Forord

Denne publikasjonen er et resultat av det arbeidet Statskonsult har iverksatt for å legge forholdene bedre til rette for bruk av elektronisk saksbehandling i statsforvaltningen. Det er således en av flere publikasjoner Statskonsult har utgitt innenfor dette området det siste året. Av tidligere publikasjoner kan nevnes "*Statens generelle kravspesifikasjon for elektronisk saksbehandling*" og veiledningen "*Innføring av elektronisk saksbehandling*".

Årsaken til denne satsningen fra Statskonsult er at det har vist seg at selv om utbredelsen av IT i statsforvaltningen er stor, gir dagens bruk av IT i saksbehandlingen små gevinster i forhold til mulighetene. Årsakene til at en ikke har lykkes å realisere hele gevinstpotensialet, kan være mange. Det er imidlertid grunn til å tro at reglene som styrer saksbehandlingen, kan være én av faktorene.

Saksbehandlingen i offentlig forvaltning er i stor grad styrt gjennom lover og forskrifter. Det er derfor viktig at regelverket er oppdatert, slik at ny teknologi kan tas i bruk på en hensiktsmessig måte. Likeledes er det grunn til å undersøke om utviklingen har ført til at det nå behøves regler på områder som tidligere ikke har vært regulert. Til en viss grad vil det nok skje tilpasninger gjennom utvidende tolkninger i forbindelse med praktiseringen av regelverket. Det vil likevel være et behov for at det på sentralt hold arbeides med å utvikle regelverket, både for å få en enhetlig praksis i forvaltningen, men også fordi lovverket må oppdateres for at det ikke skal bli for stor sprik mellom regelverk og praksis. Det vil være uheldig dersom regelverket ikke gav god veiledning om rettstilstanden fordi praksis gjennomgående gikk langt ut over ordlyden i bestemmelsene.

Selv om lovverket nok trenger en del endringer på dette området, er det ikke tvil om at mye elektronisk saksbehandling er uproblematisk å gjennomføre med dagens regelverk. Dette viser seg da også i forvaltningens daglige virke. Selv på et tradisjonelt så "vanskelig" område som elektronisk kommunikasjon med brukerne, finnes det mange eksempler på at elektronene er i ferd med å erstatte eller supplere papirskjemaer. Som eksempler her kan nevnes tollvesenets TVINN-prosjekt og innrapporteringen til arbeidsgiver/arbeidstakerregisteret, som begge åpner muligheten for brukerene til å innrapportere sine data i elektronisk form. Det er derfor ingen grunn for den enkelte etat til å sitte på gjerdet og vente på regelendringer før en tar i bruk elektronisk saksbehandling. Det bør derimot jobbes parallelt med innføring av elektronisk saksbehandling og tilpasning av regelverket.

Denne rapporten er ment å være et kart over terrenget slik det ser ut i dag. Den inneholder derfor ingen ferdige løsninger, men den vil forhåpentligvis sette fokus på noen områder der det bør arbeides videre med å endre eller videreutvikle regelverket. På noen områder vil Statskonsult kunne arbeide videre med enkelte av problemstillingene, men det vil i hovedsak være regelverksforvalterne på de ulike områdene som bør videreføre arbeidet.

Denne rapporten er utarbeidet og skrevet av rådgiver Michal Wiik Johansen fra Statskonsult. Rapporten er en videreføring av Statskonsults kartlegging av

juridiske problemstillinger som reises ved innføring av elektronisk saksbehandling (Notat 1997:3). På enkelte områder er det kun gjort små endringer i forhold til teksten i kartleggingen. Kartleggingen ble utarbeidet av spesialrådgiver Maria Strøm, spesialrådgiver Erik Bollestad og rådgiver Ragnhild Castberg Greni, alle fra Statskonsult. Konsulent Marit Kristin Larsen fra Statskonsult har også bidratt til arbeidet ved å arrangere et seminar for alle høringsinstansene.

Oslo september 1998

Jon Blaalid

Innhold

1 Innledning

1.1 Bakgrunn og formål

Helt siden det erstattet kalveskinnet, har papiret vært den dominerende bærer av informasjon om forvaltningens virksomhet. Gjennom lang tids bruk har det blitt utformet regelverk og praksis for hvordan informasjon lagret på papir skal håndteres. De seneste tiår har introdusert edb som et nytt medium for informasjonsforvaltning. Sett i forhold til den relativt korte tiden elektronisk databehandling har vært en del av offentlig forvaltning, har den fått en bemerkelsesverdig sentral posisjon. De fleste som har vært utsatt for driftsavbrudd i edb-systemet, har nok gjort seg sine refleksjoner om det avhengighetsforholdet vi har i forhold til datamaskinen. Til tross for den omfattende bruken av edb, er inntrykket at det i liten grad har vært fokusert på dette under utformingen av regelverket som regulerer forvaltningen. Generelt kan en nok si at det er en styrke at lovverket ikke er knyttet opp mot en bestemt teknologi, men det er samtidig viktig å være på vakt mot at regelverket kommer i utakt med eksisterende teknologier på en måte som gjør at rasjonelle arbeidsordninger blir avskåret av utilsiktede virkninger av regelverket.

I 1996 la «Statssekretærutvalget for IT» frem rapporten «*Bit for bit*»[1]. Rapporten beskriver noen av de muligheter og utfordringer informasjonsteknologien stiller samfunnet overfor. Rapporten beskriver også noen målsetninger for bruk av informasjonsteknologi. Flere av disse målsetningene relaterer seg til bruk av informasjonsteknologi i offentlig forvaltning. I rapportens punkt «politikk 3.8.5» heter det at «Elektronisk saksbehandling skal være en normal del av saksbehandlingen i statlig forvaltning. Papir skal gradvis erstattes med elektroniske dokumenter». Denne politikken må ses i sammenheng med punktet «politikk 3.3.6», hvor det heter at «Elektronisk kommunikasjon og bruk av nett som infrastruktur for samhandling skal bli like akseptert, tillitvekkende og ha samme juridiske holdbarhet som tradisjonell papirbasert kommunikasjon og dokumentasjon»[2]. Til sammen utgjør disse punktene en målsetning om at det skal tilrettelegges for bruk av elektronisk saksbehandling i det offentlige, samtidig som det skal være mulig for borgerne i størst mulig grad å kunne kommunisere med forvaltningen gjennom bruk av informasjonsteknologi.

På bakgrunn av dette har Statskonsult satt i gang et bredt anlagt arbeid for å tilrettelegge for elektronisk saksbehandling i statlig forvaltning. Det er allerede utgitt en generell kravspesifikasjon for elektronisk saksbehandling (SGK for elektronisk saksbehandling), samt en veiledning til denne.

Denne rapporten tar for seg juridiske problemstillinger elektronisk saksbehandling reiser i forhold til dagens regelverk. Arbeidet med rapporten ble påbegynt våren 96 ved at Statskonsult utarbeidet notatet «*Elektronisk saksbehandling - En kartlegging av juridiske problemstillinger som reises ved innføring av elektronisk saksbehandling i forvaltningen*»[3]. Notatet inneholdt et scenario som beskriver de mulighetene elektronisk saksbehandling kan tilby,

[1] *Den norske IT-veien Bit for bit*, Rapport fra Statssekretærutvalget for IT, jan 1996
[2] Denne målsetningen er videreført i St meld nr 32 1997-98, Om offentlighet i forvaltningen
[3] Notat 1997:3, Statskonsult

samt en gjennomgang av sentrale saksbehandlingsregler som må forventes å bli berørt ved bruk av elektroniske saksbehandlingssystemer. Notatet ble sendt på høring til departementene og noen underliggende virksomheter, samt til enkelte kommuner.

Formålet med notatet var å få en oversikt over:

- virksomhetenes synspunkter på eventuelle regelverkshindringer eller mangler i forbindelse med innføring av elektronisk saksbehandling
- virksomhetenes strategier og planer om innføring av elektronisk saksbehandling
- virksomhetenes eventuelle behov for bistand

Saksbehandling er en arbeidsform i de fleste statlige virksomheter. Kunnskap om de forskjellige delene av prosessen og ideer for endringsarbeid vil nødvendigvis være spredt på virksomhetens ulike funksjoner. Vi bad derfor om at så mange ulike grupperinger som mulig i virksomheten deltok i utformingen av svarene. Spesielt ble følgende grupper fremhevet:

- *Ledelsen*, på alle nivåer, fordi den er ansvarlig for saksbehandlingen og for IT-strategien, og som deltaker og premissgiver i deler av den konkrete saksbehandlingen i virksomheten
- *IT-miljøet*, fordi det besitter den tekniske kompetansen som er en av flere viktige brikker i denne sammenhengen
- *Juridiske miljøer*, fordi det her finnes kunnskap om regelverket både på generelt nivå og i forhold til den enkelte virksomhets spesialområder
- *Administrasjon*, fordi ansvaret for interne rutiner ofte er plassert der
- *Arkiv*, som sitter med nøkkelkompetanse på dagens dokumenthåndtering og god kunnskap om hvordan saksgangen i virksomheten fungerer
- *Saksbehandlere*, som brukere av de eksisterende regelverk

Høringsrunden resulterte i over førti høringssvar som i stor grad gav et godt inntrykk av de forventningene og betenkelighetene elektronisk saksbehandling blir imøtesett med i forvaltningen. Denne rapporten er en videreføring av det arbeidet høringsinstansene har gjort i forhold til å beskrive sine synspunkter på eventuelle regelverkshindringer eller mangler i forbindelse med innføring av elektronisk saksbehandling.

Rapporten belyser treffpunkter mellom forvaltningsretten og elektronisk saksbehandling der det kan være tvil om rettsreglene er til hinder for elektronisk saksbehandling. Formålet med dette er først og fremst å danne et utgangspunkt for videre arbeid med regelverksendringer. I tillegg vil kartleggingen av juridiske problemstillinger være til hjelp for de etater som benytter eller planlegger å ta i bruk elektronisk saksbehandling.

1.2 Noen utgangspunkter

1.2.1 Rapportens område

Denne gjennomgangen av juridiske problemstillinger ved elektronisk saksbehandling er ikke uttømmende. For det første fokuserer rapporten i

hovedsak fokusert på problemstillinger som er felles for hele forvaltningen. Bare der det har vært fremstillingsmessig naturlig, er problemstillinger som er spesifikke for enkelte forvaltningsvirksomheter berørt. Gjennom erfaringer med bruk av elektroniske systemer vil det dessuten ganske sikkert dukke opp nye problemstillinger som rapporten ikke berører. Det er vel også grunn til å anta at problemstillinger som i dag kan virke vanskelige, på sikt vil finne løsninger gjennom praktisk bruk. Et eksempel på dette kan være spørsmålene omkring digitale signaturer og tiltrodde tredjeparter.

Rapporten legger mest vekt på elektronisk dokumenthåndtering, men andre mer generelle forhold ved elektronisk saksbehandling, så som taushetsplikt, innsynsrett og sikkerhet berøres også. Det er imidlertid satt av liten plass til såkalt automatisk saksbehandling. Se nærmere om dette nedenfor i punkt 1.2.3.

1.2.2 Juridiske hindringer kontra teknologiske hindringer

Denne rapporten har som utgangspunkt at elektroniske dokumenter i forvaltningen i størst mulig grad bør være likestilt med papirdokumenter. De fleste som kjenner til offentlig forvaltning, vil nok være enig i at det i dag på langt nær er slik at elektronisk kommunikasjon og oppbevaring av dokumenter er likestilt med papir innenfor forvaltningen. Hovedsakelig skyldes nok dette at elektronisk kommunikasjon fremdeles er relativt nytt og således ikke har hatt tid til å få den tilliten som skapes gjennom praktisk bruk. På noen områder er det imidlertid også juridiske hindringer for å ta i bruk elektronisk kommunikasjon og dokumentasjon. Når bestemmelser som setter papiret i en særstilling vurderes ut fra målsettingen om å likestille elektroniske dokumenter med papiret, er det viktig ikke å tape av syne at det på enkelte områder kan være meget gode grunner for å sondre mellom papir og andre medier. Papiret har mange kvaliteter som lagringsmedium som det ikke for alle formål er like enkelt å finne et alternativ til. Utgangspunktet om likestilling mellom papir og elektroniske lagringsmedier må derfor fravikes dersom informasjonsteknologien ikke kan tilby de samme kvalitetene som papiret. I disse tilfellene foreligger det ikke en juridisk, men en teknologisk hindring.

1.2.3 Elektronisk saksbehandling kontra automatisk saksbehandling

Elektronisk saksbehandling må ikke forveksles eller oppfattes som synonymt med automatisk saksbehandling. I dette dokumentet brukes begrepet «elektronisk saksbehandling» om all saksbehandling som i større eller mindre grad gjør bruk av informasjonsteknologi i saksbehandlingsprosessen. Dette spenner fra saksbehandling der pc brukes som skriveverktøy, til automatiserte avgjørelser som fattes av en datamaskin etter at de relevante verdiene er lagt inn. Det skal imidlertid påpekes at det finnes viktige vesensforskjeller mellom IT som tilbyr saksbehandleren støtte i saksbehandlingsprosessen, og IT som i henhold til forhåndsdefinerte kriterier fatter beslutninger automatisk.

Automatiske saksbehandlingssystemer er i stor grad virksomhetsspesifikke, og har således ingen sentral plass i en gjennomgang av generelle forvaltningsrettslige problemstillinger ved elektronisk saksbehandling. Automatisk saksbehandling innenfor områder med ikke-standardisert saksbehandling vil f.eks. reise juridiske og praktiske problemstillinger av en helt

annen karakter enn for virksomheter med høy grad av standardisert saksbehandling. Når dette utgangspunktet er slått fast, må det presiseres at også saksflytsystemer kan tilby mer eller mindre automatiserte prosesser. Ett eksempel på dette kan være at saksbehandlingssystemet varsler om frister i saksbehandlingsprosessen som er hjemlet i regelverket, eller at systemet automatisk sender varsel til de involverte partene.

1.3 Den videre fremstillingen

Rapporten er delt i seks hovedkapitler – elektronisk kommunikasjon, offentlighet og innsynsrett, saksbehandlingsregler, taushetsplikt, personvern og arkiv. Under hvert emne gjøres det kort rede for de viktigste rettsreglene som regulerer vedkommende område. Deretter følger et ekstrakt av de problemstillingene som er tatt opp i høringsrunden. Hvert tema avsluttes med kommentarer til de problemstillingene som berøres av høringsinstansene. Under noen av temaene er det også tatt opp problemstillinger som ikke er berørt av høringsinstansene, men som Statskonsult har blitt oppmerksom på under arbeidet med rapporten.

Rapporten avsluttes med en oppsummering av noen områder der dagens regelverk kan synes å være noe i utakt med utviklingen av informasjonsteknologien. Det gjelder både områder der regelverket er til hinder for utnyttelse av fordeler informasjonsteknologien kan tilby, og områder der informasjonsteknologien medfører andre konsekvenser som neppe var vurdert ved utformingen av regelverket. Det er også gitt noen anbefalinger på områder der det er viktig å videreføre arbeidet for å tilpasse lovverket til mulighetene og utfordringene ved elektronisk saksbehandling.

Rapporten har to vedlegg. Det første vedlegget inneholder et scenario som beskriver hvordan saksbehandlingen kan arte seg når en benytter elektronisk saksbehandling helt fra saken starter hos søkeren, og til den er ferdigbehandlet av forvaltningen. Det andre vedlegget er en fremstilling av hvordan en ordning med digitale signaturer kan funksjonere. For lesere som ikke har kjennskap til virkemåten til digitale signaturer, kan det være en fordel å lese dette vedlegget i forbindelse med rapportens kapittel 2.

2 Elektronisk kommunikasjon

2.1 Hjemmelsgrunnlaget

Det skal innledningsvis presiseres at bruken av elektronisk kommunikasjon allerede i dag er meget omfattende innenfor offentlig forvaltning. Det skulle i denne sammenheng være tilstrekkelig å minne om alle de millioner data som hvert år overføres fra banker, forsikringsselskaper og liknende til skattemyndighetene i forbindelse med skatteberegningen. Likeledes utveksles det årlig enorme mengder data fra ulike organer inn til Statistisk sentralbyrå. De fleste av disse overføres i elektronisk form. Dette er bare to av mange eksempler på at elektronisk kommunikasjon benyttes i ordinær saksbehandling. I tillegg vet en at e-post brukes i stort omfang til uformell kontakt mellom saksbehandlere. Det er således ikke noe nytt at elektronisk kommunikasjon benyttes i offentlig saksbehandling. Dette kapitlet vil imidlertid hovedsakelig dreie seg om de områder der elektronisk kommunikasjon ikke er særlig vanlig. Særlig gjelder dette kontakt mellom offentlige organer og brukerne når dette ikke er avtalt på forhånd.

Lovverket inneholder en rekke bestemmelser som fastsetter at henvendelser til eller fra forvaltningen skal være skriftlige. Ett eksempel på dette er forvaltningsloven (fvl) § 23, som bestemmer at et enkeltvedtak som hovedregel skal være skriftlig. Skriftlighetskrav finner en også i form av plikt til å nedtegne muntlige forhandlinger (fvl § 11 c). På noen områder er det også bestemmelser om at det må benyttes spesielle skjemaer for enkelte typer henvendelser. En slik bestemmelse finner en f.eks. i ligningsloven § 4-3 om selvangivelse. Andre bestemmelser kan på en indirekte måte legge føringer for hvilke medier som kan benyttes ved henvendelser til forvaltningen. Forvaltningsloven § 32 b bestemmer f.eks. at en klage skal være undertegnet av klageren eller hans fullmektig.

Enkelte bestemmelser av denne typen kan fremstå som hindringer for elektronisk kommunikasjon mellom forvaltningen og borgerne. Stadig flere både i og utenfor forvaltningen ønsker å ta i bruk elektronisk kommunikasjon for å hente ut de effektivitets- og kvalitetsgevinstene som elektronisk kommunikasjon kan tilby. Det er derfor i første omgang viktig å klargjøre hvilke bestemmelser som er til hinder for å ta i bruk elektronisk kommunikasjon. Dersom en finner bestemmelser som er til hinder for elektronisk kommunikasjon, må det vurderes om bestemmelsene har støtte i reelle innvendinger mot denne typen kommunikasjon, eller om de er vedtatt i en kontekst der elektronisk kommunikasjon ikke var en aktuell problemstilling. Det må med andre ord vurderes om eventuelle stengsler for elektronisk kommunikasjon er en utilsiktet virkning av reglene, og ikke et uttrykk for reelle problemer.

2.2 Virksomhetenes kommentarer

Ikke uventet varierer det i hvilken utstrekning høringsorganene benytter seg av elektronisk kommunikasjon med brukerne. Det er hovedsakelig ved kontakt med andre offentlige virksomheter og større private foretak elektronisk kommunikasjon benyttes utover det rent sporadiske. Det er en videreutvikling av den elektroniske kommunikasjonen med disse aktørene som på kort sikt anses

som mest aktuell for de fleste høringsinstansenes vedkommende. Når det gjelder elektronisk kommunikasjon med privatpersoner er det en større skepsis til hvor raskt dette vil kunne få noe omfang av betydning. Det påpekes bl.a. at de fleste privatpersoner per i dag ikke har det nødvendige utstyret. Det er imidlertid problematikken rundt sikkerhet som gjør at de fleste antar det vil ta tid, og kreve betydelige ressurser, før en vil kunne tilby elektronisk kommunikasjon som et alternativ for samtlige som ønsker det. Mange instanser legger vekt på at dokumenter og opplysninger må få bevare sin konfidensialitet og integritet. Flere tar også opp problemet med å frembringe en metode for å etablere tillit til at avsender av et dokument faktisk er den som angis i dokumentet. Dette gjelder både dokumenter som kommer inn til det offentlige, og dokumenter fra det offentlige til private. Digitale signaturer og tiltrodde tredjepartsløsninger fremholdes av flere som en viktig forutsetning for å kunne utvide bruken av elektronisk kommunikasjon.

2.3 Utfyllende kommentarer

2.3.1 Nærmere om skriftlighetskravet

Som ovenfor nevnt, stiller regelverket på flere områder krav om skriftlighet. Det er viktig å være oppmerksom på at en ved tolkning av slike skriftlighetskrav, som ved all annen lovtolkning, ikke kan basere seg ene og alene på ordlyden i bestemmelsene. Når en skal vurdere innholdet i bestemmelser som setter krav til skriftlighet, er det også viktig å se på de hensynene som ligger til grunn for kravet. Dersom et dokument har en form som imøteser alle hensyn bak skriftlighetskravet kan dette tale for å tolke ordlyden utvidende. Det vil si at en form som rent umiddelbart oppfattes å ligge utenfor den tradisjonelle oppfattelsen av ordet skriftlighet, likevel kan ligge innenfor de rammene bestemmelsen setter.

Selv om hensynene riktignok kan variere noe i forhold til den enkelte bestemmelse, er nok de fleste av denne typen krav satt ut fra bevishensyn. En har for visse typer saker ønsket å sikre at det for ettertiden finnes dokumentasjon på hva som er besluttet, uttalt eller søkt om. Bak de ulike skriftlighetskravene ligger det nok for enkelte bestemmelsers vedkommende også andre supplerende hensyn. Eksempler på slike supplerende hensyn kan være hensynet til orden, effektivisering gjennom standardisering (f.eks. ligningsloven § 4-3) og hensynet til seremoni ved enkelte viktige disposisjoner (f.eks. ved inngåelse av ektepakt). Det vil nok likevel være slik at dersom en for bevishensynets vedkommende kan oppnå samme effekt ved bruk av elektroniske dokumenter som ved papir, vil nok andre hensyn bak skriftlighetskravene la seg imøtekomme på de fleste områder. Når dette er sagt, vil det selvfølgelig være andre hensyn bak enkelte skriftlighetskrav som ikke blir tilstrekkelig imøtekommet ved bruk av elektroniske dokumenter. For denne typen dokumenter må en holde seg til de mediene som ivaretar disse hensynene.

En annen viktig begrunnelse for skriftlighetskravet er ønsket om å ha bevis for *hvem* som har stått bak en beslutning, søknad eller uttalelse. Sistnevnte er imidlertid sterkest knyttet til signaturproblematikken og vil bli behandlet nedenfor.

2.3.2 Må skriftligheten være knyttet til papir?

Skriftlighetskrav er som nevnt oftest satt ut fra et bevishensyn. Det sentrale ved å kreve at en disposisjon skal skje skriftlig, er at det skal finnes et fysisk uttrykk for disposisjonen som til en viss grad er uavhengig av tid og rom. Det skal altså være mulig å få kjennskap til disposisjonens innhold fra andre kilder enn de personene som var til stede da disposisjonen ble foretatt. Når en disposisjon er dokumentert, er en mindre avhengig av nøytrale vitner. Samtidig vil et dokument ikke påvirkes av tiden på samme måte som vitners hukommelse.

Ut fra en formålsbetraktning må en anta at skriftlighetskravet også forutsetter at disposisjonen fremkommer på et medium som muliggjør forflytning av dokumentasjonen, samtidig som den har varighet over tid. For å ta et ikke særlig praktisk eksempel, vil skrift i sand typisk ikke kunne oppfylle de hensyn kravet til skriftlighet er satt til å ivareta.

Tekst som er lagret ved hjelp av edb, må etter en ren semantisk forståelse karakteriseres som skriftlig. Selv om et elektronisk dokument dypest sett er en rekke av elektriske impulser, er det liten tvil om at et elektronisk tekstdokument slik det fremstår på en skjerm, dekkes av skriftlighetsbegrepet. Spørsmålet blir dermed om elektronisk lagret tekst også er egnet til å ivareta hensynene bak skriftlighetskravene.

2.3.3 Lagring over tid

Edb-lagret materiale kan lagres i lang tid uten at den tekniske kvaliteten forringes. I forhold til langtidslagring har elektroniske dokumenter noen fortrinn som papirdokumenter ikke har. Edb-lagret materiale falmer ikke, sikkerhets-kopier vil være nøyaktig lik originalen, og det vil være små problemer med å innrette seg slik at en har kopier av alle dokumenter dersom det skulle skje noe med originaldokumentene. Selv om edb-materialet kan lagres over tid, er det viktig å være oppmerksom på at IT-utviklingen kan føre til at en får vanskeligheter med å hente frem gammelt edb-materiale. For å hente frem edb-lagret materiale må en ha tilgang til maskinvare som forstår koden dokumentene er lagret i. En må også ha kunnskap til å operere maskinvaren som skal lese programmene. Teknologi og programmering vil endre seg over tid. Dersom en ikke er påpasselig med å trekke med seg kunnskap om de forlatte teknologiene, kan det bli problematisk å få frem arkivert materiale. Denne problematikken har litt humoristisk blitt formulert som et behov for ikke bare å arkivere dokumentene, men også maskinvare og personell. Poenget er å illustrere at edb-materialet er avhengig av omgivelsene på en helt annen måte enn papir. Et papir vil kunne leses av alle lesekyndige som forstår språket dokumentet er skrevet på. Et edb-dokument er skrevet i et digitalt kodespråk svært få mennesker forstår. Dersom en ikke har maskinvare som kan oversette kodespråket til klartekst, vil dokumentet være til liten nytte. Den mest hensiktsmessige måten å sikre seg mot dette på er å sørge for å utarbeide rutiner for å konvertere gammelt materiale til nytt format når utviklingen gjør dette nødvendig. Formatproblematikken vil også gjøre seg gjeldende i forhold til arkivreglene og vil bli nærmere behandlet nedenfor. Det er imidlertid grunn til å merke seg at også krav om skriftlighet forutsetter at det er mulig å hente frem dokumenter i sin opprinnelige form i lang tid etter arkivering.

2.3.4 Format

Et elektronisk dokument kan fremstilles og oppbevares i mange ulike formater. Et dokument i ett format kan ikke uten videre hentes opp på en hvilken som helst datamaskin. En nødvendig forutsetning for å kunne åpne et dokument er at en har programvare som kan lese det formatet dokumentet er laget i, eventuelt et program som kan oversette dokumentet til et format en har program til å lese. Det finnes imidlertid et utall av forskjellige formater, og det vil i praksis ikke være mulig å lage programmer som kan oversette alle formatene. Dette vil kunne innebære en hindring for å innrømme borgerne en ubetinget rett til elektronisk kommunikasjon med forvaltningen. Dersom borgerne fritt skulle kunne velge hvilket format kommunikasjonen skal foregå på, vil forvaltningen i teorien måtte ha mulighet til å lese alle typer formater. Dette vil være praktisk umulig på grunn av antallet forskjellige formater. Situasjonen vil kunne sammenliknes med om forvaltningen skulle motta henvendelser på en rekke forskjellige språk. De mest vanlige språk som engelsk, fransk og tysk ville nok kunne håndteres greit, men en henvendelse fra en fjerntliggende øy i Stillehavet ville det nok avstedkomme betydelige problemer å få oversatt. Når fremmede språk ikke skaper nevneverdige problemer i dag, er nok dette i stor grad geografisk betinget. Det er i det praktiske liv sjelden at en Vest-Samoaner ønsker å kommunisere med trygdekontoret i Volda. Dataformater har ikke samme geografiske tilhørighet som språk. Selv om de fleste som ønsker kontakt med forvaltningen vil kunne betjenes ved hjelp av de vanligste formatene, vil «eksotiske» dataformater like godt kunne påtreffes i Norge som i Vanuatu.

På bakgrunn av det ovennevnte, vil det ikke være praktisk mulig å gi borgerne rett til å kommunisere elektronisk med forvaltningen, uten å innføre visse begrensninger i hvilket format som kan benyttes. Hvordan disse begrensningene skal utformes er et spørsmål som må utredes nærmere. Det største juridiske problemet i denne sammenheng vil sannsynligvis være at det vil kunne virke konkurransevridende å utelukke formater fra å benyttes til kommunikasjon med det offentlige.

2.3.5 Underskrifter og digitale signaturer

Den personlige underskriften har lang tradisjon som garantist for at dokumenter er ekte. Underskriften nyter stor tillit som autentitetsbevis både hos det offentlige og i handelslivet, til tross for at det kan være vanskelig for en ufaglært å avsløre en falsk underskrift. At den personlige underskriften vil endres over tid, kompliserer også ekthetskontroller. Selv om det ikke er en uoverstigelig oppgave å forfalske en underskrift, oppstår det relativt sjelden tvister om underskrifters ekthet. At underskriften i praksis fungerer så godt som autentitetsbevis er nok hovedgrunnen til den tillit den nyter. Dersom en ser på hvilken objektiv sikkerhet mot forfalskning underskriften tilbyr, er det ikke grunn til å ha overdreven tillit til den som autentitetsbevis. Dette er det viktig å ha in mente når en vurderer digitale signaturer som alternativ metode for å autentisere dokumenter.

I diskusjonen om digitale signaturer møter en ofte spørsmålet om en slik signatur er gyldig som erstatning for en håndskrevet underskrift. Et slikt spørsmål lar det seg ikke gjøre å svare et entydig ja eller nei på.

Den håndskrevne underskriften har minst to viktige funksjoner. Underskriften er i noen sammenhenger et rent bevismiddel for å knytte en person til en disposisjon. Det er denne funksjonen som kommer til uttrykk når en f.eks. undertegner en avtale om kjøp av ny pc. I andre sammenhenger må en benytte håndskrevet underskrift fordi loven stiller krav om det for at et dokument skal være gyldig. Et eksempel på dette er forvaltningsloven § 32, som bestemmer at klager skal være underskrevet. Som oftest er det slik at det også er bevishensyn som ligger bak lovens krav om at et dokument skal være undertegnet. Lovgiver har for enkelte typer dokumenter vurdert det som så viktig å sikre at det finnes bevis for at dokumentet virkelig kommer fra den som står angitt som utsteder, at det er satt krav om at dokumentet skal være underskrevet for å være gyldig. Eksempler på dette ser vi i sjekkloven § 1 og arveloven § 49, som bestemmer at henholdsvis sjekker og testamenter skal være underskrevet.

Selv om det stort sett er det samme hensynet som ligger til grunn enten en underskriver et dokument fordi loven krever det eller fordi en på eget initiativ ønsker å skaffe seg bevis for ettertiden, er det i forhold til problemstillingen rundt digitale signaturer en viktig juridisk forskjell mellom de to tilfellene. Det må foretas ulike tilnærminger avhengig av om dokumentet må underskrives for å oppfylle lovens formkrav, eller om det underskrives av rene bevishensyn.

2.3.5.1 Bevisvekt

For dokumenter som ikke er undergitt formkrav, vil underskriften først og fremst ha betydning som bevismiddel. Dette betyr at domstolene i siste instans må ta stilling til om dokumentet virkelig stammer fra den som ifølge dokumentet står anført som utsteder. Dette avgjør retten på fritt grunnlag. Retten er ikke bundet av om dokumentet er undertegnet av vedkommende eller ikke. Dette følger av prinsippet om fri bevisbedømmelse, se tvistemålsloven (tvml) § 183. Tvistemålsloven § 261 bestemmer riktignok at dokumenter som etter sin form og sitt innhold fremstiller seg som offentlige, formodes å være ekte og uforfalsket. Tilsvarende bestemmer tvml § 262 at et privat dokument som er egenhendig underskrevet med navn, avgir fullt bevis for at innholdet skriver seg fra den som har undertegnet dokumentet, dersom innholdet ikke gir særlig grunn til mistanke om noe annet. Dette er imidlertid ikke annet enn en presisering av den frie bevisbedømmelsen. Selv uten bestemmelsene i §§ 261 og 262, ville det naturlige utgangspunktet være at dokumentet stammer fra den som har underskrevet det. Når spørsmålet er hvorvidt dokumentet kan knyttes til den angivelige utstederen, gir det derfor liten mening å snakke om en digital signaturs gyldighet som sådan. Spørsmålet her vil være om hvor stor sikkerhet den digitale signaturen gir for at ikke andre enn utstederen kan stå bak dokumentet. Dette vil på samme måte som ved en håndskrevet underskrift, være en ren bevisvurdering.

Hvor stor bevisvekt en digital signatur skal tillegges må avgjøres i det konkrete tilfellet, jf. prinsippet om fri bevisbedømmelse. Med kunnskap om virkemåten til digitale signaturer kan en likevel si noe generelt om hvor stor tillit en kan feste til en digital signatur[4].

Sikkerheten i en digital signatur avhenger av to hovedfaktorer. For det første vil den tekniske sikkerheten avhenge av hvor avansert algoritmen som benyttes i

[4] Se nærmere om dette i vedlegg 1

krypteringen er og hvor lang kodenøkkelen er. Dernest vil sikkerheten avhenge av hvor godt en kan hindre at uvedkommende får kjennskap til kodenøkkelen.

Det er allment anerkjent at de krypteringsalgoritmene som i dag benyttes i digitale signaturer, er praktisk talt umulig å knekke dersom en benytter en kodenøkkel med mange nok siffer. En kan dermed trygt gå ut fra at en digital signatur i praksis ikke lar seg forfalske ved å knekke krypteringen.

Det vil imidlertid være en enkel sak å forfalske en digital signatur dersom en får tilgang til avsenders private kodenøkkel. Sikkerheten til en digital signatur avhenger dermed også av hvordan de private kodenøklene beskyttes. Kodenøklene er av en slik lengde at det er svært vanskelig for et menneske å huske dem. Det vil derfor være påkrevet å lagre kodene på et elektronisk lagringsmedium, f.eks. et smartkort med PIN-kode. Sikkerhetsproblematikken rundt dette er kjent fra betalingskortene. Oppstår det sikkerhetsbrudd ved at koden er blitt kjent for andre, vurderes korteierens forhold opp mot en aktsomhetsstandard. Dersom et betalingskort og kode oppbevares på en slik måte at uvedkommende får tak i dem, vil som oftest korteieren måtte bære tap som oppstår ved misbruk. Dette utgangspunktet vil også kunne benyttes i forhold til digitale signaturer. Problemet med digitale signaturer er at de kan misbrukes på måter som gir andre følger enn økonomisk tap. I saker som ikke først og fremst dreier seg om plassering av økonomisk ansvar, kan en ikke uten videre benytte den samme tilnærmingen til problemet som ved betalingskort, dersom korteier hevder at det er andre som har misbrukt kortet hans. Særlig tydelig er dette i forhold til straffesaker. En kan som eksempel tenke seg en situasjon der noen har avslørt at et dokument er falskt. Dokumentet er signert av A. A benekter imidlertid å ha utstedet dokumentet, og hevder at noen andre må ha fått tak i hans smartkort og kode og benyttet hans digitale signatur. Ut fra en aktsomhetsvurdering vil nok A kunne bli økonomisk ansvarlig for det tapet som måtte oppstå ved bruk av dokumentet, men det vil på dette grunnlaget ikke være mulig å ilegge strafferettslige sanksjoner for f.eks. brudd på straffeloven § 189, som setter straff for den som avgir uriktig erklæring om visse forhold. For å straffedømme A må det bevises at det faktisk er A som har signert dokumentet. Dette vil kunne bli adskillig vanskeligere enn dersom en hadde hatt en håndskrevet signatur.

Det er likevel slik at digitale signaturer basert på moderne teknologi i de fleste tilfeller vil tilby større sikkerhet mot endringer og forfalskninger enn håndskrevne signaturer. Den digitale signaturen vil således i minst like stor grad som underskriften være en garanti for at et dokument virkelig stammer fra den som anføres som utsteder.

Det bør derfor vurderes å gi digitale signaturer basert på moderne teknologi den samme status som tvml. § 262 gir den håndskrevne underskriften.

2.3.5.2 Formkrav

For de typer dokumenter der lovgivningen setter krav om underskrift, stiller spørsmålet om gyldighet av digitale signaturer seg noe annerledes. For denne typen dokumenter blir spørsmålet for det første om den digitale signaturen oppfyller lovens formkrav, og for det andre om den digitale signaturen ivaretar de hensynene krav om underskrift er begrunnet i.

Hovedhensynet bak formkrav om underskrift av dokumenter er som regel bevishensyn. Formkravene gjelder som oftest dokumenter som gir uttrykk for viktige disposisjoner det er svært viktig å skaffe bevis for. Et eksempel på dette er som nevnt arveloven § 49, som bestemmer at et testamente må være underskrevet. På den annen side er det liten tvil om at det daglig foretas disposisjoner av stor betydning på områder der lovgivningen ikke setter spesielle formkrav. Det er f.eks. ikke noe formelt i veien for å inngå avtaler i hundremillioners-klassen uten å underskrive noe dokument. Det er derfor grunn til å anta at det for enkelte dokumenters vedkommende også er andre hensyn enn bevisfunksjonen som er av betydning. Når ektefelleloven § 54 setter krav om at en ektepakt skal underskrives av ektefellene i nærvær av to vitner, er det nok også fordi dette skal være med på å markere at ektefellene foretar en alvorlig handling som bør gjennomtenkes nøye. I tillegg sikrer formkravene i disse tilfellene at ektefellene inngår avtalen med andre til stede, slik at mulighetene for tvang, svik e.l. reduseres.

Når det eksisterer et lovkrav om at et dokument skal være underskrevet, kan dette være et hinder for å bruke elektroniske dokumenter. Forvaltningsloven § 32 bestemmer f.eks. at en klage skal være undertegnet, og at en telegrafisk klage uten ugrunnet opphold må bekreftes skriftlig. Det er vel tvilsomt om lovgiver har ment å utelukke andre autentiseringsmekanismer som er like anvendelige og sikre som en håndskrevet underskrift, men det vil likevel være noe anstrengt å innfortolke digitale signaturer under begrepet underskrift. I dette tilfellet kan det synes som at lovens ordlyd stenger for en hensiktsmessig ordning, uten at dette bygger på et bevisst valg fra lovgivers side. Det er grunn til å anta at det i lovverket finnes en rekke slike underskriftskrav som ikke er tuftet på reelle innvendinger mot å benytte digitale signaturer.

Selv om det på svært mange områder ikke vil være noen grunn til å skille mellom håndskrevet underskrift og digitale signaturer er det likevel enkelte bestemmelser av denne typen som gir uttrykk for et hensiktsmessig forbud mot andre autentiseringsmekanismer enn den håndskrevne underskriften. Det kan for eksempel tenkes at det vil by på problemer å håndtere digitale signaturer for dokumenter som etter sitt innhold er ment å sirkulere blant flere som gir sin påtegning. Eksempler på slike dokumenter kan være ihendehavergjeldsbrev. Likeledes kan det av praktiske årsaker være vanskelig å få til en ordning med elektroniske førerkort. Det kan også være slik at vanskelighetene med å opprettholde påliteligheten til en digital signatur over lang tid[5], kan innebære at det for visse dokumenters vedkommende ikke vil være hensiktsmessig å likestille digitale signaturer med håndskrevet underskrift.

Men selv om det altså kan tenkes praktiske problemer for enkelte dokumenttyper, er det viktig å presisere at for det overveiende antall av dokumenter i det offentlige vil digitale signaturer gi en bedre sikkerhet for autensitet enn den håndskrevne underskriften. For hvilke dokumenter en bør utvise forsiktighet med å godta digitale signaturer, må en vurdere konkret.

En svært viktig forutsetning for å legge til rette for bruk av digitale signaturer, og derigjennom en utvidet bruk av elektronisk kommunikasjon, vil derfor være å gjennomgå lovverket for å avgjøre hvilke av underskriftsbestemmelsene som bør endres, slik at det også blir mulig å benytte digitale signaturer.

[5] Se nærmere om dette i vedlegg 2

En måte å foreta en slik gjennomgang på kan være å revidere hver enkelt bestemmelse som inneholder krav om underskrift. Dette vil i så fall innebære endringer av svært mange lover, noe som vil være tidkrevende både for forvaltningen og Stortinget. En mer praktisk tilnærming vil nok være å gi en generisk bestemmelse om at der lovbestemmelser benytter underskrift, omfatter dette også digitale signaturer dersom annet ikke er bestemt i forbindelse med det enkelte underskriftskrav. Dersom unntak fra hovedregelen om likestilling av underskrift og digital signatur kan gis i forskriftsform, vil en få en adskillig mer fleksibel og håndterlig ordning. De regelverksansvarlige organene kan da gjennomgå regelverket innenfor sin sektor og gjøre de unntakene de anser som nødvendige.

Digitale signaturer fremholdes i høringssvarene av de fleste som en viktig forutsetning for å etablere en effektiv elektronisk kommunikasjon. Uansett hvilken av de to metodene som benyttes for å tilpasse regelverket til en bredere bruk av elektronisk kommunikasjon, vil det være et tidkrevende arbeid. Det er derfor svært viktig at arbeidet med å gjennomgå regelverket påbegynnes snarest.

2.3.6 Usignerte elektroniske dokumenter

Det er en rekke dokumenter som kommer til, eller sendes fra det offentlige, som ikke er underlagt noe lovhjemlet underskriftskrav, og som en ut fra bevishensyn heller ikke trenger å kreve underskrevet eller signert. Det kan tenkes andre autentiseringsmekanismer som ikke er like sikre som digitale signaturer, men likevel sikre nok. Et forvaltningsorgan som har regelmessig kontakt med en definert gruppe aktører, kan f.eks. ha et passordsystem for å bekrefte autentisiteten til de som henvender seg til forvaltningsorganet elektronisk. Dette systemet benyttes f.eks. av flere banker, da gjerne med et elektronisk kort som genererer et engangspassord. Det finnes med andre ord en rekke muligheter til å autentisere partene i en elektronisk kommunikasjon ut over digitale signaturer. Ulempene er at disse mekanismene ikke på samme måte kan knyttes til selve dokumentet, slik som digitale signaturer. Dersom forvaltningsorganet kan være trygg på at en innkommet melding virkelig kommer fra den som angir seg som utsteder, vil dette i de fleste tilfeller være tilstrekkelig dersom det ikke er en lovbestemmelse som krever at dokumentet skal være underskrevet. Hvilket sikkerhetsnivå en bør legge seg på, må avgjøres konkret i forhold til hver enkelt dokumenttype. Det er ikke gitt at det bør stilles like strenge krav til at autentiseringen skal kunne knyttes direkte til dokumentet i en søknad om parkeringsplass som i et vitnemål.

For noen dokumenters vedkommende er det ikke nødvendig med noen form for autentiseringsmekanismer. Når lovgivningen ikke setter krav til underskrift, må en som nevnt vurdere om det ut fra bevishensyn er nødvendig at et dokument er signert. Dette er slett ikke alltid tilfelle. Ved utveksling av dokumenter mellom to forvaltningsorganer vil det ofte være unødvendig å forlange at dokumentene skal være signert. Dersom f.eks. et trygdekontor skal orientere sosialkontoret om et vedtak som er truffet, vil det neppe være nødvendig å signere kopien av vedtaket for at sosialkontoret skal kunne ha tillit til dokumentet. En elektronisk versjon av vedtaket må derfor kunne sendes usignert til sosialkontoret for bruk i deres saksbehandling. Dersom det i ettertid skulle oppstå tvil om innholdet i vedtaket, vil jo originalen likevel være hos trygdekontoret.

Også for enkelte dokumenter som kommer fra kilder utenfor forvaltningen, vil det ikke være nødvendig å kreve noen særlige former for autentisering. Det vil f.eks. ikke være noe i veien for å behandle en begjæring om innsyn etter offentlighetsloven, selv om denne er sendt som en usignert e-postmelding. Selv om noen skulle ha forfalsket en slik begjæring, risikerer en ikke annet enn at en som ikke har bedt om det, får tilsendt et offentlig dokument. Det vil i de fleste tilfeller heller ikke være særlige problemer med å behandle en stillingssøknad på bakgrunn av en usignert søknad. En annen sak er at vedlegg som vitnemål og attester kan innebære at en ønsker en mulighet til å autentisere disse dokumentene med en viss sikkerhet. I hvilke tilfeller en kan godta usignerte dokumenter som et saksdokument, må avgjøres individuelt. Skjønnstemaet i en slik vurdering må være hvor viktig det er i ettertid å kunne dokumentere med stor sikkerhet hvem som er avsender.

3 Offentlighet og innsynsrett

3.1 Hjemmelsgrunnlaget

3.1.1 Offentlighetsloven

Offentlighetsloven (offvl) gir enhver rett til å gjøre seg kjent med de saksdokumentene som faller inn under loven, og ikke er spesielt unntatt (f.eks. opplysninger som er undergitt taushetsplikt). Unntakene kan ses på som et kompromiss mellom interessen i offentlighet på den ene siden, og ønsket om å beskytte enkeltindivider mot uønsket publisitet, samt behovet for å beskytte samfunnsmessige interesser (som for eksempel rikets sikkerhet) på den andre siden.

Offentlighetsloven § 2 etablerer offentlighet som utgangspunkt for forvaltningens saksdokumenter. Fravikelse av dette utgangspunktet må bestemmes i lov eller i medhold av lov. Både offentlighetsloven selv og andre lover har mange slike unntak. De viktigste er unntaket for en virksomhets interne dokumenter samt unntaket for taushetsbelagte opplysninger. Offentlighetsloven retter seg i første rekke mot papirdokumenter, men det er gitt en forskrift i medhold av offentlighetsloven § 3 som gir regler for hvordan dokumentbegrepet skal forstås i forhold til elektroniske dokumenter.

Loven gjelder – med unntak for Stortinget, virksomheter for Stortinget og saker som behandles etter rettspleielovene – for all virksomhet som drives av organ for stat eller kommune. Loven gjelder i tillegg for private rettssubjekter når de treffer enkeltvedtak eller utferdiger forskrifter.

Offentlighetsprinsippet gir den som ønsker det økt mulighet for å orientere seg om forvaltningens virksomhet og eventuelt ta opp kritikkverdige forhold. Det er i særlig grad massemedia som har benyttet seg av denne retten. Dette har bidratt til å gi publikum bedre innblikk i forvaltningens virksomhet og fungerer også som ledd i den demokratiske kontrollen med forvaltningen. Men loven gir også enkeltpersoner anledning til på eget initiativ å skaffe seg kjennskap til hva som foregår i forvaltningen og opptre som deltakere i den offentlige meningsutvekslingen. Offentlighetsloven bidrar på denne måten til effektivitet i folkestyret. Ulempen med bestemmelsene om offentlighet er at det kan medføre merarbeid for forvaltningen og vanskeliggjøre forvaltningens arbeid ved at det kan bli stor oppmerksomhet omkring enkelte saker, slik at de krever mer ressurser enn sakens størrelse og betydning egentlig skulle tilsi.

Det er også verdt å merke seg at personregisterloven § 7, tredje ledd har en bestemmelse om offentlighetens innsyn. Her gis alle en rett til å få opplyst hvilke typer opplysninger som er tatt inn i registre som føres i et organ for stat eller kommune.

3.1.2 Partsinnsyn etter forvaltningsloven

I tillegg til den generelle adgangen til å kreve innsyn i forvaltningens saksdokumenter etter offentlighetsloven, har sakens parter en utvidet innsynsrett etter forvaltningslovens regler om partsoffentlighet, jf fvl § 18.

Forvaltningsloven inneholder ikke noen særbestemmelse om anvendelse på edb-lagret materiale. Det hersker en viss uenighet om forskriften fra offentlighetsloven kan anvendes analogisk, om en kan nå frem ved utvidende tolking eller om en er henvist til en generell anmodning om å gi partene innsyn også i tilfeller der informasjonen er lagret ved hjelp av edb.

Alternativt må partene henvises til å påberope seg reglene i offentlighetsloven. Dette er imidlertid ikke helt tilfredsstillende fordi reglene om partsinnsyn går noe lengre når det gjelder innsyn i blant annet taushetsbelagte opplysninger. Det er ikke grunn til å akseptere noen innskrenkning i partenes innsynsrett på grunn av den måten opplysningene er lagret på. Praktisk sett utgjør imidlertid disse ulikhetene neppe noe stort problem.

De særlige reglene om unntak for forvaltningens interne dokumenter antas ikke å bli påvirket av overgang til elektronisk saksbehandling og behandles ikke nærmere her.

3.1.3 Innsynsrett etter personregisterloven

Innsynsretten etter personregisterloven § 7 gir de registrerte rett til kunnskap om og kontroll med innholdet i personopplysninger som lagres eller bearbeides elektronisk. Bestemmelsen pålegger registereiere å gi de registrerte informasjon om hvilke opplysninger om dem selv som er registrert i den enkelte virksomhet. Plikt til å gi innsyn utløses på forespørsel fra den registrerte. Den enkeltes rett til innsyn er begrenset til personopplysninger som danner grunnlag for avgjørelser. Den samme adgangen til å unnta interne dokumenter etter fvl. § 18 gjelder også etter personregisterloven. Bestemmelsens siste ledd gir adgang til å gjøre unntak fra innsynsretten i forskrift. Den enkeltes rett til innsyn i opplysninger om seg selv går lenger enn innsynsretten etter forvaltningsloven. Innsynsretten etter personregisterloven er generell og uavhengig av tilknytning til en konkret sak. Hovedregelen er at virksomhetens svar på den registrertes begjæring om innsyn skal gis skriftlig jf. forskrift til personregisterloven §§ 1-1 og 1-2. Plikt til å korrigere opplysningene etter § 8 kan være et resultat av den registrertes innsyn.

3.2 Virksomhetenes kommentarer

Praktisk talt alle organene oppgir at det overveldende antall begjæringer om innsyn kommer fra pressen. Det forekommer ifølge høringsmaterialet nesten ikke at privatpersoner benytter seg av innsynsretten. Det antas at dårlig tilgjengelighet på postjournalen er en begrensende faktor for innsynsretten. Mange av organene peker på at det ved bruk av elektroniske hjelpemidler vil være mulig å tilrettelegge innsynsmuligheten på en slik måte at flere privatpersoner kan nyttiggjøre seg innsynsretten på en enklere måte. Det er enighet om at en bedre tilgjengelighet til postjournalen vil føre til flere innsynsbegjæringer og større arbeidsbyrde for organene. Det fremholdes at det i denne sammenheng ville være ressursbesparende dersom allmennheten også fikk direkte elektronisk tilgang til de offentlige dokumentene. De som foreslår dette, peker på at det vil betinge en grundigere forhåndsvurdering av om dokumentene omfattes av offentlighetsloven. I dag vurderer de fleste offentlige virksomheter spørsmål om unntak fra offentlighet når dokumentet føres i postjournalen. Ved en konkret begjæring om å få se dokumentet foretas det en ny gjennomgang før dokumentet

utleveres. Med direkte tilgang for allmennheten vil en miste muligheten til en ekstrakontroll før utleveringen. Enkelte virksomheter er bekymret for at dette skal kunne føre til en overforsiktighet som gjør at det unntas flere dokumenter fra offentlighet enn det offentlighetsloven gir grunnlag for. Også i forbindelse med elektronisk innsyn er høringsinstansene opptatt av at det er viktig at en kan ha tillit til at sikkerheten er god nok.

Det er bred enighet om at dagens regelverk ikke vil være til hinder for å gi allmennheten innsyn gjennom bruk av elektroniske hjelpemidler. Det påpekes imidlertid at dokument- og saksbegrepet i fremtiden kan bli en begrensende faktor for innsynsretten.

3.3 Utfyllende kommentarer

3.3.1 Dokumentbegrepet

Offentlighetsloven har ingen definisjon av begrepet "dokument". En kan heller ikke ta utgangspunkt i at begrepet betyr det samme som i andre lover. For eksempel antas straffeloven § 179 og avleveringsloven å operere med avvikende (og videre) dokumentbegreper. På bakgrunn av lovens formål og det som er sagt i forarbeidene, er det imidlertid klart at alle skrevne tekster samt kart, skisser fotografier o.l. er dokumenter i lovens forstand. Mikrofilm av makulerte papirdokumenter omfattes også.

Derimot er det antatt at edb-lagret materiale opprinnelig ikke var omfattet av lovens dokumentbegrep. Ved en lovendring i 1982 ble det derfor gitt hjemmel for å gi forskrifter om lovens anvendelse på materiale som er "utarbeidet, overført eller lagret ved hjelp av elektronisk databehandling", jf. § 3 siste ledd. Forskriften som ble gitt med hjemmel i § 3, gir innsynsretten anvendelse på den "naturlige enhet tekst eller opplysninger som på utskrift fra systemet framstår som ett dokument". Det er altså et typisk "papirorientert" dokumentbegrep som er benyttet.

Dagens teknologi gir muligheter for på en enkel måte å gjøre tilgjengelig også andre typer informasjon enn den som tradisjonelt har vært omfattet av dokumentbegrepet. Eksempler på slik informasjon er digitale lyd- og bildeopptak. Det er ikke usannsynlig at slike "multimediadokumenter" i fremtiden kan bli en vanlig del av visse typer saker. Et digitalisert billedopptak kan f.eks. benyttes i stedet for en befaring i byggesaker. Forskriften om rett til innsyn i edb-lagret materiale kan vanskelig sies å omfatte edb-lagret lyd/bilde da denne informasjonen vanskelig kan vurderes mot kriteriet "på utskrift fra systemet fremstår som ett dokument".

Videre reiser dokumentbegrepet problemer i forhold til såkalt hyperlenking av dokumenter. Hyperlenking vil si at det i et dokument er en elektronisk referanse til et annet dokument eller til en annen del av dokumentet som kan befinne seg et helt annet sted enn det opprinnelige dokumentet. Ved å klikke på lenken – det vil si referansen til det nye dokumentet – vil datamaskinen automatisk vise det nye dokumentet. På denne måten kan det oppstå tvil om hvor et dokument ender og et annet begynner.

Det bør derfor vurderes om dokumentbegrepet er et godt utgangspunkt for offentlighetens tilgang til offentlig informasjon. I kontekst av den digitale

utviklingen vil nok offentlighet knyttet opp mot informasjonen, uavhengig av om den er en del av et dokument, gi en bedre rettighet for borgeren. Problemstillingen kan illustreres med et eksempel der informasjon er lagret i en database. Opplysninger fra databasen kan settes sammen på mange ulike måter, som på hver sin måte kan gi verdifull informasjon. Opplysningene kan med andre ord settes sammen til mange ulike dokumenter. Før forvaltningen har satt sammen informasjonen ved et søk kan det vanskelig sies å ha eksistert et dokument som inneholder opplysningene. Med utgangspunkt i det eksisterende dokumentbegrepet vil offentligheten dermed ikke ha adgang til informasjon som det vil være lite resurskrevende for forvaltningen å fremskaffe.

Begrensningen i offentlighetens adgang til å kreve at forvaltningen systematiserer informasjonen har vært begrunnet i hensynet til å begrense forvaltningsorganenes arbeidsbyrde. Av samme grunn må krav om å gjøre seg kjent med det offentlige innholdet av et dokument knytte seg til en tydelig identifisert sak. Som ovenfor nevnt har den teknologiske utviklingen medført så store endringer i lagringsstrukturen for offentlige opplysninger, at det kan være på sin plass å vurdere oppmykninger i forhold til identifikasjonskravene.

Selve nøkkelen til offentlighet – muligheten til å kunne individualisere saker – ligger i dag i publikums rett til innsyn i en journal eller et liknende register, jf. offvl. § 2 andre ledd. Ved gjennomgang av journalene kan allmennheten følge med på hvilke saker som behandles av forvaltningen. Av forarbeidene til lovendringen i 1982 Ot. prp. nr. 4, følger det at begrepet liknende registre ikke omfatter interne hjelperegistre. Dette begrenser imidlertid neppe forvaltningsorganets adgang til å legge til rette for at den som krever innsyn, selv kan utnytte søke- og gjenfinningsverktøy til journalen og dermed få en bedre mulighet til å individualisere saker. En slik tilgang til informasjonen i elektroniske systemer kan, når forholdene først er lagt til rette, gis uten vesentlig merarbeid eller kostnad for forvaltningen. Dette synes også å være godt i samsvar med hensynene bak innsynsretten.

Elektronisk saksbehandling kan også på andre måter bidra til å effektivisere gjennomføring av innsynsretten. Det kan f.eks. gis adgang til den offentlige delen av sakens dokumenter via spørrerens egen pc, på dedikerte pc'er hos forvaltningsorganet eller på "torgterminaler" på offentlige servicekontorer. Slike tiltak vil øke tilgjengeligheten til materialet det ønskes innsyn i. Fysisk avstand vil da spille en mindre rolle for faktisk tilgang til offentlige dokumenter. Innsyn i journaler og dokumenter kan gjøres like enkelt for en innbygger i en kommune på Vestlandet som for en som er bosatt i Oslo. Det er imidlertid på det rene at innsyn via egen pc ikke vil være et tilfredsstillende tilbud for alle. Av hensyn til publikum vil forvaltningen derfor fortsatt bli nødt til å opprettholde et system der krav om innsyn også kan imøtekommes ved utlevering av papirutskrifter for de dokumentene der det er mulig, eventuelt ved sakkyndig bistand med bruk av pc'er.

Som ovenfor nevnt er flere typer dokumenter og opplysninger unntatt fra offentlighet, jf. offvl § 5a. Dette betyr at det må kontrolleres at det ikke utleveres dokumenter det ikke er anledning til å utlevere, samt at det for dokumenter som er unntatt offentlighet med hjemmel i § 5 (interne dokumenter), må vurderes om det skal praktiseres meroffentlighet. Slik avgjørelse må skje etter en *individuell* vurdering av dokumentene og opplysningene. Automatisk merking på bakgrunn av dokument- eller sakstype er ikke tilstrekkelig for å unnta dokumentet fra

innsyn. Dette innebærer at mange dokumenter som det begjæres innsyn i, må innom en saksbehandler for vurdering av om hele eller deler av dokumentet er unntatt. Dette kan innebære en ikke ubetydelig forsinkelse, samtidig som det ligger en begrensning i at det må skje i forvaltningens arbeidstid.

3.3.2 Særlig om postjournaler

Offentlighetsprinsippet gjelder foruten sakens dokumenter også forvaltningsorganets journal og andre «liknende registre». Liknende registre kan f.eks. være postlister som føres i stedet for en journal. Hele journalen eller det liknende registeret er offentlig, også innføringer vedrørende interne dokumenter som ikke i seg selv uten videre er undergitt innsynsrett.

En utfordring vil være å ivareta rutiner som både sikrer publikums og forvaltningsorganets oversikt over dokumentene. Eksempelvis kan nevnes forvaltningens mulighet for å etterspore et dokument som er mottatt av organet ad elektronisk vei, eller via internpost. Det er også viktig å legge til rette for at innsynsretten kan gjennomføres ved at journaler eller liknende registre også omfatter elektronisk basert informasjon, slik at saker det kan være aktuelt å kreve innsyn i, kan individualiseres. Utfordringen blir særlig synlig når det gjelder elektronisk post og internpost, som avhengig av hvordan systemet er innrettet, kan gå direkte mellom den enkelte saksbehandler og avsender/mottaker av informasjonen uten at forvaltningsorganets arkiv eller ekspedisjon blir involvert.

Relevant saksinformasjon skal journalføres etter de samme retningslinjene, uavhengig av forsendelsesmåten. Dersom reglene om journalføring likevel ikke følges i tilfredsstillende grad ved bruk av elektroniske systemer, kan det stilles spørsmål om den enkelte saksbehandlers edb-baserte oversikter over mottatt og avsendt elektronisk post utgjør et slikt «liknende register» som er gjenstand for innsyn etter journalregelen.

Forvaltningsorganet har ikke etter offentlighetsloven noen generell plikt til å føre journal. Manglende journalføring på grunn av sviktende rutiner kan derfor ikke uten videre utvide innsynsretten til andre interne registre som ellers kunne vært unntatt innsynsrett. Dessuten ville det være betydelige praktiske problemer knyttet til en slik ordning. Det utgjør i og for seg ingen umiddelbar grunn til å unnta fra innsynsretten at de aktuelle opplysningene kan være vanskelig tilgjengelige, men publikums kunnskap om selve sakens eksistens kan være avskåret dersom journalen ikke er tilgjengelig som innfallsport.

En annen sak er at manglende journalføring vil være i strid med de retningslinjene som gjelder for organets saksbehandling, jf. Arkivinstruksen 5.4.1.[6] Det antas dessuten at forvaltningsorganet av hensyn til sin egen saksbehandling må etablere systemer som gjør sentralisert kontroll med flyten av opplysninger mellom saksbehandlere og publikum mulig, og at et slikt system vil legge til rette for gjennomføring av innsynsretten.

[6] *Instruks for arkivarbeidet i forvaltningen* av 30.11.1984

3.3.3 Innsyn i all relevant informasjon

Selv om overgangen til elektronisk saksbehandling ikke medfører prinsipielle endringer i innsynsretten, kan muligheten for innsyn i de opplysningene et forvaltningsorgan har tilgang til og forholder seg til i en konkret sak, bli vanskeliggjort ved at organet ikke lenger behøver motta det vesentlige av informasjonen på papir, men f.eks. kan gjøre oppslag direkte mot ulike databaser og informasjonssystemer. Selv om den som krever innsyn etter omstendighetene kan kreve innsyn hos den som har ansvaret for det aktuelle informasjonssystemet (forutsatt at det er et forvaltningsorgan, informasjon som tilfredsstiller lovens krav osv.), kan det bli vanskelig for vedkommende å få oversikt over hva som egentlig er relevante opplysninger i saken, eller i alle fall hvilke typer av opplysninger forvaltningen har forholdt seg til i det enkelte tilfelle og hvor de kan søkes. Slik sett kan en vurdere om det på sikt vil bli nødvendig med en særskilt oversikt over de registrene forvaltningsorganet anser relevante og konsulterer i den enkelte sak som et ledd i å opprettholde reelle muligheter for gjennomføring av innsynsretten.

3.3.4 Direkte innsyn

Elektronisk saksbehandling vil kunne forenkle gjennomføringen av offentlighetsprinsippet og innsynsretten. For enkelte typer dokumenter vil det være uproblematisk å gi allmennheten direkte tilgang til offentlige dokumenter. Typiske eksempler på dette kan være reguleringsplaner o.l. Her kan det tenkes at forvaltningen legger ut dokumentet i tilknytning til journalen, slik at den som ønsker det, kan gå direkte fra journalen til dokumentet.

Når det gjelder dokumenter der det kan være tvil om dokumentet skal unntas offentlighet, er en slik direkte tilgang mer betenkelig. Dersom organet allerede ved journalføringen må ta endelig stilling til om dokumentet er offentlig, kan det være grunn til å frykte at dokumenter blir unntatt fra offentlighet «for sikkerhets skyld». Muligheten for en ny vurdering av offentlighet ved en konkret henvendelse er sannsynligvis en mekanisme en bør beholde for dokumenter som ikke helt opplagt er offentlige.

Selv om et dokument ikke er offentlig, kan det være at enkelte likevel har rett til å se dokumentet. Partene i en sak kan for eksempel ha rett til å se sakens dokumenter selv om de skulle inneholde taushetsbelagte opplysninger. Likeledes vil en etter personregisterloven ha rett til å se opplysninger om en selv. Denne typen innsyn vil også kunne skje elektronisk. Dette ville imidlertid stille meget strenge krav til sikkerhet. En måtte ha mekanismer som sikret at ingen kunne skaffe seg uautorisert tilgang til slike opplysninger.

3.3.5 Elektronisk publisering av visse beslutninger

Lovverket inneholder en rekke bestemmelser om hvordan forvaltningen skal sørge for, eller legge forholdene til rette for, at borgerne informeres om det offentliges virksomhet. Eksempler på en regel av denne typen er forvaltningsloven § 16, som bestemmer at partene i en sak skal ha skriftlig forhåndsvarsel før vedtak treffes. Andre mer generelle bestemmelser av denne type finner en i lov om Norsk lovtidend og forvaltningsloven § 38, som har regler for hvordan lover og forskrifter skal kunngjøres. Likeledes gir

offentlighetslovens bestemmelser om allmennhetens tilgang til det offentliges dokumenter, borgerne mulighet til å holde seg informert om forvaltningens virksomhet.

Et viktig hensyn bak disse bestemmelsene er at det er en nødvendig forutsetning for et vel fungerende demokrati at borgerne sikres muligheten til å orientere seg om det offentliges virksomhet. Det offentlige bør derfor bestrebe seg på å sørge for at mest mulig informasjon om offentlige beslutninger som har betydning for den enkeltes retter og plikter, blir gjort enkelt tilgjengelig for allmennheten. Særlig gjelder dette bestemmelser det medfører straffeansvar å bryte. Det er i norsk rett et meget strengt krav til borgerne om å holde seg orientert om hvilke regler som gjelder på alle livets områder. Det skal meget til for å slippe unna straffeansvar under henvisning til at en ikke kjente til at det en gjorde ikke var tillatt. Sett på bagrunn av dette må en kunne si at det offentlige må ha et særlig ansvar for at informasjon om denne typen regler er enklest mulig tilgjengelig.

Informasjonsteknologien tilbyr en mulighet til å distribuere store mengder informasjon raskt og billig. Gjennom nettsider eller elektroniske oppslagstavler kan informasjon om lover, forskrifter, dommer og liknende, gjøres tilgjengelig på en langt enklere og mer effektiv måte enn hva situasjonen er i dag. I dag finnes det få bestemmelser som gir borgerne rett til tilgang til offentlig informasjon i elektronisk form. Det finnes imidlertid ett eksempel i lov om offentlige anskaffelser § 12, der det er en bestemmelse om plikt til å utlyse visse offentlige anbud elektronisk gjennom den såkalte TED-databasen. TED-databasen er en åpent tilgjengelig database med alle offentlige anbudsinnbydelser over en viss størrelse innenfor EØS.

En rekke forvaltningsorganer tilbyr riktignok i dag informasjon gjennom sine hjemmesider på Internett. Dette er ofte i tillegg til informasjon om organet, informasjon om det regelverket de forvalter, samt viktige vedtak organet har truffet. Det bør likevel vurderes om det ikke er på tide å lovfeste en generell plikt til å kunngjøre visse beslutninger elektronisk. Dette bør som et minimum omfatte lover og sentrale forskrifter, men det bør også vurderes om ikke dommer og andre viktige beslutninger bør være alminnelig tilgjengelig i elektronisk form. Eksempler på slike andre viktige beslutninger kan være kommunale reguleringsvedtak, prinsipielle vedtak fra Forbrukerombudet, Datatilsynet o.l.

Det skal avslutningsvis nevnes at Lovdata gir gratis tilgang til lover og forskrifter over Internett. Dette er imidlertid et tilbud fra en privat stiftelse og ingen lovfestet rett for offentligheten.

4 Taushetsplikt

4.1 Hjemmelsgrunnlaget

4.1.1 Forvaltningsmessig taushetsplikt

Enhver som utfører arbeid eller tjeneste for et forvaltningsorgan, har taushetsplikt om visse ting vedkommende får kjennskap til i sin tjeneste. Taushetsplikten etter forvaltningsloven omfatter to typer opplysninger. For det første gjelder det opplysninger om noens personlige forhold, og for det andre opplysninger om forretningsforhold o.l. som det av konkurransemessige grunner kan være av betydning å hemmeligholde. Taushetsplikten er regulert i forvaltningsloven §§ 13-13e. I tillegg finnes taushetspliktregler flere steder i særlovgivningen.

Forvaltningen mottar en rekke opplysninger som den som opplysningen gjelder, ikke nødvendigvis ønsker å dele med andre. Ofte har ikke den som gir fra seg opplysningene noe valg. Vedkommende må f.eks. gi fra seg opplysningene for å motta et gode, eller fordi loven pålegger ham å gi fra seg opplysningene. Rimelighetshensyn tilsier at de som må avgi opplysninger til offentlig forvaltning til gjengjeld beskyttes av regler om taushetsplikt. Forvaltningen har også en selvstendig interesse i at regler om taushetsplikt er på plass. Taushetspliktreglene kan blant annet bidra til å skape tillit til forvaltningen. Publikum vil antakelig være mer villige til å gi korrekte og fullstendige opplysninger når de vet at det de forteller ikke kommer videre. Det er derfor ikke bare viktig at taushetsplikten faktisk blir overholdt, publikum må også ha tillit til at så er tilfelle.

Taushetsplikten retter seg mot *arten* av de opplysninger en tjenestemann mottar, og er i utgangspunktet medieuavhengig. Det kan likevel tenkes at overgangen til datamaskinbasert kommunikasjon medfører at opplysninger som ellers ikke ville blitt nedtegnet finnes representert i en form som gjør særlige tiltak nødvendige. Dette griper likevel ikke inn i det prinsipielle spørsmålet om taushetspliktens omfang.

Taushetsplikten innebærer en plikt til både å unnlate å meddele eller utlevere taushetsbelagt informasjon og å hindre at uvedkommende på annen måte får adgang eller kjennskap til slik informasjon, herunder sikre slikt materiale mot uautorisert innsyn på betryggende måte, jf. fvl § 13 første ledd og § 13c annet ledd. Dette må antas å gjelde både ved mottak, lagring og overføring av opplysninger.

4.1.2 Gradert informasjon m.v.

Om tilgang til og overføring av gradert informasjon gjelder særlige regler om bruk av kryptering og akkreditert samband, jf. sikkerhetsinstruksen, beskyttelsesinstruksen og datasikkerhetsdirektivet. Disse reglene vil ikke bli nærmere behandlet her.

4.1.3 Personregisterloven

Bestemmelsene om taushetsplikt suppleres dessuten av personregisterlovens bestemmelser. Likeledes vil konsesjoner gitt med hjemmel i personregisterloven inneholde bestemmelser som skal ivareta de samme hensyn som taushetsplikten. De særlige spørsmålene som personregisterloven reiser, er behandlet i kapittel 6.

4.2 Virksomhetenes kommentarer

Alle høringsorganene er underlagt lovbestemt taushetsplikt, de fleste etter forvaltningslovens bestemmelser. Enkelte virksomheter er underlagt taushetsplikt i særlovgivning. Ingen av særlovene synes å inneholde bestemmelser som i forhold til elektronisk saksbehandling og taushetsplikt innebærer prinsipielle forskjeller fra forvaltningsloven.

De fleste høringsinstansene definerer taushetsplikt og elektronisk saksbehandling som en teknisk utfordring. Det fremholdes at bruk av edb ikke frembringer problemstillinger av en annen karakter enn hva tilfellet er med manuelle systemer. Den viktigste utfordringen er å finne tekniske løsninger som sikrer at ikke uvedkommende får tilgang til opplysningene under bruk, oppbevaring eller oversendelse.

Mange av høringsinstansene bruker telefaks til å overføre taushetsbelagt informasjon. De fleste av organene har utarbeidet spesielle sikkerhetsrutiner for denne typen overføringer. Disse strekker seg fra enkle administrative rutiner som å ringe opp mottaker før utsendelse, til bruk av tekniske sikkerhetsløsninger som f.eks. kryptering.

4.3 Utfyllende kommentarer

4.3.1 Sikringstiltak

I forbindelse med overgang til elektronisk saksbehandling kan det reises spørsmål om hvilke *sikringstiltak* som eventuelt må iverksettes for å tilfredsstille kravene om taushetsplikt. Dette gjelder både for informasjonsflyten internt i forvaltningen og ved mulig elektronisk overføring mellom forvaltningen og partene i saken

IT-sikkerhet knyttes tradisjonelt til begrepene kvalitet, tilgjengelighet og konfidensialitet. I forhold til taushetsplikt er det konfidensialitetsaspektet som er det sentrale. I kapitlet om personvern behandles sikkerhetsspørsmålene ut fra en bredere tilnærming.

Spørsmålet om i hvilken grad taushetsbelagt informasjon rettmessig kan overføres mellom forvaltningsvirksomheter antas ikke å bli berørt av overgangen til elektronisk saksbehandling og vil ikke bli nærmere behandlet her. Derimot kan overgangen til elektronisk saksbehandling, avhengig av de sikkerhetstiltakene som iverksettes i forbindelse med f.eks. deling av edb-systemer, medføre at en større gruppe personer *rent faktisk* får tilgang til informasjonen enn det som har vært tilfelle tidligere.

Forvaltningsloven åpner for at opplysninger som er underlagt taushetsplikt, kan gjøres tilgjengelig for andre tjenestemenn innenfor samme organ eller etat hvis det trengs for en effektiv arbeids- og arkivordning, jf. fvl. § 13b nr 3. Det ligger ingen prinsipielt nye spørsmål i dette knyttet til overgangen til elektronisk saksbehandling, men det vil nok kreves større årvåkenhet når det gjelder innretningen av blant annet tilgangskontrollsystemer for å avbøte virkningen av at avstand og fysisk lokalisering ikke lenger spiller noen rolle for muligheten til å få tilgang til opplysninger. Effektiv tilgangskontroll i det elektroniske arkivet vil kunne forbedre den reelle etterlevelsen av taushetsplikten internt i organet. Se for øvrig også nedenfor om eksterne medhjelpere.

Videre kan det stilles spørsmål om taushetsplikten generelt er til hinder for å overføre taushetsbelagte opplysninger i datanettverk (utenfor kontrollert område) uten at særskilte sikkerhetstiltak er iverksatt. Dette gjelder både mellom forvaltningsvirksomheter og mellom forvaltningen og den opplysningene gjelder.

Taushetsbelagt informasjon er ikke en ensartet type opplysninger. Det spenner over alt fra typisk sensitive opplysninger om helseforhold, til mer trivielle opplysninger der den enkeltes interesse i beskyttelse kan være helt marginal. Når fvl § 13 c bestemmer at taushetsbelagt informasjon skal oppbevares på en betryggende måte, må det antas at opplysningenes karakter må ha en innvirkning på hva som kan karakteriseres som betryggende. Opplysninger som enten vil medføre stor skade dersom de ble kjent, eller som er av en slik karakter at det må antas at uvedkommende vil kunne gjøre kvalifiserte forsøk på å få tilgang til dem, må oppbevares på en annen og sikrere måte enn mer trivielle opplysninger. Dette utgangspunktet må også få gjennomslag for annen behandling enn ren oppbevaring. Det vil med andre ord si at denne betraktningen må legges til grunn også når det vurderes om det er gjort tilstrekkelig for å hindre at uvedkommende får tilgang til opplysningene under forsendelse, jf. fvl § 13.

Det er derfor neppe grunnlag for å anta at bestemmelsene om taushetsplikt utgjør noe generelt hinder for overføring av opplysninger i datanettverk uten særlige sikringstiltak. Hvilke krav som må stilles til sikring, må vurderes i forhold til opplysningenes karakter. De mest sensitive opplysningene antas dessuten å falle inn under datasikkerhetsdirektivet eller bestemmelser gitt med hjemmel i personregisterloven om bruk av sikringstiltak ved overføring i datanettverk, og må således sikres i henhold til disse regelverkene.

Vurderingen av hvilke opplysninger som kan overføres i usikrede nett, og hvilke opplysninger som krever særlige tiltak, kan imidlertid ikke avgjøres generelt etter opplysningstype, men må avgjøres av en saksbehandler i hvert enkelt tilfelle.

Den som personopplysningen gjelder, kan dessuten (vanligvis) gi samtykke til å unnta opplysninger fra taushetsplikten. I forbindelse med overføring av opplysninger i usikrede nett kan det imidlertid stilles spørsmål både om hjemmelsgrunnlaget for slikt samtykke og om hvordan innhenting av samtykke eventuelt skal administreres.

For det første vil den aktuelle personen sjelden ha tilstrekkelig kunnskap om den risikoen for utilsiktet spredning som eventuelt ligger i den aktuelle formidlingskanalen. Dette blir i så fall en utfordring for forvaltningens veiledningsplikt. For det andre vil det være en utfordring å administrere et system med særlig samtykke til elektronisk overføring av opplysninger. Det kan også reises spørsmål om hvilke krav en må stille til et samtykke til å sende

taushetsbelagt informasjon i åpne nettverk. En henvendelse til forvaltningen i form av f.eks. usikret elektronisk post, kan neppe betraktes som et samtykke til å sende svar på samme måte. Man ville f.eks. ikke anta at en henvendelse til forvaltningen som er sendt på et åpent postkort, ville gi forvaltningen noen rett til å svare på samme måte dersom opplysningene det gjaldt var underlagt taushetsplikt.

Hvorvidt kravet til samtykke er oppfylt må selvfølgelig vurderes i hvert konkrete tilfelle. Det bør imidlertid unngås at det utvikles en praksis der taushetsbelagt informasjon regelmessig formidles over usikrede nettverk på bakgrunn av samtykke. Dersom behovet for rask formidling av sensitiv informasjon forekommer hyppig et organ, bør det bygges inn sikringsfunksjoner i meldingsformidlingen, f.eks. gjennom krypterte meldinger eller sikrede linjer. Det vil være betenkelig om brukere av forvaltningen annet enn i helt spesielle tilfeller må gi samtykke til en redusert diskresjon for å oppnå god effektivitet.

4.3.2 Sertifisering av IT-sikkerhet

Som flere av høringsinstansene påpeker, vil sikkerheten i IT-systemene være av betydning for hvordan taushetsbelagte opplysninger kan skjermes for uvedkommende. Ofte vil det være vanskelig for den enkelte virksomhet å vurdere hvorvidt et IT-anlegg tilbyr tilstrekkelig sikkerhet. En slik vurdering krever en IT kompetanse de færreste virksomheter besitter. Virksomheten vil dermed svært ofte være overlatt til leverandørens vurdering av sitt eget produkt. Dette kan løses ved å opprette en sertifiseringsordning. Gjennom en sertifiseringsordning kan man sikre at datasikkerheten testes mot gitte kriterier av uavhengige eksperter.

Høsten 1997 leverte Rådet for IT-sikkerhet en rapport om sertifisering av IT-sikkerhet[7]. Rapporten inneholder bl.a. en beskrivelse av ulike former for sikkerhetssertifisering, samt en undersøkelse av hvilke behov som finnes for en sertifiseringsordning. For nærmere informasjon om sertifisering vises til denne rapporten.

En vurdering av hvorvidt taushetspliktreglene er oppfylt i forhold til sikring av dataanlegg, kan ikke ses isolert som et spørsmål om faktisk sikkerhet. Som ovenfor nevnt har forvaltningen en egeninteresse i at konfidensielle opplysninger behandles på en betryggende måte. Det må antas at publikum vil ha lettere for å gi fra seg opplysninger dersom de føler seg sikre på at disse ikke blir kjent for uvedkommende. Dette hensynet bak taushetspliktreglene ivaretas ikke dersom publikum ikke har tillit til at datasystemene er trygge. Det spiller i denne sammenhengen således en underordnet rolle om datasystemet faktisk er sikkert dersom store deler av publikum ikke har tiltro til dette. Taushetspliktreglene har også som funksjon å betrygge den enkelte om at personlige opplysninger om dem ikke blir kjent for andre. Den enkeltes opplevelse av denne betryggelsen vil knytte seg til vedkommendes oppfatning av sikkerheten. Denne oppfatningen trenger ikke å være i samsvar med den faktiske sikkerheten. Vedkommende vil like fullt lide et velferdstap dersom han bekymrer seg for at personlige opplysninger om ham skal tilflyte uvedkommende. Dette er forhold det må tas hensyn til når en tar i bruk IT i behandlingen av sensitiv personinformasjon. At

[7] *Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner*, Sluttrapport 13. november 1997, Rådet for IT-sikkerhet

IT-sikkerheten er gjort til gjenstand for vurdering av uavhengig ekspertise, vil sannsynligvis ha stor betydning for den alminnelige tilliten til sikkerheten i et system.

4.3.3 Eksterne medhjelpere

Bruk av elektroniske saksbehandlingssystemer vil for de fleste offentlige virksomheter medføre at en blir avhengig av ekstern bistand for å implementere og vedlikeholde systemene. Ofte vil slike operasjoner innebære at den eksterne konsulenten må ha tilgang til data i systemet, f.eks. for å rette feil. I andre tilfeller der slik tilgang ikke er nødvendig, vil det likevel være svært vanskelig for den ansvarlige å kontrollere at den eksterne datakonsulenten ikke tilegner seg informasjon fra systemet. Det er ikke urimelig å anta at en datakonsulent under et oppdrag vil kunne kopiere en hel database fra f.eks. et sosialkontor uten at dette blir oppdaget.

Det kan reises spørsmål om en slik tilgang for eksterne konsulenter er forenlig med forvaltningslovens taushetsbestemmelser. Som ovenfor nevnt åpner fvl § 13 b for at taushetsbelagte opplysninger kan gjøres tilgjengelig for andre tjenestemenn *innen* organet i den utstrekning dette er nødvendig for å oppnå en hensiktsmessig arbeidsordning. Det ville selvfølgelig være umulig å gjennomføre en arbeidsordning der hver enkelt tjenestemann skulle være ansvarlig for drift og vedlikehold av sitt eget datautstyr. Det er derfor liten tvil om at bestemmelsen gir anledning til å gi en tjenestemann innenfor organet tilgang til taushetsbelagte opplysninger dersom dette er nødvendig for drift eller vedlikehold av utstyret. Det må således antas at taushetsbestemmelsen åpner for i visse tilfeller å gi en intern driftsavdeling tilgang til informasjon i datasystemet. Når opplysninger i forbindelse med drifts- eller vedlikeholdsoppdrag gjøres tilgjengelig for personer *utenfor* organet, er dette anstrengt i forhold til ordlyden i § 13 b. Denne problemstillingen er imidlertid ikke berørt av høringsinstansene. Det kan synes som om dette ikke oppfattes som noe problem. Dette kan komme av at også eksterne konsulenter har taushetsplikt om forhold de får kjennskap til gjennom oppdraget. Det kan likevel være grunn til å vurdere om det bør skje endringer i regelverket i forhold til eksterne konsulenter. Per i dag finnes ingen formelle krav til datakonsulenter. Det er opp til det enkelte forvaltningsorgan å vurdere skikketheten til eksterne datakonsulenter. Tatt i betraktning at eksterne konsulenter kan få kjennskap til svært sensitiv informasjon, bør det, når stadig mer av informasjonshåndteringen skjer ved hjelp av edb, vurderes å opprette en godkjenningsordning for datakonsulenter som utfører oppdrag som innebærer at det må gis tilgang til taushetsbelagt informasjon.

Datatilsynet har i enkelte konsesjoner stilt krav om at eksterne databehandlere må ha databehandlingskonsesjon, som beskrevet i personregisterloven § 22. Det kan imidlertid reises adskillig tvil om denne bestemmelsen tar sikte på foretak som driver drift og vedlikehold av edb-utstyr. Databehandling er i pregl. § 22 beskrevet som virksomhet som består i å bearbeide personopplysninger for andre ved elektroniske hjelpemidler. Dette passer ikke særlig godt på foretak som bare vedlikeholder utstyr og programmer uten å foreta noen bearbeiding av opplysningene i systemet. Det er under enhver omstendighet i beste fall tvilsomt om en databehandlingskonsesjon gir oppdragsgiveren anledning til å gjøre taushetsbelagt informasjon tilgjengelig for oppdragstakeren.

5 Personvern

5.1 Hjemmelsgrunnlag

Personvernreglene skal beskytte den personlige integriteten og består av det ulovfestede personvernet og det lovregulerte personvernet. Som viktige elementer i det lovfestede personvernet kan nevnes injurielovgivningen, personregisterloven og taushetsbestemmelser i ulike lover. Det vil i tillegg til taushetspliktreglene særlig være personregisterlovens bestemmelser som får direkte betydning for anvendelsen av elektronisk saksbehandling.

Personregisterlovens hovedformål er å ivareta enkeltindividets interesse i å beskytte sin personlige integritet når det gjelder registrering, lagring, bruk og utveksling av personopplysninger.

Grunnleggende begreper i personregisterloven er «personopplysning» og «personregister» jf. § 1. Informasjon om både juridiske og fysiske personer omfattes av begrepet personopplysning. Registerbegrepet er basert på kriteriet for gjenfinning av personopplysninger. Det betyr at hvis en med en viss grad av treffsikkerhet kan gjenfinne enkeltpersoner i en samling av personopplysninger, så foreligger det et register.

De reglene i personregisterloven som i hovedsak vil få betydning for elektronisk saksbehandling, befinner seg i lovens kapittel 3, alminnelige regler om personregistre, og kapittel 4, om plikt til å søke samtykke til å opprette personregistre.

Høsten 1995 ble det nedsatt et utvalg for å utrede behovet for revisjon av personregisterloven. Behovet for revisjon er dels begrunnet i at den teknologiske og økonomiske utviklingen har ført til at regelverket ikke virker fullt ut tilfredsstillende, og dels i at EUs direktiv om beskyttelse av personopplysninger nødvendiggjorde en gjennomgang av norsk lovgivning for å bringe den i samsvar med direktivets krav. Utvalget la våren 1997 frem sin innstilling med forslag til lov om behandling av personopplysninger[8]. Det er ment at denne loven – personopplysningsloven – skal tre i stedet for personregisterloven.

Utkastet til personopplysningslov inneholder en rekke bestemmelser som vil få betydning for behandling av personopplysninger uavhengig av om denne skjer elektronisk eller manuelt. Utkastet legger f.eks. opp til en plikt for behandleren til å informere den opplysningene gjelder dersom opplysningene innhentes fra andre kilder en den registrerte. Videre foreslås det en utvidet plikt for den behandlingsansvarlige til etter forespørsel å informere den registrerte om formål med behandlingen, hvor opplysningene er hentet fra, hvem som er ansvarlig for behandlingen m.m. Under punktet utdypende kommentarer vil noen av bestemmelsene i utkastet som må antas å få særlig betydning for elektronisk saksbehandling, bli behandlet.

[8] NOU 1997:19 *Et bedre personvern*

5.2 Virksomhetenes kommentarer

Flere av virksomhetene påpeker at edb gir enklere tilgang til opplysninger, og at dette må tas hensyn til ved bruk av elektroniske saksbehandlingssystemer. Det er videre bred enighet om at teknologien alene neppe er avgjørende for hvordan personvernhensynene ivaretas. Den generelle oppfatningen er at elektronisk behandling av personopplysninger vil fordre at det utarbeides både gode rutiner og tillitvekkende sikkerhetsløsninger. Strengere tilgangsbegrensninger internt i virksomhetene fremheves bl.a. som et viktig virkemiddel. Selv om de fleste virksomhetene som nevnt ikke anser teknologien som den eneste kritiske faktoren for personvernet, er det ikke tvil om at den tekniske sikkerheten anses som et meget viktig element for å oppnå et godt personvern.

Det er få av virksomhetene som kommenterer hvordan saksbehandlernes personvern kan berøres av elektronisk saksbehandling. Blant de virksomhetene som tar opp dette forholdet, er det stor sprik i synspunktene på bruk av opplysninger som genereres ved bruk av systemet. En av høringsinstansene mener at opplysninger som genereres ved saksbehandlernes bruk av systemet, bør kunne brukes til en objektiv effektivitetsmåling av saksbehandlerne. En annen instans mener at det bør vurderes å legge inn begrensninger for hvor mye opplysninger systemet skal kunne generere om saksbehandlernes arbeid, ut fra at denne type opplysninger etter deres syn ikke er egnet til effektivitetsmålinger.

Selv om personverntruslene ikke er like tydelig definert av alle høringsinstansene, er det generelle inntrykket at det betraktes som en viktig forutsetning for å lykkes med elektronisk saksbehandling at det fokuseres på de personvernmessige aspektene, og at disse tas hensyn til ved utforming av regler og teknologi.

5.3 Utfyllende kommentarer

Personregisterloven § 9 bestemmer at en må ha tillatelse (konsesjon) fra Kongen for å føre personregister som gjør bruk av elektroniske hjelpemidler eller som inneholder sensitive opplysninger. Som personregister regnes personopplysninger som er lagret systematisk slik at opplysninger om den enkelte person kan finnes igjen (personregisterloven § 1). Et elektronisk saksbehandlingssystem vil svært ofte inneholde personopplysninger. Søkemulighetene i dokumentlageret vil gjøre at det som regel vil være enkelt å søke frem opplysninger om en bestemt person. Selv om personregisterloven med forskrifter inneholder en rekke unntak fra konsesjonsplikten, vil nok svært mange elektroniske saksbehandlingssystemer være eller inneholde et konsesjonspliktig personregister. For konsesjonspliktige registre vil Datatilsynet etter søknad vurdere hvorvidt det skal gis konsesjon. Som et ledd i dette skal Datatilsynet vurdere om bruk av personregisteret kan volde problemer for den registrerte som ikke kan løses ved å gi regler for registeret (personregisterloven § 10). Hvilke regler som kan gis, fremgår av personregisterloven § 11. Etter denne bestemmelsen kan Datatilsynet gi regler om:

1) innsamling og kontroll av de opplysninger registeret kan inneholde
2) behandling og lagring av disse opplysningene
3) adgangen til samkjøring med andre personregistre (kobling)

4) bruk av fødselsnummer (fødselsdato og personnummer)
5) utlevering av opplysninger, bl.a. om opplysninger kan overføres til andre registre
6) omfanget og innholdet av den informasjon som skal gis ved meldinger eller andre henvendelser til den registrerte
7) den enkeltes rett til å kreve opplysninger etter § 7
8) retting av opplysninger og rutiner av registeret
9) ajourføring av registeret
10) sletting eller ikke-bruk av opplysninger etter en viss tid, og eventuelt overføring av registeret til arkivverket

Hvilke regler som gis og det nærmere innholdet i reglene, avgjøres etter en konkret vurdering av det enkelte register. Formålet for registeret og opplysningenes sensitivitet er vesentlige vurderingstemaer.

Konsesjons- og meldeplikt – personopplysningsloven

Utkastet legger opp til å erstatte store deler av dagens konsesjonsordning med en meldeplikt. Mens det i dag er konsesjonsplikt for alle elektroniske personregistre som ikke er positivt unntatt, skal det etter personopplysningsloven bare søkes om konsesjon i de tilfellene der sensitive opplysninger benyttes for å treffe enkeltvedtak. Meldeplikten suppleres med en rekke andre tiltak så som utvidet plikt om varsling til den registrerte, og en vid innsynsrett. I tillegg gis Datatilsynet en generell inngrepshjemmel med mulighet til å pålegge tvangsmulkt ved ulovlig behandling.

Endringen vil medføre at de fleste saksbehandlingssystemer i det offentlig vil gå fra å være konsesjonspliktige til å bli meldepliktige. Meldeplikten innebærer at det må sendes en melding til Datatilsynet om den behandlingen av personopplysninger som planlegges. Meldingen skal inneholde opplysninger om hva som er behandlingens formål, hvem som er ansvarlig og en del andre karakteristika, jf. utkastet § 32. Det vil i motsetning til i dag ikke være nødvendig å få en eksplisitt tillatelse fra Datatilsynet.

For behandlinger som fortsatt vil være konsesjonspliktig, skal i hovedsak de samme vurderingstemaer som i personregisterloven legges til grunn.

5.3.1 Sikkerhet[9]

Elektronisk lagret og søkbar informasjon øker mulighetene for ekstern og intern tilgang. Når det gjelder sikkerhetsregulering som skal skille mellom lovlig og ulovlig tilgang til informasjon, har utviklingen av nye sikkerhetsløsninger gitt bedre muligheter for informasjonsbeskyttelse enn det som har vært mulig for papirbasert informasjon. Økt bruk av elektronisk post og annen nettverkskommunikasjon til utveksling av dokumenter med personopplysninger vil kanskje skape de største utfordringene for elektronisk saksbehandling. Foruten beskyttelse mot ulovlig ekstern tilgang kan også den interne tilgangen differensieres i langt større grad enn i papirarkivene. Dette muliggjør optimalt samsvar mellom tilgang til opplysning og behovet for den.

[9] Se også punkt 4.3.2 om sertifisering av IT-sikkerhet.

Personregisterloven § 8b gir adgang til å regulere sikkerheten i systemer der personopplysninger lagres og brukes. Hensikten med å gi sikkerhetsregler for personopplysninger er dels å sikre informasjonen mot tilgang fra uvedkommende, dels å sikre at informasjonen er tilgjengelig når det er behov for den og dels å sikre at opplysningene er av tilstrekkelig kvalitet i forhold til det formålet de skal brukes til. Et sykehus vil typisk ha behov for alle disse typene av sikkerhet knyttet til sine edb-systemer.

Konfidensialiteten for personopplysninger kan sikres ved tilgangskontroll som begrenser informasjonsadgangen til beskyttelsesverdig informasjon internt i en virksomhet. De saksbehandlerne som har behov for informasjonen som ledd i saksbehandlingen kan for eksempel få tilgang, samtidig som det legges inn mer eller mindre omfattende begrensninger for andre. Tilgangskontrollen kan differensieres slik at informasjon gjøres langt mindre tilgjengelig enn i dagens papirbaserte arkiver. Andre tiltak kan være nødvendige for å sikre opplysningene mot at utenforstående får tilgang til dem. Her kan lagring på fysisk isolerte maskiner, brannvegg og kryptering være noen av mulighetene.

Tilgjengelighet av personopplysninger er også en sentral del av IT-sikkerheten. Det er viktig at vitale opplysninger er mulig å fremskaffe selv om dataanlegget skulle være nede eller ødelagt. Her vil regler og rutiner for back-up-kopier være viktige elementer i datasikkerheten.

Når det gjelder kvaliteten på opplysninger, har personregisterloven en egen bestemmelse om dette i § 8. Se nærmere om dette i pkt 5.3.3.

Regler om sikkerhet kan gis enten som forskrift eller enkeltvedtak. Frem til i dag er det ikke gitt forskrifter på dette området. Datatilsynet innarbeider regler for sikkerhet i samtlige konsesjoner og har gitt separate sikkerhetsbestemmelser for føring av registre som har selvstendig lovhjemmel og inneholder sensitive opplysninger: «*Krav til sikring av medisinsk informasjon*», samt krav til sikring av personregistre som er lagret i edb-systemer tilknyttet eksterne systemer via ulike nettverksløsninger: «*Sikkerhetsregulering av delte edb-systemer*». Konsesjonenes sikkerhetsbestemmelser stiller krav om tilgangskontroll internt i virksomheten, og til kommunikasjonskontroll, kryptering, lukket nettverk eller kommunikasjonsforbud via nettverk mot eksterne trusler. Kravene til sikkerhetstiltak varierer avhengig av det konkrete beskyttelsesbehovet for de opplysningstypene som ligger i registeret.

Sikkerhetsregler – personopplysningsloven

Det foreslås mer konkrete sikkerhetsregler i utkastet i forhold til personregisterloven. I utkastet § 11 pålegges den behandlingsansvarlige å sørge for tilstrekkelig sikkerhet. Det skal gjennomføres en sikkerhetsvurdering som skal danne grunnlag for å etablere og vedlikeholde sikkerheten. Alle sikkerhetstiltak skal dokumenteres slik at det i ettertid kan kontrolleres at tiltakene er fulgt opp i praksis.

Ovennevnte forutsetter en bevisst og aktiv holdning til datasikkerheten hos de virksomheter som behandler personopplysninger. Det er grunn til å tro at dette alene vil medvirke til å eliminere mange av de truslene som høringsinstansene peker på. For de fleste virksomheter vil en sikkerhetsgjennomgang med systematisk oppfølgning kunne danne grunnlag for å lage administrative rutiner og til å foreta den teknologitilpasning som til enhver tid er nødvendig for å

opprettholde forutsetningene for et godt personvern. En må nok imidlertid være innstilt på at en sikkerhetsvurdering i enkelte tilfeller kan konkludere med at det ikke er kostnadseffektivt å gjennomføre elektronisk saksbehandling. Dette vil avhenge av hvilke opplysninger det er tale om, hvilket miljø de behandles i og hvilke teknologiske muligheter som er tilgjengelig.

Siste ledd i § 11 gir Kongen anledning til å gi forskrifter om sikkerhetsregulering. Det kan være grunn til å anta at denne bestemmelsen vil bli brukt til å gi utfyllende sikkerhetsbestemmelser på visse områder. Dette er tidligere gjort ved enkeltvedtak fra Datatilsynet, jf. f.eks. ovenfor om krav til sikring av medisinsk informasjon.

5.3.2 Kvalitet

Krav til kvalitet på opplysninger må alltid vurderes opp mot formålet for bruken av dem. I enkelte sammenhenger kan cirka-opplysninger være av tilstrekkelig kvalitet, mens det i andre sammenhenger kan være helt avgjørende å ha helt eksakte opplysninger. Ligningsmyndighetene kan for eksempel beregne hva som vil være riktig skattetrekk ut fra opplysninger om forventet omtrentlig inntekt. Når skatten skal endelig beregnes, er det derimot nødvendig med helt eksakte opplysninger om inntekten.

Personregisterloven § 8 stiller krav til kvalitet på opplysninger i registre som brukes til å fatte avgjørelser. Regelen skal sikre korrekt avgjørelsesgrunnlag og pålegger korrigeringsplikt for uriktige eller ufullstendige opplysninger samt plikt til å begrense eventuell skade som måtte være påført den registrerte ved bruk av ukorrekt informasjon. Korrigering innebærer at opplysningene endres i form av retting, sletting eller supplering. Det fremgår ikke av bestemmelsens ordlyd at korrigering skal foretas i virksomheten av eget tiltak, men dette forutsettes i forarbeidene til personregisterloven. Videre vil virksomheten ha plikt til å korrigere etter pålegg fra Datatilsynet og på initiativ fra den registrerte.

Kvalitet – personopplysningsloven

Utkastet til personopplysningsloven § 25 er en bestemmelse som i hovedtrekk tilsvarer personregisterloven § 8. I tillegg har utkastet en del andre bestemmelser som er ment å sikre kvalitet ved elektronisk opplysningsbehandling.

Som et ledd i denne kvalitetssikringen har utkastets § 22 en bestemmelse som under visse forutsetninger gir den enkelte rett til å kreve begrunnelse for automatiserte avgjørelser. Med automatiserte avgjørelser menes avgjørelser som utelukkende er basert på automatisert behandling. Dersom mennesker tar del i prosessen ved f.eks. å tolke datamaskinbehandlingen, anses behandlingen ikke som fullstendig automatisert. Det er videre et vilkår for retten til begrunnelse at avgjørelsen er av en slik art at den er bestemmende for rettigheter eller plikter til den det gjelder. Dersom disse vilkårene er oppfylt, har vedkommende rett til å få en redegjørelse for reglene i datamaskinprogrammet som ligger til grunn for avgjørelsen.

Selv om det er grunn til å anta at bruken av slike automatiserte beslutningssystemer vil øke i utbredelse i fremtiden, er det likevel liten grunn til å tro at denne bestemmelsen vil bety omfattende endringer for forvaltningens saksbehandling. Bestemmelsen vil på forvaltningsrettens område i hovedsak

fremstå som en presisering av den allerede eksisterende veiledningsplikten i forvaltningsloven § 11.

Som et ytterligere ledd i kvalitetssikringen av elektronisk behandling av personopplysninger, gir utkastet § 27 i visse tilfeller den enkelte rett til å kreve manuell behandling av personopplysninger. I tillegg til vilkårene om at det må dreie seg om en automatisert avgjørelse som er bestemmende for rettigheter eller plikter (jf. ovenfor), er det også et vilkår om at avgjørelsen karakteriserer personlige egenskaper. Det er videre et unntak for retten til å kreve manuell behandling dersom det er truffet tilstrekkelige tiltak for å sikre den enkeltes personvern, og at avgjørelsen enten er hjemlet i lov eller knytter seg til oppfyllelsen av en kontrakt.

Det er ikke grunn til å anta at bestemmelsen vil få særlig stor innflytelse på elektronisk saksbehandling i sin alminnelighet. Den vil i likhet med § 22 ikke berøre saksflytsystemer, da disse ikke utelukkende baseres på automatisk behandling. Det vil videre være slik at de fleste avgjørelser som er bestemmende for rettigheter eller plikter, eller som vil ha vesentlig betydning for den enkelte, vil være hjemlet i lov. Forvaltningen må da sørge for å treffe tiltak som er tilstrekkelig for å sikre den enkeltes personvern. Datatilsynet vil i medhold av § 40 kunne gi pålegg om hva som skal til for at et slikt tiltak skal anses som tilstrekkelig.

Der det kan kreves manuell behandling, vil dette være oppfylt ved en manuell etterkontroll av den automatiserte avgjørelsen. Forutsetningen er imidlertid at etterkontrollen er reell.

5.3.3 Virkeområde personregisterlov – personopplysningslov

I utkastet foreslås det at personopplysningsloven skal ha et noe annet virkeområde enn personregisterloven. Dette kan få en viss betydning for hvilke elektroniske saksbehandlingssystem som vil falle inn under loven.

Etter utkastet skal personopplysningsloven bare gjelde for behandling av opplysninger om fysiske personer, jf. § 2, 1) . Dette innebærer at en rekke registre og saksbehandling i tilknytning til disse som i dag reguleres av personregisterloven og bestemmelser fattet i medhold av denne, vil falle utenfor personopplysningslovens virkeområde. Det gjelder f.eks. store deler av foretaksregisteret, momsregisteret og annen saksbehandling rettet mot foretak.

Mens personregisterlovens virkeområde er knyttet opp mot hvorvidt personopplysningene er en del av et register, legger utkastet opp til at all behandling av personopplysninger skal omfattes av personopplysningsloven. Dette vil innebære en utvidelse som vil få betydning for elektronisk saksbehandling. Saksbehandling som tidligere ikke var regulert av personregisterloven fordi personopplysningene ikke var en del av et register, vil nå bli underlagt bestemmelsene i personopplysningsloven.

5.3.4 Datalogger

Et kjennetegn ved datamaskiner er at opplysninger om bruken av dem kan registreres i maskinene. Dette gjøres ved at det i de ulike programmene som benyttes, settes opp en loggfunksjon som fortløpende registrerer opplysninger om bruk. Loggen har i hovedsak betydning for oppklaringer av sikkerhetsbrudd i

systemet og som hjelpemiddel for å disponere ressursene i et nettverk. Avhengig av hvordan loggene er oppsatt vil en kunne registrere hvem som har brukt maskinen, hvor lenge og hva som er gjort. Det vil f.eks. være mulig å registrere når maskinen blir slått på, om den blir benyttet til tekstbehandling eller spill, hvor mange ganger et dokument sendes fra saksbehandler til overordnet før det sendes ut, hvor mange saker den enkelte produserer i løpet av et tidsrom, hvor lenge maskinen er påslått uten å bli brukt osv. Dette er opplysninger som selvfølgelig også kan være fristende å benytte til effektivitetsmålinger.

Per i dag er en datalogg der opplysningene kan føres tilbake til identifiserbare enkeltpersoner unntatt fra konsesjonsplikt etter forskrift til personregisterloven § 2-20. Bestemmelsen begrenser bruken av datalogger til å omfatte administrasjon av systemet, og til å oppklare/avdekke sikkerhetsbrudd i systemet.

Bruk av loggen til andre formål enn etterforsking av sikkerhetsbrudd og ressursdisposisjoner reiser flere personvernmessige problemstillinger. Bruk av denne typen informasjon vil innebære en relativt nærgående overvåking av den enkeltes arbeidsdag, og vil kunne oppleves som en krenkelse av den personlige integriteten. Opplysninger fra en datalogg vil dessuten i de aller fleste tilfeller være lite egnet til effektivitetsmålinger. Selv om en av loggene kan lese hvor mange saker en person har behandlet og hvor lang tid vedkommende har brukt, sier loggen ingenting om vanskelighetsgraden av sakene eller hvor mye tid vedkommende har brukt til å hjelpe kollegaer. Opplysninger som på en dataskjerm fremstår som objektive fakta, vil med andre ord i realiteten ofte inneholde en rekke feilkilder som vil kunne føre til feilaktige beslutninger eller ubegrunnede holdninger ovenfor den registrerte.

Ukritisk bruk av informasjon til et annet formål enn det den er innsamlet for, illustrerer en klassisk problemstilling. Opplysninger som for ett formål representerer nyttig og nødvendig informasjon, kan for et annet formål representere en trussel for den enkeltes krav på integritetsvern.

I henhold til utkast til personopplysningslov vil de fleste datalogger som disse være unntatt fra konsesjonsplikt. Tatt i betraktning den betydelige trusselen mot den personlige integriteten denne typen opplysninger kan representere, bør det vurderes om det er behov for å forskriftsregulere dette området for å sikre en betryggende behandling av denne type informasjon. I utkast til personopplysningslov foreslås en hjemmel til å gi slik forskrift.

5.3.5 Bruk av digitale signaturer

Som det fremgår av vedlegg 2 om digitale signaturer, er det enkelte ordninger av denne typen som betinger medvirkning av tiltrodde tredjeparter (TTP) som kan administrere de offentlige kodenøklene. Når en mottaker mottar en melding, vil han måtte gå til TTP for å få kodenøkkelen. Dersom TTP registrerer hvilke nøkler som leveres ut til hvem, vil han etter hvert opparbeide seg et register med informasjon om hvem som har sendt meldinger til hvem og når dette har skjedd. Et omfattende register over kommunikasjon mellom enkeltmennesker eller mellom enkeltmennesker og forvaltningen vil kunne representere en trussel mot den personlige integritet. TTPkan for eksempel se hvor ofte enkeltpersoner har hatt kontakt med et trygdekontor eller sosialkontor. Også ut fra andre synsvinkler vil det være betenkelig at denne typen informasjon samles og registreres i omfattende registre.

Det bør derfor vurderes hvorvidt det er behov for å regulere innsamling og bruk av denne type opplysninger.

5.3.6 Elektroniske postjournaler

Elektronisk lagring av dokumenter vil gjøre det relativt enkelt for forvaltningen å gi offentligheten elektronisk tilgang til offentlige dokumenter jf. ovenfor om offentlighet og innsyn. Dersom alle offentlige postjournaler blir lagt ut på Internett med mulighet for den som ønsker det å laste ned de dokumenter han ønsker, vil dette føre til en dramatisk utvidelse av offentlige dokumenters tilgjengelighet. Det vil f.eks. være mulig å lage et program som overvåker postjournalene og melder fra til eieren etter gitte kriterier. En privatperson kan f.eks. programmere programmet til å laste ned alle dokumenter som sendes til eller fra noen i nabolaget, en advokat kan sette sitt program til å laste ned alle i et bestemt område som har kontakt med kommunens etat for byggesaker slik at disse kan tilbys hans tjenester, en journalist kan sette sitt program til å laste ned alle henvendelser til eller fra det offentlige som berører en definert gruppe kjendiser osv. Mulighetene for bruk/misbruk er mange. En må med andre ord være oppmerksom på at økt tilgjengelighet for offentlige dokumenter etter all sannsynlighet også vil føre til økt bruk og til nye bruksområder, særlig sett i sammenheng med den økte mulighet for selektering som elektroniske medier tilbyr. Dette vil føre til et mer gjennomsiktig samfunn, der den enkeltes mulighet til å ta kontakt med det offentlige uten at andre enn de som har en spesiell interesse får kunnskap om dette reduseres. Dette kan føre til at enkelte vil vegre seg for å ta kontakt med det offentlige.

Elektronisk tilgang til offentlige dokumenter vil etter all sannsynlighet gi en så dramatisk endring av dagens bruk av offentlighetsloven, og vil reise personvernmessige problemstillinger av en slik karakter at saken bør gjøres til gjenstand for politisk vurdering.

6 Arkiv

6.1 Hjemmelsgrunnlaget

Dagens regelverk for arkiv er instruksbasert, hjemlet i forvaltningens generelle instruksjonsmyndighet. Instruksene gjelder i statsforvaltningen. Det er utarbeidet flere instrukser på området:

- *Instruks for arkivarbeid i statsforvaltningen* (arkivinstruksen), sist endret 30.11.1984
- *Retningslinjer for innføring av edb-baserte journalsystemer i statsforvaltningen* av 1984
- *Regler for avlevering av arkivmateriale fra statsforvaltningen til Arkivverket* av 1985
- *Krav til bruk av mikrofilm i statsforvaltningen* av 1988
- *Retningslinjer for bygging, sikring, innredning og bruk av arkiver i kommunale, fylkeskommunale og statlige administrasjoner* av 1985
- *Instruks for arkivbegrensning og kassasjon i statsforvaltningens arkiver* av 1988
- *Felles arkivnøkkel for statsforvaltningen* av 1989
- *Felles kassasjonsregler for statsforvaltningen* av 1989.

Stortinget vedtok høsten 1992 lov om arkiv, jf. Ot.prop. nr 77 (1991-92). Begrunnelsen for å få en egen lov på dette området var at det ble ansett formålstjenlig å få lovfestet arkiveringsplikt i det meste av offentlig forvaltning, og å få samlet de forskjellige påleggene i én lov. Formålet med loven er å

> «tryggja arkiv som har monaleg kulturell eller forskningsmessig verde eller som inneheld rettsleg eller viktig forvaltningsmessig dokumentasjon, slik at desse kan verta tekne vare på og gjorde tilgjengelege for ettertida».

Arkivloven hjemler at det vedtas forskrifter for den konkrete gjennomføring av intensjonene i loven. Loven er ikke trådt i kraft, og forskriftene er ennå ikke vedtatt.

Arkivloven, og forarbeidene til denne, har i begrenset grad behandlet innføring av elektronisk saksbehandling i forvaltningen. Arkivloven har imidlertid et vidt dokumentbegrep som også innbefatter elektroniske dokumenter.

Arkivloven § 2a og b:

> § 2 a: Dokument: medium som lagrar informasjon for seinare lesing, lyding, framsyning, eller overføring.
> § 2 b: Arkiv: dokument som vert til som lekk i ei verksemd

6.1.1 Hensyn

Arbeid med arkiv skal ivareta to hovedhensyn:

- ivaretagelse av materiale for ettertiden
- sikre effektivitet og etterprøvbarhet i bruk (daglig drift).

Dessuten kan journalens praktiske funksjon i forhold til offentlighetens innsynsrett være et hensyn som må ivaretas ved overgang til nye systemer i tilknytning til elektronisk lagring av dokumenter.

6.2 Virksomhetenes kommentarer

De fleste av virksomhetene oppgir å ha et elektronisk journalsystem. Det er imidlertid et lite fåtall som har elektronisk arkiv. De fleste virksomhetene har elektronisk journalføring. Dokumentene arkiveres derimot i et papirarkiv. Hos en virksomhet blir alle dokumentene arkivert elektronisk for daglig bruk, mens papirdokumentene arkiveres i et "skyggearkiv". Det varierer fra virksomhet til virksomhet hvem som har adgang til det elektroniske journalsystemet. Hos noen virksomheter er det bare arkivpersonalet som har adgang, mens hos andre har saksbehandlerne lese- og søkeadgang. Hos noen helt få har saksbehandlerne selv adgang til å foreta registreringer. Virksomheter som tillater saksbehandlere å registrere dokumenter, påpeker hvor viktig det er de får en grundig opplæring.

Flere av foretakene har opprettet en egen postkasse for mottak av saksrelatert e-post. De som ikke har slikt sentralt postmottak, har rutiner som tilsier at saksbehandleren sender e-post som kommer direkte til ham til registrering dersom innholdet er arkivverdig. Ingen av virksomhetene oppgir at e-postmeldingen bare lagres elektronisk.

De fleste virksomhetene antar at det fortsatt vil være behov for å arkivere dokumenter i papirform i mange år fremover. De tror likevel at elektroniske arkiv vil bli mer og mer vanlig, og at papirarkivet bare vil bli en back-up av de elektroniske. Sikkerhetsproblemer, spesielt faren for ikke å klare å holde arkivmaterialet tilgjengelig, oppgis hyppigst som grunner for at papirarkivet bør beholdes. I tillegg påpekes det at det byr på problemer i forhold til gjeldende regelverk å oppbevare saksdokumenter kun i elektronisk form.

6.3 Utfyllende kommentarer

I dag er arkivene i forvaltningsorganene samlinger av papirbaserte saksdokumenter. Når vi i det følgende omtaler «arkiv», vil begrepet omfatte de tilsvarende elektroniske dokumentene. Begrepet «dokumentlager» brukes om det elektroniske arkivet *og* virksomhetens øvrige elektroniske dokumenter.

Hele arkivregelverket er i dag orientert mot dokumentet som et fysisk objekt. Det tas i liten grad høyde for at det er dokumentets innhold som skal brukes i saksbehandlingen og som i de fleste tilfeller er det en ønsker å bevare for ettertiden. Begrepsapparatet er knyttet til bruk av papir som medium.

Arkivinstruksen er i dag på noen områder svært detaljert når det gjelder hvordan arkivarbeidet skal utføres. Regler som retter seg mot behandling av papiret, som f.eks. punkt 5.1 om stempling av post og punkt 5.3 om bilegging av saker, kan omformuleres slik at funksjonen bestemmelsen skal sikre, ivaretas også i et elektronisk system. Bestemmelser om funksjonalitet som f.eks. punkt 5.8 om kopibok kan utgå, da funksjonaliteten ivaretas av det elektroniske systemet. Ved innføring av elektronisk saksbehandling i forvaltningen vil det altså være behov for å vurdere flere typer endringer i bestemmelsene i arkivregelverket.

En del oppgaver er lagt til arkivet fordi dette har vært et knutepunkt for virksomhetens dokumenthåndtering. Det gjelder for eksempel mulighet for registrering av saker/dokumenter, restansekontroll og praktisk håndtering av innsyn. Det kan være grunn til å revurdere *ansvarsplasseringen* for de ulike oppgavene i lys av de mulighetene som ligger i elektroniske systemer for dokumenthåndtering og saksbehandling.

Elektroniske saker og dokumenter vil i utgangspunktet til enhver tid være tilgjengelige for alle i virksomheten. Tilgjengeligheten kan begrenses ved tilgangskontroll. Det kan innføres *ulike nivåer av tilgangsrettigheter*, knyttet til personer, funksjoner etc, slik at bare de som har behov for tilgang, faktisk har den. Dette kan særlig være aktuelt i virksomheter som behandler taushetsbelagt eller sensitiv informasjon, eller informasjon som av andre grunner bør skjermes. Se også om taushetsplikt i kapittel 12.

Når saker og dokumenter er papirbaserte, er det et problem at de kan komme bort, enten under saksbehandlingen eller ved transport. De elektroniske dokumentene vil derimot hele tiden befinne seg i det elektroniske dokumentlageret, selv om de også er i bruk i saksbehandlingen eller «til utlån». I et elektronisk system vil truslene ha en annen karakter. De elektroniske dokumentene vil kunne endres, slettes eller være tilgjengelige for andre enn de som er autoriserte brukere dersom sikkerhetssystemene ikke er gode nok.

I et elektronisk dokumentlager kan en saksbehandler selv søke etter og få tilgang til de ønskede dokumentene. Dette vil effektivisere saksbehandlingen, og det vil åpne for at dokumentlageret kan fylle også andre funksjoner. Dokumentlageret kan også fungere som presedensarkiv, ved at deler av dokumentmengden tilrettelegges for særlige søk. Fordelene ved en slik løsning er at terskelen for å bruke presedenser blir lavere: brukergrensesnittet vil være det samme som saksbehandleren er vant til, og selve innleggelsen av dokumentene i «presedensarkivet» blir enklere. Vedlikeholdet av «presedensarkivet» vil imidlertid måtte gjennomføres på samme måte som i frittstående presedensarkiver; uten vedlikehold vil det raskt miste sin verdi.

6.3.1 Mottak av innkommende post

I henhold til arkivinstruksen punkt 4 er arkivet forvaltningsorganets postmottak. All post som er adressert til forvaltningsorganet sendes til arkivet, enten til organets fellesarkiv, eller direkte til et delarkiv hvis brevet er adressert dit. Arkivet har ansvaret for sortering av den innkomne posten, og for å videresende den til rette vedkommende. Post som kommer direkte til en saksbehandler, for eksempel e-post, telefaks eller liknende, skal sendes til arkivet for registrering dersom innholdet er arkivverdig.

Ved innføring av elektronisk dokumentlager og saksbehandling må det tas stilling til hvordan forvaltningsorganets mottak av elektroniske dokumenter skal organiseres og drives. Hvis det velges andre generelle rutiner for innkommende post enn via arkiv/felles postmottak, må det etableres *mottaksrutiner som sikrer korrekt journalføring* og videre behandling for de elektroniske dokumentene, jf. også Administrasjonsdepartementets veiledning om bruk av e-post i statsforvaltningen.

Innføring av elektronisk saksbehandling vil muliggjøre hurtig og direkte ekstern kommunikasjon mellom en saksbehandler og en part eller et annet organ. Det må

i den forbindelse tas stilling til om det er ønskelig at henvendelser kan sendes direkte til den avdelingen som behandler saken, eventuelt til en saksbehandler, uten å gå veien om arkivet. I så fall må det innarbeides rutiner som sikrer

- at saker og dokumenter blir registrert på en korrekt måte,
- at ledelsesnivået er informert om de henvendelsene som kommer inn til organet, og hvilke ekspedisjoner som sendes ut. Dette kan f.eks. ordnes ved automatisk rapportering fra journalsystemet, som gjøres tilgjengelig for ledere eller andre som har behov for det

At brev sendes direkte til en saksbehandler, forekommer også ved bruk av ordinær post, enten fordi parten bevisst har adressert brevet til saksbehandler, eller fordi vedkommende ikke er klar over at dokumenter i en sak skal adresseres til organet og ikke til saksbehandleren. Likeledes kan det forekomme at sakspost sendes direkte til en saksbehandler ved bruk av bud eller ved personlig overlevering i et møte eller liknende. Dersom en saksbehandler får et saksdokument direkte inn til seg, må han sørge for å få det registrert hos arkivet. Det vil i så måte ikke være noe forskjell på vanlige brev og e-post som sendes direkte til saksbehandleren. En av e-postens fremste fordeler er at den kan brukes til rask og direkte kontakt mellom kommunikasjonspartene. Den som sender en e-postmelding, kan frykte at denne fordelen forsvinner dersom meldingen sendes til et postmottak som skal sende den videre til saksbehandleren. Han vil derfor ofte ønske å sende meldingen direkte til saksbehandleren. Dette kan også skje i samsvar med saksbehandlerens ønske. E-post kan i denne sammenheng best sammenlignes med telefaks. Det er derfor grunn til å anta at mengden saksdokumenter som sendes direkte til en saksbehandler uten å gå innom arkivet, vil øke når e-post benyttes i saksbehandlingen.

For at arkivet skal kunne ha en oversikt over organets dokumenter, er det derfor av stor viktighet at det innarbeides rutiner for hvordan e-post som kommer direkte til en saksbehandler skal håndteres. Slike rutiner kan eventuelt innarbeides i saksbehandlingssystemet. Systemet kan f.eks. automatisk be saksbehandleren ta stilling til om tilsendte dokumenter er å betrakte som saksdokumenter. Dersom saksbehandleren svarer ja på dette, ber systemet om at dokumentet registreres. Avhengig av arbeidsfordelingen i vedkommende organ foretar enten saksbehandleren registreringen, eller så sendes dokumentet til arkivet for registrering.

6.3.2 Journalføring

Det forutsettes i arkivinstruksen at det føres journal, uten at det er noe klart formulert krav. Dette vil sannsynligvis komme som et klart krav i den nye arkivforskriften. Journalen skal inneholde opplysninger om all innkommende og utgående post, samt enkelte interne dokumenter. Journalen er i dagens system en inngangsport til arkivet. Det er i journalen endringene i arkivet kommer frem, og den er en forutsetning for allmennhetens bruk av innsynsretten. I en virksomhet som benytter elektronisk saksbehandling, vil den samlede dokumentmengden være tilgjengelig via gjennomgående søkemuligheter. Dette vil være hensiktsmessig for saksbehandlere og ledere internt, men vil også kunne utnyttes i forhold til parters og allmennhetens innsynsrett. Søkemulighetene vil på den

annen side kunne reise visse personvernmessige problemstillinger. Disse er omhandlet i kapitlet *Personvern.*

Journalføringen ivaretar flere funksjoner som skal sikre effektivitet, etterprøvbarhet og forsvarlig saksbehandling. I henhold til arkivinstruksen er det følgende minimumskrav til innholdet i en journal:

- Dato for innkomst
- Journalnummer
- Avsender
- Ekstraherte opplysninger om innhold/emne
- Dokumentets datering
- Journalnummer
- Kontor/saksbehandlers initialer
- Ekspedisjonsrubrikk (mottaker)
- Ekspedisjonsdato
- Anmerkningsrubrikk

Journalen har ulike funksjoner. Den spiller i dag en viktig rolle i forbindelse med identifisering av saker og dokumenter, slik at arkivpersonalet lettere kan administrere de til dels store arkivvolumene. Journalen er i dag også viktig for å kunne foreta en reell etterprøving av forvaltningens behandling av en sak. Forutsatt at den er ført riktig og fullstendig, vil journalen spille en rolle ved at det er mulig å rekonstruere saksforløpet hvis dokumentene skulle komme bort. Ved innføring av elektroniske dokumenter vil de forskjellige søkemulighetene, den tilgjengeligheten og de alternative måter å sortere/gruppere dokumentene på som teknologien gir, kunne ta over en del av disse funksjonene.

Journalen er også et viktig hjelpemiddel for praktisering av offentlighetsloven. Journalene fungerer som «inngangsporten» til de sakene/dokumentene forvaltningen behandler. Dersom et saksdokument ikke registreres i journalen, vil ikke offentligheten være kjent med at dokumentet eksisterer. Retten til å kreve å få se innholdet i dokumentet i henhold til offentlighetsloven vil dermed bli illusorisk. Det er derfor også av hensyn til offentlighetens tilgang til forvaltningens dokumenter av stor viktighet at journalen er komplett. Det største faremomentet i denne sammenheng vil sannsynligvis være e-post som sendes direkte til en saksbehandler. Dersom virksomheten ikke har tilstrekkelige rutiner for registrering av denne typen post, kan journalen fort bli mangelfull. Dersom den offentlige journalen skulle bli svært mangelfull, kan det reises spørsmål om virksomhetens e-postlogger må betraktes som et «lignende register» i henhold til offentlighetsloven § 2, andre ledd.

Arkivinstruksen har ikke noe krav om at det kun er arkivpersonalet som kan føre opplysninger inn i journalen, selv om dette i praksis er den løsningen som er valgt i virksomhetene. Det antas derfor ikke å bryte med instruksen om noen av opplysningene føres automatisk eller av saksbehandlerne. Det avgjørende må være at en sikrer seg at de korrekte opplysningene faktisk blir registrert.

Registreringsrutinene må legges opp slik at journalopplysningene blir ført korrekt og komplett. Det kan legges opp kontroll- eller verifiseringrutiner som i større grad enn i manuelle systemer sikrer korrekt innhold, slik de edb-baserte journalsystemene til en viss grad gjør i dag.

6.3.3 Restansekontroll

Arkivet har i dag et ansvar for å følge opp saker, samt å påse at frister overholdes. Dette gjøres ved at arkivet holder en oversikt over de sakene som forelegges andre, og som forutsetter svar. Videre skal arkivet sende ut restanselister for å påse at saker ferdigbehandles innen en viss tid. De nærmere regler for denne oppfølgingen er i arkivinstruksens punkt 8.

I praksis vil det ofte være vanskelig for arkivet å holde oversikt over hvorvidt en sak faktisk er avsluttet eller om det innkomne dokumentet bare er avskrevet mot et brev der det spørres etter mer informasjon.

Ved elektronisk saksbehandling vil oppfølging av saker kunne skje automatisk ved hjelp av saksflytsystemet. Funksjonaliteten vil lett kunne utvides til også å omfatte refordeling av saker om en saksbehandler f.eks. er syk, eller om arbeidsbelastningen blir for stor på enkelte av saksbehandlerne. Slik refordeling kan legges opp som en automatisert rutine eller som en støttefunksjon for den som har fordelingsansvar. Oppfølgingen vil ved bruk av saksflytsystemer dermed kunne knyttes direkte opp mot saksbehandlingsprosessen og ikke til det enkelte dokument, slik situasjonen er i dag. Det vil i denne forbindelse være naturlig å vurdere å flytte oppfølgingsansvaret fra arkivet over til den som har det overordnede ansvaret for saksbehandlingen i gruppen, avdelingen eller virksomheten.

6.3.4 Utlån av arkivmateriale

Arkivinstruksen punkt 6 har regler om hvordan arkivet skal være behjelpelig ved utlån av dokumenter både til intern bruk hos det enkelte forvaltningsorganet og til eksterne rekvirenter eller lånere. Formålet med disse bestemmelsene er at arkivet skal vite hvor dokumentene befinner seg, forsikre seg om at ikke uvedkommende har tilgang til dokumentene, og å unngå at dokumenter går tapt.

Utlån vil ikke være aktuelt for elektronisk lagrede dokumenter. Elektroniske kopier eller utskrifter vil det ikke være aktuelt å kreve inn igjen. Dermed vil administrasjon av utlånene bortfalle. For interne brukere vil det være tilgangskontrollen som bestemmer for hvilke dokumenter eller saker den enkelte saksbehandler skal få tilgang til. Henvendelser til arkivet for å låne saksinformasjon vil bare være aktuelt i forhold til deler av arkivet som ikke er elektroniske. Eksempler på slike tilfeller kan være spesialarkiv over jord- eller vannprøver, bøker eller større publikasjoner det ikke er mulig eller formålstjenlig å skanne inn.

Arkivet må eventuelt også kunne bistå eksterne «låntakere» som har behov for hjelp til å finne de riktige sakene eller dokumentene.

6.3.5 Reduksjon av arkivvolumet og bortsetningsarkiv

Arkivinstruksen inneholder bestemmelser om arkivlegging, kassasjon og plassering av arkivmateriale i bortsettingsarkiv. Reglene har flere begrunnelser, hvorav de viktigste er at det aktive arkivet ikke blir uhåndterlig stort. I tillegg holdes kostnadene ved lagring på et akseptabelt nivå, samt at innholdet begrenses til det som sannsynligvis har interesse for ettertiden.

Arkivlegging er regulert i arkivinstruksen punkt 5.10. Elektroniske saker vil ikke inneholde lånekort, binderser e.l., men virksomheten bør utvikle en felles strategi for sletting av midlertidig materiale, evt. basert på rutinene som i dag gjelder for papirbaserte konsepter. Denne oppgaven ligger i dag til arkivet, «i tvilstilfelle i samråd med saksbehandler». Med den tilgangen en saksbehandler vil få til de elektroniske dokumentene, kan det være grunn til å vende ansvarsforholdet her. Saksbehandleren kan like gjerne være den som gjennomgår saken, og «i tvilstilfelle» får hjelp fra arkivet. Arkivet vil på denne måten først og fremst ha en kvalitetssikringsfunksjon. En slik løsning vil kreve en kompetanseoverføring fra arkivpersonalet til saksbehandlerne i forhold til arkivverdighetsvurderingen.

Behovet for å sette bort saker og dokumenter til bortsettingsarkiv vil ikke være like fremtredene ved bruk av elektronisk dokumentlagring som det er i dag. Det er likevel hensyn som tilsier at en fortsatt bør strebe etter å begrense arkivvolumet. For det første tar lagring av elektroniske saker og dokumenter også plass, selv om problemet er i en annen skala enn for papirbaserte dokumenter. Elektronisk lagringskapasitet blir stadig billigere og mer effektiv, og det er grunn til å tro at teknologiutviklingen på sikt vil eliminere dette som problem. For det andre vil gjenfinning av relevante dokumenter bli vanskeligere hvis det er for mange dokumenter tilgjengelig for søking. Dette har igjen to implikasjoner. Det ene er at søketiden blir unødvendig lang. Den andre at det blir for mange treff i søkene, slik at de relevante dokumentene kan «stikke seg bort» mellom mange tilsynelatende aktuelle dokumenter (støy- eller over-load-problemet). Dette kan være argumenter for å innføre en annen type «bortsettningsarkiv». Det kan ordnes ved at dokumentlageret deles, slik at alle dokumenter som ble opprettet for mer enn f.eks. to måneder siden, og som ikke er del av en aktiv sak, automatisk flyttes over til en annen del av arkivet. Denne delen av dokumentlageret vil selvfølgelig også være tilgjengelig for søk dersom en bruker ønsker det.

6.3.6 Arkivavgrensing

Arkivinstruksen punkt 10 pålegger forvaltningen en generell plikt til å foreta arkivavgrensning og kassasjon i samsvar med gjeldende regelverk. Det er forvaltningsorganet selv som har ansvaret for å foreta utvelgelsen av hvilken informasjon som er *arkivverdig* og av interesse for senere forskning eller annen anvendelse, på bakgrunn av de bestemmelsene som er gitt om dette. I dag foregår reduksjonen i det papirbaserte arkivvolumet i tre trinn, først ved arkivlegging, deretter ved lagring i bortsettingsarkiv. Siste trinn i reduksjonen av arkivvolumet foregår ved avlevering til Arkivverket.

Edb-lagret materiale skal avleveres når det ikke lenger er i forvaltningsmessig bruk, arkivinstruksen punkt 9.2, 1. ledd, 2. setning. *Regler for avlevering av arkivmateriale fra statsforvaltningen til arkivverket* fra 1985 presiserer i punkt 4.3 denne plikten til en gjennomgang med etterfølgende avlevering hvert 5. år. Løpende edb-registre skal avleveres til bestemte tider, etter avtale med Arkivverket. Edb-materiale skal reduseres etter de samme prinsippene som annet materiale, jf. *Felles kassasjonsregler for statsforvaltningen*, punkt 1 i kapitlet om edb-materiale.

6.3.7 Lagring og overlevering av edb-materiale

Lagring hos Arkivverket har i hovedsak vært papirbasert. Gjeldende instrukser avspeiler i stor grad problemet med en stadig voksende arkivmasse. Å lagre store mengder papir er kostbart og ressurskrevende. Reglene om arkivbegrensning og kassasjon er derfor et uttrykk for et kompromiss mellom å destruere deler av materialet og å bevare det som er arkivverdig.

Disse kostnadshensynene vil i liten grad gjøre seg gjeldende ved lagring av elektroniske dokumentarkiv i fremtiden. Lagringsmedia blir stadig mer effektive og billige. Kassasjon har imidlertid ikke bare en side mot lagringskostnader, men også i forhold til *oversiktlighet* for det lagrede materialet. Dessuten er det et poeng å holde arkivvolumet nede for å lette formatkonverteringer. Av denne grunn vil det være hensiktsmessig å ha kassasjonsregler, men kriteriene for utvelgelse må vurderes ut fra de nye lagringsmulighetene.

Arkivinstruksene er, som vi har vært inne på tidligere, dokumentorienterte. Regelverket forutsetter lagring av selve papirdokumentet. Reglene om lagring av edb-materiale synes å være rettet mot opplysningsregistre i større grad enn dokumentarkiver. Det kan stilles spørsmål ved hvilke av papirets funksjoner som må anses relevante eller nødvendige ved overgang til eventuell elektronisk lagring. Er det det visuelle uttrykket dokumentet har, er det informasjonsinnholdet papiret er bærer av, eller er det selve papiret? For de tilfellene der dokumentets fysiske beskaffenhet har betydning, vil det være lite hensiktsmessig å lagre dokumentet elektronisk. Det er imidlertid grunn til å anta at dette vil utgjøre en liten del av den samlede dokumentmassen. Slike dokumenter må nok på samme måte som jord- og vannprøver fortsatt arkiveres på tradisjonell måte.

Allerede i 1984 åpnet Arkivverket for at arkivering og avlevering av arkiv også kunne foregå på mikrofilm. Mikrofilm ivaretar de to første funksjonene ovenfor. Det må tas stilling til om det vil være nødvendig å oppbevare elektroniske dokumenter både som bilder og som maskinlesbare tekster. Standardformater for slik oppbevaring må utredes.

6.3.8 Langtidslagring

Forvaltningen har plikt til å ta vare på arkivmateriale som har, eller antas å ha, interesse for ettertiden. Å sikre at materiale fra vår samtid er tilgjengelig for fremtidig forskning er en viktig del av det generelle kulturvernet. Arkivloven, som ennå ikke er trådt i kraft, nevner i sin formålsparagraf at dette er hovedbegrunnelsen for å ha arkiv. Det antas at dette også er et av hovedhensynene bak de retningslinjene og instruksene som Riksarkivaren har vedtatt på dette området.

Arkivinstruksen forutsetter at offentlige forvaltningsvirksomheter har arkiv. Arkivinstruksen punkt 9.3 pålegger organet en plikt til å levere fra seg materiale til Arkivverket. Et mellomtrinn er innført ved krav om bortsettingsarkiv, punkt 9.2, dit materialet flyttes når det ikke lenger er i aktiv bruk.

En vesentlig problemstilling i forhold til langtidslagring på et elektronisk medium er å kunne holde dokumentene tilgjengelig over tid.

Problemet oppstår fordi det stadig utvikles nye formater for produksjon av dokumenter samtidig som eldre formater går ut av bruk. Dette gjør det vanskelig å kunne hente frem et elektronisk dokument som er produsert med gammel teknologi. Denne problemstillingen er berørt under kapitlet *Elektronisk kommunikasjon*, men trenger å belyses nærmere i forhold til arkivering.

For at det skal være praktisk mulig å gjennomføre slike konverteringer etter hvert som teknologien endres, må sannsynligvis alle eksisterende dokumenter være lagret i samme, eller i et begrenset antall formater.

Et forvaltningsorgans dokumenter kan grovt deles opp i tre, de dokumenter som produseres av organet selv, de som mottas fra andre forvaltningsvirksomheter, og de som mottas fra andre. Når det gjelder organets egne dokumenter vil disse i første omgang være uproblematiske i forhold til format. Organet vil her selv kunne bestemme hvilket format som skal brukes. Likeledes vil det være relativt overkommelig å enes om en felles standard for forvaltningens dokumenter. Når det gjelder andres henvendelser til forvaltningen kan det være mer problematisk å begrense formatvariasjonen. Se nærmere om dette under kapitlet *Elektronisk kommunikasjon*. For denne typen dokumenter må forvaltningen sannsynligvis basere seg på å konvertere innkomne dokumenter til ett eller noen få lagringsformater før arkivering.

Organene må imidlertid også etter at dokumentene er konvertert til lagringsformatet påse at materialet holdes tilgjengelig. Dette innebærer bl.a. et ansvar for å konvertere de arkiverte dokumentene til nye lagringsformat dersom den teknologiske utviklingen gjør dette nødvendig. Etter dagens regelverk er det enkelte organ ansvarlig for å holde sitt arkiverte materiale tilgjengelig i opptil 25 år. Etter denne tid skal materialet overføres til Riksarkivet, som da overtar ansvaret for å holde det tilgjengelig. Det er ikke usannsynlig at et arkivert dokument må konverteres til nytt format en eller flere ganger i løpet av en 25-årsperiode. Det kan i denne sammenheng stilles spørsmål ved om det er hensiktsmessig at ansvaret for konvertering ligger hos det enkelte organ i så lang tid. Arbeidet med å holde edb-materiale tilgjengelig over tid krever en viss spesialkompetanse. Det bør derfor vurderes å endre reglene slik at edb-lagret materiale overføres til en sentral institusjon innen kortere tid. Den sentrale institusjonen kan da tilføres de ressursene og den kompetansen som trenges.

7 Saksbehandlingsregler

7.1 Hjemmelsgrunnlaget

På samme måte som tradisjonell saksbehandling vil selvfølgelig elektronisk saksbehandling reguleres av en rekke bestemmelser i flere ulike lover og forskrifter. Den viktigste loven for saksbehandling i det offentlige er forvaltningsloven av 10. februar 1967. Loven inneholder generelle regler om saksbehandling i forvaltningen og gjelder alle forvaltningsorganer dersom annet ikke er bestemt i medhold av lov. I kartleggingsnotatet som ligger til grunn for denne rapporten, er enkelte bestemmelser i forvaltningsloven drøftet som særlig interessante i forhold til elektronisk saksbehandling. Dette er § 11 om veiledningsplikten samt reglene i kapittel 4, 5 og 6 som omhandler henholdsvis saksforberedelsen ved enkeltvedtak, regler om selve vedtaket og regler om klage og omgjøring.

I tillegg til forvaltningsloven finnes det en del ulovfestede regler for forvaltningens saksbehandling. Dette er overordnede prinsipper som kan få betydning f.eks. for gyldigheten av et vedtak selv om ingen formelle saksbehandlingsregler er brutt. Særlig kvalitetskravet som kommer til uttrykk gjennom prinsippet om en forsvarlig saksbehandling, er interessant i forhold til elektronisk saksbehandling.

Også særlover kan ha egne bestemmelser om saksbehandlingen på visse områder. Et slikt eksempel er ligningsloven som har egne saksbehandlingsregler for ligning av skatt og trygdeavgift. Slike særbestemmelser vil ikke bli berørt i det følgende.

7.2 Virksomhetenes kommentarer

De fleste av virksomhetene oppgir at reglene for deres saksbehandling i hovedsak følger av forvaltningsloven. Noen virksomheter oppgir å ha utfyllende regler i særlovgivningen, mens noen få oppgir å ha hovedtyngden av saksbehandlingsreglene i særlovgivningen.

De fleste virksomheter uttrykker forventninger til mulighetene for effektivisering og kvalitetsheving i saksbehandlingen. I denne sammenheng fremholdes muligheten for automatisering av enkelte prosesser, samt økt mulighet for tilgang til informasjon fra eksterne databaser eller web-sider. Det er et generelt inntrykk at saksbehandlingsreglene ikke vil skape særlige problemer i forbindelse med overgang til elektronisk saksbehandling.

Behovet for en ordning med pålitelige signaturer på elektroniske dokumenter nevnes imidlertid av flere som en viktig forutsetning for å kunne utvide bruken av elektronisk saksbehandling.

Det påpekes også at forvaltningsloven i stor grad tar individuell saksbehandling som utgangspunkt. Dette er til hinder for å automatisere saksbehandling, som forutsetter at det legges til grunn et individuelt skjønn i den enkelte sak. Et annet eksempel som nevnes er forskjellen mellom generell informasjon og individuell veiledning. Gjennom å klippe og lime fra ulike informasjonskilder kan det skapes at inntrykk av at den informasjonen som gis er individuelt tilpasset den konkrete

sak. Det fremholdes som viktig at en er seg bevisst skillet mellom informasjon og veiledning.

7.3 Utfyllende kommentarer

7.3.1 Veiledningsplikten

Ifølge § 11 har forvaltningsorganene en alminnelig veiledningsplikt innenfor sitt område. Formålet med bestemmelsen er å sikre at parter og andre interesserte gis adgang til å sikre sine interesser best mulig. Veiledningen kan typisk være å orientere om rettsreglene på gjeldende område, eller redegjøre for saksbehandlingsregler som kommer til anvendelse, og om hvilke rettigheter og plikter partene har etter forvaltningsloven.

Elektronisk saksbehandling vil kunne styrke ivaretakelsen av de hensynene veiledningsplikten bygger på. Den enkelte forvaltningstjenestemann vil kunne få en betydelig bedre tilgang til informasjonen og det vil være lettere å kunne veilede, selv om den tjenestemannen som mottar henvendelsen ,eventuelt ikke er den samme som behandler saken eller slike saker. Han vil med enkle søk i ulike informasjonsbaser eller systemer for saksflyt kunne undersøke en enkelt saks status eller hvordan bestemte typer av saker behandles. Med elektronisk saksbehandling vil det ikke lenger være avgjørende om den tjenestemannen som behandler den bestemte saken er til stede. Hans kolleger vil kunne veilede i hans sted.

Også med hensyn til plikten til å vise til rette offentlige organ der henvendelser er gjort med feil adresse, vil elektronisk saksbehandling gjøre veiledningsplikten lettere. Her kan en tenke seg utviklet informasjonssystemer som gjør det enkelt for alle offentlige tjenestemenn å orientere seg i forhold til hvem som gjør hva i det offentlige. Ytterligere videreutviklet kan en slik veiledningsplikt tenkes utført i offentlige informasjonsskranker, for eksempel plassert i biblioteker eller sentrale offentlige kontorer (trygdekontoret, ligningskontoret, det offentlige servicekontoret e.l.). Dette gjelder både med hensyn til hvordan enkeltsaker behandles og hvem som behandler de enkelte sakene.

Slik veiledningsplikten er uttrykt i fvl. § 11, begrenses ikke mulighetene for bruk av elektronisk saksbehandling. I tillegg vil elektronisk saksbehandling kunne realisere de ønskemål som uttrykkes i Statssekretærutvalgets rapport *Den norske IT-veien Bit for bit*. Det vises i denne sammenheng til rapportens punkt 3.8.2: «Offentlig forvaltning bør systematisk bruke elektronisk informasjon i sitt informasjonsopplegg overfor publikum, medier og næringsliv». Ved hjelp av elektroniske søkesystemer vil offentlig informasjon kunne gjøres betydelig mer tilgjengelig.

Det er imidlertid viktig å være på vakt mot at den elektroniske informasjonen erstatter den individuelle veiledningen. I enkelte sammenhenger vil det ikke være tilstrekkelig å henvise en part til å søke i generell informasjon, eller eventuelt oversende et utdrag av slik generell informasjon. I noen tilfeller vil forvaltningen ha en plikt til å bistå parten med individuell veiledning i forhold til en konkret sak. I hvilke tilfeller det må ytes veiledning utover å gi generell eller mer eller mindre tilpasset informasjon, må avgjøres etter en konkret vurdering. Viktige

vurderingstemaer vil i denne sammenheng være sakens viktighet, informasjonens detaljeringsgrad og partens evner og resurser.

7.3.2 Utredningsplikten

Det følger av forvaltningsloven § 16 at sakens parter skal varsles når det forberedes å fatte et vedtak. Videre skal forvaltningsorganet påse at saken er så godt opplyst (utredet) som mulig før vedtak treffes. Med disse reglene ønsker en å sikre at vedtak er velfundert og basert på grundige undersøkelser, slik at blant annet vilkårlighet unngås. Partene vil ofte være en nyttig informasjonskilde for forvaltningsorganet, og reglene om varslingsplikt og utredningsplikt utfyller hverandre.

Det må imidlertid understrekes at utredningsplikten ikke strekker seg inn i det uendelige. Av hensyn til behovet for effektiv saksbehandling må forvaltningsorganet på et visst punkt sette strek for utredningen. Det må med andre ord gjøres en konkret avveining mellom behovet for grundighet og behovet for effektiv forvaltning.

Elektroniske saksbehandlingssystemer vil kunne medvirke til en effektivisering av saksbehandlingen. Eksempelvis vil forvaltningsorganets utredningsplikt kunne gjøres betydelig lettere og grundigere gjennom søk i tilgjengelige informasjonsbaser, arkiv, presedensarkiv, det elektroniske dokumentlageret o.l. Med hensyn til et elektronisk dokumentlager kan dette organiseres på måter som gjør det mulig å foreta fulltekstsøk, søk på emneord, søk på person osv. Her vil det ligge et stort potensiale for å gjøre informasjon tilgjengelig om dokumentlageret tilpasses de funksjonelle behov hver enkelt virksomhet har.

Likeledes vil kommunikasjonen mellom vedtaksorganet og eventuelle andre forvaltningsvirksomheter som har relevant saksinformasjon, kunne gjennomføres hurtigere. Denne effektiviseringen kan føre til at saker løses raskere, noe som også de involverte partene vil oppleve som fordelaktig. Dette behovet for raske, men samtidig riktige, beslutninger blir tydelig eksempelvis der næringsutvikling fordrer offentlige tillatelser. Prosjekters investeringsbeslutninger må ofte stå i stampe og avvente en offentlig godkjennelse som er nødvendig i saken.

For å sikre at formregler følges, som f.eks. varsling av partene, kan det i et elektronisk saksbehandlingssystem benyttes maler som sikrer at disse reglene følges. En annen funksjon som kan bygges inn, er at et vedtak ikke kan sendes til parten dersom det ikke er angitt opplysninger om klageadgang som beskrevet i forvaltningsloven § 27.

7.3.3 Kvalitetssikring

Forvaltningens saksbehandling skal forutsetningsvis være av god kvalitet. Resultatet av saksbehandlingen, enten det er ulike former for vedtak, innstillinger, proposisjoner, meldinger eller annet, bør derfor gjennomgå nødvendig kvalitetssikring.

Begrepet kvalitetssikring benyttes ikke i saksbehandlingsreglene. Forvaltningen pålegges altså ikke eksplisitt å kvalitetssikre seg selv, men det ulovfestede prinsippet om forsvarlig saksbehandling forutsetter at saksbehandlingen inneholder kvalitetssikringsrutiner. Kvalitetssikringshensynet kommer også

indirekte frem gjennom den arbeidsprosessen som regelverket pålegger saksbehandlingen.

Som et eksempel på dette kan nevnes to-instans-systemet (underinstans - klageinstans) som er med på å kvalitetssikre enkeltvedtak. Andre eksempler er påleggene om utredningsplikt og begrunnelse for vedtak, som også er kvalitetssikrende elementer i saksbehandlingen. Ytterligere et eksempel på saksbehandlingsregler som virker kvalitetssikrende, finner vi i *Reglementet for departementenes organisasjon og saksbehandling* § 9. (Det siktes her til 1984-versjonen av dette reglementet). Under overskriften «Utkast til avgjørelse o.l.» gis det her regler som sikrer at utkast utarbeides på et lavere nivå (normalt saksbehandlernivået) for så å sendes oppover i hierarkiet for kvalitetssikring. Alle som deltar i behandlingen av en sak, skal påføre den sin signatur – en regel som sikrer at en i ettertid kan kontrollere at blant annet kvalitetssikring virkelig er gjennomført. Nok et eksempel hvor et slik kvalitetssikringselement kommer til uttrykk, er i det samme reglementet § 12 - «Undertegning og parafering». Ifølge denne regelen skal all utgående korrespondanse som inneholder avgjørelser, undertegnes av departementslederen eller den han bemyndiger. I tillegg skal korrespondansen paraferes av den nærmeste underordnete eller en annen tjenestemann.

I hvilken grad kvalitetssikringen svekkes eller styrkes gjennom elektronisk saksbehandling er et spørsmål om hvordan den elektroniske kommunikasjonen internt organiseres. Teknologisk vil det antakelig ikke være problematisk å modellere denne slik at regeleksemplene over etterleves. Et saksflytsystem kan f.eks. nekte utsendelse av en sak før den nødvendige undertegning og parafering er gjort. Hvilke slike kvalitetssikrende elementer som skal legges inn i saksflytsystemet må vurderes konkret i forhold til sakstype og organ. Det bør i denne sammenheng også vurderes om de ulike kvalitetssikringstiltakene skal være absolutte eller om de skal kunne overstyres av en saksbehandler.

Ved innføring av automatiserte prosesser er det viktig å være oppmerksom på at forvaltningsretten forutsetter en individuell behandling av saker. Dersom en forsøker å automatisere prosesser som er forutsatt å inneholde innslag av skjønn, kan en meget raskt komme i konflikt med dette prinsippet. Hvilke automatiske prosesser som kan installeres i hvilken type saksbehandling beror på en konkret vurdering. Generelt kan en imidlertid si at for at en prosess skal kunne automatiseres, må det være mulig å definere klare og entydige kriterier for hvilke hendelser eller verdier som skal sette i gang prosessen, og hvilket resultat prosessen skal føre til.

Avslutningsvis skal det nevnes at en klage alltid vil forutsette en individuell behandling. Det kan således vanskelig tenkes situasjoner der en automatisert klagebehandling ville være i tråd med god forvaltningsskikk. Unntaket fra dette må være dersom det uriktige vedtaket skyldes systemfeil. I slike tilfeller må forvaltningsorganet kunne kjøre sakene på nytt når de blir gjort oppmerksom på feilen. Dette kan da innebære at noen av vedtakene blir omgjort på bakgrunn av klage, mens andre blir omgjort av eget tiltak.

8 Oppsummering/anbefalinger

Dette kapitlet inneholder en oppsummering av noen av de punktene som er omtalt foran. Oppsummeringen tar for seg de områdene der det straks bør settes i verk tiltak for å tilpasse regelverket til elektronisk saksbehandling. På de fleste av disse områdene anbefales det at det arbeides videre med problemstillingene som er skissert i denne rapporten. Dette arbeidet forutsettes iverksatt av det eller de organ som har regelverkansvaret på vedkommende område.

Kapitlet inneholder videre noen råd til den som gjør bruk av eller som tenker på å anskaffe elektroniske saksbehandlingssystemer. Disse rådene tar utgangspunkt i områder der rapporten viser at det kan oppstå problemer i forhold til regelverket når en benytter elektronisk saksbehandling. I tillegg er det angitt noen generelle forhold en bør være oppmerksom på ved bruk av elektronisk saksbehandling. Råd/anbefalinger som retter seg mot brukerne, er satt i en ramme.

8.1 Kompetanseheving

De siste tiårene har vist at IT-utviklingen går meget fort. Det er ingen grunn til å tro at dette vil forandre seg med det første. Det er ingen dristig spådom at IT i fremtiden vil tas i bruk på stadig flere områder og vil bli brukt til enda flere oppgaver. En bør være svært varsom med å anta at informasjonsteknologien utvikler seg i et vakuum uavhengig av, og uten å påvirke eksisterende rammevilkår. Som ved all annen utvikling og nyskaping kan det oppstå et behov for å styre eller påvirke denne utviklingen ved hjelp av lover og forskrifter. Denne rapporten er et eksempel på at elektronisk saksbehandling vil være ett område der utviklingen sannsynligvis ganske raskt vil kreve modifikasjoner i dagens regelverk. Det vil etter all sannsynlighet oppstå nye behov for endringer eller tilpasninger i regelverket etter hvert som IT tas i bruk på nye områder innenfor forvaltningen.

IT er et komplekst og til dels komplisert område i rask utvikling. Det setter høye krav til kompetanse hos regelverkutviklerne/-forvalterne. Arbeidet med denne rapporten har vist at det innenfor forvaltningen er et stort behov for kompetanseheving på området jus/IT. Det foreslås derfor at det iverksettes tiltak for å bygge opp nødvendig kompetanse på dette området. Slike tiltak kan dels være å drive opplæring, og dels å etablere et tettere samarbeid med miljøer som har kompetanse på området. Det vil også være viktig for forvaltningen at den kompetansen som finnes i enkelte etater eller hos enkelte personer i forvaltningen, kommer større deler av forvaltningen til gode.

8.2 Elektronisk kommunikasjon

Digitale signaturer vil være av sentral betydning for å utvide mulighetene for en vid adgang for borgerne til elektronisk kommunikasjon med forvaltningen. Det bør utredes hvordan en kan etablere en praktisk ordning med digitale signaturer.

Det må kartlegges hvilke formkrav som påbyr bruk av papir, som kan erstattes med bestemmelser som tillater bruk av elektroniske dokumenter. Dette gjelder både der formkravet er knyttet direkte til papir og der formkravet er knyttet til en personlig underskrift. Dette arbeidet vil være av vesentlig betydning for å

kunne ta i bruk digitale signaturer, og dermed digital kommunikasjon, på et bredere område enn i dag. Dersom regelverket inneholder hindringer for å ta i bruk elektroniske dokumenter, vil en bare i begrenset grad kunne hente ut gevinstene ved å etablere en ordning med digitale signaturer. Det anbefales at arbeidet med å kartlegge regelverket på dette punktet påbegynnes straks. Det anbefales videre at arbeidet gjennomføres sektorvis, slik at regelverksforvalterne gjennomgår regelverket på sine respektive områder.

Det vil være umulig for forvaltningen å håndtere ethvert dataformat i kommunikasjonen med publikum. Det må tas stilling til hvordan en skal avgrense omfanget av hvilke formater som kan benyttes.

Det kan være vanskelig å oppbevare en sikker digital signatur over lang tid. Har virksomheten dokumenter som må kunne autentiseres med stor sikkerhet etter lang tid, bør en vurdere andre autentiseringsmekanismer.

Har virksomheten mulighet til å lese, eventuelt oversette de vanligste typene dokumentformat?

Det er ikke i alle sammenhenger rettslig sett nødvendig at et saksdokument er utstyrt med underskrift eller digital signatur. Vurder hvorvidt virksomheten mottar henvendelser der autentisering av avsender ikke er av avgjørende betydning.

8.3 Offentlighet og innsynsrett

Elektroniske postjournaler publisert over Internett vil øke borgernes muligheter for å orientere seg om forvaltningens virksomhet. På den annen side vil en øking av tilgjengeligheten av hvem som har kontakt med forvaltningen, kunne medføre problemstillinger av personvernmessig art. Det bør utredes hvordan en kan øke tilgjengeligheten av postjournaler samtidig som den enkeltes personvern ivaretas.

Ved elektronisk oppbevaring vil informasjon ved hjelp av liten ressursbruk kunne sorteres og hentes frem uavhengig av hvilke dokumenter informasjonen stammer fra. Dette gir mulighet for i større grad å løsrive offentlighetsloven fra dokumentbegrepet. Hvorvidt dette vil være hensiktsmessig bør vurderes nærmere. Det bør i denne sammenheng vurderes om en slik utvidet innsynsrett eventuelt bør omfatte alle typer offentlig informasjon, eller om det er områder der en slik utvidet sorteringsadgang vil kunne medføre uheldige konsekvenser.

Det offentlige bør tilstrebe at flest mulig, på en enkel og rimelig måte, kan sette seg inn i det offentliges virksomhet. Det bør derfor vurderes om det er visse typer offentlig informasjon borgerne bør ha tilgang til i elektronisk form, og om dette bør være en lovfestet rett. Særlig gjelder dette informasjon om regelverket.

Har virksomheten rutiner som sørger for at også saksdokumenter som er innkommet med e-post, fremkommer i den offentlige journalen?

Har virksomheten rutiner for å oppfylle begjæring om innsyn etter offentlighetsloven, forvaltningsloven og personregisterloven?

8.4 Taushetsplikt

De aller fleste forvaltningsorganer vil ha behov for bistand fra eksterne krefter for å reparere eller vedlikeholde utstyr og programvare som benyttes i virksomheten. Det gjelder også for utstyr og programmer som behandler taushetsbelagte opplysninger. Det kan reises tvil om taushetspliktreglene åpner for å gi eksterne konsulenter tilgang til taushetsbelagt informasjon. Det bør vurderes om det er nødvendig med endringer i de ulike taushetspliktbestemmelsene. I denne sammenheng bør det også vurderes om det vil være hensiktsmessig å opprette autorisasjon eller kontrollordninger for foretak som yter tjenester som innebærer at de må ha tilgang til taushetsbelagt informasjon.

Har virksomheten tilstrekkelig IT-sikkerhet? Er det foretatt en vurdering av risikoen for at uvedkommende skal få tilgang til taushetsbelagte opplysninger og hvilke skader dette vil medføre? Finnes det dokumenterte rutiner for å minske risikoen for taushetsbrudd?

Har virksomheten rutiner for å sikre at eksterne IT-medhjelpere undertegner taushetserklæring?

Hvilke krav stilles ellers til eksterne IT-medhjelpere?

8.5 Personvern

Når offentlige dokumenter lagres elektronisk, medfører det en økt mulighet for å gjøre informasjon lettere tilgjengelig for allmennheten. Geografisk avstand mister betydning, og det er enorme muligheter for å selektere informasjon ved å bruke små ressurser. Dette vil kunne innebære en styrking av de hensyn som ligger til grunn for offentlighetsloven, men vil samtidig kunne reise problemer i forhold til den enkeltes personvern. Med dette utgangspunktet må det klargjøres hvor grensene mellom offentlighet og personvern skal gå.

Elektroniske saksbehandlingssystemer har potensiale til å registrere store deler av den enkelte saksbehandlers hverdag. Det må tas stilling til hvilken informasjon som skal kunne registreres i et saksbehandlingssystem, og hvilken bruk som skal kunne gjøres av informasjonen.

Ordninger med digitale signaturordninger som forvaltes av tiltrodde tredjeparter kan gi mulighet for å registrere hvem som kommuniserer med hvem. Det må tas

stilling til i hvilke tilfeller slik informasjon skal kunne registreres, og hvilken bruk som skal kunne gjøres av den.

Har virksomheten de nødvendige konsesjonene fra Datatilsynet? Har virksomheten rutiner for å sikre konfidensialitet, kvalitet og tilgjengelighet av personopplysninger? Har virksomheten dokumenterte rutiner for å sikre at edb-logger ikke benyttes til andre formål enn administrasjon av systemet og oppklaring av sikkerhetsbrudd?

8.6 Arkiv

Det må avgjøres på hvilket format elektronisk lagret materiale skal overleveres til Riksarkivet.

Det bør vurderes en kortere avleveringstid enn 25 år på elektronisk lagret materiale. Det synes lite hensiktsmessig at den enkelte etat skal være ansvarlig for å holde elektronisk materiale tilgjengelig i lang tid etter at etatens behov for dokumentene er opphørt.

Har virksomheten dokumenterte rutiner for håndtering av saksdokumenter som sendes direkte til en saksbehandler? Registreres elektroniske saksdokumenter i den offentlige journalen? Har virksomheten dokumenterte rutiner for konvertering av gamle lagringsformater?

Vedlegg 1

Oversiktsscenario

Nedenfor finner du et scenario, en beskrivelse av en tenkt saksbehandling av en tilfeldig valgt sak i forvaltningen. Denne måten å gjennomføre saksbehandling på krever at vi har utviklet og etablert nødvendig infrastruktur, programmer og rutiner, samt kompetanse hos personalet, slik at saksbehandlingen kan gjennomføres på et akseptabelt nivå.

Behandling av konsesjonssak 22240000
Arne Bang Bangsen sitter hjemme om kvelden. Klokken nærmer seg 22. Han er i ferd med å avslutte utfyllingen av et søknadsskjema om konsesjon for sin nye fiskebåt. Konsesjonsskjemaet lå på Fiskeridirektoratets hjemmesider på Internett, og han overførte det til sin egen pc for noen timer siden. Han fyller ut det elektroniske skjemaet etter anvisning fra programmet som følger med. Data om hans enmannsforetak blir hentet automatisk fra Enhetsregisteret. Han supplerer selv med opplysninger om sin nye båt og fiskekvoten.

Når skjemaet er ferdig utfylt, starter Arne e-postprogrammet på pc'en sin. Han skriver en melding til Fiskeridirektoratet om at han nå oversender søknaden, og legger ved det elektroniske søknadsskjemaet. Deretter signerer han digitalt, krypterer meldingen og sender den til Fiskeridirektoratet.

Postmottakets Guri J. Jansen kommer på jobb neste dag klokken åtte. Hun slår på pc'en sin og åpner Fiskeridirektoratets elektroniske postkasse. Det ligger 35 meldinger i den. Disse har kommet til i løpet av ettermiddagen og natten. Den sjette meldingen hun åpner er fra Arne Bang Bangsen. Meldingen er kryptert, så hun må dekryptere den. Deretter må hun sjekke at meldingen virkelig kommer fra Arne Bang Bangsen. Ikke overraskende gjør den det! Så lenge dette systemet har vært i drift har det bare forekommet feil en håndfull ganger. Guri legger Arnes melding og alle andre meldinger hun har åpnet og verifisert i sin egen utkurv.

Fiskeridirektoratet har et elektronisk saksflytsystem. I dette systemet er det forhåndsdefinert saksgang for de ulike sakstypene direktoratet behandler. Når det legges dokumenter i medarbeidernes utkurv, blir saksflytsystemet aktivisert. Dokumenter som legges i postmottakets utkurver, blir overført til en medarbeider som registrerer dem. Meldingene og dokumentene legges i kø til det er ledig registreringskapasitet.

Arkivar Kari L. Landvik blir først ledig, og plukker opp Arnes søknad. Kari taster inn «Arne Bang Bangsen» og stikkord fra søknaden for å sjekke om det er relevante saker eller dokumenter i Fiskeridirektoratets elektroniske arkiv fra før. Hun finner Arne Bang Bangsens søknad om fiskekvote fra 1987. Ved å fylle ut registreringsbildet for saksmapper oppretter hun en elektronisk saksmappe. Hun henter frem skjermbildet for journalføring og registrerer Arnes melding og søknad hver for seg. De dokumentene som nå hører til saken, knyttes til saksmappen med en elektronisk lenke. I Fiskeridirektoratets system gjøres dette ved at Landvik klikker på dokumentene, drar dem opp til ikonet som viser saksmappen og slipper dem der. Også et standardskjema for konsesjonssaker lenkes til saksmappen. Saksmappen lenkes sammen med Arnes 1987-sak.

Registreringen er fullført, og hun starter prosessen «konsesjon» i saksflytsystemet og legger pekeren til saksmappen i utkurven sin.

Saksflytsystemet styrer nå saken etter den predefinerte saksgangen for konsesjonsbehandling. Alle innkomne dokumenter går først til avdelingsleder Trym S. Stiansen, eller hans stedfortreder. Klokken 9.15 begynner han å gjennomgå innkurven sin. For å unngå dobbeltlagring av dokumenter og usikkerhet om hvilken versjon som er den siste, er det bare pekere til arkivdokumentene som distribueres til saksbehandlere og ledere. Pekeren til Arne Bang Bangsens sak ligger først. Stiansen dobbeltklikker på den og saksmappen vises på skjermen hans. Stiansen ser raskt gjennom meldingen og søknaden. Han ser at Arne Bang Bangsen påberoper seg spesielle egenskaper ved båten for å få konsesjon. Han noterer noen anvisninger om hvordan dette skal håndteres i saksmappens felt for kommentarer. Han husker med gru på den første tiden de hadde dette systemet. Da var det bare plass til tre linjer med merknader. Den nye versjonen de har i dag, utvider feltet etter som han skriver.

Ved å legge pekeren i utkurven ville saken igjen blitt styrt videre av saksflytsystemet, og gått til første ledige saksbehandler i seksjon for fiskebåter. Stiansen vet imidlertid at Kyrre K. Lubben i fiskebåtseksjonen er spesialist på katamaraner og vil kunne behandle denne saken best og raskest. Stiansen bruker saksflytsystemets funksjoner for manuell saksfordeling. Denne overstyrer den automatiske gangen i saken, og saken blir dirigert til Kyrre K. Lubben. Pekeren til saken legges i innkurven til Kyrre.

Kyrre K. Lubben sitter på kontoret sitt med lukket dør og røyker dagens første rullings. Det etter hvert så velkjente dampbåtulet fra saksflytsystemet kaller ham til pliktene. Han stumper røyken og åpner innkurven. Der finner han pekeren til saken til Arne Bang Bangsen. Han henter saksmappen og skriver inn sine egne initialer i saksbehandlerfeltet. Kyrre ser gjennom saken, henter opp den tidligere saken og blar gjennom dokumentene på skjermen. Han starter nettlosen sin, slår opp i Fiskeridepartementets sentrale database over fiskebåter og henter noen data derfra. Informasjonen lagrer han i et dokument som han åpner i tekstbehandleren sin. For å spare tid har de nå fått lagt inn de vanligste beregningene som ikoner han kan klikke på ved behov. Han legger inn de aktuelle tallene, klikker på ikonet, og resultatet dukker opp i dokumentet. Han sammenlikner resultatene med Arnes søknad ved å stille dokumentene ved siden av hverandre på skjermen. Deretter lagrer han dokumentet i det elektroniske saksarkivet. Når han ber tekstbehandlingssystemet om å lagre, dukker et forenklet registreringsbilde opp som må fylles ut før dokumentet kan lagres.

Lubben ringer til byråsjef Gerd H. Oppesen i Fiskeridepartementet og diskuterer noen generelle spørsmål knyttet til regelverket for konsesjoner med henne. Mens han snakker, noterer han på et papirark som ligger ved siden av pc'en. Etter avsluttet samtale legger Kyrre arket i skanneren ved siden av pc'en. Notatene hans dukker opp på skjermen som et elektronisk dokument. Han registrerer også dette dokumentet ved hjelp av det forenklede registreringsskjemaet og lagrer.

Det er noen spesielle elementer i søknaden til Arne Bang Bangsen som Kyrre vil diskutere med sin kollega Bernt G. Lupsk, seksjonens ekspert på fangstberegning. Lupsk har hjemmekontor på småbruket sitt i Ytre Enfold. Kyrre ringer Bernt og ber om en «Globalt vindu»-samtale. De starter hver på sin side et program for dette. Programmet gjør det mulig for Bernt å se søknaden til Arne Bang Bangsen på sin pc-skjerm mens han snakker i mikrofonen og hører

stemmen til Kyrre i hodetelefonen. De styrer hver sin markør i dokumentet. De snakker om et bestemt felt i søknaden der dataene ikke stemte med Kyrres beregninger. Bernt G. Lupsk peker på et annet felt i søknaden og sier at divergensen har sammenheng med opplysningene der. Kyrre ser feilen og takker for hjelpen. De avtaler et møte i en annen sak neste mandag. Bernt legger avtalen inn i begges kalendere.

Kyrre kan nå skrive utkast til svar på søknaden til Arne Bang Bangsen. Han utfører oppgaven «vedtak», som bl.a. henter frem den rette dokumentmalen. Saks- og referanseopplysninger blir automatisk overført til dokumentet fra saksmappen og det innkomne dokumentet (søknaden fra Arne Bang Bangsen). Kyrre ferdigstiller vedtaksdokumentet ved å klippe inn noe tekst fra andre dokumenter og skrive inn resten. Vedtaksdokumentet registreres og lagres. Han gjør seg ferdig med oppgaven «vedtak». Saksflytsystemet sender så pekeren til saksmappen tilbake til Stiansen, som skal se på saken. Avdelingsleder Stiansen har noen kommentarer til utkastet. Han utfører oppgaven «kommentar», som lager en kopi av utkastet, og arbeider på kopien i revisjonsmodus. Her blir forslagene til tillegg i teksten markert med streker i margen og rød skrift, og forslagene til utgående tekst blir blå, slik at det er lett å se dem. Revidert kopi blir automatisk lagret i det elektroniske arkivet lenket til Kyrre K. Lubbens opprinnelige utkast og til saksmappen. Kyrre godtar Stiansens rettelser, fjerner revisjonsmodusen slik at markeringene forsvinner og lagrer dokumentet revidert. Kyrre K. Lubbens navn er påført svarbrevet. Kyrre legger pekeren i utkurven sin. Saksflytsystemet legger pekeren i avdelingslederens innkurv. Stiansen hører sin yndlingsarie fra pc'en. Den varsler om at det ligger dokument for undertegning i innkurven. Han ser raskt over brevet og påfører sin digitale signatur. Han utfører oppgaven «ekspedisjon» som resulterer i at pekeren til saken havner i arkivarens innkurv. Kari i arkivet sjekker ved hjelp av dokumentnummeret om brevet er journalført riktig i arkivet. Hun låser dokumentet ved å endre tilgangen til bare leseadgang. Brevet til Arne Bang Bangsen krypteres og Stiansens signatur verifiseres. Kari sender så det signerte og krypterte svarbrevet som vedlegg til en e-postmelding til Arne Bang Bangsen. Arne ser i postkassen sin rett etter nyhetene på TV56. Han ser meldingen fra Fiskeridirektoratet og dobbeltklikker på den, og verifiserer ved hjelp av den digitale signaturen at meldingen virkelig kommer fra direktoratet. Etter å ha dekryptert meldingen kan han lese Fiskeridirektoratets vedtak. Han løper til kjøleskapet og åpner en pils!

Vedlegg 2

Digitale signaturer og tiltrodde tredjeparter

Digitale signaturer og kryptering

En digital signatur har i likhet med den personlige underskriften som hovedfunksjon å verifisere at en melding kommer fra den som er angitt som avsender. En digital signatur kan i tillegg til å autentisere avsenderen ha den egenskapen at den avslører om noen har endret meldingen etter at den ble signert.

Moderne digitale signaturer bygger på en teknologi som kalles asymmetrisk nøkkelkryptografi. Digitale signaturer behandles ofte i sammenheng med kryptering. Det er viktig å ha klart for seg at selv om digitale signaturer og asymmetrisk kryptering fungerer etter de samme prinsippene, har de to helt forskjellige funksjoner. Det er fullt mulig å signere en melding uten å kryptere den og motsatt.

For å kunne forstå hvordan en digital signatur basert på asymmetrisk nøkkelkryptografi funksjonerer, må en vite litt om kryptering. Kryptering betyr å omdanne klartekst til kode. Dette gjøres ved å omforme klarteksten gjennom bruk av en algoritme og en kodenøkkel. En algoritme er en beskrivelse av den regneoperasjonen som benyttes for å kryptere dokumentet. En svært enkel måte å kryptere en tekst på kan være å forskyve alle bokstavene 3 plasser til høyre i alfabetet slik at A blir D, D blir H osv. Algoritmen er da beskrivelsen av hvordan en har forvansket teksten, altså flytt bokstavene X plasser til høyre i alfabetet, mens kodenøkkelen er verdien som benyttes for X, i dette tilfelle 3.

Når teksten er kastet rundt på denne måten, vil den bli uleselig for en uvedkommende. For den som kjenner algoritmen og kodenøkkelen som er benyttet, vil det imidlertid være en enkel sak å dekryptere meldingen ved å forskyve bokstavene 3 plasser til venstre.

Når kryptering skjer ved hjelp av datamaskiner, består koden av meget kompliserte algoritmer og lange kodenøkler, noe som gjør det svært vanskelig å knekke koden. Prinsippet er likevel i og for seg det samme som i bokstavbyttekoden.

Asymmetrisk nøkkelkryptografi betyr at det benyttes en nøkkel til krypteringen og en annen til dekrypteringen. Nøklene forholder seg til hverandre på den måten at når en melding er kryptert ved hjelp av den ene nøkkelen, kan den bare dekrypteres ved hjelp av den andre og omvendt. En av nøklene er det bare parten selv som kan kjenne til. Denne kalles den «private nøkkelen». Den andre nøkkelen kan være åpent tilgjengelig. Denne kalles for den «offentlige nøkkelen». Dette betyr at:

- det som lar seg dekryptere med den offentlige nøkkelen, bare kan ha vært kryptert med den private nøkkelen
- det som er kryptert med den offentlige nøkkelen, bare kan dekrypteres med den private nøkkelen

Når en avsender skal signere et dokument, bruker han den private nøkkelen. Signeringen skjer ved at datamaskinen regner ut en såkalt hash-verdi for

dokumentet. Hash-verdien er en tallverdi som regnes ut på bakgrunn av tegnene i meldingen – hvor mange de er, hvilke de er og hvor de er plassert. Alle dokumenter vil således ha en bestemt hash-verdi, som vil endres dersom dokumentet endres. Selv en liten endring i dokumentet vil føre til en stor endring av hash-verdien. Når hash-verdien er beregnet, blir den kryptert ved hjelp av avsenders private kodenøkkel. Den eneste måten å dekryptere hash-verdien på er nå å bruke avsenderens offentlige kodenøkkel. Den krypterte hash-verdien sendes så til mottaker sammen med meldingen. Når meldingen kommer frem beregner mottagers datamaskin på nytt hash-verdien av dokumentet. Deretter blir den krypterte hash-verdien som er sendt sammen med dokumentet, dekryptert ved hjelp av avsenders offentlige nøkkel. Dersom de to hash-verdiene stemmer overens, vet mottakeren helt sikkert at dokumentet kommer fra avsenderen og at ingen har endret på det underveis.

Sikkerheten i en digital signatur avhenger av to hovedfaktorer. Den tekniske sikkerheten avhenger først og fremst av hvor avansert algoritmen som benyttes i krypteringen er og hvor lang kodenøkkel som benyttes. Det er allment anerkjent at de krypteringsalgoritmene som i dag benyttes i digitale signaturer, er praktisk talt umulig å knekke dersom kodenøkkelen er lang nok. En kan dermed trygt gå ut fra at en digital signatur i praksis ikke lar seg forfalske ved å knekke krypteringen. Den andre avgjørende faktoren for sikkerheten av en digital signatur er at den private nøkkelen ikke blir kjent for andre. Dersom en annen person kjenner den private kodenøkkelen, vil vedkommende kunne gi seg ut for å være nøkkeleieren. Som nevnt innledningsvis kan en digital signatur også beskytte dokumentet (informasjonen) mot manipulasjon under transport og lagring. En må imidlertid være oppmerksom på at en digital signatur ikke hindrer noen i å endre informasjonen, men den avslører om en slik endring er gjort. Videre er det verdt å være oppmerksom på at digitale signaturer ikke forvrenger selve meldingen på noen måte. Den fremstår som fullt lesbar under hele forsendelsen. Den digitale signaturen kan sies å være en «tilleggsinformasjon» om avsender og dokumentet. Dersom en ønsker å sikre meldingen mot innsyn fra uvedkommende, må meldingen krypteres. Hvis en benytter seg av asymmetrisk nøkkelkryptering til krypteringen av selve meldingen, skjer dette ved at avsenderen bruker mottakerens offentlige nøkkel til å kryptere selve meldingsteksten. Mottakeren kan da bruke sin private nøkkel til å dekryptere meldingen.

Tiltrodd tredjepart

Et annen problemstilling ved digitale signaturer er å innrette seg slik at en kan være sikker på at den offentlige nøkkelen virkelig tilhører vedkommende den utgir seg for å tilhøre. Digitale signaturer løser ikke identifikasjonsproblemet dersom avsenderen kan få mottakeren til å tro at den offentlige nøkkelen han presenterer tilhører en annen. A kan for eksempel utgi seg for å være B og sende en signert melding til M. Sammen med meldingen sender han en offentlig kodenøkkel som han utgir for å tilhøre B. Dersom M benytter den medsendte nøkkelen for å bekrefte signaturen, vil det for ham se ut som om meldingen kommer fra B.

Dette kan løses ved at partene tar kontakt med hverandre og utveksler nøkler før meldingsutvekslingen tar til. Hvis partene ikke kjenner hverandre fra før, må de legitimere seg for hverandre, slik at de er sikre på at den andre er den han utgir seg for å være. Problemet med en signaturordning som baserer seg på

nøkkelutveksling direkte mellom partene, er at partene må gjøre avtale på forhånd. En kan f.eks. ikke sende en melding direkte til sitt trygdekontor uten først å ha bekreftet sin offentlige kodenøkkel.

En måte å løse dette problemet på er gjennom medvirkning av en såkalt Tiltrodd Tredje Part (TTP). TTP er en uavhengig instans som administrerer de offentlige kodenøklene. Dette må være en instans som har en slik tillit at TTP'en kontrollerer identiteten til den som ønsker kodenøkler før de utstedes til vedkommende. Den private nøkkelen gis til eieren, mens TTP holder oversikt over de offentlige nøklene. En forutsetning for at dette systemet skal virke er selvfølgelig at TTP'en nyter tillit hos alle parter i en meldingsutveksling.

Administrasjonen av de offentlige nøklene kan skje på to måter. TTP kan opprette et register over alle offentlige nøkler. Dette registeret vil ha såkalt positiv troverdighet. Det vil si at den nøkkelen som i registeret står registrert på A, virkelig tilhører ham. Når mottakeren får en melding fra A tar han derfor kontakt med registeret og får utdelt A sin nøkkel. As nøkkel signeres av TTP, slik at mottaker kan være sikker på at nøkkelen virkelig kommer fra TTP.

Mottaker bruker så denne nøkkelen til å verifisere signaturen. Når mottakeren først har fått As nøkkel, kan han lagre den hos seg selv og bruke den om igjen senere. Problemet med dette er at han ikke vil fange det opp dersom A bytter kodenøkkel. Dette kan A bli nødt til å gjøre hvis han mister sin private nøkkel eller at uvedkommende får tilgang til den. Det er da svært viktig at A melder fra til TTP straks. Dersom andre en A kjenner til As private kodenøkkel vil disse kunne utgi seg for å være ham. TTP vil derfor utferdige nye nøkler til A. Dersom B etter dette tidspunkt bruker den kopien av As nøkkel som han har liggende hos seg selv til å verifisere As signatur, vil han ikke oppdage at det er en annen som gir seg ut for å være A. Det er derfor viktig at TTP har gode tilbakekallingsrutiner for kodenøklene.

Den andre måten å innrette systemet på er at TTP utsteder en nøkkelsertifikat for A's nøkkel. Nøkkelsertifikatet er A sin offentlige nøkkel signert av TTP. A kan dermed sende nøkkelsertifikatet sammen med meldingen til mottakeren. Mottaker kan dermed få bekreftet TTP sin signatur og dermed være sikker på at den tilsendte nøkkelen virkelig tilhører A.

Ordninger med tiltrodde tredjeparter innebærer i og for seg bare at identifikasjonsproblemet forskyver seg til å gjelde identifisering av TTP'en. Dette kan imidlertid løses ved såkalt sertifisering og kryss-sertifisering. Dette behandles ikke her.

Lagring av digitale signaturer

Ofte er det ikke nok for en mottaker bare selv å være sikker på at et dokument kommer fra A, han må også kunne bevise det for andre. Behovet for å kunne bevise det kan være til stede i mange år etter at dokumentet ble utferdiget. Hvis en som eksempel tenker seg et elektronisk testament, vil det ikke være nok at den som mottar testamentet er sikker på at det kommer fra testator. Det viktigste er at en i det senere arveoppgjør kan avgjøre om testamentet ble signert av testator. Dette vil ikke uten videre være enkelt dersom det går lang tid fra testamentet utferdiges til arveoppgjøret finner sted. Testator kan ha byttet kodenøkler flere ganger i denne perioden. Problemet blir da å kunne dokumentere hva som var testators offentlige kodenøkkel på det tidspunktet

testamentet ble signert. Dette betyr med andre ord at en for å kunne bevise testamentets ekthet må oppbevare det signerte testamentet, den offentlige kodenøkkelen og en bekreftelse på gyldigheten av kodenøkkelen på det tidspunktet testamentet ble signert. Dette vil nødvendigvis sette strenge krav til rutiner og tekniske løsninger for arkivering for digitale signaturer som skal oppbevares over lang tid.

Ikke-benekting

En TTP kan ha mange roller i tillegg til nøkkelhåndteringsfunksjonen som er beskrevet ovenfor. Èn slik funksjon er å opptre som en notarius publicus i forhold til meldingsutveksling mellom brukerne. Dette gjøres ved at TTP'en logger og overvåker meldingsutveksling mellom gitte parter. En slik logg vil gi en oversikt over avsendelse og mottak av meldinger mellom partene, og dermed gjøre det mulig å fastslå med relativt stor sikkerhet om en part har mottatt en melding eller ikke. Siden hovedhensikten med en slik notarius publicus funksjon er å gjøre det vanskelig for mottaker å nekte for at han har mottatt meldingen eller for avsender å nekte for at han har sendt den, kalles tjenesten ofte for «ikke-benekting». Ordningen kan sammenliknes med å sende et rekommandert brev. Siden denne funksjonen er mye lettere å bruke på elektronisk post enn på ordinær post, er det grunn til å anta at det vil bli sendt flere «rekommanderte» elektroniske meldinger enn hva tilfellet er med ordinære brev i dag. Denne type logging kan imidlertid reise personvernmessige problemstillinger. Disse er berørt i kapitlet om personvern.

REFERANSER

Tittel:	Elektronisk saksbehandling – noen juridiske problemstillinger ved elektronisk dokumenthåndtering
Forfatter(e):	Michal Wiik Johansen
Statskonsults rapportnummer:	1998:13
Prosjektnummer:	180.02
Prosjektnavn:	Elektronisk saksbehandling
Prosjektleder:	Michal Wiik Johansen
Oppdragsgiver(e):	Forvaltningen generelt
Resymé:	Offentlig saksbehandling styres av en rekke regler. Ved overgangen fra papir til elektronisk saksbehandling er det derfor viktig å kartlegge hvilke regler som kan være til hinder for elektronisk saksbehandling, for så å vurdere om disse reglene bør endres.
Arbeidsområde:	Informasjonsteknologi
Emneord:	Elektronisk saksbehandling, juss
Dato:	September 1998
Sider:	58 pluss vedlegg
Pris:	kr 100,-
Utgiver:	Statskonsult Direktoratet for forvaltningsutvikling Postboks 8115 Dep 0032 OSLO