installert, samt eventuelle bruker-håndbøker. Å forsøke å knekke koden uten krypteringsnøkkelen vil høyst sannsyn-

---

[2] Utdrag fra BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE, *A Joint Project of the International Association of Chiefs of Police and the United States Secret Service (http://www.treas.gov/usss/index.htm?electronic_evidence.htm&1)*

lig være bortkastet, med mindre algoritmen er svært enkel eller du finner passordet til nøkkelen. I den forbindelse er det viktig at du finner ut hvor brukeren har oppbevart sine krypteringsnøkler. Disse kan ligge på en diskett eller på datamaskinen.

Filer kan også være passordbeskyttet, for eksempel ved hjelp av passordbeskyttelsen i Word.



Figur 1: Passordbeskyttelse av fil i Microsoft Word

Dersom den mistenkte ikke gir fra seg passordet kan en siste utvei være at du forsøker å knekke filene. Gå da frem på følgende måte:

- Let etter passord som er skrevet ned, enten på en papirlapp eller i en tekstfil.
- Forsøk med ord, navn eller tall som kan knyttes til den mistenkte.
- Ta kontakt med programvareprodusenten, for eksempel Microsoft Norge, å få deres hjelp til å knekke passordet.
- Finn og bruk passord-knekker program på Internett. De fleste av disse programmene benytter det som kalles "brute force" eller "ordbok" angrep, og vil være nyttige for mindre avanserte passord.

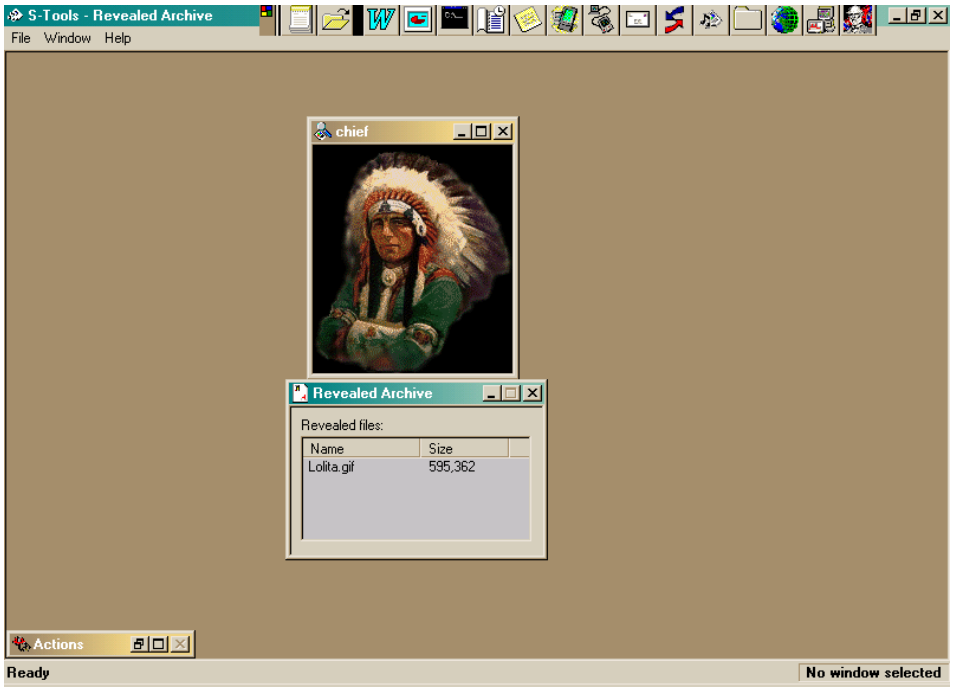
I de aller fleste filfeller vil oppgaven med å knekke krypterte og passordbeskyttede filer ikke være noe som utføres ved det enkelte politikammer eller lensmannskontor, men bli overlatt til spesialister sentralt. Men det finnes flere måter en mistenkt kan skjule dokument eller bilder på, og en av de mest kjente metodene er det som kalles Stegonografi. I motsetning til kryptografi som gjør en fil uleselig gjør stegonografi filen usynlig. Den mistenkte kan da nekte for at det finnes ulovlig materiale på hans maskin. Stegonografi skjuler data, enten det er i form av tekst eller bilder, inne i annen data. Billed- og lydfiler inneholder nemlig ubrukte eller lite viktige områder og disse områdene kan benyttes til å lagre data.

La oss si at du har tatt beslag i datautstyr hos en som er mistenkt for å spre barnepornografi på Internett. Men de eneste bildene du kan finne på datamaskinen er bilder av indianere. Og siden data kan lagres i bilder uten at bildene nødvendigvis forandrer utseende eller kvalitet har du neppe noen muligheter til å oppdage om stegonografi er benyttet.

Men har du mistanke om at dette kan være tilfelle må du lete etter stegonografi-program på datamaskinen. Det finnes ulike program for dette, men et eksempel er S-Tools som kan lastes ned fra Internett.

Figur 2 viser et eksempel på at et bilde er skjult i annet bilde ved hjelp av S-Tools.

Vær også observant på at mapper og filer kan være lagret som "skjulte" eller "slettet" og derfor ikke synlig. Der finnes ulike program som kan benyttes til å søke etter og finne slike mapper og filer. Orienter deg om hvilke program som finnes og sørg får at du har disse tilgjengelig.



Figur 2: Eksempel på et bilde skjult i et annet bilde ved hjelp av S-Tools

Det du nå har lest gjelder kun dersom du er polititjenestemann. Dersom du er IT-ansvarlig og oppdager et tilfelle av datakriminalitet skal du nøye deg med å anmelde forholdet til nærmeste politikammer eller lensmannskontor.

La oss tenke oss at du er IT-sjef ved en høgskole. Studenthyblene er oppsatt med Internett-tilknytning via høgskolens nettverk. En dag får du en e-post fra UNINETT om at det er rapportert et forsøk på å angripe en virksomhets data-system. Du får oppgitt ip-nummeret til maskinen som har stått for angrepet og ser straks at dette nummeret tilhører en studenthybel. Du tar kontakt med Studentsamskipnaden og sammen finner dere frem til en hybel. Nå kan du varsle

dine overordnede og i samarbeid med dem kalle studenten inn til et møte. Dersom ikke den fornærmede part (den virksomheten som ble angrepet) anmelder det, er det egentlig ikke så mye du kan gjøre. Men det er fullt mulig å anmelde forholdet for å gi et kraftig signal til studentene om at slik virksomhet ikke blir godtatt. Du må da imidlertid regne med at saken blir henlagt. Men under ingen omstendighet har du lov til å ransake hybelen og foreta beslag i det som måtte være der av elektronisk utstyr.

4.2 Informasjonsteknologi og Lov om opphavsrett til åndsverk

Folk flest synes nok at det må være greit å kopiere dataprogram, og reflekterer nok ikke så mye over at dette faktisk er straffbart. Dataprogrammer er i utgangspunktet opphavsrettslig beskyttet. Det betyr at de ikke kan brukes uten rettighetshavernes samtykke. Dette reguleres av Lov om opphavsrett til åndsverk med videre der lovens §12 avgrenser retten til kopiering til eget bruk.

Som databruker skaffer du deg lisens ved å kjøpe program med lisens hos en dataforhandler. Etterhvert har svært mange dataprogrammer blitt tilgjengelige på Internett. Dersom programmene ikke er frigitt for spredning av rettighetshaver, vil det å laste dem ned til egen maskin være straffbart etter åndsverkloven § 54. Strafferammen er bøter eller fengsel inntil tre måneder, men inntil tre år dersom det foreligger særlig skjerpende omstendigheter.

Det finnes programvare som er frigitt for spredning, såkalt "freeware". Det finnes også mellomformer som "shareware" og "trialware". Dette er gjerne programmer som fritt kan brukes et gitt antall dager før programmet må lisensieres. Dersom du er i tvil om hvorvidt et dataprogram er opphavsrettslig beskyttet, kan du kontakte BSA (Business Software Alliance, telefon 80080055, URL: http://www.bsa.org/europe/norway). BSA representerer programvareprodusentene og er en verdensomspennende organisasjon for bekjempelse av piratkopiering.

I likhet med straffeloven skal vi ikke ta for oss hele Lov om opphavsrett til åndsverk, men ta ut de paragrafene som er av interesse for oss som IT-brukere. Vi skal derfor i det følgende se litt nærmere på lovens § 12 som avgrenser retten til kopiering til eget bruk.

Men først en definisjon av begrepet "åndsverk". Et åndsverk er et resultat av en skapende individuell innsats. Lovens § 1 sier det slik:

> ***§ 1**. Den som skaper et åndsverk, har opphavsrett til verket.*
>
> *Med åndsverk forståes i denne lov litterære, vitenskapelige eller kunstneriske verk av enhver art og uansett uttrykksmåte og uttrykksform, så som*
>
> 1. *skrifter av alle slag,*
> 2. *muntlige foredrag,*

3. *sceneverk, så vel dramatiske og musikkdramatiske som koreografiske verk og pantomimer, samt hørespill,*
4. *musikkverk, med eller uten tekst,*
5. *filmverk,*
6. *fotografiske verk,*
7. *malerier, tegninger, grafikk og lignende billedkunst,*
8. *skulptur av alle slag,*
9. *bygningskunst, så vel tegninger og modeller som selve byggverket,*
10. *billedvev og gjenstander av kunsthåndverk og kunstindustri, så vel forbildet som selve verket,*
11. *kart, samt tegninger og grafiske og plastiske avbildninger av vitenskapelig eller teknisk art,*
12. *datamaskinprogrammer,*
13. *oversettelser og bearbeidelser av verk som er nevnt foran.*

Her ser vi at lovens § 1 i pkt 12 nevner *datamaskinprogrammer*.

Programmer er altså å regne som et verk som er skapt av en individuell innsats og følgelig beskyttet av loven. I de fleste andre tilfeller som loven regner som åndsverk tillates det at man tar en kopi til privat bruk. Dette reguleres av lovens § 12.

> ***§ 12**. Når det ikke skjer i ervervsøyemed, kan enkelte eksemplar av et offentliggjort verk fremstilles til privat bruk. Slike eksemplar må ikke utnyttes i annet øyemed.*
>
> *Bestemmelsen i første ledd gir ikke rett til å*
>
> *a) ettergjøre bygningskunst gjennom oppføring av byggverk,*
>
> *b) fremstille maskinlesbare eksemplar av datamaskinprogram, eller*
>
> *c) fremstille eksemplar av kunstverk ved fotokopiering, avstøpning, avtrykk eller tilsvarende fremgangsmåte når eksemplaret kan oppfattes som originaleksemplar.*
>
> *Bestemmelsen i første ledd gir ikke rett til å la fremstillingen utføre ved fremmed hjelp når det gjelder gjenstander av kunsthåndverk og kunst-industri, skulptur, billedvev eller kunstnerisk gjengivelse av andre kunstverk. Gjelder det musikkverk eller filmverk, kan fremstillingen av eksemplar ikke utføres ved fremmed hjelp som medvirker i ervervsøyemed.*

La du merke til det klare unntaket for programvare her?

Loven gir altså klar beskjed om at kopiering av programvare til privat bruk ikke er tillatt.

Case 1: Marte Kirkerud og Office 97

Marte Kirkerud var student ved Høgskolen i Lillevik. Ad omveier hadde hun fått fatt i en av høgskolens CD`er med programmet Office 97. Hun tok det med seg hjem og installerte det på sin datamaskin. CD`en hørte til Høgskolens samling av SELECT-CD`er slik at serienummeret var ferdig installert i programmet, noe som gjorde det uproblematisk for Marte å installere Office-pakken på sin maskin.

Case 2: Peder Ås og de hemmelige programbasene

Peder Ås var en ivrig internettbruker og vel kjent med hvor på Internett det ble lagt ut piratkopierte programvarepakker med lisensnummer. Han var stadig ute på nettet og hentet ned siste nytt i ulike programtyper. Peder Ås var veldig fornøyd med dette, fordi han sparte en masse penger. Og dessuten var det jo andre som hadde lagt programmene ut på Internett, han lastet dem jo bare ned – og det kunne det vel ikke være noe galt i.

Hva synes du?

La oss så avslutte dette delkapittelet med å se på lovens §§ 39g - 39h.

> ***§ 39g.*** *Opphavsrett til datamaskinprogram som er skapt av en arbeidstaker under utførelsen av oppgaver som omfattes av arbeidsforholdet eller etter arbeidsgivers anvisninger går, med den begrensning som følger av § 3, over til arbeidsgiveren, med mindre annet er avtalt.*

Hvis du jobber som programutvikler i en virksomhet og har som arbeidsoppgave å utvikle en bestemt type programvare, så kan du ikke ta med deg den programvaren og benytte den som du selv vil, dersom du slutter eller blir oppsagt.

> ***§ 39h.*** *Rettmessig erverver av datamaskinprogram kan fremstille eksemplar av, endre og bearbeide programmet i den utstrekning det er nødvendig for å bruke programmet i samsvar med dets formål, herunder også for å rette feil i programmet.*
>
> *Den som har rett til å bruke et datamaskinprogram, kan fremstille sikkerhetseksemplarer i den utstrekning det er nødvendig for utnyttelsen av programmet.*
>
> *Den som har rett til å bruke et eksemplar av et datamaskinprogram kan, i forbindelse med slik lesning, fremvisning på skjerm, kjøring, overføring eller lagring av programmet brukeren er berettiget til å utføre, iaktta, undersøke eller prøve ut hvordan programmet virker for å fastslå ideene og prinsippene som ligger til grunn for de enkelte deler av programmet.*
>
> *Bestemmelsene i andre og tredje ledd kan ikke fravikes ved avtale.*

§ 39hs andre ledd er mest interessant for vår del. Mange brukere ved en institusjon tror at denne bestemmelsen gir den enkelte bruker lov til å ta en kopi av programmet for å ha det som reserve dersom noe skjer med den opprinnelige installasjonen, for eksempel på en reise eller på et lengre studieopphold.

Men i slike tilfeller er det aldri den enkelte ansatt i en virksomhet som er å regne som rettmessig erverver, men institusjonen som sådan, representert ved IT-personalet.

Men som privatperson med egenkjøpt program har du lov til å lage deg en sikkerhetskopi av programvaren.

I tillegg til Lov om opphavsrett til åndsverk vil de individuelle lisensavtaler regulere dine rettigheter og plikter i forhold til programvare.

4.3 Informasjonsteknologi og personvern

Informasjonsteknologien har gitt oss verktøy som kan gi automatisk støtte for innsamling og lagring av informasjon. Dermed har vi også fått et verktøy for å lage flere informasjonsregistre over personer som vi enten kan benytte enkeltvis eller slå sammen for å få et mest mulig helhetlig bilde av en person.

I vårt samfunn er du og jeg registrert i en rekke ulike registre, både offentlige og private. Antallet registre som inneholder persondata ligger på noe over 1 million. Det sier seg selv at i en slik oppsamling og organisering av personopplysninger kan det forekomme sensitive opplysninger om en person. Og at flere slike registre til sammen kan gi informasjon som er sensitiv. En slik samling av sensitive opplysninger kan være, eller oppfattes å være, en krenkelse av den enkelte persons privatliv. For å føre kontroll med denne type informasjon fikk vi i 1978 Personregisterloven, som så 1. januar 2001 ble avløst av Personopplysningsloven (Lov om behandling av personopplysninger).

For å påse at ditt og mitt personvern blir ivaretatt ble det i 1980 opprettet et frittstående administrativt organ underlagt justisdepartementet, som fikk navnet Datatilsynet. Datatilsynets oppgaver er regulert av Personopplysningslovens kapittel VIII, § 42 og er beskrevet som følger:

Datatilsynet skal

a) *føre en systematisk og offentlig fortegnelse over alle behandlinger som er innmeldt etter § 31 eller gitt konsesjon etter § 33, med opplysninger som nevnt i § 18 første ledd jamfør § 23,*
b) *behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette,*
c) *kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet,*

d) holde seg orientert om og informere om den generelle nasjonale og internasjonale utviklingen i behandlingen av personopplysninger og om de problemer som knytter seg til slik behandling,

e) identifisere farer for personvernet, og gi råd om hvordan de kan unngås eller begrenses,

f) gi råd og veiledning i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder bistå i utarbeidelsen av bransjevise atferdsnormer,

g) etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om behandling av personopplysninger, og

h) gi Kongen årsmelding om sin virksomhet.

I tillegg til Datatilsynet har vi nå også fått en Personvernnemd som består av syv personer, der leder og nestleder oppnevnes av Stortinget mens de øvrige fem oppnevnes av Kongen. Nemndas oppgave er å behandle og avgjøre klager på Datatilsynets avgjørelser. I likhet med Datatilsynet er også Personvernnemda et uavhengig forvaltningsorgan som er administrativt underordnet Kongen og Justisdepartementet.

4.3.1 Hva er personvern?

I norsk juridisk teori er personvern definert som den mulige interesse du har av å føre kontroll med den informasjon som beskriver deg selv. Det som her er lagt til grunn er at det er den aktuelle eller mulige bruk av informasjonen som kan føre til en krenkelse av ditt personvern. En slik definisjon betyr at så lenge informasjonen er lagret på en slik måte at ingen praktisk eller teoretisk kan benytte seg av opplysningene, så vil der heller ikke kunne foreligge fare for krenkelse av personvernet. Tradisjonelt blir personvernet sett på som en samling interesser som knyttes mot den som skal vernes. Disse interessene er delt i syv hensyn, der fire knyttes til individet mens tre er av mer almen samfunnsinteresse.

De syv hensyn

Christopher Sjule satt og kjedet seg på sitt kontor i Høgskolen i Lillevik. For å få tiden til å gå klikket han vilkårlig rundt i de ulike nettverksmappene han fikk opp på sin kontor PC. Plutselig rettet han seg opp i stolen; Heisann! “Personalmappe”, dette kan bli spennende tenkte Christopher Sjule fornøyd og begynte å lese om sine kolleger.

a) Diskresjon

Eieren av et personregister skal sørge for at uvedkommende ikke får tilgang til registeret. Dette betyr at eieren må ha regler for taushetsplikt, hva som kan registreres og gode sikringstiltak. Det skulle altså ikke vært mulig for Christopher Sjule å få tilgang til personalmappen med personopplysninger om sine kolleger ved Høgskolen i Lillevik.

Ved samme høgskole som Christopher Sjule satt Marte Kirkeby og leste forbauset gjennom de opplysninger som var registret om henne i Høgskolens personalmappe. "Herregud!" tenkte hun forskrekket, "her vrimler det jo av feil!"

b) Innsyn

Marte Kirkeby kunne sitte å lese gjennom de opplysninger som var registrert om henne, fordi den registrert skal ha rett til å vite hva som er registrert om vedkommende. At det vrimlet av feile opplysninger om henne skulle ikke ha forekommet, da det også er krav om

c) Fullstendighet

Dette betyr at det som registreres må være riktig og tilstrekkelig

Gamle enkefrue Karlsen i Lillevik tusler mot postkassen sin for å hente avisen. Forbauset ser hun at det sammen med avisen også ligger en katalog for pornografiske filmer. Navn og adresse var korrekt, men hun hadde da ikke bestilt noe slikt! Enkefru Karlsen kaster katalogen sint i søppelkassen

d) Privatlivets fred

Den registrerte har rett til å bli beskyttet mot for eksempel aggressiv markedsføring som følge av at man står i et kunderegister. Det er ganske vanlig at kunderegistre selges, slik at Enkefru Karlsen i Lillevik trenger ikke å ha bestilt pornografiske videoer for å få en slik katalog i posten. Men enkefruen har rett til å kreve seg slettet fra dette firmaets kundeliste, slik at hun slipper å få reklame derfra. Dette hjemles i Personopplysningslovens § 26.

"Privatlivets fred" er det uttrykk som danner grunnlaget for våre tanker om personvernet. I 1890 årenes USA hevdet to jurister, Samuel D.Warren og Louis D. Brandeis, at det i amerikansk rett eksisterte en såkalt "right to privacy". De to juristene satte i gang sin debatt om "privatlivets fred" på bakgrunn av at datidens presse stadig hadde oppslag om kjente enkelt personers private forhold.

Peder Ås åpnet konvolutten fra Teknisk etat i Lillevik kommune og leste avslaget om bygging av garasje på tomten sin. Avslaget var holdt i en standardisert form og viste til at vedtaket var basert på Lillevik kommunes nye databaserte saksbehandlingssystem.

e) Tap av forvaltningens menneskelige trekk

Dersom vi får en fullstendig automatisering av tjenester, for eksempel i butikker, banker, og i forvaltningen generelt, vil dette kunne føre til mangel på menneskelig kontakt.

Dersom forvaltningsvedtak i altfor stor grad baseres på datamaskiner, vil den enkelte borger kunne ha vanskelig for å forstå saksbehandlingen eller resultatet av en sak. Peder Ås har krav på å få en begrunnelse for vedtaket, både i henhold til Forvaltningslovens § 24 og i henhold til Personopplysningsloven. I Personopplysningslovens § 22 heter det at:

"Hvis en avgjørelse har rettslig eller annen vesentlig betydning for den registrerte og fullt ut er basert på automatisk behandling av personopplysninger, kan den registrerte som avgjørelsen retter seg mot, kreve at den behandlingsansvarlige gjør rede for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen."

Lars Holm er ansatt i Nasjonal Sikkerhetsmyndighet, et organ underlagt Forsvarsdepartementet som har til oppdrag å drive penetrering og monitoring av offentlige nettverk. Akkurat i dag var hans oppgave å overvåke all e-post til og fra ForsvarsTekno A.S som nettopp har fått en kontrakt med Hæren for levering av et nytt våpensystem. All e-post som blir sendt og mottatt av ledelse og de ansatte blir nøye lest og arkivert.

f) Maktmisbruk og urimelig kontroll

Enkeltmennesket må kunne vernes mot urimelig kontroll fra myndighetenes, eller andre grupper/ og eller personer i samfunnet. Av og til vil enkeltmenneskenes vern mot urimelig kontroll komme i konflikt med statens interesse av å verne sin sikkerhet. Akkurat det skal vi se litt nærmere på i underkapittel 4.4.3. Mens du leser videre kan du jo tenke litt på hvor du syns grensen mellom rimelig kontroll og urimelig kontroll bør gå.

Siri Holm gjespet. Det hadde vært en lang dag. Nå gjenstod en viktig sak før hun kunne ta kvelden. Alle opplysningene lå inne på etatens datasystemer, og hun klikket på ikonet som skulle gi henne tilgang. Men ingenting skjedde. Hun grep telefonen og ringte til IT-avdelingen. Etter noen minutter ringte en fortvilt konsulent tilbake. "Datasystemet er brutt sammen. Totalt serverkrasj. Og vi har ikke noe backup!"

g) Samfunnets robusthet

Dette siste hensynet dreier seg om sikkerhet mot sammenbrudd i forvaltningens databehandling. Et slikt sammenbrudd kan få alvorlige følger for enkeltmennesker, enten det gjelder behandling av vedtak eller utsendelse av trygd.

4.3.2 Hva er det som vernes etter Personopplysningsloven?

Etter Straffelovens § 390 er det straffbart å krenke "privatlivets fred ved å gi offentlig meddelelse om personlige eller huslige forhold". Straffelovens § 390 er selve hovedregelen i norsk rett om det som angår privatlivets fred, og var den viktigste lovregelen om personvern inntil vi fikk Personregisterloven i 1978.

Den nye Personopplysningsloven som trådde i kraft 1. januar 2001 gir den enkelte et enda bedre personvern i og med at den kommer til anvendelse på elektronisk behandling av personopplysninger mer generelt, og på manuell behandling av personopplysninger (dvs behandling uten bruk av elektroniske hjelpemidler) når personopplysningene inngår i eller skal inngå i et personregister. Loven innfører også en ytterligere understrekning av den enkeltes rett til å verne om sitt privatliv, og den enkeltes rett til innsyn i hvilke opplysninger som er innsamlet om vedkommende.

Hva defineres som sensitiv informasjon?

Sensitive personopplysninger er opplysninger om:

a) *Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning.*
b) *At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling.*
c) *Helseforhold*
d) *Seksuelle forhold*
e) *Medlemskap i fagforeninger.*

Personopplysningsloven § 2

Tidligere måtte du søke Datatilsynet om konsesjon for å opprette et personregister, men med den nye Personopplysningsloven kreves dette nå kun dersom du skal opprette et register med sensitive personopplysninger. (§ 33). For et personregister med ikke-sensitiv personinformasjon kreves det nå bare at du melder det inn til Datatilsynet (§§ 31 og 32)

Hvordan få konsesjon på personregister?

Den som ønsker å opprette et register som er konsesjonspliktig etter

Personopplysningsloven, må fylle ut Datatilsynets søknadsskjema som enten kan lastes ned fra Datatilsynets hjemmeside www.datatilsynet.no eller fåes tilsendt ved henvendelse til Datatilsynet, telefon: 22396900, telefaks: 22422350, eller via e-post: postkasse@datatilsynet.no

Søknadsskjemaet behandles så av Datatilsynet.

Når du først har fått konsesjon på et register, kan dette registeret kun benyttes til det sett med informasjon og til det spesifikke formål registeret ble opprettet for. Du

kan altså ikke underveis bestemme deg for å benytte opplysningene i registeret til andre formål for eksempel ved å koble dem til andre registre for å få mer informasjon. Dette reguleres av lovens § 11 *Grunnkrav til behandling av personopplysninger*, b) og c) som følger:

b) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet,

c) ikke brukes senere til formål som er uforenelig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker,

Et annet svært viktig punkt med den nye Personopplysningsloven er retten til å reservere seg mot direkte markedsføring. Denne retten er hjemlet i lovens § 26, der det blir slått fast at Kongen kan opprette et sentralt reservasjonsregister for direkte markedsføring der du får adgang til å sperre ditt navn mot bruk til direkte markedsføring. Alle som driver med direkte markedsføring, vil ha plikt til å oppdatere sitt eget adresseregister mot reservasjonsregisteret slik at når du har reservert deg slipper du å bli utsatt for direkte reklame.

4.3.3 Personverninteresser kontra andre interesser

Det er ikke uproblematisk å hevde et sterkt personvern i et samfunn som vårt. I mange tilfeller kan personvernet være til hinder for effektivitet, kommersielle interesser, etterforskning i straffesaker, samfunnets behov for sikkerhet, forbrukerinteresser, forskning, ol. Etter 11. september 2001 vil mange hevde at samfunnet må få benytte seg av alle metoder som kan gi myndighetene en mulighet til å være i forkant av terrorister og kriminelle.

Når det gjelder straffesaker kommer hensynet til personvernet og hensynet til bekjempelse av kriminalitet særlig sterkt frem i forbindelse med barnepornografi. I 1998 nektet Telenor politiet innsyn i sine abonnements registre utfra personvernhensyn, med støtte fra Datatilsynet. Politiet ønsket et slikt innsyn for å løse en barnepornografisak.

Case 1: Operasjon Katedral

Det surrer svakt i en kaffetrakter. Klokken er 05.00 en onsdag morgen. På et lite kontor i Oslo sitter Harry Hansen, spesialetterforsker i Økokrim. Harry Hansen sitt spesialfelt er kampen mot barnepornografi. Han ser trett på klokken. Det har vært en lang natt og en tidlig morgen. Men snart vil ting skje.

Det plinger svakt i datamaskinen hans og varsler en ny e-post. Harry Hansen klikker på den og ser at den er fra det britiske politiet. Meldingen er adressert ikke bare til ham, men også til kolleger i Finland, Sverige, Østerrike, Belgia, Frankrike, Tyskland, Italia, Portugal, USA og Australia. Det er klarsignalet. Operasjonen kan starte.

Harry Hansen griper etter telefonen og gir en kort beskjed.

Presis klokken 06.00 banker politifolk på 95 dører over hele verden med ett samlet formål: Å sprenge en pedofil sirkel som distribuerer barnesex på Internett.

En time senere ser Harry Hansen igjen på klokken. Den er nå 07.00. En melding kommer frem på dataskjermen hans. Det er en beskjed fra operasjonssentralen. Rundt 100 personer er nå hentet ut fra sine stuer og soverom. Av disse er åtte norske. Datamaskiner med kolossal kapasitet, samt tusenvis av disketter, er blitt beslaglagt i tidenes største barneporno-razzia..

Harry Hansen smiler svakt. Kanskje de denne gang har klart å rette et avgjørende slag mot distributører av barnepornografi?

Klokken er blitt 10.00 og den første listen over de norske arrestasjonene dumper inn i Harry Hansens elektroniske postkasse.

Den ene av nordmennene på listen er en mann i 40-årene, som under kodenavnet "Jeltsin" surfet rundt på nettet og blottet sine siste barneofre for sine åndsfrender i en ulovlige Internett-klikk. En annen nordmann påstår at han kun har vært inne en eneste gang på en barnepornoside på Internett. Mannens advokat beskyldte politiet for å ransake på et altfor spinkelt grunnlag.

Harry Hansen fnyser irritert. I følge de opplysninger Økokrim har var ikke denne databasen noe man tilfeldig ramler borti; den krever en bevisst handling fra brukeren, som trenger passord eller annen form for kode for å komme inn i basen.

Han strekker hånden ut etter kaffekoppen og sukker. Selv om aksjonen har vært vellykket lurer han på om det egentlig er noen vits. Tidligere saker har vist at straffen for denne typen forbrytelser er relativt mild: av de 23 personer som tidligere hadde blitt pågrepet i lignende saker, ble hovedmannen kun dømt til fengsel i 120 dager. Han slapp å sone 60 av dem, men fikk inndratt filmer, utstyr og 75 000 kroner i kontanter. Og hva med dem de hadde tatt denne gangen? Harry Hansen sukker igjen og setter fra seg kaffekoppen. Det er på tide å skrive rapport om operasjonen.

Case 2: Telenor Nextels taushetsplikt

I 1998 meldte nyhetene at Telenor Nextel nektet å oppgi navn på Internett-brukere i politiets søkelys uten rettslig kjennelse. Økokrim mente at en slik praksis ville hemme politiets arbeid. Bakgrunnen for uenigheten var en barnepornografi-sak der Kripos og Økokrim krevde å få opplyst hvem som var eier av et abonnement som ble brukt, og hvilket telefonnummer som ble brukt til å koble det opp på nettet. Økokrim mente at et krav om rettslig kjennelse kunne føre til så store forsinkelser at opplysninger om brukerne kunne bli slettet, og at viktig bevismateriale dermed kunne forsvinne.

Telenor Nextel på sin side hevdet at selskapet har plikt til å forlange rettslig kjennelse før man utleverte slik informasjon. Uenigheten mellom politiet og Telenor dreide seg i stor grad om hvilken type opplysninger som måtte utlevers. Politiet mente at dette utelukkende var abonnementsinformasjon som telefonnummer, navn og adresse. Etter at telekommunikasjonsloven ble endret sommeren 1998 var ikke disse opplysningene lenger taushetsbelagt. Telenor Nextel mente imidlertid at dette var opplysninger om trafikk- og samtaledata, som sa noe om når personene var koblet opp, og hva de foretok seg. Slik informasjon mente Telenor Nextel fortsatt var taushetsbelagt.

Hvordan vi skal gå frem for bekjempe slike ting som barnepornografi på Internettet, er et meget omdiskutert spørsmål. Tidligere justisminister Aud Inger Aure betegnet i sin periode et tysk forslag om å innføre kontroll av Internett som svært interessant. Tyskerne ville overvåke prategrupper og elektronisk post, samt hindre brukere i å operere anonymt på nettet. Også det norske Økokrim har sine synspunkter på dette.

(Fra Nettavisen 06. sept 2000)

Økokrim vil ha id-kontroll på Internett

Økokrim vil at alle nettbrukere må identifisere seg, i et forsøk på å bekjempe den stadig voksende kriminalitet i tilknytning til Internett.

Hvis Økokrim for gjennomslag for sitt syn, vil all surfingen du foretar på nettet bli registrert. Førstestatsadvokat Inger Marie Sunde sier til TV 2 at hun ser for seg at alle som bruker Internett må identifisere seg gjennom å bruke et elektronisk kort.

Økokrim ønsker også at Internettkafeer og andre steder der er mulig å koble seg på nettet, må loggføre hvilke sider kundene har vært inne på.

Disse loggene skal politiet så ha krav på å få utlevert, mener Økokrim. Samtidig vil de også heve strafferammen for datainnbrudd, forby anonyme mobiltelefoner, og innføre forbud mot salg av anonyme kontantkort.

Fra 1.1.2002 fikk vi en ny sikkerhetslov, Lov om forebyggende sikkerhetstjeneste, der det blant annet fastslås regler som sikrer kontroll med informasjon som behandles, lagres eller transporteres i informasjonssystemer. I henhold til lovens kapittel tre er det opprettet et eget sentralt organ som kalles Nasjonal Sikkerhetsmyndighet, som skal sikre at skjermet informasjon forblir skjermet. NSM skal i sitt arbeide kunne overvåke kommunikasjon i offentlige nettverk for å sikre mot beskyttelsesbrudd og angrep fra hackere.

(Fra Nettavisen 08. des 2000)

Nettet overvåkes av hemmelig nettverk

POT og Forsvarets etterretningstjeneste samarbeider med 15 store norske bedrifter om å beskytte seg mot dataangrep. Sårbarhetsutvalgets leder Kåre Willoch støtter overvåkningen.

Også Datatilsynet støtter overvåkningen.

- Dette er et prosjekt som skal forsøke å kartlegge trusselbildet som datakriminalitet representerer. Datatilsynet er grundig orientert, og kan ikke se at personvernet rammes i det hele tatt, sier Datatilsynets direktør George Apenes til Nettavisen.

E-overvåking

Ifølge Digitoday.no er samarbeidet et hemmelig nettverk der 15 av Norges viktigste firmaer samarbeider med overvåknings- og etterretningsstaben i politiet og Forsvaret. Samarbeidet skal settes i gang på nyåret for å beskytte norsk næringsliv mot dataangrep fra hackere og industrispionasje. Stortinget er ikke informert.

Beskyttelse mot hackere

– Samarbeidet gjør datasikkerheten bedre, sier brigader Jan Erik Larsen, som ikke ser hensikten med å orientere Stortinget så lenge overvåkningen kun skjer for å beskytte seg mot datakriminalitet.

Apenes mener at et slikt samarbeid er positivt.

Ingen grunn til panikk

"Overvåkningssystemet" som det offentlige og private Norge samarbeider om er i realiteten ikke noe annet enn en samordning av hva enhver organisasjon som tar datasikkerhet på alvor bør utføre.

I praksis fungerer systemet slik at bedriftene kontrollerer datatrafikken på bedriftens brannvegg. Dermed kan det oppdages hvis noen har uærlige hensikter og forsøker å bryte seg inn i datasystemet. Dersom det oppdages noe unormalt blir de andre deltagerbedriftene i nettverket varslet, slik at de kan sikre sine systemer mot inntrengerne.

Kåre Willoch, som leder Sårbarhetsutvalget, synes at det var på høy tid å etablere et slikt samarbeid for å slå tilbake mot datakriminalitet. Han synes ikke det er betenkelig at Stortinget ikke ble orientert om prosjektet.

Leser ikke e-post

Overvåkningen innebærer ikke at trafikken på Internett overvåkes i sin alminnelighet. Vanlige nettbrukere har derfor ingenting å engste seg for. Ansatte i deltagerbedriftene behøver heller ikke være bekymret for at noen skal lese innholdet i e-postmeldingene de sender ut.

– Dette dreier seg overhodet ikke om noe kontroll av innhold, sier Larsen.

Atle Nygård i nettoperatøren Infostream sier til Nettavisen at de ikke har fått noen forespørsel om å delta i prosjektet. Han mener det også vil være ulovlig dersom aksessleverandøren overvåker trafikken på nettet. I samarbeidsprosjektet det her er snakk om, foregår det ingen slik kontroll.

Det eneste som blir underlagt kontroll er forsøk på datainnbrudd. Det påståtte overvåkningssystemet fungerer dermed som datasikkerhet og har ingenting med overvåkning å gjøre.

Kan en slik overvåking som beskrevet ovenfor være i strid med hensynet til personvernet? Begrunn svaret.

I forbindelse med hensynet til rikets sikkerhet og bekjempelse av kriminalitet vil vårt personvern også være påvirket av internasjonale lover og regler. Et eksempel på en slik avtale er Schengen-avtalen som Norge undertegnet i desember 1996. Denne avtalen inneholder bla opprettelsen og drift av et eget informasjonssystem (SIS), der det i utgangspunktet skal registreres kriminelle. Dette systemet gjør det mulig å samkjøre store mengder av personopplysninger. Kritikerne av systemet hevder at de fleste av de som er registrert i systemet er mennesker som kommer fra land utenfor Schengen og som har forbrutt seg mot utlendingslovene i det enkelte Schengen land.

Det hevdes videre at dersom du er sammen med en person som blir overvåket av en eller annen grunn, vil også du bli registrert i basen til SIS. I 1997 ble det matet inn 5,6 millioner nye registreringer, noe som da gav et antall registreringer på litt over 14 millioner. Det totale antallet treff på søking i SIS-arkivet i 1997 var litt under 37 000. 14 806 av disse var på utlendinger som ble nektet adgang på yttergrensene, de fleste flyktninger eller asylsøkere som hadde søkt om opphold i Schengen-land tidligere. 18 902 treff var på ettersøkte kjøretøyer, 3320 var på personer ettersøkt for kriminelle forhold og 1.690 var på personer som ble overvåket.

I forbindelse med SIS er det også utviklet et system for utveksling av tilleggsinformasjon om personer registrert i SIS, som kalles SIRENE. SIRENE påstås å være mindre regulert enn SIS, og de opplysninger som spres skal være mer omfattende og uten klare grenser. Borgerrettsorganisasjonen Statewatch har uttalt at det ikke finnes klare bestemmelser om beskyttelse og sikring av personopplysninger i SIRENE, og selv om den enkeltes mulighet til å få innsyn i SIS-registrene skal følge nasjonal lovgivning, så er denne innsynsretten sterkt innskrenket. Statwatch mener også at slik SIS er organisert vil det være fare for at gal informasjon registreres og at grensene for hvem som kan registreres ikke er strenge nok.

Schengen-avtalen trådde i kraft 25. mars 2001.

4.3.4 Svekker vi selv personvernet?

Da lovforslaget om sikkerhetstjenesten første gang ble lagt frem var debatten både blant politikere og folk flest så og si ikkeeksisterende. Har du lest noen debatt om den nye Sikkerhetsloven? Og tenkte du i såfall over eventuelle personvern-problemer i forbindelse med den loven? Tenker du noen gang over ditt personvern og hvordan det kan svekkes?

"....Ifølge Forsvarsdepartementet må ikke monitoring forveksles med avlytting, monitoring betyr nemlig "medlesing av kommunikasjon". Dette er kreativ bruk av nytale. På godt norsk betyr monitoring overvåking. Når Forsvarsdepartementet på denne måten greier å tilsløre begrepene setter de også en annen premiss for debatten. Det er klart vanskeligere å være uenig med "medlesing" enn med overvåking."

(Fra artikkelen "Nytale og overvåking" av Roar Nerdal, Computerworld 28. feb. 1997)

No word in the B vocabulary was ideologically neutral. A great many were euphemisms. Such word, for instance, a joycamp (forced-labour camp) or Minipax (Ministry of Peac i.e. Ministry of War) meant almost the exact opposite of what they appeared to mean.

George Orwell: 1984, Newspeak

Fra debatten om Sikkerhetsloven i Odelstinget 10. februar kl. 18, 1998

Gunnar Halvorsen (A) : Under § 21 om vurderingsgrunnlaget for sikkerhetsklarering gir komiteens flertall uttrykk for at en ved tvil bør be den som skal klareres, om opplysninger om lovlig politisk engasjement. Arbeiderpartiet mener dette er prinsipielt galt, og viser til drøfting av dette spørsmålet i proposisjonen. Lovlig politisk engasjement kan aldri være relevant i denne forbindelse. Denne uenigheten har ingen betydning for lovteksten, som er betryggende nok. Det andre punktet med uenighet er mer omfattende. Flertallet, alle unntatt Fremskrittspartiet og Høyre, står fast på forslaget til § 25, som fastslår at hovedregelen skal være at avslag på søknad om sikkerhetsklarering skal begrunnes.

Øystein Djupedal (SV) : Men som en mer prinsipiell betraktning kan en selvsagt spørre om det er nødvendig at loven skal favne så vidt som den faktisk gjør, og inkludere for eksempel kommunesektoren. Dette vil kunne ha som konsekvens at flere dokumenter vil bli unntatt fra offentlighet. I tillegg er SV generelt skeptisk til å videreføre det en kan kalle militære lover, til det sivile samfunn.

Fra debatten om Sikkerhetsloven i Lagtinget 19. februar kl. 15.10 1998

Statsråd Dag Jostein Fjærvoll: La meg først få vise til innlegg og debatt i Odelstinget. Sikkerhetsloven vil, som mange har påpekt tidligere, medføre en styrket rettsstilling for den enkelte bl.a. ved at den som undergis sikkerhetsklarering, i større utstrekning enn tidligere skal informeres om utfallet og få begrunnelse for avgjørelsen, som igjen vil medføre at klageadgangen blir mer reell. Representanten Hans J. Røsjorde har redegjort for synet til mindretallet i komiteen, og dette mindretallet gikk da også i Odelstinget inn for at klareringsnektelse ikke skal begrunnes. Etter mitt syn vil dette innebære et tilbakeskritt når det gjelder rettighetene til den som skal klareres. Lovens begrunnelsesplikt formaliserer kun gjeldende praksis. I de fleste saker gis det i dag begrunnelse. Det åpnes imidlertid for at begrunnelsen kan unnlates når sterke hensyn taler for det.

(Kilde: www.stortinget.no)

Hvilke personvernhensyn er det som kommer til uttrykk i disse utdragene?

Hvor mange av oss er det som tenker over og protesterer på at butikker og andre tjenesteleverandører registrere våre kjøpevaner? Eller at mye av det vi gjør på Internett blir loggført og lagret i ulike baser?

Case: En vanlig dag i Anne Kirkeruds liv

Anne Kirkerud er en helt vanlig kvinne i en helt vanlig by i Norge. Det er mandags morgen og tid for nok en arbeidsdag.

Klokken

07.30 Det er tid for å dra på jobben. Som så mange andre har også Anne tyverialarm. I det hun låser seg ut og slår på alarmen, blir dette registrert hos vaktselskapet hun benytter.

08.00 Anne ringer en bekjent fra mobiltelefonen. Det registreres hvem hun ringer til og hvor lenge hun snakker, samt nøyaktig hvor hun befinner seg.

08.10 Anne passerer bomringen. Hun har bombrikke på bilen og det registreres at hun passerer og når på dagen det er.

08.20 Anne parkerer bilen i parkeringshuset, som er videoovervåket.

08.30	Anne bruker sitt adgangskort for å komme inn på jobben. Tidspunktet blir registrert, i tillegg blir hun videoovervåket ved inngangen
08.35	Anne logger seg på datamaskinen sin. IT-seksjonen kan sjekke tidspunktet hun logget seg på – og kan på ethvert tidspunkt sjekke nøyaktig hva hun holder på med på skjermen sin
09.00	Anne sjekker e-posten sin – og sender noen grove karakteristikker av IT-seksjonen der hun jobber til noen venner. Dette kan også IT-seksjonen sjekke, samt norsk sikkerhetstjeneste
10.20	Anne logger seg på Internett og ser innom RVs vev-sider. Vevsidene hun var innom lagrer informasjon om maskinen hennes. Denne informasjonen kan IT-seksjonen sjekke, samt politiet dersom sidene hadde vært ulovlige
11.30	I lunsjen pleier Anne å ta seg en tur ned i kiosken for å spille Lotto. Spillkortet hennes avslører hvor hun spiller fra, når og for hvor mye. Kortet inneholder også opplysninger om hvor mye hun har spilt for siden kortet ble kjøpt, og hvilke spill det er spilt på.
11.35	Anne trenger mer penger og rusler en tur i minibanken. Der registreres uttaket hennes, og hun blir videofilmet mens hun er der
11.40	Anne benytter også lunsjpausen til å ta seg en tur på Polet og kjøpe noen flasker rødvin. Visa-kortet hunbetaler med viser hvor hun har vært, samtidig blir hun videoovervåket.
12.15	Anne blir registrert når hun går inn på jobben igjen – hun har brukt 15 minutter for mye på lunsjpausen.
13.00	Anne ringer en privat samtale hun hverken ønsker at sjefen eller familien skal vite om. Men bedriften hennes registrerer hver eneste samtale på telefonnummer.
14.00	Anne ringer telegiro og betaler studielånet og siste film i filmklubben. Beløpet hun betaler og til hvem registreres.
15.55	Anne drar fra jobben fem minutter for tidlig, noe som registreres.
16.10	Mens Anne sitter i bilen blir hun overvåket både med fjernsynskameraer og ulike sensorer, i regi av veimeldingssentralen.
16.30	Anne går innom Rimi for å handle mat. Hun benytter sitt dominokort, som forteller hvor hun handler, og hvor mye hun handler for.
17.00	Anne kommer hjem og slår av alarmen. Dette registreres av vaktselskapet.
17.15	Anne åpner dagens post. Der finner hun direkteadressert reklame med tilbud om billig stereoanlegg, fordi et firma som lever av å selge adresselister registrerte hennes kjøp av en radio på postordre for fem år siden.
21.00	Anne ringer kjæresten sin. Hvem hun ringer til og når registreres.

De færreste av oss opplever på kroppen hva det vil si at personvernet langsomt forsvinner. Det er først når vi blir nektet innreisetillatelse til et annet land, blir

utsatt for avhør av et fremmed lands politi ved innreise eller ikke får den jobben vi åpenbart var kvalifisert for, at det å bli overvåket og registrert plutselig blir ubehagelig.

Intet nytt under solen

Problemstillingen Landets sikkerhet/ oppklaring av kriminell aktivitet kontra Personvernet er ikke noe som oppstod som en følge av Internett.

Nedenfor kan du lese et eksempel fra den kalde krigens tid, før innføringen av en personvernlov.

Eksempelet er fra en redegjørelse som tidligere personalsjef ved Norsk Hydro, Magnus Hole Jacobsen, kom med i juni 1977.

"Ved alle produksjonssteder og ved hovedkontoret var det påbud om at ingen ekstern søker kunne ansettes før vedkommende politisk var sjekket gjennom Overvåkingen. Sjekkingen gjaldt alle typer av stillinger, fra nederst til øverst, med full adgang til sjekking av hvilken som helst person. De eneste opplysninger Overvåkingen trengte var vanlige persondata for å fastslå identiteten. Ved slik sjekking kunne det gis følgende opplysninger: Medlemskap i NKP, visse kontakter innen "partiet" eller konkrete tegn på sympati, slektninger som var medlem, deltatt i visse demonstrasjoner, fredsmøter eller fredsfestivaler i inn- og utland, engasjert i visse solidaritetskomiteer og lignende."

(Fra Ført bak lyset – 30 år med NATO av Kari Enholm, PAX Forlag A/S 1979, side 138).

Hvis du i dag skulle ha laget et register basert på slike personopplysninger som nevnt ovenfor, måtte du da ha søkt Datatilsynet om konsesjon eller ville det ha vært tilstrekkelig å inngi melding om registeret?

Undersøkelser viser at folk flest nok er opptatt av personvernet i prinsippet mens straks det å gi fra seg personopplysninger kan være til personlig fordel, så som å få tilgang til telefonkatalogen på Internett eller å få tilgang på et kjøpekort med ulike rabattordninger, forsvinner folks bekymringer for sitt personvern.

Men hva kan vi egentlig gjøre for å beskytte oss selv mot krenkelser av personvernet?

Her er noen forslag:

1. Bruk de rettigheter du har etter Personopplysningsloven aktivt. Se særlig lovens kapittel III, §§ 18 - 24 og kapittel IV, §§ 25 - 28.
2. Tenk deg om før du sier ja til kjøpekort og andre tilbud som krever registrering av personopplysninger.
3. Husk at når du er ute på Internett legger du igjen et "visittkort" som avslører hvor du kommer fra, hvilken datamaskin du har og andre detaljer. Du kan unngå

dette ved å enten konfigurere din vevleser til ikke å godta bruk av "Cookies". I tillegg kan du benytte deg av ulike anonymiseringstjenester, som for eksempel www.anonymizer.com. Dette er tjenester som lar deg benytte deres server for videre surfing på nettet. Dermed peker sporene dine tilbake til anonymizer og ikke til deg. Nedenfor ser du to eksempler på dette. Først hva anonymizer finner ut om deg når du går dit fra din egen maskin:

You`re located i Norway (Kongdom of).
Your Internett browser is Mozilla/4.0b5 [en] (Win98; I).
You are coming from BadKarma.hitra.vgs.no.
You just visited the New Yorker Cartoon.

Så kan du ta en tur til anonymizer via dem selv og da får du følgende informasjon:

You are affiliated with The Anonymizer Group.
You`re located around Pittsburgh, PA (MAP)
Your Internet browser is Mozilla/4.0b5 [en] (via THE ANONYMIZER!).
You are coming from WW.anonymizer.com.

Fra det øyeblikket du surfer via en anonymitetstjeneste vil ingen internettsider du er innom få vite noe om hvem du er og hvor du kommer fra.

4. Det å sende e-brev er det samme som å sende et postkort via vanlig post. Alt du skriver er åpent tilgjengelig for alle. For å beskytte e-posten din mot innsyn kan du benytte deg av et krypteringsprogram som kalles PGP. PGP står for Pretty Good Privacy og er regnet som et av verdens sikreste krypteringsprogram. Et kryptert e- brev vil være vanskelig (og kanskje nesten umulig) å lese for andre enn den du sender det til. Dette programmet kan du fritt laste ned fra nettet og er gratis å bruke. Du finner det på www.pgp.com. (Se kapittel 3.6.11 for mer om sikkerhet og e-post).
5. Slett alle vedlegg du får via e-post med mindre du har bedt om dem eller vet hva de inneholder. Et vedlegg kan inneholde virus (se kapittel 3.6.12), men det kan også inneholde et skjult program (såkalt Trojansk hest) som kan overvåke alt du foretar deg på din datamaskin.

Kanskje du kan finne flere forslag ? Eller er det kanskje bare tull med slike forslag? Hva mener du? Begrunn svaret.

Tenk igjennom:

Hvilken holdning har du til ditt personvern,

- i prinsippet?
- i praksis?

4.4 Arbeidsmiljøloven

I 1956 kom Lov om arbeidervern og gav for første gang arbeidstakere og arbeidsgivere en lov som regulerte rettigheter og plikter på arbeidsplassen. I 1977 trådde en ny lov i kraft som stillte strengere krav til arbeidsmiljøet og arbeidsgiverens ansvar for et godt arbeidsmiljø. Denne loven ble så endret i 1995, og i februar 2004 avla Arbeidslivslovutvalget forslag til nye endringer i loven. I hovedsak ser det ikke ut til at endringene direkte vil gripe inn i de deler av arbeidsmiljøloven vi som teknologer er interessert i, men i formålsparagrafen i dagens lov står det en målsetting om at arbeidsmiljøet skal ha en velferdsmessig standard i samsvar med den teknologiske og sosiale utviklingen i samfunnet. Utvalgets flertall foreslår at dette strykes, og at bedriftenes og arbeidstakernes behov sidestilles. Hvorvidt dette vil kunne skape problemer for arbeidstakerne i forhold til deres rettigheter ved innføring av ny teknologi vil være umulig å si, før endringene eventuelt blir vedtatt. Den paragraf i Arbeidsmiljøloven som først og fremst vil angå en systemutvikler er § 12. Denne bestemmelsen i loven setter krav til arbeidsgiver om tilrettelegging av arbeidet. Paragrafens første punkt slår fast at:

> Teknologi, arbeidsorganisasjon, utførelse av arbeidet, arbeidstidsordninger og lønnssystemer skal legges opp slik at arbeidstakerne ikke utsettes for uheldige fysiske eller psykiske belastninger, eller slik at deres mulighet for å vise aktsomhet og ivareta sikkerhetshensyn forringes. Nødvendige hjelpemidler for å hindre uheldige fysiske belastninger skal stilles til arbeidstakernes disposisjon. Arbeidstakerne skal ikke utsettes for trakassering eller annen utilbørlig opptreden.

Her ser vi at ordet Teknologi er nevnt, men dette henspeiler ikke utelukkende på informasjonssystemer som sådanne, men er ment å dekke innføring av all teknologi. Likevel vil det også dekke vårt område, fordi en innføring av et informasjonssystem kan tenkes å medføre fysiske og psykiske belastninger for arbeidstakerne.

En innføring av et rent IT-basert system for en bedrifts kontorpersonale vil for eksempel kunne føre til belastningsskader i håndledd, den såkalte "musesyken", eller i nakke og rygg på grunn av feil sittestilling og problemer med øynene på grunn av. for mye stirring på en dataskjerm. Dersom arbeidstakerne ikke får tilstrekkelig opplæring i å bruke et databasert system, kan dette medføre psykiske problem i form av en følelse av utrygghet og liten selvtillit i forhold til arbeidet. For å unngå at slike problemer oppstår, krever arbeidsmiljøloven videre i punkt 3, § 12 at:

> *Arbeidstakerne og deres tillitsvalgte skal holdes orientert om systemer som nyttes ved planlegging og gjennomføring av arbeidet, herunder om planlagte endringer i slike systemer. De skal gis den opplæring som er nødvendig for å sette seg inn i systemene, og de skal være med på å utforme dem.*

Opplæring og medvirkning er to nøkkelbegrep i dette punktet. I en innføringsfase av nye IT-systemer skal særlig de tillitsvalgte i tillegg til den opplæring som gis til samtlige berørte, gis tilstrekkelig innføring i generell datamaskinteknikk. Videre skal de ha opplæring i prosjektarbeid og systemarbeid, slik at de kan delta aktivt i systemutformingen.

For at både de tillitsvalgte og de øvrige arbeidstakere skal kunne sette seg inn i hva som skal skje, skal all informasjon om de aktuelle systemene gis i en oversiktlig form og i et språk som kan forstås av personer uten spesialkunnskap på området. I tillegg til § 12 regulerer også § 9, pkt 1, 2. ledd bruken av IT på en arbeidsplass, i form av et krav om at det ved oppstilling og bruk av tekniske innretninger og utstyr skal sørges for at arbeidstakerne ikke blir utsatt for uheldige belastninger ved støy, vibrasjon, ubekvem arbeidsstilling og lignende

I tillegg til selve arbeidsmiljøloven er det utarbeidet ulike forskrifter som ytterligere understreker de enkelte områder av loven. I denne sammenheng er Forskrift om arbeid ved dataskjerm av 15. desember 1994 av interesse for oss. Forskriften understreker Arbeidsmiljølovens § 12s krav om opplæring, i sitt kapittel 6, § 12 der det står.

> *Alle arbeidstakere skal få nødvendig opplæring i bruk av dataskjerm-arbeidsplassen før de begynner med denne type arbeid, og hver gang arbeidsplassens utforming endres vesentlig. Opplæringen skal gis på et språk som arbeidstakerne forstår.*

Forskriften tar ellers for seg krav til tilrettelegging og organisering av dataskjerm-arbeidsplasser, samt krav til arbeidsplassen som sådan, herunder skjerm, tastatur, arbeidsbord, arbeidsstol, belysning, støy, varme, stråling og fuktighet. Det settes også krav til særlige vernetiltak som er definert, som krav om oppfølging av arbeidstakers syn.

Men like viktig for en som er ansvarlig for et IT-system i en virksomhet, er det at forskriften også definerer sitt virkeområde, og begrenser hvilke arbeidstakere som skal regnes inn under forskriften.

Case: Nye briller til Marte Kirkerud og Christoffer Sjule

Ved Høgskolen i Lillevik er det 107 ansatte, hvorav 10 arbeider i administrasjonen. En av disse er Marte Kirkerud. Hun jobber med det nye databaserte økonomi-systemet og sitter ved sin datamaskin hele dagen. Hun har klaget til personalsjefen over problemer med synet og hodepine når hun har sittet lenge ved dataskjermen. Personalsjefen sender saken over til IT-leder som tar en prat med Marte Kirkerud. Siden hun har sitt arbeide direkte knyttet til et datasystem vet IT-lederen at hun kommer inn under §1 i Forskrift om arbeid ved dataskjerm, som sier at *Denne forskrift gjelder for arbeidstakere, som jevnlig og under en betydelig del av sitt arbeide, utfører arbeid ved en dataskjerm.*

IT-leder tilbyr derfor Marte Kirkerud å ta en øyeundersøkelse og synsprøve på høgskolens regning. Dersom det er nødvendig vil høgskolen dekke utgifter til briller, iht kravet i forskriftens §11, pkt 4.

Utgifter knyttet til syns- og øyeundersøkelser samt til spesielle synskorigerende hjelpemidler som følge av denne paragraf, skal dekkes av arbeidsgiver.

Ved samme høgskole arbeider også Christopher Sjule som idrettslærer. Han benytter sin datamaskin mest til e-post og tekstbehandling. Også Christopher Sjule klager over synet og vil ha dekket time hos optiker og nye briller. IT-leder ser nærmere på forskriftens § 1:

Denne forskrift gjelder for arbeidstakere, som jevnlig og under en betydelig del av sitt arbeide, utfører arbeid ved en dataskjerm.

Forskriften gjelder ikke:

- *arbeid av tilfeldig og kortvarig karakter*
- *datautstyr installert på eller i transportmateriell, kjøretøyer og arbeidsmaskiner*
- *datautstyr som først og fremst brukes av publikum*
- *bærbart datautstyr ved kortvarig, ikke permanent bruk*
- *regnemaskiner, kassaapparater, vanlig utformede skrivemaskiner, og alt lignende utstyr som har en fremvisningsskjerm for data.*

Skal Christopher Sjule få dekket time hos optiker og eventuelle nye briller?

Hva syns du?

I tillegg har Arbeidstilsynet gitt ut en "Veiledning om arbeid ved dataskjerm" som er ment å skulle være et hjelpemiddel for både arbeidsgiver og arbeidstaker og gi informasjon om hvordan arbeid ved en datamaskin kan planlegges og utformes slik at det oppfyller kravene i forskriften.

4.4.1 Dataavtalen mellom LO og NHO

I tillegg til at du må ta hensyn til arbeidsmiljøloven med forskrifter, skal du også være klar over at LO og NHO har inngått en avtale som omfatter teknologi og systemer som brukes ved planlegging og gjennomføring av arbeidet, samt systemer for lagring og bruk av persondata. Første gang en slik avtale ble inngått var i 1974 ved Viking - Askim. I 1975 kom en avtale mellom LO og NHO og mellom staten og de statsansatte. Denne avtalen kalles "Dataavtalen" og er fortsatt gjeldende. Denne avtalen er på mange måter en utdypning og en understrekning av Arbeidsmiljølovens § 12 om arbeidstakers rett til medvirkning og opplæring. I tillegg har den et eget kapittel om persondata der det henvises til personloven, men der det samtidig understrekes at en innsamling, lagring, bearbeiding og bruk av slike data ikke skal skje uten saklig grunn og ut fra hensynet til bedriften. Etter avtalen skal bedriften kartlegge hvilke typer persondata som skal samles inn, lagres, bearbeides

og brukes ved hjelp av IT. Samtidig skal arbeidsgiver i samarbeid med de tillitsvalgte utarbeide instruks for lagring og bruk av persondata.

Case 1: Adgangskontroll og videoovervåking ved Høgskolen i Lillevik.

Høgskolen i Lillevik ligger i en liten utkantkommune og har sjelden vært plaget av innbrudd. Ledelsen er imidlertid redd for at dette bare er et spørsmål om tid og har kontaktet et firma med tanke på å innføre systemer for adgangskontroll og videoovervåking. IT-leder som også er sikkerhetsansvarlig ser på hvilke tekniske løsninger som er aktuelle. Hun tar så kontakt med de ansattes fagforeninger for å høre deres syn på saken og involvere dem i det videre arbeidet, i tråd med arbeidsmiljølovens § 12. Hun tar også kontakt med Datatilsynet og får der vite at registre som opprettes i forbindelse med adgangskontroll er konsesjonspliktige dersom arbeidstakernes passeringer blir registrert. Høgskolen i Lillevik søker Datatilsynet om konsesjon for et slikt register.

Høgskolen i Lillevik ønsker også å innføre fjernsynsovervåking av personalrommet på nattetid, fra klokken 22.00 og til klokken 07.00. Begrunnelsen for det er at det på personalrommet henger en imponerende samling malerier som høgskolen har samlet gjennom 80 år, og som representerer store verdier. I sitt møte med de ansattes organisasjoner henviser ledelsen, ved IT-leder, til Lov om Personregistre, kapittel 9a § 37a der slik overvåking tillates dersom det er et særskilt behov for overvåking. Fagforeningene godtar dette, men forlanger at opptakene slettes etter hvert og ikke blir utlevert til noen, med mindre det er til politiet i forbindelse med innbrudd og tyveri av malerier. Fagforeningene forlanger også at det settes opp skilt som tydelig viser at fjernsynsovervåking foregår. Fagforeningene ønsker også at Høgskolen i Lillevik skal be Datatilsynet om en uttalelse om planene for fjernsynsovervåking.

Case 2: Lillevik Sveiseindustri a.s

Lillevik Sveiseindustri a.s. jobber med sveiseoppdrag innen skips- og oljeplattformbransjen. Bedriften har 60 ansatte fordelt på tre avdelinger, administrasjon, produksjon og lager. Ledelsen har i lengre tid ønsket å effektivisere administrasjonen og lageret, og har til slutt bestemt seg for å innføre IT som et hjelpemiddel for en slik effektivisering. Siden ledelsen ikke selv har kunnskaper om informasjonsteknologi leier de inn en konsulent fra Lillevik Data.

I forbindelse med systemeringsarbeidet henviser konsulenten til arbeidsmiljølovens § 12 og dataavtalen mellom LO og NHO, og ber om at de ansattes tillitsvalgte trekkes inn i arbeidet med utformingen av datasystemet, enten ved at samtlige tillitsvalgte er med eller at de ansatte velger en felles "datatillitsvalgt". Konsulenten informerer så om at den eller de tillitsvalgte må få tilgang til all dokumentasjon og

programmer, samt opplæring i system- og prosjektarbeid og bruk av datasystemer. Konsulenten understreker også at det er i viktig i det videre arbeidet at ledelsen og den eller de tillitsvalgte på en lettforståelig måte informerer de ansatte om bruken av det nye datasystemet, og at det utformes planer for og gjennomføres opplæring i bruk av systemet for alle de aktuelle arbeidstakerne.

4.5 Juridiske ressurser på Internett

Harry Hansen sukket tungt og satt fra seg kaffekoppen. Ute falt snøen stille over parkerte biler, vegbelysning og en og annen paraply. Det var ikke mange ute nå en tidlig morgenstund. Det nye årtusen var knappe åtte timer gammelt og folk flest sov de uskyldiges søvn. Men noen av dem var atskillig mindre uskyldig enn andre og det var takket være dem at Harry Hansen, spesialetterforsker i Økokrim, satt på sitt kontor og sukket. Foran ham på bordet lå en åpen saksmappe og stirret på ham. Harry Hansen stirret tilbake og sukket igjen. En komplisert sak der flere lover var brutt. Nå gjaldt det å finne frem de aktuelle lover og paragrafer til den avsluttende rapporten. Harry Hansen strakte seg mot hyllen over skrivebordet og trakk ut en stor, rød bok med gullskrift på omslaget. Boka veide ca 2 kg og var på 2751 sider, registeret medregnet.

Det er ikke rart at Harry Hansen sukker, for Norges Lover er ingen lett bok å bla i. Bare vekta er nok til at motet nesten svikter når du skal finne frem til en lov. Og dessuten er boka dyr å kjøpe. Men i dag er det slett ikke nødvendig å kjøpe Norges Lover for å finne frem til en lov eller en paragraf. Det eneste du behøver er en datamaskin koblet mot Internett.

Figur 3: Lovdata sin hjemmeside

Når du er vel ute på nettet er det bare å skrive www.lovdata.no i nettleserens adressefelt og vips så har du tilgang på:

- Ajourførte lover
- Ajourførte forskrifter
- Norsk Lovtidend
- Rundskriv
- Nye avgjørelser fra Høyesterett og lagmannsrettene

Lovdata er en privat stiftelse som ble opprettet i 1981 av Justisdepartementet og Det juridiske fakultet ved Universitetet i Oslo. Formålet med Lovdata er å opprette, vedlikeholde og drive systemer for rettslig informasjon.

Figur 4: Juridisk Nettviser sin hjemmeside

I tillegg har de juridiske fakultetsbibliotekene i Norge samarbeidet om å utvikle en portal for jus, kalt Juridisk Nettviser. Portalen har som målsetting å være en hovedportal for norske jurister, jusstudenter og andre i Norge som vil ha tak i juridisk informasjon. Nettviseren inneholder informasjon fra ulike juridiske fagområder, rettskilder nasjonalt og internasjonalt, samt pekere til annen juridisk informasjon på nettet. Du finner portalen på adressen www.ub.uio.no/ujur/baser/index.html.

Dersom du syntes de juridiske aspekter ved IT er interessant, kan det være lurt å melde deg inn i Norsk forening for jus og edb. Da får du tilsendt tidsskriftet Lov og Data som inneholder artikler og referat fra saker og dommer innenfor dette emnet. Se også http://it-mo.hinesna.no/~pag/foreles2003.html for nettforelesninger innen IT og jus. Forelesningene kan fritt benyttes av alle som er interessert.

4.6 IT-ansattes etiske ansvar

Det å være den som besitter kunnskap om informasjonsteknologi på en arbeidsplass gir deg et viktig ansvar. Dette gjelder særlig dersom du er ansatt som IT-

ansvarlig. Ditt ansvar blir da ikke bare å sørge for at andre ansatte ikke bryter lover eller lisensbestemmelser, men også å sørge for at din egen sti er ren.

Som IT-ansvarlig bør du forsøke å etterleve følgende sett med regler:

1. En IT-ansvarlig må ha høy integritet

Som IT-ansvarlig kan du daglig få tilgang til sensitiv og privilegert informasjon. Du har plikt til å beskytte all slik informasjon mot innsyn fra utenforstående og til å overholde din taushetsplikt.

Du skal kjenne til og overholde alle interne regler for databruk, og de lover og regler som ellers gjelder i samfunnet for bruk av datautstyr.

2. En IT-ansvarlig skal ikke unødvendig krenke brukernes rettigheter

Som IT-ansvarlig skal du aldri benytte deg av dine systemrettigheter til å gi deg selv tilgang til andre brukeres personlige områder. Du skal heller ikke tolerere at andre brukere gir seg selv en slik tilgang.

3. All kontakt med IT-brukerne skal være preget av høy profesjonell standard

Som IT-ansvarlig skal du sørge for å informere brukerne om alle forhold som er viktige for deres databruk.

Din oppførsel skal være preget av høflighet og ærlighet. Særlig skal du være ærlig om din egen faglige kunnskap og mangel på sådan.

4. Som IT-ansvarlig skal du holde deg oppdatert på ditt fagområde

Siden IT-teknologien utvikler seg så raskt skal du alltid bestrebe deg på å utvikle og holde vedlike din egen kunnskap.

5. En IT-ansvarlig bør ha høy arbeidsmoral

Som IT-ansvarlig bør du gjøre alt for at det du gjør i ditt arbeide er preget av høy moralsk og faglig standard.

Dette settet med regler er oversatt fra de etiske reglene til det amerikanske The System Administrators Guild.

Tenk igjennom

- Hva er din mening om disse reglene?
- Er disse punktene tilstrekkelige eller må det legges til flere?
- Er slike regler viktige? I så fall hvorfor det?

Gå ut på Internett og se om du kan finne ut om det er laget et sett med etiske regler for norske IT-ansvarlige.

4.7 Avslutning

Det kan være vanskelig å ha oversikt over alle de lover og regler som du vil komme i kontakt med i en jobb som IT-konsulent, systemansvarlig, IT-sjef , IT-lærer eller rett og slett vanlig databruker. Ja det kan faktisk nesten være en umulighet. Men du vil garantert ha nytte av en viss juridisk kunnskap. Hva ville du for eksempel gjøre dersom Microsoft Norge og Business Software Alliance kommer på uanmeldt besøk til din virksomhet og krever å få gjennomføre en husundersøkelse for å se om du har fulgt lisensbestemmelsene for din Microsoft programvare?

Case: Kan Microsoft foreta husundersøkelser? (Utdrag fra artikkel publisert på KVASIR 28.01.99, av P.A.Godejord)

I nettutgaven av Computer World, onsdag 27. januar 1999, står en artikkel fra fredag 22. januar samme år med overskriften "Fullt ut lovlig", der det står i beskrivelsen av artikkelen at "*Husundersøkelser, anmeldelser og razzia. Microsoft lar ingen midler være uprøvd når det gjelder å sette en stopper for piratkopiering av programvare.*"

Artikkelen nevner at BSA (Business Software Alliance) i sin kamp mot pirat-kopiering ønsker seg hjemmel til å foreta husundersøkelser. Deretter siteres den norske sjefen for Microsoft, Ole M. Settevik, som i artikkelen blant annet uttaler: "-*Jeg stiller meg bak den jobben BSA Norge gjør, og en åpning i lovverket gir adgang til å utføre husundersøkelser.* "

Noen nærmere henvisning til hvilken åpning i lovverket som gir BSA fritt spillerom for sine drømmer forekommer ikke, noe som er svært beklagelig siden det sikkert er flere fagfolk enn meg som gjerne skulle ha visst hva slags åpning det her var snakk om og hvor i lovverket den lå. Men når Computerworld ikke vil avklare det, får en prøve å finne ut av det på egen hånd. La oss se litt nærmere på begrepene Husunder-søkelser, anmeldelser og razzia. At Microsoft via BSA eller på egen hånd kan gå til anmeldelse av enkeltpersoner eller virksomheter som bryter lisensbestemmelsene er hevet over tvil. Programvare omfattes av Lov om opphavsrett til åndsverk mv og lovens §§ 39g - 39i omhandler datamaskinprogrammer. Lovens § 12 avgrenser retten til kopiering til eget bruk.

Det oppsiktsvekkende i denne artikkelen er antydningen om at Microsoft kan benytte seg av husundersøkelse og razzia. Bruk av husundersøkelser reguleres allerede i Grunnlovens § 102, der det fastslås at "*Hus-Inkvisitioner maa ikke finde Sted, uden i kriminelle Tilfælde*". At piratkopiering av programvare er å regne som et kriminelt tilfelle er klart etter lov om opphavsrett. La oss så se på den loven som regulerer adgangen til bruk av husundersøkelser, nemlig Lov om rettergangsmåten i straffesaker (Straffeprosessloven).

Dennes kapittel 15 tar for seg bruken av slike tvangsmidler. Straffeprosessloven slår fast at beslutning om husundersøkelse eller razzia skal foretas enten av retten eller av påtalemyndighet. Ingen steder ligger det en hentydning til at andre enn disse kan beslutte og foreta slike tvangstiltak. Loven regner opp følgende som defineres som å ha påtalemyndighet:

1. riksadvokaten og den assisterende riksadvokaten,
2. statsadvokatene, statsadvokatfullmektigene og hjelpestatsadvokatene,
3. politimestrene, visepolitimestrene, overvåkingssjefen, politiinspektørene, politiadvokatene, politiadjutantene og politifullmektigene for så vidt de har juridisk embetseksamen og gjør tjeneste i embete eller stilling som er tillagt påtalemyndighet,
4. lensmennene.

Selv om det antakelig ville ha vært en oppfyllelse av BSA og Microsoft sine inderligste drømmer, finnes her ikke et punkt 5 som gir de to ovennevnte påtalemyndighet. Der ligger heller ingen forskrifter til loven som gir en slik "åpning" som det sjefen for Microsoft Norge nevner. Er det da nye endringer av Straffeprosessloven på gang? Med bevende hjerte iler man til ODIN, statens felles informasjonstjener. Kan der ligge noe der? Men nei. Mangt og mye har Det Norske Kongelige Justis- og Politidepartement gitt ut, men noen endringer av Straffeprosesslovens kapittel 15 finnes ikke.

Også Forvaltningsloven regulerer bruken av husundersøkelse i sin § 15, 1. ledd. De som her har adgang til dette er forvaltningsorgan, definert i Forvaltningslovens § 1. Microsoft og BSA har ingen delegert lovgivningsmyndighet eller annen rett til å fastsette rettigheter og plikter for den enkelte borger eller en ubestemt krets av borgere. Den eneste retten de har er å fastsette kontraktsregler for de borgere eller virksomheter som kjøper programvare hos Microsoft. En slik rett gjør ikke Microsoft eller BSA til et forvaltningsorgan.

Nåvel, men hva så med den kontrakt den enkelte bruker eller institusjon har inngått med Microsoft? Ligger der noen hjemmel til husundersøkelse eller razzia? Microsoft behandler dette i sin hovedavtale, henholdsvis Select 3.0 og Select 4.0, og fastsetter følgende:

"Select 3.0 – Punkt 5.b.
Revisjonsrettigheter: .....Microsoft forbeholder seg retten til å kontrollere hver Select-Kunde og hver av Hovedkundens Affilierte Selskaper i løpet av Hovedavtaleperioden, og ytterligere ett (1) år etter Hovedavtalens opphør, under den forutsetning at slike kontroller utføres i vanlig arbeidstid og på en slik måte at de ikke har noen urimelig innvirkning på driften av foretaket til Select-Kunden og Hovedavtalens Affilierte Selskaper."

"Select 4.0 –Punkt 10.b
Revisjonsrettigheter:.....MS hovedselskap og MS Registreringsselskap forbeholder seg retten til å revidere den Registrerte Kunde og Hovedkundes Affilierte

*Selskap i løpet av den periode Hovedavtalen er i kraft og i en periode på et (1) år deretter, forutsatt at slik(e) revisjon(er) foretas i normal arbeidstid og på en slik måte at den ikke unødvendig forstyrrer virksomheten hos den Registrerte Kunde eller Hovedkundens Affilierte Selskap."*En virksomhet eller enkeltbruker som har underskrevet denne avtalen er følgelig forpliktet til å la Microsoft få foreta en revisjon av lisensbruken på Microsoft sin programvare. Men avtalen legger opp til at dette skal gjøres i samarbeid med kunden, jfr "*...foretas i normal arbeidstid og på en slik måte at den ikke unødvendig forstyrrer virksomheten hos den Registrerte Kunde eller Hovedkundens Affilierte Selskap.*" Husundersøkelse og razzia er to begrep som normalt er knyttet til situasjoner der samarbeidsviljen er nokså dårlig.

Ut fra avtalen må vi kunne anta at en kunde har anledning til å avvise en revisjon dersom Microsoft ønsker å gjøre den utenfor ordinær arbeidstid eller dersom den unødig forstyrrer virksomheten, men da må kunden i samarbeid med Microsoft finne en anledning til å gjennomføre revisjonen på et bedre tidspunkt. Dersom en SELECT kunde nekter Microsoft å foreta en revisjon i det hele tatt, vil det være et klart kontraktbrudd, men det gir likevel ikke Microsoft anledning til å foreta en razzia eller en husundersøkelse.

I flere artikler på nettet, blant annet i Nettavisen og IT-kanalen, benytter BSA (eller den enkelte journalist) seg av begrepet "*Sivil husundersøkelse"*, men et slikt begrep finnes der ingen støtte for i lovverket. I de samme artikler nevnes det at man har gått og vil gå "rettens vei" for å få gjennomført en husundersøkelse. Det siste er jo ikke spesielt oppsiktsvekkende. Har Microsoft mistanke om at kunden benytter piratkopier av Microsoft-program, kan de selvsagt anmelde kunden for mulige brudd på Åndsverkloven og la påtalemyndigheten utføre en ransaking av kundens bolig eller virksomhet, samt ta beslag i eventuell piratkopiert programvare. Men ikke under noen omstendighet kan Microsoft eller BSA på egen hånd ta i bruk denne type tvangsmidler. Ut fra dette blir Computerworld sin bruk av overskriften "Fullt ut lovlig" og Ole M. Setteviks uttalelse om at "*,.. og en åpning i lovverket gir adgang til å utføre husundersøkelser.*" direkte feil.

Nå har du fått litt kunnskap om informasjonsteknologiens ulike juridiske sider. Ta med deg det du har lest i dette kapittelet når du nå i neste del av boka skal lære om organisasjonene og IT. Juss, organisasjon, samfunn, etikk og politikk er alle stikkord som er nøye forbundet med IT. Og på websiden http://it-mo.hinesna.no/~pag/foreles2003.html finner du 20 webbaserte forelesninger som søker å understreke nettopp dette.

Forhåpentligvis vil du etter dette studiet bli et enda mer aktivt samfunnsmedlem, som stiller kritiske spørsmål til hvordan samfunnet benytter seg av informasjonsteknologien. Teknologien er i seg selv nøytral og uten moralsk innhold. Det er brukerne som bestemmer om den blir brukt til å nå positive eller negative mål.

Spørsmål til ettertanke

1. Diskuter hvordan forslaget til Økokrim om at alle nettbrukere må identifisere seg vil innvirke på personvernet. Begrunn svaret.
2. Diskuter i lys av hendelsen den 11. september 2001 hva som kan defineres som rimelig kontroll fra en stats side overfor sine borgere, og hva som er urimelig kontroll.

   Begrunn svarene
3. I delen om arbeidsmiljø og IT hadde vi et case om synstest og briller på arbeidsgivers regning. Gå tilbake til det og svar på om hvorvidt Christopher Sjule skal få dekket synstest og briller.