

## Oppsummering DR11002, 17. april 2007

Informasjonstilgang, overvåkning og kontroll

Ulike perspektiver:  
Rettigheter, regelverk, interesser, makt

## Innsynsrett vs. plikt til å gjøre informasjon tilgjengelig

NB! Flere innsynsrettigheter kan gjelde samtidig for samme opplysning eller dokument

	Tilgjengelig for "alle"	Tilgjengelig for berørte personer/organisasjoner
Tilgjengeliggjøring uten forutgående forespørsel	Publiseringsplikter "Publicatio legis"-prinsippet, Grunnloven. § 84, Lov om Norsk Lovtidend Kommuneloven § 4 Fvl § 37 (høring og varsling)	Opplysningsplikter Forelegge saksopplysninger, forvaltningsloven § 17 Informasjon om behandling av personopplysninger, personopplysningsloven §§ 19-21
Tilgjengeliggjøring etter forespørsel	Offentlighetsprinsippet Offentlighetsloven, - Innsynsrett for "enhver" - Visse unntak - Plikt til å vurdere meroffentlighet	(Individuell) innsynsrett Partsinnsyn (i saken), fvl § 18 Innsyn i registrerte opplysninger, personopplysningsloven § 18 Innsyn i "regelinnholdet" til grunn for helautomatiske beslutninger, personopplysningsloven § 22

## Informasjonsrett, grunnleggende

- Ytringsfrihetskommisjonen, har munnet ut i endret § 100 i Grunnloven (i 2004)
- Offentlighetslovutvalget, har munnet ut i ny offentlighetslov
  - (vedtatt av Stortinget i mai 2006, ikke i kraft ennå)
- Pensumartiklene omhandler (blant annet) forarbeider til disse lovendringene

## Grunnlovens nye § 100

- Ytringsfrihetens begrunnelser (NOU-en kap. 2)
  - Sandhedssøgen,
  - Demokrati
  - Individets frie Meningsdannelse
- Informasjonsfriheten (NOU-en kap. 5.4)
  - Ret til Innsyn i Statens og Kommunernes Akter
  - [Ret til] at følge Forhandlingene i Retsmøder og folkevalgte Organer
- Klarere angitte grenser for ytringsfriheten
  - Personvern, beskytte barn (primært filmsensur)
  - Ellers kreves konkret lovhjemmel når ytringsfriheten skal begrenses

## NOU 2003:30, ny offentlighetslov

- Kapittel 17: Innsynsprosessen
  - Gjennomgang av *saksbehandlingsreglene* for innsyn
  - Grunnleggende påstand/hypotese: "Selv om saksbehandlingsreglene i seg selv ikke skal utvide eller innsnevre innsynsretten [...], vil de rent faktisk kunne ha en slik virkning"
- Kapittel 18: Nye former for åpenhet – ...
  - Drøfting av et konkret detaljpunkt i mandatet, om det bør være plikt til å gjøre tilgjengelig på Internett:
    1. Elektroniske postjournaler
    2. "Selve dokumentene" i elektronisk form

## Ny offentlighetslov, om innsynsprosessen:

- Teknologinøytrale regler er ønsket
- Beslutning om innsyn ikke enkeltvedtak (etter forvaltningsloven)
- "Mildt krav" til å identifisere det du vil ha innsyn i
- Organet må selv vurdere om innsyn skal gis (uavhengig av andre organers tidligere vurderinger)
- Ikke mer presist angitte tidsfrister for å gi innsyn
- Fortsatt papirkopi som hovedregel (også åpent for elektronisk kopi og for muntlig orientering)
- Hovedregelen er fortsatt gratis innsyn (unntak må forskriftsfestes, fortrinnsvis for "bearbeidet" informasjon)
- Avslag må henvise til hjemmel, begrunnelse kan kreves

## Ny offentlighetslov, om elektronisk tilgjengeliggjøring

- Effektivisering kan oppnås
- Mer innsyn kan oppnås
- Vanskeligere å ivareta personvern (unntak fra offentlighet gjelder opplysninger underlagt taushetsplikt, men ikke dermed nødvendigvis alle personopplysninger)
  - Mengdeproblem, lett å søke
  - Puslespiddoktrinen (sette sammen personprofiler)
- Utvalget ønsket en viss begrenset plikt til å tilgjengeliggjøre elektronisk journal
- Mulighet for, men ikke plikt til, å tilgjengeliggjøre selve dokumentene elektronisk

## Innsynsrett, grunnleggende

- Innsynsrettighetene er sterkest innenfor det offentlige fordi det her gjelder et *offentlighetsprinsipp*
- Viktige lover som gir innsynsrett
  - Grunnloven § 100 femte ledd:

"Enhver har Ret til Innsyn i Statens og Kommunernes Akter og til at følge Forhandlingerne i Retsmøder og folkevalgte Organer. Det kan i Lov fastsættes Begrænsninger i denne Ret ud fra Hensyn til Personvern og af andre tungtveiende Grunde."
  - Offentlighetsloven (innsyn for alle)
  - Personopplysningsloven (innsyn for alle og for registrerte personer)
  - Forvaltningsloven (innsyn for parter i forvaltningssaker)
  - Miljøinformasjonsloven (innsyn for alle i miljøinformasjon)
  - Kommuneleven (innsyn for alle i sakslister og adgang for alle til møter)
- Innsynsrett overfor private eksisterer innen spesifikt angitte områder; viktigst er innsynet etter personopplysningsloven

## Innsynsretten etter personopplysningsloven § 18

- **Dette har dere testet ut selv!**
- Alle har rett til å vite hvilke typer behandling av personopplysninger som skjer i offentlige og private virksomheter (kan også være hos personer)
- Alle har rett til å få bestemte opplysninger som beskriver hvorledes personopplysninger blir behandlet
- Alle har rett til å spørre om det blir behandlet opplysninger om dem, og i tilfellet få innsyn i opplysninger om egen person
- Enkelte unntak gjelder, se § 23.

## Rettslig regulering av Internett, grunnleggende

- **Forhold vedrørende Internett reguleres av den vanlige lovgivningen**
  - Noen særregler, eks. e-forvaltning, opphavsrett
  - Og verdt å merke seg: **"Datakriminalitet" på vei inn som egen kategori i ny straffelov**
- Internett kan gjøre det krevende å ta stilling til hvilket lands lov som gjelder, og hvem som skal avgjøre rettsspørsmålene
- Internett kan gjøre det vanskelig å etterforske ulovlige handlinger (ytringer mv)

## Personvern og Internett

- Personopplysninger kan inngå i Internettbruk på 3 måter:
  - Publisere personopplysninger (f.eks. på nettsider)
  - Åpent samle inn opplysninger (f.eks. via nettsider)
  - Logge aktiviteter på nettet (f.eks. logger som viser informasjonssøk)
- Personopplysningsloven legger begrensninger på hva som kan behandles av personopplysninger i tilknytning til Internett
- Vær spesielt oppmerksom på:
  - Det gjelder unntak fra store deler av loven for kunstneriske, litterære, journalistiske og opinionsdannende formål (§ 7)
  - Behandling av personopplysninger må alltid ha *rettslig grunnlag* (§§ 8 og 9)
  - Det stilles krav til fastsettelse av *formål* (§ 11)
  - Det stilles krav til opplysningskvalitet (§ 11 og § 27)
  - Det gis omfattende rettigheter til *innsyn* og *informasjon* (kap III)
  - Det kan være plikt til å *melde* til Datatilsynet (§§ 31 og 32)
  - Det kan være *konsesjonsplikt* dersom opplysningene er sensitive (§ 33)

## Opphavsrett og Internett

- Opphavsrett (til tekst, bilde, lyd, funksjoner, formgivning mv)
  - Krav til verkshøyde
  - Økonomisk opphavsrett
  - Ideell opphavsrett
- Tre aktuelle problemstillinger:
  - Er det materialet du skaffer deg tilgang til opphavsrettslig beskyttet?
  - Er det materialet du selv utarbeider og/eller gjør tilgjengelig på nettet opphavsrettslig beskyttet?
  - Hvem har opphavsretten?
- Materiale som fritt kan brukes
  - Når opphavsmannen har gitt sin tillatelse
  - Materiale som har "falt i det fri" (70 år etter opphavsmannens død)
  - Offentlige saksdokumenter, lover, dommer mv
  - Det er lov å sitere

## Fem teknologiske/metodeorienterte perspektiver på kontroll og overvåkning

<i>Interception</i>	Filtrering	Trafikkdata	Adferdsdata	Sikkerhets-tiltak
<i>Oppfangning</i> (en parallell til <i>avlytting</i> )	Innholds-kontroll, sensur	Logge; IP-adresser, når, hvor	Registrere; brukeres valg og handlinger	Hindre angrep, regulere tilgang osv.

- Mesteparten av denne oppsummeringen er stoff fra forelesningen 27. februar om overvåkning og kontroll av internett
- ... men mye av innholdet i Gisle Hannemyrs forelesning 6. mars, **om maktperspektiver**, kan også plasseres i skjemaet ovenfor

## "Interception"

- Mangler dessverre et ord som dekker godt nok
  - En av betydningene som dette er oversatt med i engelsk-norsk ordbok er "*oppsnapping*"
  - Handler om å fange opp innholdet i det som kommuniseres, oftest uten at de som kommuniserer vet om det
  - Sammenlignbart med *avlytting*, men omfatter alle typer data, ikke bare lyd
- I internett-sammenheng ofte omtalt som *pakkesniffing*
  - Men det uttrykket dekker ikke alle former for *interception*

## "Interception", rettslige spørsmål

- "Interception" kan være ulovlig avlytting, noe som hackere driver med
- Kan også være ledd i feilsøking og monitorering av eget nettverk – helt akseptabelt
- Det er også et verktøy for politi og etterretning
  - Rettslig regulert: Må holde seg innenfor lover og **regler om akseptable metoder** for etterforskning og bevissikring m.m.
  - Mye internasjonalt samarbeid om metode-reglene
    - men likevel en del forskjeller i hva som aksepteres
  - En generell fellesbetegnelse for "interception"-verktøy som brukes i politiarbeid er "*policeware*"

## Filtrering (å sile innhold)

- Rettslig regulering
  - **Handler om "de store spørsmålene": Ytringsfrihet, demokrati, personvern**
  - Lovforbud mot uønsket innhold, vs. "alminnelig folkeskikk"?
  - Ferske interessante lovforslag (Datakrimutvalget, Faremoutvalget)
- Aktører, roller og ansvar
  - Styrte av offentlige myndigheter vs. styrt av private virksomheter?
  - Arbeidsgiver?
  - Foreldre?
  - Nettsteds- eller kommunikasjonsleverandør?
  - ... eller eventuelt styrt av brukeren selv?

## Filtrering

- Filtrering er en samlebetegnelse for alt fra spam-kontroll til statlig sensur
- To hovedstrategier for filtreringsprogrammer:
  - filter basert på **automatisk analyse** av innholdet
  - filter basert på (manuell) **vurdering** av innholdet
  - Noen programmer, for eksempel en del spam-filtre, bruker begge disse strategiene i kombinasjon

## Filtrering

- Typisk for filter basert på **automatisk analyse**:
  - Kan anvendes på både kommunikasjons- og innholdstjenester
  - Baserer seg på ordlister
  - Ofte telling av antall forekomster, eventuelt også "veking" av visse ord og kombinasjoner for å avsløre uønsket innhold
  - Automatisk analyse av bilder, lyd, video etc. for å avdekke uønsket innhold er svært vanskelig og ressurskrevende
- Fordeler med automatisk analyse:
  - man prøver å "ta ballen, og ikke mannen", aktører og adresser ikke blir stengt ute på forhånd
- Ulemper med automatisk analyse:
  - Kan ikke brukes effektivt på annet innhold enn tekst
  - Upresist, stor fare for å filtrere feil

## Filtrering

- Filter basert på **vurdering av innhold**
  - Manuell, menneskelig vurdering av det enkelte nettsted eller den enkelte siden
  - Statisk prinsipp: Filtreringen fjernes ved ny manuell vurdering, det holder ikke bare å endre innholdet
  - Passer kun for innholdstjenester
    - Kommunikasjonstjenester er for dynamiske
- To hovedmekanismer for statisk filtrering
  - Svartelister ("opt-out")
    - Blokkerer adresser/sider som står på listen (mindre strengt)
  - Hvitelister ("opt-in")
    - Slipper bare inn adresser/sider som står på listen (strengere)

## Filtrering

- "Hybrid"-strategi: Merking av innhold
  - Egner seg til statiske innholdstjenester, men gir et betydelig oppdateringsproblem
  - Fordel: Kan brukes på bilder og video, ikke bare tekst
  - Hovedproblemet: Hvem skal merke?
    - En del innholdsleverandører merker selv, frivillig ("vi driver med porno og vedstår oss det, vi setter nivå 4 i de html-dokumentene dette gjelder")
    - Kan også være filterleverandøren eller en uavhengig tredjepart som merker – da settes de merkede nettstedene på svartelister, egen liste for henholdsvis nivå 1, nivå 2 osv.
  - Et annet problem: Kulturforskjeller
    - Oppfattes "clothed sexual touching" likt i Sverige og USA?

## Filtrering, rettslige spørsmål

- Ytringsfrihet, utgangspunktet
  - Filtrering av statiske innholdstjenester er en form for forhåndssensur, og det er strenge grenser for å kunne drive forhåndssensur i norsk rett
  - Grunnlovens § 100, fjerde ledd:  
"Forhaandscensur og andre forebyggende Forholdsregler kunne ikke benyttes, medmindre det er nødvendigt for at beskytte Børn og Unge imod skadelig Paavirkning fra levende Billeder. Brevcensur kan ei sættes i Værk uden i Anstalter"
  - Beskyttelse av barn og unge er altså et mulig unntak
  - Ellers må man forutsette stor grad av frivillighet

## Filtrering, rettslige spørsmål

- Men: Dette rammes ikke av vernet mot forhåndssensur:
  - At man selv velger å beskytte seg med filter
  - At foreldre filtrerer barnas bruk av nettet
- Litt mer i grenselandet:
  - Arbeidsgivers filtrering av ansattes nettilgang
    - Arbeidsgiveren har en styringsrett, og kan iverksette tiltak for å hindre at firmaets omdømme blir skadet, eller for å unngå at de ansatte kaster bort arbeidstiden
    - Men det er ikke like akseptabelt å iverksette forhåndssensur for å "unngå skadelig påvirkning" eller fri meningsdannelse
    - Arbeidsgivers adgang til å filtrere må derfor ses i sammenheng med det aktuelle formålet

## Trafikkdata

- Krav om at leverandøren av nettjeneste skal logge trafikkdata, og ta vare på dem en viss tid
- Også krav om at de skal slettes etter en viss tid
- Logger brukes også til andre formål enn overvåking, men det er for å støtte etterforskningsformål at det nå har kommet krav til lagringstid
- Trafikkdata kan som regel avdekke følgende:
  - IP-adresse (brukerens datamaskin-identifikasjon)
  - Tidspunkt
  - Hvilken brukerkonto (hos leverandør av nettjenester) som er pålogget med den identifiserte datamaskinen på dette tidspunktet
  - Hvilke nettsider som er besøkt

## Trafikkdata, rettslige spørsmål

- Utgangspunkt: **EUs datalagringsdirektiv**
  - Fører til lenger lagring av trafikkdata (2 år), med det formål å kunne få brukbare spor til etterforskning
- Motstående hensyn: **Personvern**
  - Lagringsreglene heftig debattert i en rekke innlegg i Aftenposten i november/desember 2006...
    - Guro Slettemark (Datatilsynet): "Hele folket under mistanke"
    - Inger Marie Sunde (Stipendiat, og sekretær for Datakrimutvalget): "Jeg vet jeg ikke er paranoid"
    - Guro Slettemark: "Råtner på rot"
    - Thomas Mathiesen (professor i retts sosiologi): "Farlig overvåking"
    - Inger Marie Sunde: "Gamle menns redsel"

## Adferdsdata

- Kan til dels bruke noe av den samme typen logging som trafikkdata, men:
  - Det er (normalt) *nettstedets* behandlingsansvarlige, og ikke ISP, som logger
  - Nettstedet vet ikke hvem som egentlig er abonnenten bak et konotonavn
  - Det som logges er bevegelser, valg, søkestrenger etc.
- Personvernøkende teknologier
  - Et slags "mottiltak" mot registrering av adferdsdata;
    - Ikke for å unngå eller forby registrering og bruk av det
    - Men for å gi brukeren selv kunnskap om og kontroll med hvilke adferdsdata som registreres (personvern hensyn)

## Adferdsdata, rettslige spørsmål

- Ikke så "fundamentale" hensyn som ved spørsmål om filtrering, men mange relevante elementer av rettsregler:
  - Personvern, rett til innsyn og krav til å innhente samtykke
  - Avtaler mellom innholdsleverandør og bruker? (Rimelige vilkår? Jevnbyrdige eller ikke jevnbyrdige parter?)
  - I hvor stor grad er adferdsdata nødvendig for å kunne ivareta opphavsrett eller informasjonssikkerhet?
- Maktperspektiv: "Lillebror ser deg"

## Sikkerhetstiltak

- Virksomheter (firmaer, offentlige etater, universiteter osv.) legger oftest opp sikkerhetstiltak i sitt driftsmiljø:
  - Viruskontroll, hindre skadelig programvare
  - Brannmurer, og IDS ("Intrusion detection system")
  - Spamfiltrering, hindre uønsket/meningsløst innhold
  - Tilgangskontroll
  - Passiv beskyttelse, for eksempel "herding" av driftsmiljø
  - Ikke alle sikkerhetstiltak har spesifikt med virksomhetens bruk av eller tilgjengelighet på Internett å gjøre

## Sikkerhetstiltak, rettslige spørsmål

- Mange ulike regelverk som stiller krav til informasjonssikkerhet
  - I liten grad direkte knyttet til internett, men reglene er likevel i **høy grad relevante for tjenester på nettet**
- Det stilles en del krav til at virksomheter på nettet driver med overvåking og kontroll – av sikkerheten
  - Alle de fem "metodeperspektivene" som er gjennomgått her kan være relevante og legitime kontrollmetoder
  - ... men de kan også misbrukes, til å gjennomføre **uforholdsmessig kontroll** (på bekostning av yttringsfrihet og personvern)
  - Et spørsmål om å balansere ulike hensyn

## Korte "rettslige stikkord"

Interception	Filtrering	Trafikkdata	Adferdsdata	Sikkerhets-tiltak
<p><i>Straffe-prosess</i></p> <p>krav til at det foreligger (tilstrekkelig alvorlig) mistanke</p>	<p><i>Ytrings-friheten</i>, (og dens grenser)</p> <p>offentlighets-prinsippet</p> <p>styringsrett (i arbeidsgiver-forhold etc.)</p>	<p><i>Ekomloven</i> fra 2003</p> <p>(+ straffeprosess)</p> <p>Utgangspunkt i EU-direktiver ("ekom-pakken" en håndfull ulike direktiver)</p>	<p><i>Pol § 21</i> (om person-profiler)</p> <p>Også mer generelt er bestem-melser i pol relevante</p>	<p>Ulike regler om sikkerhet</p> <p>Svært ofte vil <i>Pol § 13</i>, med pof-forskriftens kapittel 2, være mest relevant</p> <p>(Sikkerhetslov med forskrift, for forhold som gjelder <i>rikets sikkerhet</i>)</p>