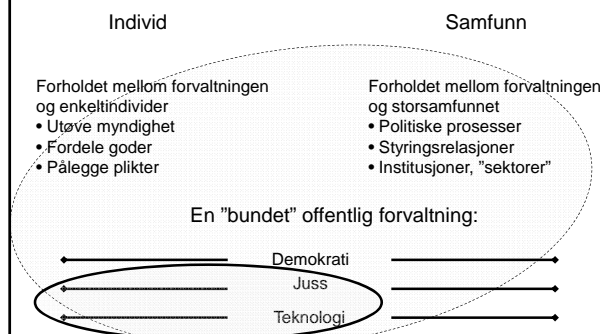


## Transformering av lover og regler til programkode

Forelesning, DRI3010, 14. oktober 2009

## Systemutvikling og automatisering av beslutninger



## Den offentlige forvaltningens myndighetsutøvelse overfor enkeltindivider

- Oppgaver og institusjoner med politisk mandat
  - Oftest "omformet" til et rettslig mandat (lov)
- Materielle regler og rettigheter
  - "Enkle" (deterministiske) regler
    - Hvor mye skatt skal betales av inntekt x?
    - Hvor mye får y utbetalt under sin pappapermisjon?
  - Komplekse saker, skjønnsbaserte regler
    - Hvilket behov for beskyttelse har asylsøker z?
    - Vil "barnets beste" i sak s være å flytte til fosterhjem, eller kan foreldrene settes i stand til bedre omsorg?
  - Norsk offentlig forvaltning; "salig blanding" av ulike typer materielle regler

## Prosessuelle regler og rettigheter

- Overordnede hensyn
  - Rettssikkerhet
  - Personvern
  - Menneskerettigheter
- Mer operative regler
  - Krav til å skaffe relevante opplysninger i saken
  - Veiledningsplikt
  - Begrunningsplikt
  - Taushetsplikt
  - Innsynsrett
  - Klageadgang

## Bruk av IT i forvaltningens myndighetsutøvelse

- Bruk av IT gir aldri "fritak" fra krav til å overholde både materielle og prosessuelle regler
- Noen spørsmål til "automatiserte beslutninger":
  - Hva slags materielle regler egner seg til å håndteres i et IT-system?
  - Hvordan kan prosessuelle regler ivaretas?
  - Hvilke deler av arbeidet bør (eller må) utføres manuelt – utenfor IT-systemene?
- Denne delen av DRI3010, litt i dybden om:
  - Utvikling av systemer med rettslig innhold
  - Hvordan styrke rettssikkerheten ved bruk av IT

## Generelle utviklingstrekk i forvaltningens bruk av IT

- 1960-70-årene
  - Sentrale systemer, enkle prosesser/store volum
  - Relativt få brukere
- 1980-90-årene
  - IT brukes i store deler av saksbehandlingsprosessen
  - De fleste ansatte bruker IT til sine oppgaver
- Sent 1990-tall og fremover
  - IT brukes i helhetlige saksbehandlingsprosesser
  - eForvaltning, også borgerne bruker IT i "sin del" av saksbehandlingen (f.eks. elektronisk søknad)

(En liten parentes; utviklingstrekk i hva rettsinformatisk *forskning* har vært opptatt av)

- 1970-80-årene
  - Mulighetene for å representere "juridisk skjønn" i datamaskinprogrammer
  - Personvern ("interesseteorien")
  - Tekstbaser og tekstøk (Lovdata)
- 1990-årene
  - "Registerkobling" og gjenbruk av opplysninger (personvernvingling)
  - Automatiserte beslutninger ("enkel" saksbehandling)
- 2000 og fremover
  - Internett, internasjonal regulering
  - Informasjonssikkerhet
  - E-forvaltning

IT-systemene som er i fokus i denne delen av DRI3010

- Beslutningssystemer – noen eksempler:
  - Det meste av trygdesystemene i NAV
  - Skatteetatens likningssystemer
  - Bostøtteordningen
- Beslutningsstøttesystemer – noen eksempler:
  - Arbeidsformidling og -kvalifisering i NAV
  - Barnevernstjenesters IT-verktøy
- eForvaltning
  - Altinn, innrapportering og utsendelse
  - "Min fastlege" ([www.nav.no/minfastlege](http://www.nav.no/minfastlege))

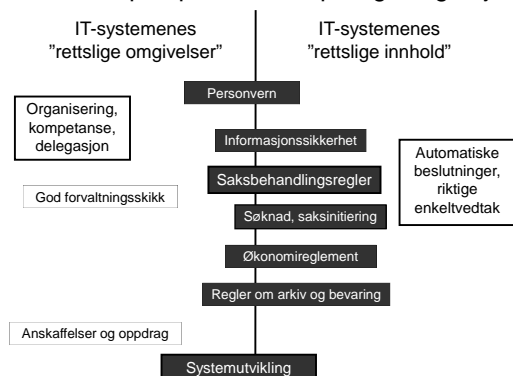
"Rettslig kvalitet" i disse typene systemer

- Riktige (materielle) vedtak
  - Både helt og delvis automatiserte beslutninger
- Tilstrekkelig sikkerhet
- Personvern
  - Relevante, nødvendige opplysninger som behandles
  - Innsyn, samtykke, korrigeringsrett osv.
- Rettssikkerhet
  - Beslutningsgrunnlag, begrunnelser, forståelighet osv.
- Robust og vedlikeholdsvennlig
  - Tilpasning til nye/endrede materielle regler
  - Feilretting, forståelighet osv.

"Rettslig innhold" i IT-systemer

- Det rettslige innholdet "blir til" i en *systemutviklingsprosess*
- Systemutvikling er **valg og beslutninger**
  - Å utforme rettslige innhold i et IT-system er en rettslig beslutning
- Viktig forskjell:
  - Hvordan er en bestemt rettslig regel representert i et IT-system, eks:
    - Kriterier for å få alderspensjon
    - Rett håndtering av forskjellig sivilstatus i ulike regelverk osv.
  - Hvilke regelverk *rundt et IT-system* som påvirker beslutningene i utviklingsprosessen, eks:
    - Sikkerhetskrav
    - Arkivdanning og arkivering
    - Økonomiregelverk
    - Anskaffelsesregelverk osv.

Infrastrukturperspektiv, samspill og integrasjon



Om begrepet "transformering"

Bokmålsordboka

TILSLAGSORD ARTIKKEL FRA BOKMÅLSORDBOKA (offisiell rettskriving)  
 transformere **transforme're** v2 (fra lat., av *trans-* og *formare* 'danne') omforme, omdanne, særli: overføre elektrisk strøm fra én spenning til en annen

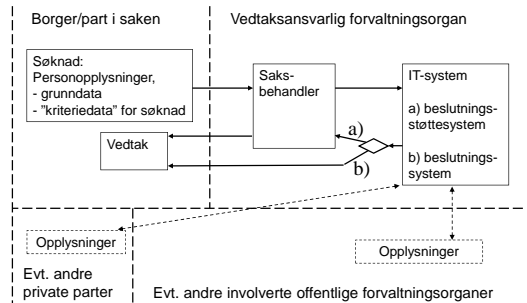
- I forvaltningsinformatikk:
  - "datamaskinprogrammet er en *alternativ representasjon* av den rettslige normen" (Bing, 1984)
  - "transformering fra regeltekst i naturlig språk til edb-program innebærer noe prinsipielt forskjellig fra 'oversettelse' i vanlig forstand, bl.a pga de *utvalg* og *suppleringer* som foretas" (Schartum, 1993)

## Nærmer om transformering:

- Transformeringen skjer – i hovedsak – under systemutvikling
  - Kravspesifisering, designvalg, programmering
- Noe av transformeringen skjer under *bruk*
  - Tolkning av hva som skal registreres, bruk av koder
- Transformering omfatter både *materielle* regler og *prosessuelle* regler
- *Utvalg og supplering* av rettskildene er rettslige beslutninger

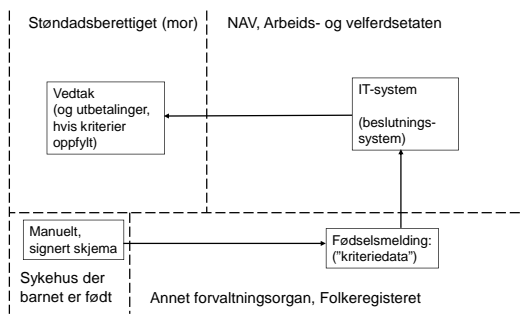
## IT-støtte i offentlig saksbehandling

"Typisk prosess:"



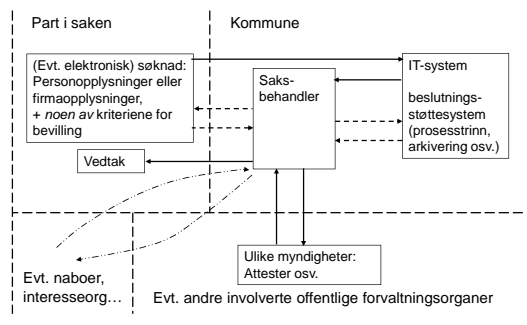
## Variant; barnetrygd

Hel-automatisert beslutning



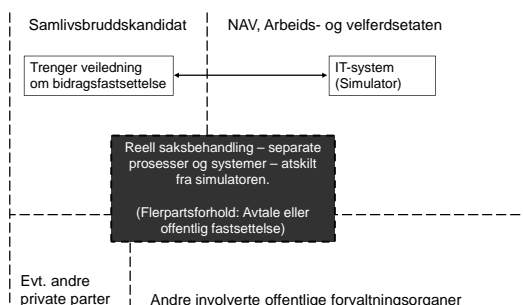
## Variant; skjenkebevilling

"Svak beslutningsstøtte", hovedsakelig manuell behandling



## Variant; vedtakssimulator

Veiledningsformål, publikumløsning uten reell saksbehandling



## Hovedbegreper fra artikkelen "Dirt in the Machinery of Government":

- "Transformering av rettskilder"
  - Kap. 6: Dekningsgrad/utstrekning
  - Kap. 7: Grad av transformering - formalisering
  - Kap. 8: *Utvalg* av "transformerbare" operasjoner
  - Kap. 9: *Supplering* av rettskildene
  - Kap. 10: "Tvisom" eller gal representasjon av normen
- "Transformering av sakens faktum"
  - Kap. 11: Bruker/saksbehandlers tolkning og forståelse av hvordan systemet skal brukes

## Systemtransparens

**transparen't** a2 (også utt -an>g; gj fr fra mlat, av *transparere* 'være synlig gjennom', av *trans-* og lat. *parere* 'være synlig')  
gjennomsiktig, gjennomskinnelig

- **Hva er systemtransparens? I grove trekk innebærer det at det transformerte, rettslige innholdet skal være**  
**tilgjengelig, forståelig og forsvart** Egenskaper
- **Hvorfor systemtransparens?**
  - Et (av mange) midler for å realisere viktige hensyn som rettssikkerhet, demokrati og personvern Mål/idealer
- **Hvordan oppnå systemtransparens?**
  - Styring, organisering/medvirkning, dokumentasjon, opplæring osv. Virkemidler/metoder

## Forståelighet

- Forvaltningens generelle veiledningsplikt, fvl. § 11
  - "å gi parter og andre interesserte adgang til å vareta sitt tarv i bestemte saker på best mulig måte"
- Pol § 22, innsyn ved helautomatiske beslutninger
  - "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"

## Forsvarbarhet

- Generell begrunnelsesplikt, fvl. §§ 24 og 25
- Klagerett, fvl. § 28
  - Alle avgjørelser kan normalt påklages i én instans, som kan "prøve alle sider ved saken"
- Reservasjonsretten for helautomatiske avgjørelser, pol § 25
  - Den som en fullt automatisert avgjørelse som nevnt i § 22 retter seg mot eller som saken ellers direkte gjelder, kan kreve at avgjørelsen overprøves av en fysisk person.

## "Dirt in the machinery...", kap. 12

- Dokumentasjon gir transparente systemer
- "Rettslig dokumentasjon"
  - Konkrete koblinger mellom rettskildene og datamaskinprogrammet
  - Vise fram/tydeliggjøre tolkningsvalg og *beslutningene* under transformering
- Dokumentasjon på to nivåer:
  - "Programnær", teknisk orientert dokumentasjon (for legalitetskontroll)
  - "Rettskildenær", mindre formalisert (for veiledning)

## Mer fra kapittel 12

- To nivåer av dokumentasjon:
  - Bør være så like hverandre at det ikke feiltolkes mellom dem
    - Problemer som ikke drøftes: Er dette mulig? Er det effektivt/hensiktsmessig?
  - Dokumentasjonen "leses begge veier": Bedre mulighet for å bruke *systemutviklingen* som verktøy for å forenkle og forbedre regelverket bakenfor
- Handler også om *tilgjengeliggjøring*
  - Selve systemene bør også publiseres
    - Problem som ikke drøftes: Opphavsrett, eierskap
    - Problem som bare så vidt berøres: Borgernes forkunnskaper

## Dokumentasjon som virkemiddel for systemtransparens

- Systemdokumentasjon som "Kinder-egg", løser tre ting på en gang...
  - Dokumentasjonen er et *håndfast produkt*, som er egnet for tilgjengeliggjøring
  - Dokumentasjonen beskriver systemets innhold i *naturlig språk*, som er mer forståelig
  - Dokumentasjonen kan (forhåpentligvis) *beskrive samsvaret* mellom rettskilder og transformering, som gjør IT-systemets transformerte regelverk forsvart

## Dokumentasjonsproblem I, "hvor i IT-systemet har de ulike rettskildene blitt av"

	Database-definisjoner	Programkode-moduler	Lagrete, formaliserte data
Positive definisjoner	tabeller attributter prosjeksjoner	skjermbilder, inntasting og visning av data	dataverdier
Restriksjoner	integritetsregler domenerestriksjoner	kode som angir kriterier for kontroll av inntastede verdier	data som angir kriterier for kontroll av innlastete verdier
Oppdatering av data	triggere og lagrede prosedyrer	kode som setter betingelser for oppdatering	data som setter betingelser for oppdatering
Algoritmer	lagrede prosedyrer	kode som inneholder algoritmer for å beregne nye verdier	data som inneholder algoritmer for å beregne nye verdier

Transformeringsrommet

## Dokumentasjonsproblem II, form og innhold

- Hva skal dokumentasjonen inneholde, og hvordan utforme den?
  - Dokumentasjonens formål
  - Dokumentasjonens målgrupper
  - Dokumentasjonens systematikk
- Gir kravene til forståelighet og forsvarbarhet samme type dokumentasjon?
  - Eller er det behov for ulike dokumentasjon for ulike formål og målgrupper?

## Dokumentasjonsproblem III, i praksis er svært mange IT-systemer "underdokumenterte"

- "Feil profesjoner" som skriver dokumentasjon?
- Lavt prioritert i utviklingsprosjekter?
- Bi-produkt av utviklingsprosessen, vedlikeholdes derfor dårlig etter at systemet er tatt i bruk?
- Gir lite "status" å skrive dokumentasjon?

## "Dirt in the machinery...", Kap. 13-17: Ansvar og styring, organisering og deltakelse

- "Hvem"-spørsmålene
  - Hvem er ansvarlig for "godt nok" samsvar mellom rettskildene og transformerte regler i IT-systemer?
    - Rettslige utgangspunkter for ansvaret
    - Det offentliges styringsprinsipper (økonomireglementene etc.)
  - Hvem *må*  
*bør*  
*kan*  
delta i transformeringen av rettskilder?
    - Til en viss grad rettslige reguleringer
    - ... men i hovedsak spørsmål om pragmatiske valg

## Ansvar og styring

- Ansvar for en forvaltningsoppgave er
  - Noen ganger plassert direkte i lovtekst
    - Eks. Lov om utdanningsstøtte, § 16: "Lånekassen forvalter utdanningsstøtten i samsvar med bestemmelsene gitt i eller i medhold av denne lov"
  - Andre ganger er ansvaret plassert på overordnet myndighet, som delegerer oppgavene
    - Eks. Sosialtjenesteloven, § 2-1: "Kommunen er ansvarlig for å utføre de oppgaver etter loven som ikke er lagt til et statlig organ."
- Overordnede organer har *instruksjonsmyndighet* over underordnede organer (generelt ulovfestet)

## Organisering og deltakelse

- Systemer utvikles (nesten alltid) av prosjekter med sammensatt deltakelse
  - Prosjektorganisasjonen har ingen "egen myndighet", den er basert på oppdrag og delegasjon fra behandlingsansvarlig
- Er det noen som "må delta"?
  - Ansvarlig forvaltningsorgan "må" delta i utviklingen i den forstand at de er ansvarlige for resultatet
  - Medarbeidere har rett til deltakelse (gjennom medbestemmelsesapparat, jf. arbeidsmiljøloven)

## Organisering og deltakelse

- Hvem "bør eller kan delta"?
  - Eksterne brukere ("fokusgrupper", brukerrepresentanter)
  - Tilgrensende fagmiljøer i forvaltningsorganet (arkiv, økonomi, statistikk)
  - Teknologisk fagmiljø, internt eller innleide konsulenter
- Forholdet mellom profesjoner
  - Faglig ansvar, regelverkskompetanse, "hva *skal* representeres"?
  - Teknologisk kompetanse, "hva *kan* representeres"?

## Ansvar ut fra rollen "behandlingsansvarlig" i personopplysningsloven

- Pol definerer to særskilte roller, "behandlingsansvarlig", og "databehandler".
  - Behandlingsansvarlig er ansvarlig for at personopplysningsloven etterleves
  - Følger ansvarsforhold etter relevante lover, den behandlingsansvarlige må ha "rettslig evne"
  - I visse tilfeller kan det være vanskelig å plassere dette ansvaret bare ut fra definisjonen, det finnes noen eksempler på at ansvaret *plasseres konkret* i lov eller forskrift

## Pliker for "rollene" i personopplysningsloven

Utvikling	Drift
<p><i>Behandlingsansvarlig</i> har klare plikter til å "legge til rette for":</p> <ul style="list-style-type: none"> <li>- Grunnkrav og vilkår for behandling (§ 11 jf. §§ 8 og 9)</li> <li>- Sende melding om behandling til Datatilsynet innen 30 dager før</li> </ul>	<p><i>Behandlingsansvarlig</i> har ansvar for alle sider ved å etterleve krav i personopplysningsloven ("overordnet regel" om dette er internkontrollkravet i § 14 og sikkerhetskravene i § 13)</p>
<p><i>Databehandler</i> har i prinsippet ingen egne plikter knyttet til utvikling</p>	<p><i>Databehandler</i> har "negativ plikt", til å ikke behandle opplysninger på annen måte/til annet formål enn det som er skriftlig avtalt (§ 15)</p> <ul style="list-style-type: none"> <li>- Også direkte pålagt å etterleve sikkerhetskravene i § 13</li> </ul>

## Om forholdet mellom utvikling og drift

- Utvikling:
  - Forstå og implementere regler m.m.
  - "Legge til rette for" godt personvern
- Drift:
  - Følge regler, etterleve prosedyrer m.m.
  - "Realisere personvern"
- Men:
  - Ofte vanskelig og misvisende å trekke et så sterkt skille mellom utvikling og drift. Erfaringer og behov for endringer må ofte tilbakeføres til utviklingsprosesser
  - Derfor er det også behov for vekselvirkning mellom "legge til rette for" og "realisere" personvern

## "Personvernvennlig" systemutvikling (I)

- Hvordan kan mengden opplysninger som samles inn minimaliseres?
  - Hvor klart må "den registrerte" identifiseres?
  - Hvor lenge må opplysninger lagres?
- Hvordan sikres best mulig kvalitet i opplysningene
- Hvordan kan den registrerte sikres best mulig kontroll med behandlingen av opplysninger
- Er "systemavgrensning" et personvernsspørsmål?

## "Personvernvennlig" systemutvikling (II)

- Personopplysningslovens regler har betydning både for løsningsvalg "inni systemene" og for forholdet mellom system og omgivelser
- Godt personvern forutsetter god tilrettelegging av systemene
  - Dårlig forarbeid under *utvikling* gjør det vanskeligere å realisere godt personvern i den daglige *drift*
- Erfaringer fra drift og bruk tilbakeføres gjerne til senere utviklingsaktiviteter
  - Tilsvarende bør erfaringene fra hvordan personvernet *realiseres* i praksis, brukes som innspill til hvordan man senere tilrettelegger bedre for personvern