

e-signator og formkrav i lovgivningen

*delbetænkning afgivet af Justitsministeriets udvalg
om retsvirkningerne af digital signatur m.v.*

Betænkning nr. 1400

København 2000

Betænkning om e-signatur og formkrav i lovgivningen

Købes hos boghandleren
eller Statens Information
Postboks 1300, 2300 København S
Tlf. 33 37 92 28, Fax 33 37 92 80
100 kr. inkl. Moms

Tryk: Herrmann & Fischer

Publikationen kan hentes på Justitsministeriets hjemmeside
www.jm.dk/publikationer/bet1400

ISBN 87-601-8953-3

ISBN 87-601-8954-1 (Internet)

Indholdsfortegnelse

Kapitel 1. Indledning	7
1.1. Udvalgets nedsættelse og kommissorium	7
1.2. Udvalgets sammensætning	11
1.3. Udvalgets beslutning om at afgive delbetænkning	12
1.4. Sammenfatning af udvalgets overvejelser	14
Kapitel 2. De nye teknikker – digital kommunikation og elektronisk signatur	17
2.1. Indledning	17
2.2. Digitale dokumenter	18
2.3. Elektronisk signatur	24
2.3.1. Indledning	24
2.3.2. Kryptering	26
2.3.3. Certifikater og nøglecentre	31
2.3.4. Forskelle og ligheder mellem håndskrevne underskrifter og elektroniske signaturer	33
2.3.5. Kryptering med henblik på hemmeligholdelse	36
Kapitel 3. Den internationale udvikling	39
3.1. Indledning	39
3.2. EU	41
3.2.1. Direktivet om en fællesskabsramme for elektroniske signaturer	41
3.2.2. Direktivet om visse retlige aspekter af informationssamfunds- tjenester, navnlig elektronisk handel, i det indre marked	43
3.3. FN	44
3.3.1. UNCITRAL's "Model Law on Electronic Commerce"	44
3.3.2. UNCITRAL's forslag til "Uniform Rules on Electronic Signatures"	48

3.4. Initiativer i andre lande	49
3.4.1. Sverige	49
3.4.2. Norge	52
3.4.3. Finland	55
3.4.4. Tyskland	60
3.4.5. UK	62

Kapitel 4. Hittidige danske overvejelser om brugen af digital kommunikation mv.

65

4.1. Ønsket om at fremme brugen af digital kommunikation – regeringens redegørelse til Folketinget om sikker digital kommunikation	65
4.2. Forskningsministeriets udkast til lovforslag om digital signatur fra 1998	66
4.3. Lov nr. 417 af 31. maj 2000 om elektroniske signaturer	69
4.3.1. Lovens formål og anvendelsesområde	70
4.3.2. Almindelige certifikater og kvalificerede certifikater	72
4.3.3. Krav til nøglecentre	72
4.3.4. Tilsyn og anmeldelse	73
4.3.5. Nøglecentrenes erstatningsansvar	74
4.3.6. Sikre signaturgenereringssystemer	75
4.3.7. Anvendelse af elektronisk signatur på områder med formkrav	75
4.4. Forskningsministeriets pilotprojekter, Det Digitale Danmark og forskningsministerens netværksredegørelse til Folketinget	77
4.4.1. Pilotprojekter	77
4.4.2. Det Digitale Danmark	78
4.4.3. Netværksredegørelse til Folketinget	80

Kapitel 5. Formkrav og digital kommunikation

83

5.1. Indledning	83
5.2. Gennemgang af lovgivningen på udvalgte ministerområder	84
5.2.1. Erhvervsministeriet	85
5.2.2. Sundhedsministeriet	88
5.2.3. Indenrigsministeriet	91

5.2.4. Justitsministeriet	95
5.3. Inddeling efter formål	102
5.3.1. Retsvirkninger knyttet til besiddelsen af et dokument	102
5.3.1.1. Negotiabilitet	102
5.3.1.2. Dokumentation for identitet mv.	105
5.3.1.3. Dokumentation for en ret, tilstand mv.	106
5.3.2. Beskyttelses- eller advarselsfunktion (f.eks. forbrugerbeskyttelse mv.)	109
5.3.3. Bevisfunktioner	112
5.3.3.1. Erklæringer på tro og love	112
5.3.3.2. Sikkerhed for, at en meddelelse stammer fra en bestemt person, at denne person er sin fornuft mægtig mv.	114
5.3.3.3. Bevis for, at en meddelelse er modtaget eller godkendt, eller at modtageren har været til stede på et bestemt sted	116
5.3.3.4. Fastlæggelse af tidspunktet for modtagelse	118
5.3.3.5. Sikring af bevis over tid	119
5.3.4. Formkrav, som har til formål at indskærpe alvor/højtidelighed	121
5.3.5. Administrativt begrundede formkrav	122
Kapitel 6. Behovet for et lovgivningsinitiativ og udformningen heraf	127
6.1. Er der behov for et lovgivningsinitiativ?	127
6.2. Hvordan skal formkrav forstås?	129
6.2.1. Almindelige bemærkninger	129
6.2.2. Skriftlighedskrav	131
6.2.3. Underskriftskrav	133
6.2.4. Udvalgets overvejelser om forståelsen af formkrav i lovgivningen	135
6.3. Valget af lovgivningsmodel	141
6.3.1. Indledning	141
6.3.2. Kan formkravene ændres ved én eller flere generelle regler?	145
6.3.3. Metoder til ændring af formkrav i lovgivningen	149
6.3.3.1. Særskilte lovændringer	150

6.3.3.2. En generel bemyndigelseslov	150
6.3.3.3. En mellemløsning	151
6.3.3.4. Udvalgets forslag	155
6.3.4. Tilrettelæggelsen af det videre arbejde	158
6.4. Retningslinier ved ændring af formkrav	161
6.4.1. Indledning	161
6.4.2. Gennemgang af lovgivningen	161
6.4.3. Hvilke bestemmelser skal ændres?	162
6.4.3.1. Kan formålet opfyldes ved digital kommunikation?	163
6.4.3.2. Behov for identifikation af afsenderen	164
6.4.3.3. Administrative og økonomiske forhold	164
6.4.3.4. Arkivering og bevisspørgsmål	165
6.4.4. Metode ved ændring af reglerne	167

Bilag

1. Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer	173
2. Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("Direktivet om elektronisk handel")	185
3. UNCITRAL's Model Law on Electronic Commerce with Guide to Enactment	203
4. Lov nr. 417 af 31. maj 2000 om elektroniske signaturer	251

Kapitel 1. Indledning

1.1. Udvalgets nedsættelse og kommissorium

Den 3. november 1998 nedsatte Justitsministeriet et udvalg om retsvirkningerne af anvendelsen af digital signatur mv.

Udvalget fik følgende kommissorium:

” 1. Digital kommunikation mellem borgere, virksomheder, myndigheder m.v. foregår i stadigt stigende omfang, bl.a. som supplement til eller i stedet for kommunikation på papir. Hidtil har det været det mest almindelige, at digital kommunikation foregår i net med adgang for en begrænset kreds, hvor de involverede kender hinanden og på forhånd har aftalt, hvordan og med hvilken virkning kommunikationen skal foregå. Fremover forventes kommunikation via åbne net imidlertid at blive væsentlig mere udbredt.

2. I december 1997 fremlagde regeringen en redegørelse for Folketinget om sikker digital kommunikation. I redegørelsen formuleres et af de overordnede mål på dette område således, at der skal være mulighed for, at man i praksis kan anvende denne kommunikationsform på alle områder, hvor digitale meddelelser kan opfylde de samme funktioner som papirdokumenter. Under redegørelsesdebatten i januar 1998 tilsluttede et bredt flertal i Folketinget sig denne målsætning.

Ved digital kommunikation opstår der bl.a. spørgsmål om, hvordan der kan opnås tilstrækkelig sikkerhed for, at en meddelelse faktisk stammer fra den angivne udsteder, og at meddelelsens indhold ikke er ændret efter, at den er afsendt.

I lyset heraf og på baggrund af den nævnte redegørelse har Forskningsministeriet udarbejdet et udkast til et lovforslag om digital signatur baseret på såkaldt public key-kryptering, dvs. anvendelsen af private og offentlige "nøgler", der består af hver sin algoritme, som bygger på to meget store primtal og har en indbyrdes matematisk sammenhæng. Med denne teknik kan digitale meddelelser kodes ved hjælp af et edb-program og afsenderens private signaturnøgle, således at den offentlige nøgle bruges til at afkode meddelelsen.

Ved public key-kryptering er der behov for, at nogen - en såkaldt troværdig tredjepart - står inde for, at den offentlige nøgle kommer fra den angivne nøgleindehaver. Et væsentligt element i Forskningsministeriets lovudkast var på denne baggrund nogle regler om offentlig autorisation af "nøglecentre", som skal kunne bekræfte, at en offentlig nøgle kommer fra en bestemt person. Lovudkastet indeholdt bl.a. tekniske og organisatoriske regler om nøglecentrenes virksomhed samt regler om "spærring" af signaturnøgler, tidsmæssig begrænsning af, hvor længe en privat signaturnøgle kan anses for sikker, og begrænsninger i, hvilke retshandler m.v. nøglerne må bruges til.

Lovudkastet indeholdt herudover visse generelle regler om retsvirkningerne af at anvende digitale meddelelser med digital signatur. Reglerne drejede sig bl.a. om mulighederne for at opfylde skriftlighedskrav m.v. i lovgivningen med digitale meddelelser, som er påført en digital signatur. Reglerne drejede sig endvidere bl.a. om retsstillingen mellem afsenderen og modtageren af en digital meddelelse i visse særlige tilfælde, dels hvor en signaturnøgle er "spærret", dels hvor tidsgrænsen for en signaturnøgle er udløbet, dels hvor signaturnøglen anvendes uden for et på forhånd fastlagt anvendelsesområde.

3. Forskningsministeriets lovudkast har i foråret 1998 været til høring hos berørte myndigheder og organisationer m.v.

I forbindelse med høringen over det nævnte lovudkast blev der peget på, at bl.a. spørgsmålet om retsvirkningerne af at anvende digitale meddelelser med digital signatur burde overvejes nærmere af et sagkyndigt udvalg, inden der eventuelt tages initiativ til lovgivning herom.

Justitsministeriet har på denne baggrund i samråd med Forskningsministeriet besluttet at nedsætte et udvalg, der skal vurdere spørgsmålet om lovregulering af digitalt signerede meddelelsers retsvirkning. Det bemærkes, at spørgsmålet om de strafferetlige aspekter ved digital kommunikation behandles i Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet.

Forskningsministeriet agter at fremsætte et lovforslag for Folketinget om de organisatoriske og tekniske rammer for offentlig autorisation af nøglecentre, der har til opgave at fungere som " troværdig tredjepart", jf. ovenfor. Lovforslaget vil endvidere indeholde regler om nøglecentrenes ansvar over for brugerne og i den forbindelse formentlig også regler om spærring af nøgler, begrænsning af det tidsrum, hvor en privat nøgle kan anses for at være sikker, og begrænsninger i nøglernes anvendelsesområde. Lovforslaget vil blive fremsat, når der er fornøden afklaring af indholdet af et direktiv om elektroniske signaturer, som for tiden drøftes i EU, jf. nedenfor.

Denne lovgivning vil have til formål at skabe det fornødne tekniske og organisatoriske grundlag for udbredelsen af en mere sikker digital kommunikation i åbne net.

3.1. På den anførte baggrund og i lyset af den samfundsmæssige interesse i at fremme brugen af sikker digital kommunikation er det en hovedopgave for udvalget at vurdere behovet for, at der lovgives om anvendelsen af digitale meddelelser med digital signatur i forbindelse med formkrav og andre retsregler, som knytter retsvirkninger til, at en meddelelse er skriftlig og/eller underskrevet. En eventuel regulering kan enten udformes som generelle lovregler, dvs. lovregler, der omfatter hele eller større dele af lovgivningen, eller - som der allerede er eksempler på - som lovregler, der regulerer brugen af digital kommunikation på et eller nogle enkelte områder for sig. Findes der at være behov for lovgivning, bør udvalget vurdere fordele og ulemper ved de nævnte former for regulering. Finder udvalget det mest hensigtsmæssigt, at lovgivning gennemføres på hvert område for sig, bør udvalget søge at opstille nogle overordnede principper for udformningen af sådanne lovregler.

Lovgivningen indeholder flere tusind af de ovenfor nævnte formkrav m.v., og det må antages, at disse bestemmelser i en del tilfælde ikke kan fortolkes således, at der kan anvendes digitale meddelelser. Udvalget bør i sine overvejelser bl.a. tage udgangspunkt i, at krav om skriftlighed og/eller underskrift kan have en række forskellige formål, f.eks. hensynet til bevissikring, hensynet til at skabe klarhed (vished) eller hensynet til at lette administrative procedurer m.v. Formålet kan f.eks. også være at gøre de involverede parter særligt opmærksomme på visse forhold. Formkrav kan endvidere have betydning ved anvendelsen af andre retsregler som f.eks. registerretlige og arkivretlige regler og regler om aktindsigt. En række formkrav i lovgivningen følger i øvrigt af internationale forpligtelser.

Udvalget bør endvidere tage udgangspunkt i de forskelle, der er mellem digitale meddelelser og meddelelser på papir. Blandt disse forskelle kan nævnes, at oplysninger, der alene foreligger i digital form, ikke har fysisk eksistens i samme forstand som oplysninger på papir. Ved papirdokumenter foreligger der et originalt fysisk eksemplar, mens dette ikke er tilfældet ved digital kommunikation. Papirdokumenter er umiddelbart læsbare, mens digitale meddelelser dels skal transformeres fra "maskinsprog" til læsbar form, dels kun kan læses ved anvendelse af bestemte edb-programmer. Oplysninger på papir gives ved hjælp af skrift på papiret, mens digitale oplysninger kan have flere forskellige repræsentationsformer, både med hensyn til lagringen (elektronisk, optisk m.v.) og med hensyn til fremtrædelsen (skærm billede, stemmesimulering m.v.). Ændring af indholdet af et papirdokument forudsætter et fysisk indgreb, som kan spores (f.eks. ved grafologisk undersøgelse), mens ændring af indholdet af en digital meddelelse kan ske ved en ikke umiddelbart synlig ændring af bit-mønstret. I modsætning til digitale data kan papirdo-

kumenter fysisk besiddes, og derfor kan papirdokumenter bl.a. være bærere af en rettighed og være umiddelbart anvendelige som bevis.

3.2. En anden hovedopgave for udvalget vil være at vurdere spørgsmålet om eventuel særlig lovgivning om de retlige konsekvenser i forholdet mellem afsenderen og modtageren, hvis en digital signatur anvendes, efter at signaturen er blevet "spærret", hvis signaturen anvendes uden for et på forhånd angivet anvendelsesområde, eller hvis en privat nøgles tidsgrænse er overskredet. Udvalgets eventuelle forslag til lovregler herom bør udformes i lyset af den lovgivning, som Forskningsministeriet vil fremsætte forslag om, jf. ovenfor.

3.3. De ovenfor under pkt. 3.1 nævnte forskelle mellem papirdokumenter og digitale meddelelser kan rejse en række andre spørgsmål af retlig karakter, som også har betydning for, hvilke retsvirkninger digitale meddelelser kan have. Udvalget bør navnlig overveje, om der ved digital kommunikation kan opstå særlige problemer med hensyn til anvendelsen af aftalelovens regler, bl.a. om virkningen af, at en meddelelse er kommet frem eller er kommet til modtagerens kundskab. Udvalget bør endvidere på baggrund af de aftaleretlige ugyldighedsregler overveje spørgsmålet om bevisbyrden for, at en digital meddelelse med digital signatur er falsk eller forfalsket.

3.4. I det omfang udvalget vil anbefale, at der gennemføres lovgivning, skal udvalget udarbejde forslag til lovregler eller eventuelt forslag til overordnede principper for udformningen af lovregler på de forskellige enkeltområder, jf. pkt. 3.1.

Udvalget anmodes om at fremme sit arbejde mest muligt, eventuelt ved afgivelse af delbetænkninger.

4. Det forudsættes, at udvalget i sine overvejelser inddrager de synspunkter, der er kommet til udtryk i høringssvarene vedrørende Forskningsministeriets lovudkast, jf. ovenfor.

Det forudsættes endvidere, at udvalget som grundlag for sine overvejelser indhenter oplysninger om retsstillingen og erfaringerne i andre lande, herunder de øvrige nordiske lande samt bl.a. Tyskland og Italien, hvor man for nylig har gennemført lovgivning om digital signatur.

Udvalget bør endvidere være opmærksom på det arbejde vedrørende regulering af elektronisk signatur og af elektronisk handel, som foregår i FN (UNCITRAL), OECD og andre internationale fora.

Udvalget skal særligt følge det igangværende arbejde i EU med Kommissionens forslag til direktiv om en fælles ramme for elektroniske signaturer. Dette direktivforslag, der er fremsat i maj 1998, indeholder både regler om de tekniske og organisatoriske rammer for elektronisk signatur og visse regler om retsvirkningerne af anvendelsen af elektroniske signaturer. Justitsministeriet vil løbende orientere udvalget om arbejdet med direktivforslaget med henblik på, at udvalgets synspunkter kan indgå ved fastlæggelsen af den danske regerings holdning til forslaget. ”

1.2. Udvalgets sammensætning

Udvalget har ved afgivelsen af denne delbetænkning følgende sammensætning:

Vicepræsident i Sø- og Handelsretten Michael B. Elmer (formand)

Advokat Stig Bigaard, Advokatrådet

Kontorchef Kim Brinckmann, Forskningsministeriet

Dommer Ove Dam, Den Danske Dommerforening

Kontorchef Tina Füssel, Finansrådet

Lovråd Lars Hjortnæs, Justitsministeriet

Fuldmægtig Morten Mølgaard Jensen, Erhvervsministeriet

Direktør Flemming Jensen, IT-Brancheforeningen

Kontorchef Åse Kogsbøll, Forsikring & Pension

Professor Peter Møgelvang-Hansen, Handelshøjskolen i København

Cand.jur. Anette Høyrup Petersen, Forbrugerrådet

Sekretariat:

Konsulent Svend Larsen, Justitsministeriet

Fuldmægtig Carsten Oppermann, Justitsministeriet

Fuldmægtig Claus Jakobsen, Forskningsministeriet

Den 11. juni 1999 indtrådte direktør Flemming Jensen, IT-Brancheforeningen i udvalget, og afløste herved konsulent Henrik Ørum, IT-Brancheforeningen, som medlem af udvalget. I juni 2000 udtrådte kontorchef Søren Sandfeld Jakobsen, Erhvervsministeriet, af udvalget og afløstes af fuldmægtig Morten Mølgaard Jensen, Erhvervsministeriet. Den 29. august 2000 indtrådte cand.jur. Anette Høyrup Petersen, Forbrugerrådet, i stedet for Mette Reissmann, Forbrugerrådet, som medlem af udvalget. Den 1. september 2000 afløste kontorchef Kim Brinckmann kontorchef Jane Eis Larsen som Forskningsministeriets medlem af udvalget.

1.3. Udvalgets beslutning om at afgive delbetænkning

Efter kommissoriet har udvalget to hovedopgaver. For det første er udvalget blevet anmodet om at overveje, om der er behov for at lovgive om anvendelsen af digital kommunikation og elektronisk signatur i forbindelse med formkrav i lovgivningen mv. For det andet skal udvalget overveje en række andre retlige spørgsmål, som opstår i forbindelse med anvendelsen af digital kommunikation og elektronisk signatur, bl.a. spørgsmålet om, hvorvidt der er behov for at lovgive om retsforholdet mellem afgiveren og modtageren af en digital meddelelse med elektronisk signatur, ligesom udvalget skal overveje en række andre retlige spørgsmål, som opstår i forbindelse med anvendelsen af digital kommunikation, bl.a. om anvendelsen af aftalelovens regler om, hvornår en meddelelse er kommet frem.

Selv om disse to hovedspørgsmål er udslag af samme problemstilling – de retlige konsekvenser af anvendelsen af digital kommunikation – hænger de dog ikke mere sammen, end at det er muligt at besvare dem hver for sig. Man kan således udmærket tage stilling til, om krav om skriftlighed mv. i lovgivningen kan eller skal kunne opfyldes ved brug af digital kommunikation, uden at det af den grund er nødvendigt samtidig at overveje de aftaleretlige konsekvenser af denne kommunikationsform.

Udvalget er endvidere blevet anmodet om at fremme sit arbejde mest muligt, og i udvalgets kommissorium peges der i den forbindelse på muligheden for, at udvalget afgiver delbetænkninger.

En delbetænkning om forståelsen af formkrav mv. vil efter udvalgets opfattelse kunne medvirke til at fremme arbejdet med at udbrede digital kommunikation på de områder, hvor dette er hensigtsmæssigt. Samfundsmæssigt er der en betydelig interesse i at få fremmet brugen af IT (informationsteknologi), bl.a. ved at gøre det muligt for borgere og virksomheder at kommunikere digitalt med offentlige myndigheder. Formkrav i lovgivningen kan på nogle områder besværliggøre eller ligefrem hindre en sådan anvendelse. Der er derfor efter udvalgets opfattelse god grund til at fremme en hensigtsmæssig modernisering af lovgivningen.

Det har først på et relativt sent tidspunkt været muligt at gå ind i en nærmere overvejelse af udvalgets anden hovedopgave, som er at overveje behovet for at give regler om retsstillingen mellem afgiver og modtager af meddelelser forsynet med elektronisk signatur og andre civilretlige spørgsmål i forbindelse med anvendelse af digital kommunikation. Besvarelsen af disse spørgsmål har måttet afvente en afklaring af, hvordan den danske lov, der skal gennemføre EU-direktivet om elektronisk signatur, blev udformet. Det lovforslag om elektroniske signaturer, som regeringen fremsatte den 22. marts 2000, er den 18. maj 2000 blevet vedtaget af Folketinget, og først herefter er det blevet muligt for udvalget at drøfte de nævnte civilretlige spørgsmål nærmere.

Udvalgets undersøgelser har vist, at der findes et betydeligt antal formkrav i love, bekendtgørelser mv. En gennemgang af samtlige retsregler, herunder en revision af de bestemmelser, som udgør en hindring for en hensigtsmæssig IT-udnyttelse samt at udarbejde forslag til eventuel nødvendig følgelovgivning, er en omfattende opgave, som udvalget foreslår, at de enkelte ministerier anmodes om at iværksætte inden for hvert deres ressortområde. En delbetænkning vil gøre det muligt, at arbejdet i de enkelte ministerier kan

påbegyndes med det samme uden at behøve at afvente udvalgets overvejelser af de civilretlige spørgsmål.

Udvalget har på baggrund af disse overvejelser besluttet sig for i første omgang at beskæftige sig med spørgsmålet om, hvorvidt der er behov for at lovgive om anvendelsen af digital kommunikation i forbindelse med formkrav om skriftlighed mv. i lovgivningen, og at afgive denne delbetænkning om dette spørgsmål.

1.4. Sammenfatning af udvalgets overvejelser

Som grundlag for en nærmere vurdering af spørgsmålet om, hvorvidt der er behov for at lovgive om anvendelse af digital kommunikation i forbindelse med formkrav om skriftlighed mv. i lovgivningen, har udvalget foretaget en gennemgang af lovgivningen inden for 4 ministerområder. Udvalgets gennemgang har omfattet ca. 500 retsregler under Erhvervs-, Indenrigs-, Sundheds- og Justitsministeriet, som indeholder formkrav af den ene eller anden art, og som på den ene eller anden måde kan tænkes at udgøre en hindring for anvendelsen af digital kommunikation (kapitel 5).

På grundlag af gennemgangen af disse mange bestemmelser med formkrav har udvalget søgt at opstille en vejledende liste over nogle af de formål, som formkrav varetager, med henblik på at tage stilling til, om disse formål kan opnås ved brug af digital kommunikation.

Udvalget har måttet konstatere, at det er vanskeligt at udtale sig generelt om forståelsen af formkrav om skriftlighed, underskrift mv. I nogle tilfælde fremgår det klart af lovregler mv., at det er muligt at opfylde formkravet ved brug af digital kommunikation. Der findes på anden side også regler, der har et indhold, som gør det klart, at digital kommunikation ikke er mulig, og hvor der i givet fald er behov for et lovgivningsinitiativ, hvis denne

form for kommunikation skal kunne anvendes. I de fleste tilfælde fremgår det ikke klart af bestemmelserne, om de tillader brug af digital kommunikation. I mange tilfælde er formkravene nemlig blevet udformet, uden at man har haft muligheden for digital kommunikation for øje, og i sådanne tilfælde kan det være vanskeligt ved fortolkning at fastslå, hvordan bestemmelsen skal forstås. Denne fortolkningstvivel kan i sig selv udgøre en hindring for anvendelsen af digital kommunikation.

For at sikre, at lovgivningen ikke udgør en hindring for hensigtsmæssig brug af digital kommunikation, er det efter udvalgets opfattelse nødvendigt systematisk at gennemgå lovgivningen for at finde frem til de bestemmelser, som ikke understøtter den ønskede udvikling. Herefter må der tages stilling til, om de pågældende bestemmelser skal ændres, eller om problemet kan løses på anden vis, f.eks. ved en tilkendegivelse fra vedkommende myndighed om, at den forstår en bestemmelse således, at den tillader brug af digital kommunikation.

For så vidt angår de områder, hvor der herefter findes at være behov for lovændringer, har udvalget overvejet, hvilken lovgivningsmodel der bør anvendes. Et enigt udvalg har konkluderet, at det ikke er muligt at udforme en generel regel, der på én gang ændrer alle formkrav i lovgivningen. Denne konklusion svarer til, hvad man er nået frem til i bl.a. Sverige og Norge (kapitel 6.3).

Udvalget har i stedet drøftet 3 metoder til ændring af formkrav i lovgivningen, som hindrer en hensigtsmæssig anvendelse af digital kommunikation. Metoderne er: 1) traditionelle ændringslove, 2) bemyndigelse for de enkelte ministre til ved bekendtgørelse at ændre formkrav i lovgivningen, og 3) en mellemløsning af de to nævnte metoder (kapitel 6.3.3).

Udvalget anbefaler mellemløsningen, som indebærer, at der gennemføres en generel regel i forvaltningsloven, hvorved de enkelte ministre bemyndiges til ved bekendtgørelse at æn-

dre formkrav, der drejer sig om kommunikation *til* det offentlige, således at det bliver muligt at anvende digital kommunikation på dette område. På andre retsområder, som f.eks. kommunikation *fra* det offentlige og mellem borgere og virksomheder indbyrdes, vil ændringer skulle gennemføres ved særskilte lovændringer, herunder i form af samlelovforslag (kapitel 6.3.3.4).

Udvalget anbefaler, at regeringen tager initiativ til en systematisk gennemgang af lovgivningen med henblik på at finde og ændre de formkrav, som hindrer en hensigtsmæssig IT-anvendelse. Gennemgangen og vurderingen af de enkelte regler med formkrav forudsætter et indgående kendskab til de respektive retsområder, ligesom der kan være behov for at inddrage berørte organisationer, myndigheder mv. På denne baggrund finder udvalget, at det bør være de enkelte ressortministerier, der får til opgave at gennemgå hver deres ressortområde (kapitel 6.3.4).

Til brug for de enkelte ministeriers overvejelser i forbindelse med deres gennemgang og ændring af bestemmelser med formkrav har udvalget opstillet et ”katalog”, hvori udvalget redegør for nogle af de overvejelser, som de enkelte ministerier efter udvalgets opfattelse bør foretage, når de gennemgår lovgivningen på hver deres område (kapitel 6.4)

København, den 5. december 2000

Stig Bigaard	Kim Brinckmann	Ove Dam	Tina Füssel
Lars Hjortnæs	Morten M. Jensen	Flemming Jensen	Åse Kogsbøll
Peter Møgelvang-Hansen		Anette Høyrup Petersen	
	Michael B. Elmer (formand)		
/ Svend Larsen (sekretær)	Carsten Oppermann (sekretær)		Claus Jakobsen (sekretær)

Kapitel 2. De nye teknikker – digital kommunikation og elektronisk signatur

2.1. Indledning

Informationsteknologien har været kendt i mange år. Computerne har længe sat deres præg på vores dagligdag, og i de senere år har fremkomsten af det verdensomspændende computernetværk Internettet betydet en voldsom vækst i udnyttelsen af edb til både erhvervsmæssig og ikke-erhvervsmæssig brug.

Computere finder i dag anvendelse i næsten enhver sammenhæng, både privat, i erhvervslivet og i den offentlige forvaltning. Bl.a. løses tekstbehandlingsopgaver langt hurtigere og mere effektivt, når man benytter moderne edb-programmer, end da man var henvist til at skrive i hånden eller på skrivemaskine.

Anvendelsen af edb-tekstbehandling havde imidlertid i lang tid navnlig betydning som en lettelse ved udfærdigelsen af dokumenter som f.eks. breve, kontrakter eller lignende, bl.a. fordi teknikken gjorde det muligt at bruge standardformularer og at foretage rettelser, uden at være nødt til at skrive hele teksten om. I sidste ende resulterede brugen af computer og program imidlertid fortsat i et papirdokument, som kunne underskrives, med postvæsenets hjælp fremsendes til modtageren i en kuvert, læses, arkiveres og i det hele taget behandles, præcis som man hidtil havde behandlet andre dokumenttyper.

Både ud fra en praktisk og en retlig synsvinkel er der ikke stor forskel på et brev, et aftaledokument eller en anden dokumenttype, som er udarbejdet i hånden eller på en skrivemaskine, og et dokument, som er udarbejdet på en computer, og derefter udskrevet på papir.

I dag ser verden anderledes ud. Elektronisk dokumentudveksling ved brug af elektronisk post og elektronisk dataudveksling¹ er i rivende vækst, og både erhvervslivet og den offentlige forvaltning er i dag i høj grad indrettet på brugen af moderne kommunikationsteknologi, hvor oplysninger registreres og overføres, uden at der overhovedet udskrives et papirdokument. Både vigtige aftaledokumenter og mindre forpligtende beskeder, som før blev klaret med et brev, et postkort eller en telefonopringning, fremsendes nu ofte ved brug af e-post og lignende. Det forventes, at denne udvikling vil fortsætte i de kommende år, således at stadig mere kommunikation vil ske uden brug af papir.

Med denne udvikling opstår nogle til dels nye retlige spørgsmål, som knytter sig til brugen af "digitale dokumenter", dvs. læselige meddelelser, som skabes og overføres i digital form. Før man kan tage stilling til de retlige spørgsmål, som knytter sig til anvendelsen af digitale dokumenter, er det imidlertid nødvendigt at have en grundlæggende forståelse af de anvendte teknikker. I dette kapitel gives der derfor en kort indføring i de teknikker, som benyttes til oprettelse, underskrivelse og forsendelse af digitale dokumenter.

2.2. Digitale dokumenter

At noget er digitalt betyder, at det " ... udtrykker størrelsen af en mængde i opbrudte enheder i form af talværdier"². En digital meddelelse er således information i digital form, ("nuller og et-taller"). Digitale meddelelser er i sig selv uforståelige, men kan gøres tilgængelige, f.eks. ved udskrift på papir eller ved fremvisning på en computerskærm. Digital information kan lagres på digitale medier, f.eks. en harddisk på en computer, en CD-ROM eller en diskette. Informationen kan endvidere overføres fra ét digitalt lagringsmedie til et andet ved transmission via telelinier.

¹ Også kaldet EDI, som står for Electronic Data Interchange.

² Politikens Store Nye NuDansk Ordbog, 1996, Politikens Forlag A/S.

Ofte benyttes ordene ”digitalt” og ”elektronisk” i flæng. Det gælder både, når man i daglig tale beskæftiger sig med den nye teknologi, og når der i lovgivningen opstilles regler herom. At noget er elektronisk, betyder, at det består af elektroner, dvs. elektriske impulser. En elektronisk meddelelse er altså en meddelelse, der består af elektricitet. En digital meddelelse er ofte elektronisk, men dette behøver på den anden side ikke altid være tilfældet. Digitale data kan således også lagres uden brug af elektricitet, f.eks. på optiske lagringsmedier eller sendes ved brug af lysbølger, f.eks. i optiske fiberkabler.

I denne betænkning benyttes begrebet ”elektronisk signatur” som betegnelse for teknikker til at ”underskrive” digitale dokumenter, jf. nærmere herom nedenfor i kapitel 2.3., og for at sikre en klar og entydig terminologi benyttes begrebet et ”digitalt dokument” i denne betænkning til at betegne digitale meddelelser, som kan gøres læselige ved frembringelse af skrifttegn.

En digital meddelelse med et andet indhold end skrifttegn, herunder tal og symboler, er således ikke et digitalt dokument i den forstand, hvori ordene anvendes i denne betænkning. Uden for falder bl.a. digitale lydoptagelser og digitale meddelelser, som alene består af billeder (film, tegninger mv.). Rent teknisk er det muligt at forsyne en digital lydoptagelse eller en film med elektronisk signatur.

Ved drøftelsen af de retlige spørgsmål, som opstår i forbindelse med anvendelsen af digitale og elektroniske medier, er det imidlertid væsentligt at holde sig for øje, at besvarelsen af de stillede spørgsmål kan være forskellig, alt efter hvilken teknologi der er anvendt.

Som eksempel kan nævnes, at besvarelsen af spørgsmålet om, hvorvidt digitale meddelelser kan eller skal kunne opfylde formkrav i lovgivningen om brug af et dokument, skriftlighed mv., til en vis grad afhænger af, om den digitale meddelelse er læselig. Mens en digital meddelelse, som kan omsættes til skrifttegn (f.eks. en e-mail), på mange måder kan sidestilles med et papirdokument, fordi de begge overfører information ved brug af

skrifttegn, gælder det samme ikke nødvendigvis for en digital meddelelse, som indeholder lyd eller billeder. Drejer formkravet sig f.eks. om indsendelse af oplysninger til en offentlig myndighed, vil det formentlig ofte kun opleves som en beskeden ændring, hvis indsendelse ud over ved brev også kan ske ved brug af en e-mail. For modtageren er der ikke stor forskel på, om man læser informationen på et stykke papir eller på en edb-skærm. Drejer det sig derimod om at ændre et formkrav således, at det også kan opfyldes ved indsendelse af en digital lydoptagelse, bliver forskellen noget større. Modtager man en e-mail, kan man uden videre lave en udskrift på papir, som f.eks. kan indgå i myndighedens (papir-)sag, mens det med den nuværende teknik kræver en betydeligt større indsats (manuel indtastning) at overføre indholdet af en lydoptagelse til et papirdokument.

Når der skal tages stilling til, om et formkrav i lovgivningen, f.eks. om at information skal foreligge skriftligt eller at et dokument skal være underskrevet, kan opfyldes ved brug af digital kommunikation, vil det altså være af betydning, om den digitale meddelelse er skriftlig eller består af lyd eller billeder. Mens udvalget som anført nedenfor i kapitel 6.1 har fundet, at der er behov for i højere grad end hidtil at tillade anvendelsen af e-mail mv. på områder, hvor lovgivningen indeholder formkrav, er der efter udvalgets opfattelse – i hvert fald ikke på nuværende tidspunkt – ikke noget reelt behov for at tillade brug af lydoptagelser, billeder mv. på sådanne områder. I denne betænkning drøftes derfor alene spørgsmålet om brugen af skriftlige digitale meddelelser (digitale dokumenter) på områder med formkrav.

Selv om begrebet ”dokument” altså i denne betænkning anvendes til at betegne læselige meddelelser i digital form, er der grund til at fremhæve, at selv om et digitalt dokument har visse lighedspunkter med et papirdokument, så er der dog også nogle væsentlige forskelle. Disse forskelle er bl.a. af betydning, når man skal tage stilling til de retlige konsekvenser af anvendelsen af digitale dokumenter. I det følgende redegøres der derfor i oversigtsform for nogle af de væsentligste forskelle mellem papirdokumenter og digitale dokumenter.

For det første har et papirdokument et selvstændigt fysisk udtryk i form af et eller flere stykker papir, der kan opbevares, overgives, forsynes med stempler, påtegninger mv. Til forskel herfra har et digitalt dokument ikke på samme måde en umiddelbar fysisk eksistens, idet de værdier (data), som udgør dokumentet, alene består i registreringer på et lagringsmedium, f.eks. en harddisk på en computer eller en diskette. Mens et papirdokument samler en bestemt mængde oplysninger og fysisk adskiller disse fra andre data, er oplysningerne i et digitalt dokument opdelt i små dele, som lagres adskilt, og som først samles i forbindelse med visning af dokumentet på et skærbillede eller udskrift af dokumentet på papiret.

Oplysningerne i et papirdokument er endvidere ”låst” ved skrifttegnenes fysiske tilknytning til papiret, således at skrifttegnene i et papirdokument ikke uden videre kan ændre sig. Et digitalt dokument består derimod af en række oplysninger, som kan være statiske, men som også kan ændre sig løbende. En talværdi i et tekstbehandlingsdokument, som vises på en edb-skærm, kan således fremkomme som funktion af en beregning, uden at dette umiddelbart er kendeligt for læseren. Ændres et af de elementer, som indgår i beregningen, f.eks. fordi der indgår en tidsangivelse eller dato i beregningen, vil dokumentet indeholde et nyt tal, næste gang det hentes frem på skærmen.

Hertil kommer at et papirdokument er umiddelbart læseligt, idet man ved at se på dokumentet – og forudsat det er affattet på et sprog, som læseren forstår – kan gøre sig bekendt med dokumentets indhold. Et digitalt dokument vil derimod altid skulle gennemgå en behandling, før det kan læses. Dette betyder, at muligheden for at gøre sig bekendt med indholdet af et digitalt dokument afhænger af, om man har adgang til maskiner og programmer, som kan omforme dokumentets talværdier til et skærbillede eller en udskrift. Er modtageren af et digitalt dokument ikke i besiddelse af et program, der kan ”læse” det format, som dokumentet er lagret i, kan modtageren ikke gøre sig bekendt med dets indhold.

At et digitalt dokument ikke har et selvstændigt fysisk udtryk og ikke er umiddelbart læseligt, betyder, at man kan komme i tvivl om, hvordan indholdet af dokumentet skal fastlægges. Af tekniske årsager indeholder den datamængde, som opstår, når der f.eks. oprettes et tekstbehandlingsdokument, en mængde oplysninger, som ikke umiddelbart kommer til udtryk, når dokumentet fremvises på skærmen eller udskrives på papir. Et digitalt dokument indeholder bl.a. en lang række instruktioner, som computeren anvender til at præsentere dokumentindholdet på skærmen. Disse instruktioner fastlægger bl.a., hvordan skrifttegnene i dokumentet bliver præsenteret på edb-skærmen og "fortolkes" af det tekstbehandlingsprogram, som benyttes til at vise dokumentet på skærmen. Hvordan instruktionerne fortolkes, afhænger imidlertid til en vis grad af det program, som læseren benytter. Bruges et andet program end det, som dokumentet blev skabt med, skal instruktionerne måske "oversættes" (konverteres), før programmet kan forstå dem. I nogle tilfælde medfører en sådan konvertering, at dokumentet får et andet udseende, og måske ændrer indholdet af dokumentet sig ligefrem, ligesom nogle koder kan gå tabt ved konverteringen.

At et papirdokument er umiddelbart læseligt, betyder også, at det kan tjene som direkte bevis under en retssag, mens et digitalt dokument oftest vil skulle udskrives på papir eller vises på en skærm, før det kan udfylde denne funktion. Der vil derfor i givet fald kunne opstå spørgsmål om, hvorvidt udskriften er identisk med det digitale dokument.

En anden forskel på papirdokumenter og digitale dokumenter er, at man ved brug af papirdokumenter kan tale om, at der foreligger et "originaldokument", idet der normalt vil findes netop ét eksemplar af dokumentet, som er det autentiske. Der kan udfærdiges nye udgaver af det originale dokument, men disse vil alene være kopier og – med større eller mindre afvigelser fra originalen - typisk fremstå som sådanne. Netop fordi der kun findes ét originaldokument, kan man lade dette tjene som bærer af en rettighed, således at en overdragelse af dokumentet også overfører den til dokumentet hørende rettighed. En pen-

geseddel, en check og et negotiabelt gældsbrev er eksempler på papirdokumenter, der tjener som ”bærere” af rettigheder. I andre sammenhænge stiller man krav om, at et originaldokument skal fremvises eller opbevares for at dokumentere en tilladelse eller en rettighed. Det kan f.eks. være et kørekort, som dokumenterer indehaverens ret til at føre personbil, eller et næringsbrev, som hænges op i et butikslokale for at dokumentere indehaverens ret til at drive virksomhed. Fratager man indehaveren den pågældende rettighed, kan dette tilkendegives ved fratagelse af dokumentet.

Til forskel herfra giver det ikke mening at tale om ét originalt digitalt dokument. Et digitalt dokument er nemlig som nævnt ikke varigt knyttet til et fysisk medie, men består alene af gengivelser af data, som kan sammenstilles og præsenteres i en række forskellige sammenhænge. Allerede under udfærdigelsen af f.eks. et tekstbehandlingsdokument vil dette af rent tekniske årsager normalt findes i flere eksemplarer. Fremvisning af et digitalt dokument på en edb-skærm indebærer i sig selv en kopiering af dokumentet, idet selve dokumentets data befinder sig i et lager på computeren. Der kan udfærdiges et ubegrænset antal kopier af et digitalt dokument, uden at disse på nogen måde kan adskilles fra hinanden. Sikkerhedskopiering af vigtige data foretages i overensstemmelse med faste rutiner hos mange professionelle brugere. Sendes et digitalt dokument fra en computer til en anden, vil dette ligeledes resultere i, at der findes ”kopier” af dokumentet både hos afsenderen og modtageren af dokumentet, ligesom der i nogle tilfælde bliver efterladt ”kopier” af dokumentet på computere, som det har passeret undervejs.

Et yderligere punkt, hvor et digitalt dokument adskiller sig fra papirmediet, er i relation til muligheden for at bevise, at der er blevet ændret i dokumentet. Hvis der ændres i indholdet af et papirdokument, vil dette nemlig - som følge af informationens tilknytning til det fysiske medie - kunne påvises ved kontrol af dokumentet. I et digitalt dokument vil indholdet - de lagrede data - derimod som udgangspunkt kunne ændres, uden at dette behøver at efterlade sig spor. Hvis ikke der benyttes særlige sikkerhedsmekanismer, f.eks. elektro-

nisk signatur, som beskrives nedenfor, kan det således være svært at føre bevis for et digitalt dokumentets ægthed.

2.3. Elektronisk signatur

2.3.1. Indledning

Begrebet en elektronisk signatur benyttes til at betegne data, som knytter sig til en datamængde (f.eks. et digitalt dokument), og som gør det muligt at kontrollere, at datamængden stammer fra den angivne udsteder. Elektronisk signatur bruges også som betegnelse for en bestemt teknologi, som baseres på kryptering, jf. herom nedenfor. I nogle sammenhænge benyttes begrebet ”digital signatur” som betegnelse for en bestemt metode til at ”signere” digitale meddelelser. På nuværende tidspunkt dækker de to begreber imidlertid over det samme, idet digital signatur i dag er den eneste teknik på markedet.

Elektronisk signatur udfylder i relation til digitale dokumenter nogle af de funktioner, som en håndskreven underskrift udfylder i relation til papirdokumenter. Af størst betydning i relation til de spørgsmål, som behandles i denne betænkning, er, at en elektronisk signatur kan benyttes til at knytte et digitalt dokument til en bestemt person ved en ”underskrift”.

Grundtanken bag elektronisk signatur er, at brugerne udstyres med en ”privat signaturnøgle”, som bruges til at frembringe den elektroniske signatur. Hver nøgle er unik og kan således tjene til at identificere indehaveren. Når nøglen anvendes på en digital meddelelse, fremkommer en signatur, som er en kombination af den anvendte nøgle og den underliggende digitale meddelelse. Signaturen identificerer ikke i sig selv indehaveren af signaturnøglen. Hertil anvendes en anden nøgle, den ”offentlige nøgle”, der har en matematisk sammenhæng med signaturnøglen, således at en signatur, der er frembragt med den pri-

vate signaturnøgle, kun kan afkodes (“verificeres”) med den tilhørende offentlige signaturnøgle.

Når et digitalt dokument skal forsynes med elektronisk signatur, sker dette ved, at den private signaturnøgle anvendes til at kryptere dokumentet. Signaturnøglen kan f.eks. findes på et såkaldt smartcard, som ligner de almindeligt anvendte betalingskort/plastickort. Der findes dog også andre løsninger, og navnlig kan nøglen findes som et program på indehaverens computer. For at opnå beskyttelse mod uberettiget brug vil der normalt skulle indtastes en PIN-kode eller tilsvarende sikkerhedsforanstaltninger, som sikrer, at kun den rette bruger kan benytte nøglen til afgivelse af elektronisk signatur. Der er nye teknikker på vej til sikring mod misbrug af signaturnøgler, bl.a. baseret på såkaldte biometriske metoder (fingeraftrykslæsning, aflæsning af øjets iris mv.)

Når signaturnøglen anvendes på et digitalt dokument, medfører dette for det første, at indholdet af teksten kan hemmeligholdes for alle andre end dem, der er i besiddelse af den kode, som nøglen benytter. Hvis modtageren ved, at kun én anden person er i besiddelse af den benyttede kode, kan kodningen også benyttes til at fastslå, fra hvem meddelelsen stammer. Hvis en kode kun indehaves af A, og meddelelsen kun kan afkodes med A's kode, må den også være kodet af A.

Eksempel:

Hr. Jensen ønsker at signere et digitalt dokument, som skal sendes til hans pengeinstitut. Han henter dokumentet frem på skærmen på sin computer og starter det program, som bruges til at fremstille signaturen. Han bliver herefter af programmet bedt om at indtaste sin sikkerhedskode. Programmet fremstiller nu en elektronisk signatur, som knyttes til det digitale dokument. Dokumentet og signaturen fremsendes til pengeinstituttet, som bruger Hr. Jensens offentlige signaturnøgle til at kon-

trollere signaturen. Går kontrollen godt, ved pengeinstituttet, at dokumentet er signeret med Hr. Jensens private signaturnøgle.

2.3.2. Kryptering

Elektronisk signatur frembringes ved hjælp af krypteringsnøgler, der bruges på den digitale information, som ønskes signeret. Nøglerne består af såkaldte krypteringsalgoritmer, der fastlægger en fremgangsmåde til kryptering af den digitale information. Begrebet kryptering bruges som samlebetegnelse for henholdsvis enkryptering (i det følgende blot kaldet kryptering) og dekryptering. Ved kryptering gøres en meddelelse uforståelig, mens dekryptering bringer meddelelsen tilbage til sin oprindelige - forståelige - form.

Kryptering er udviklet i militært regi, hvor man allerede på et tidligt tidspunkt fandt behov for at kunne sende meddelelser, som kun kunne forstås af dem, som var i besiddelse af den benyttede kode. Den ældst kendte krypteringsmetode stammer helt tilbage fra Julius Cæsars tid, hvor den første form for kodeskrift blev indført. Kodeskrift i sin simpleste form foregår ved en forskydning af alfabetet, således at et a i den ukodede tekst eksempelvis bliver til et c i kodeteksten. Krypteringen foregår så ved at udskifte bogstaverne i den tekst, man vil sende, med de tilsvarende bogstaver i kodeteksten. Ordet "digital" bliver derved til "fkikvcn" – uforståeligt, medmindre man besidder koden:

Tekst:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	æ	ø	å
Kode:	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	æ	ø	å	a	b

Når kryptering benyttes til at udvirke elektronisk signatur, er formålet imidlertid ikke at gøre teksten uforståelig. I stedet benyttes krypteringen til at forsyne en digital meddelelse med et "stempel", den elektroniske signatur, som kun kan være udvirket ved brug af én

bestemt krypteringsalgoritme. Hvis man ved, hvem der er i besiddelse af denne algoritme, ved man således også, hvem der har "signeret" meddelelsen.

Metoder, hvor den samme kode (algoritme) bruges til at kryptere og dekryptere meddelelsen, kaldes symmetrisk kryptering. I et sådant system findes der altså kun én nøgle, der anvendes af både afsenderen og modtageren af den krypterede meddelelse.

For at et sådant system kan fungere til identifikation af afsenderen, må nøglen udveksles mellem parterne. Modtageren af den krypterede og dermed uforståelige meddelelse vil så - ved at anvende den nøgle, som han har modtaget fra A - kunne bringe klarteksten frem og dermed vide, at teksten stammer fra A.

Hvis nøglen fremsendes sammen med meddelelsen, kan en tredjemand, der opsnapper meddelelsen og nøglen, aflæse den krypterede meddelelse. En sådan tredjemand vil også kunne ændre i meddelelsen og kryptere den på ny med den medsendte nøgle, inden den sendes videre til B. Meddelelsen vil stadig fremstå, som om den er afsendt fra A.

Ved symmetrisk kryptering er det altså nødvendigt, at afsender og modtager har været i kontakt med hinanden, inden der kommunikeres digitalt. Det er endvidere nødvendigt, at nøgleudvekslingen sker på en sikker og forsvarlig måde. Kommer blot ét eksemplar af krypteringsnøglen i forkerte hænder, må begge brugere udstyres med en ny nøgle.

Da flere brugere i et sådant system kan være i besiddelse af nøglen, er der endvidere ingen sikkerhed for, hvem der er afgiver af en meddelelse. Når flere bruger den samme nøgle, kan det nemlig ikke ud fra en krypteret meddelelse afgøres, om det er A eller B, der har foretaget krypteringen.

Dette udgør ikke et problem i et lukket system, hvor parternes identitet kan fastlægges på anden vis. Her kan krypteringen blot anvendes til at sikre, at de digitale meddelelser ikke uopdaget kan ændres eller læses af uvedkommende.

Når digitale meddelelser skal udveksles i et åbent netværk som Internettet, hvor parterne i kommunikationen ikke altid kender hinanden på forhånd, opstår der imidlertid behov for løsninger, som giver en sikker identifikation af afsenderen af en meddelelse, uden at det er nødvendigt med en besværlig individuel udveksling af nøgler.

Denne mulighed giver et elektronisk signatur-system, der er baseret på asymmetrisk kryptering. I et asymmetrisk system er krypteringsnøglen og dekrypteringsnøglen ikke ens. I stedet benyttes to forskellige, men indbyrdes sammenhængende nøgler - en privat nøgle, som indehaveren bruger til at signere (kryptere) med, og en offentlig nøgle, som modtageren bruger til at kontrollere (dekryptere) signaturen med.

Elektronisk signatur, der er baseret på asymmetrisk kryptering, kaldes også for et "offentligt nøgle-system" eller på engelsk "Public Key Infrastructure" (PKI).

De to nøgler i et "offentligt nøgle-system" er indbyrdes forbundet således, at det kun er den offentlige nøgle, der kan dekryptere en tekst, som er krypteret med den tilhørende private nøgle. Omvendt kan en digital meddelelse, der kan dekrypteres med den private nøgle, kun være krypteret ved hjælp af den tilhørende offentlige nøgle.

Da en meddelelse, der er krypteret med den private nøgle, kan dekrypteres med en anden nøgle - den offentlige nøgle - er det ikke nødvendigt at videregive den private nøgle til den, der skal kunne dekryptere meddelelsen. I stedet foregår identifikationen af afsenderen ved, at modtageren bruger den offentlige nøgle til at dekryptere signaturen med. De to nøgler indgår som nævnt i et nøglepar. Hvis modtageren ved, hvem den offentlige nøgle tilhører, ved han derfor også, hvem den private nøgle tilhører.

Den private nøgle kan dermed bevares fortroligt hos nøgleindehaveren og således under visse betingelser give bevis for, hvem der er udsteder af et digitalt dokument.

Har nøgleindehaveren nemlig holdt sin private nøgle utilgængelig for andre, vil modtageren af en meddelelse, der kan dekrypteres med den tilhørende offentlige nøgle, vide, at meddelelsen må være krypteret af indehaveren af den private nøgle.

For at give denne sikkerhed må systemet endvidere være indrettet således, at det ikke er muligt at regne sig tilbage til den private nøgle ud fra den offentlige nøgle. Hvis dette var muligt, ville enhver, der kom i besiddelse af den offentlige nøgle, nemlig kunne skabe en kopi af den private nøgle og dermed kunne udgive sig for at være den oprindelige indehaver af den private nøgle.

Ligesom ved systemer baseret på symmetrisk kryptering, krypterer afsenderen den digitale meddelelse, han vil sende til modtageren. Forskellen er, at krypteringen i denne situation sker med afsenderens private nøgle, som er forskellig fra den offentlige nøgle, som teksten skal dekrypteres med. Resultatet af krypteringen er en datafil, som er et produkt af anvendelsen af den elektroniske signatur. Når den elektroniske signatur kommer frem til modtageren, dekrypterer denne signaturen med afsenderens offentlige nøgle.

Resultater dekrypteringen i en forståelig meddelelse, kan modtageren med en høj grad af sandsynlighed gå ud fra, at signaturen er afgivet af indehaveren af den offentlige nøgle.

Hvis dekrypteringen med den offentlige nøgle ikke medfører en forståelig meddelelse, er dekrypteringen mislykket, og modtageren af meddelelsen kan ikke gå ud fra, at signaturen stammer fra indehaveren af den pågældende offentlige nøgle.

Årsagen til, at dekrypteringen mislykkes, kan være, at meddelelsen slet ikke er blevet krypteret med den tilhørende private nøgle. Årsagen kan imidlertid også være, at meddelelsen er blevet ændret undervejs. Som anført udgør den elektroniske signatur en kombination af den anvendte krypteringsalgoritme og den underliggende digitale meddelelse. Ændres den krypterede meddelelse, bliver resultatet af dekrypteringen også forskelligt fra den oprindelige meddelelse, og i sådanne tilfælde vil dekrypteringen ikke resultere i en forståelig tekst.

Som det fremgår, er det af stor betydning, når man skal vurdere, om en elektronisk signatur stammer fra en bestemt person, om den anvendte signaturnøgle er sikret mod eftergørelse. Kan man nemt regne sig frem til den private nøgle ud fra den offentlige, er signaturen ikke noget godt bevis for, fra hvem meddelelsen stammer. Hvor let eller svært det er at eftergøre en privat signaturnøgle, afhænger af den krypteringsalgoritme, på hvilken nøglen bygger. Er algoritmen meget kompliceret opbygget, er det svært at bryde koden. Efterhånden som tiden går, bliver det imidlertid under alle omstændigheder lettere og lettere at bryde sådanne koder, fordi computernes regnekraft bliver større og større. En hurtig computer kan måske i dag bryde en algoritme, som for 10 år siden blev betragtet som helt sikker. Man sonderer derfor mellem forskellige typer af signaturnøgler, afhængig af hvilken algoritme ("nøglelængde") der anvendes. I det nye EU-direktiv om elektronisk signatur, som beskrives nærmere i kapitel 3.2.1., anvendes betegnelsen en "kvalificeret elektronisk signatur" om signaturer, som lever op til visse tekniske mindstekrav. Disse krav vil løbende blive justeret, efterhånden som den tekniske udvikling gør det nødvendigt med mere og mere komplicerede nøgler.

2.3.3. Certifikater og nøglecentre

I et "offentligt nøgle-system" hænger den elektroniske signaturs værdi som identifikation af afgiveren nøje sammen med, at modtageren er i besiddelse af afgiverens offentlige nøgle og har sikkerhed for, hvem den offentlige nøgle tilhører.

Hvem den offentlige nøgle tilhører, fremgår normalt af et "elektronisk certifikat". Certifikatet er knyttet til den offentlige nøgle og indeholder en identifikation af indehaveren af nøglen. I certifikatet kan der også optages andre oplysninger, f.eks. en besked om, at indehaveren er ansat i et bestemt firma eller et billede af nøgleindehaveren.

I certifikatet kan der også optages oplysninger om anvendelsesbegrænsninger, således at det f.eks. anføres, at indehaveren af nøgleparret kun ønsker at bruge sin elektroniske signatur til kommunikation med det offentlige, men derimod ikke til køb af varer og lignende.

I princippet kan et sådant certifikat udstedes af enhver. For at opnå en troværdig identifikation er der imidlertid behov for, at certifikatet er udstedt af en uafhængig tredieperson, som begge parter kan have tillid til. Denne funktion har et såkaldt nøglecenter. Der findes allerede i dag nøglecentre rundt omkring i verden, og efterhånden er der også kommet danske centre til. Der findes vistnok endnu ikke danske centre, som tilbyder certifikater til offentligheden. Endnu er certifikater forbeholdt visse grupper af brugere, men dette vil utvivlsomt ændre sig i løbet af kort tid.

Nøglecentre har som hovedopgave at knytte en bestemt person sammen med et nøglepar til afgivelse af elektronisk signatur. Nøglecentret kan selv udstede nøgleparret til en kunde og i den forbindelse udstede et certifikat til kunden. Et certifikat kan også udstedes til en kunde, som allerede er i besiddelse af et nøglepar til elektronisk signatur, og som blot anmoder nøglecentret om at udstede et certifikat til nøgleparret.

Et certifikat sammenknytter altså i princippet en person og en offentlig signaturnøgle. Sikkerheden for rigtigheden af oplysningerne i certifikatet - mest væsentligt naturligvis identifikationen af nøgleindehaveren - afhænger af kvaliteten af nøglecentrets kontrol. Sikkerheden for, at en signatur stammer fra den, der i certifikatet angives som indehaver af den pågældende offentlige signaturnøgle, afhænger endvidere af, om den private nøgle opbevares på sikker måde, således at andre ikke kan anvende den.

Når en person henvender sig til et nøglecenter og anmoder om at få udstedt et certifikat til sin elektroniske signatur, må nøglecentret kontrollere ansøgerens identitet. Kontrollens grundighed vil bl.a. afhænge af, hvad certifikatet og signaturen skal anvendes til. Et certifikat, der alene skal anvendes til identifikation af nøgleindehaveren ved mindre væsentlige transaktioner, behøver måske ikke at være lige så troværdigt og bygge på lige så omfattende undersøgelser som et certifikat, der skal anvendes ved mere væsentlige transaktioner.

Alt afhængig af, hvilken sikkerhed for indehaverens identitet der er nødvendig, kan nøglecentret f.eks. kræve, at ansøgeren personligt møder op hos en af nøglecentrets afdelinger, medbringende billedlegitimation. En sådan kontrolprocedure vil kunne tilvejebringe en høj grad af sikkerhed for ansøgerens identitet.

Eksempel

Fru Hansen ønsker at signere et digitalt dokument, som skal sendes til hendes pengeinstitut. Hun henter dokumentet frem på skærmen på sin computer og starter det program, som bruges til at fremstille signaturen. Hun bliver herefter bedt om at indtaste sin kode. Programmet fremstiller nu en elektronisk signatur, som knyttes til det digitale dokument. Dokumentet og signaturen fremsendes til pengeinstituttet, som bruger fru Hansens offentlige signaturnøgle til at kontrollere den elektroniske

signatur. Den offentlige nøgle kan være indeholdt i et certifikat, der sendes sammen med den elektroniske signatur og meddelelsen. Den offentlige nøgle kan eventuelt også hentes hos nøglecentret, der har udstedt certifikatet. Pengeinstituttet anvender den offentlige nøgle til at kontrollere den elektroniske signatur. Går kontrollen godt, véd pengeinstituttet, at dokumentet er signeret med fru Hansens private signaturnøgle.

I eksemplet i kapitel 2.3.1. med hr. Jensen havde parterne på forhånd udvekslet den nøgle, som skulle kontrollere signaturen, og dér kunne den alene anvendes over for pengeinstituttet. I det netop nævnte eksempel med fru Hansen henter pengeinstituttet derimod nøglen enten fra certifikatet eller fra nøglecentret, og denne signatur kan altså anvendes over for flere forskellige parter.

2.3.4. Forskelle og ligheder mellem håndskrevne underskrifter og elektroniske signaturer

Når elektronisk signatur anvendes til at “signere” digitale dokumenter, udføres der funktioner, som på mange måder svarer til dem, der udføres, når et papirdokument forsynes med en håndskreven underskrift. På nogle punkter kan der således sættes lighedstegn mellem de to måder at “underskrive” et dokument, mens der på andre punkter er forskelle.

Underskriftens grundlæggende funktion er at knytte et bestemt fysisk objekt, f.eks. et papirdokument, til en bestemt person. At underskriften har denne funktion, hænger sammen med, at en underskrift er personlig. En eftergjort underskrift vil være afgivet med andre midler – en anden hånd – end en ægte underskrift, og de deraf følgende fysiske forskelle vil normalt gøre det muligt at vise, at underskriften er falsk. Sikkerheden mod falsk er altså høj, men dog ikke fuldstændig.

En elektronisk signatur er ikke på samme måde som en håndskreven underskrift knyttet til en person. Sikkerheden for, at en elektronisk signatur stammer fra den angivne udsteder, hænger i stedet sammen med, at den pågældende er i besiddelse af den private signaturnøgle, som benyttes til at fremstille den pågældende signatur. Som nævnt ovenfor vil der endvidere ofte blive knyttet en yderligere sikkerhedsanordning til systemet, f.eks. ved krav om, at der afgives en hemmelig kode (PIN-kode), som kun nøgleindehaveren er i besiddelse af. Selv om der således normalt vil være en høj grad af sikkerhed for, at en elektronisk signatur stammer fra den angivne udsteder, er denne sikkerhed dog ikke fuldkommen. Får en anden rådighed over den private signaturnøgle og den tilhørende PIN-kode, vil den pågældende kunne afgive en elektronisk signatur, som vil fremtræde fuldstændig, som var den afgivet af nøgleindehaveren selv. Det kan altså ikke efterprøves ud fra den elektroniske signatur, om den er afgivet af nøgleindehaveren eller af en anden.

En elektronisk signatur kan således i princippet ”deles” af flere personer, f.eks. således, at man giver sin private nøgle og den tilhørende kode til en person, der skal handle på éns vegne. Modtageren af signaturen vil ikke ud fra den signerede meddelelse kunne se, at signaturen er anvendt af en anden end den, som certifikatet er udstedt til. Gør man dette, løber man dog en risiko for, at den pågældende (også) anvender signaturen til andet, end hvad der var aftalt.

Der vil således kunne opstå spørgsmål om, i hvilket omfang indehaveren af en signatur bliver bundet, hvis signaturen anvendes af en anden. Som anført ovenfor i kapitel 1 vil udvalget behandle bl.a. disse spørgsmål i en senere betænkning.

At en håndskreven underskrift tjener til at identificere en bestemt person, hænger som nævnt sammen med, at underskriften er personlig. Kontrollen af, om en underskrift stammer fra den angivne underskriver, kan foretages ved at bede den pågældende om at afgive en underskrift og derefter sammenligne de to. Ved elektronisk signatur er der ingen fast fysisk sammenhæng mellem nøgleindehaveren og den elektroniske signatur. I stedet

sker kontrollen af, hvem der er indehaver af signaturen, ved, at det undersøges, hvem nøglecentret angiver som nøgleindehaver i det certifikat, som er knyttet til den pågældende nøgle. Om identifikationen i certifikatet er korrekt, vil som anført ovenfor bl.a. afhænge af, hvilken kontrol nøglecentret foretager i forbindelse med udstedelsen af certifikatet. Det vil kunne forekomme, at et certifikat udstedes til en anden end den, som det angiver som nøgleindehaver.

Ofte benyttes en underskrift ikke blot til at knytte en bestemt person til et bestemt dokument, men også som et udtryk for en viljeserklæring fra underskriverens side. Ved at underskrive dokumentet tilkendegiver underskriveren at ville være bundet af dokumentets indhold. En elektronisk signatur vil på helt samme vis kunne tjene som udtryk for nøgleindehaverens vilje til at blive bundet.

Ved en håndskreven underskrift på et papirdokument sker der en fysisk sammenknytning mellem oplysningerne i dokumentet og underskriften, som giver en vis – om end begrænset - beskyttelse mod, at indholdet efterfølgende ændres. Der kan ske ændringer i teksten, men disse vil normalt give sig et fysisk udtryk, som vil kunne konstateres efterfølgende. Indeholder dokumentet flere sider, vil en underskrift på sidste side dog ikke beskytte mod, at en af de andre sider udskiftes. Visse dokumenter underskrives eller paraferes dog med initialer på hver side for at opnå sådan beskyttelse. En elektronisk signatur giver en væsentligt højere grad af beskyttelse mod efterfølgende ændringer i det digitale dokument. Da signaturen som nævnt udregnes på grundlag af hele det signerede dokument, vil enhver nok så lille ændring i dokumentet vise sig ved kontrol af signaturen.

En håndskreven underskrift er konstant i den forstand, at dens værdi som bevis for, at et dokument er underskrevet af en bestemt person, ikke ændrer sig nævneværdigt, selv om der er gået lang tid, siden underskriften blev afgivet. Til forskel herfra aftager bevisværdien af en elektronisk signatur, efterhånden som tiden går. Det skyldes, at de krypteringsalgoritmer, som benyttes i den private og offentlige signaturnøgle, bliver lettere at efter-

gøre, efterhånden som computerne får større regnekraft. En elektronisk signatur er derfor kun sikker i et begrænset tidsrum, f.eks. nogle år.

At identifikationen af en elektronisk signatur afhænger af indholdet af det tilknyttede certifikat, betyder endvidere, at modtageren af en elektronisk signatur er nødt til at kontrollere certifikatet, før modtageren kan være sikker på, hvem der er afsender. Denne kontrol er også nødvendig, fordi en elektronisk signatur kun har en begrænset levetid. Efter et stykke tid er den benyttede algoritme ikke længere så sikker mod eftergørelse, som den har været, og certifikatet vil derfor ofte indeholde en "udløbsdato", efter hvilken certifikatet ikke længere er gyldigt. Fra dette tidspunkt kan man altså ikke længere stole lige så sikkert på, at en elektronisk signatur stammer fra den, der er angivet i certifikatet.

Da signaturnøglen endvidere vil kunne komme i forkerte hænder, indrettes certificeringsordninger normalt sådan, at et certifikat kan spærres, hvis der er mistanke om, at den private signaturnøgle bliver misbrugt. Spærring kan også blive aktuel, hvis den tekniske udvikling går hurtigere end forudsat, således at den private signaturnøgle kan eftergøres, før certifikatet udløber. Vil man som modtager af et digitalt dokument med elektronisk signatur gardere sig mod skuffelser, bør man derfor også kontrollere, om certifikatet er spærret.

2.3.5. Kryptering med henblik på hemmeligholdelse

Som nævnt ovenfor benyttes der kryptering til at fremstille en elektronisk signatur, og krypteringsteknikkerne udspringer af et ønske om at hemmeligholde information. Når kryptering anvendes til at afgive elektronisk signatur, sker dette imidlertid oftest på en måde, der ikke indebærer hemmeligholdelse af indholdet af den digitale meddelelse, der signeres. Selve meddelelsen fremsendes således normalt i uforvansket form, men der er

ikke noget til hinder for, at produkter til afgivelse af elektronisk signatur også benyttes til at foretage kryptering med henblik på hemmeligholdelse.

Spørgsmålet om, i hvilket omfang det skal være muligt for myndighederne at gribe ind over for krypterede digitale meddelelser, f.eks. i forbindelse med efterforskning af kriminalitet og til militære formål, er omdiskuteret, både i Danmark og i udlandet. Det falder uden for udvalgets kommissorium at beskæftige sig med disse spørgsmål, og i denne betænkning tages der derfor ikke stilling hertil.

Kapitel 3. Den internationale udvikling

3.1. Indledning

Brugen af digital kommunikation gør det på mange måder lettere at indgå aftaler med en modpart, som befinder sig i et andet land. Elektronisk handel, dvs. markedsføring og indgåelse af aftaler om levering af varer eller tjenesteydelser ved brug af digitale kommunikationsmidler som f.eks. Internettet, foregår således ofte mellem parter i forskellige lande.

Usikkerhed om retsreglerne, f.eks. om elektronisk signatur opfylder et formkrav eller vil kunne benyttes som bevis under en eventuel retssag i et andet land, kan betyde, at parterne holder sig tilbage fra at benytte digital kommunikation til aftaleindgåelse. Det er derfor vigtigt at skabe klarhed over sådanne formkrav, navnlig ved at finde fælles løsninger, således at forskelle i landenes retssystemer ikke lægger unødige hindringer i vejen for en hensigtsmæssig udnyttelse af teknologiens fordele.

På internationalt plan har der da også været iværksat en række initiativer med henblik på at tilvejebringe fælles retlige rammer for den elektroniske handel. FN's kommission for international handelsret (UNCITRAL) har udarbejdet en modellov om elektronisk handel, som bl.a. indeholder regler om anvendelsen af digital kommunikation og elektronisk signatur på områder med formkrav. I UNCITRAL arbejder man i øjeblikket videre med at udarbejde "ensartede regler" (Uniform Rules) om elektronisk signatur, som bl.a. drejer sig om retsvirkningerne af anvendelsen af elektronisk signatur.

I EU har man også fundet, at der er behov for fælles løsninger på området for elektronisk handel mv., og der er således vedtaget to direktiver vedrørende elektronisk signatur og elektronisk handel. Direktiverne har til formål at fremme det indre markeds funktion, bl.a. ved at skabe fælles EU-regler om visse retlige spørgsmål i forbindelse med digital

kommunikation. Direktiverne indeholder bl.a. bestemmelser om retsvirkningerne af elektronisk signatur og om anvendelsen af digital kommunikation på områder, hvor lovgivningen indeholder formkrav.

Spørgsmålene om de retlige aspekter af anvendelse af digital kommunikation og elektronisk signatur er også blevet drøftet i enkeltlande. Bl.a. har en række delstater i USA og nogle lande i Europa gennemført lovgivning om elektronisk signatur, anvendelse af digital kommunikation på områder med formkrav om skriftlighed mv., og i en række andre lande overvejer man i øjeblikket, om der er behov for ny lovgivning.

Den retlige regulering af anvendelsen af digital kommunikation kan ikke anskues ud fra en isoleret dansk synsvinkel. På nogle områder er der vedtaget EU-regler, som skal gennemføres i dansk ret, og også på andre områder kan der være god grund til at hente inspiration i de løsninger, som andre lande har gennemført eller overvejer at gennemføre. Hensynet til at undgå retsusikkerhed taler for, at man vælger fælles løsninger på alle de områder, hvor det er muligt og hensigtsmæssigt.

I dette kapitel redegøres for nogle af de overvejelser om behovet for at regulere retsvirkningerne af digital kommunikation mv., som man har gjort sig i andre europæiske lande, samt for de initiativer, som EU og FN har taget på området. Et fyldestgørende referat af de mange lovgivningsinitiativer, som tages i disse år, ville blive meget omfattende og kan ikke rummes inden for rammerne af denne betænkning. Tanken med de følgende afsnit er derfor ikke at give et fuldstændigt overblik over den internationale udvikling, men blot at redegøre for nogle erfaringer, som i særlig grad kan tjene til inspiration, når man beskæftiger sig med spørgsmålet om formkrav i lovgivningen i forbindelse med anvendelsen af digital kommunikation.

3.2. EU

3.2.1. Direktivet om en fællesskabsramme for elektroniske signaturer

Europa-Kommissionen fremsatte i maj 1998 et forslag til direktiv om en fælles ramme for elektroniske signaturer, og som nu foreligger som Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer. Direktivet er optaget som bilag 1 til denne betænkning.

Direktivet har til formål at lette brugen af elektronisk signatur og at bidrage til den retlige anerkendelse heraf. For at nå disse mål indeholder direktivet fælles standarder for de produkter, der benyttes til at afgive og kontrollere elektronisk signatur, regler om etablering og drift af nøglecentre samt visse regler om retlig anerkendelse af elektronisk signatur.

I artikel 1, som fastlægger direktivets anvendelsesområde, fastslås det, at direktivet ikke omfatter “aspekter i forbindelse med kontraktens indgåelse og gyldighed eller andre retlige forpligtelser, som ifølge national ret eller fællesskabsret er undergivet formkrav, og det berører heller ikke de regler og begrænsninger, der efter national ret eller fællesskabsret gælder for anvendelsen af dokumenter”. Bestemmelsen betyder, at det fortsat vil være op til medlemsstaterne at afgøre, på hvilke retsområder og i hvilke situationer man vil acceptere brugen af digital kommunikation. Det gælder også spørgsmålet om, hvorvidt medlemsstaterne vil acceptere, at elektronisk signatur skal opfylde formkrav om underskrift mv. Direktivet vil således ikke få betydning for spørgsmålet om, hvorvidt formkrav i lovgivningen om skriftlighed eller underskrift kan opfyldes ved brug af digital kommunikation og elektronisk signatur.

I direktivets artikel 5, stk. 1, knyttes visse retsvirkninger til en såkaldt “avanceret elektronisk signatur”, som er en elektronisk signatur, der lever op til særligt høje sikkerhedskrav. Reglerne i artikel 5 går ud på, at en “avanceret elektronisk signatur”, som er frem-

bragt på sikker vis, skal kunne benyttes som bevis i retssager, samt at medlemsstaterne skal sikre, at elektronisk signaturer, som lever op til EU-reglerne, opfylder krav i national ret om signatur på digitale meddelelser. Det sidste led i bestemmelsen indebærer, at hvis national lovgivning indeholder krav om, at en digital meddelelse skal være forsynet med signatur eller lignende, så skal dette krav anses for opfyldt, hvis der er brugt en “avanceret elektronisk signatur”. Et sådant krav kan enten forekomme, hvor der er givet en udtrykkelig regel om, at digital kommunikation kan anvendes på et bestemt retsområde, eller fordi en regel med et generelt formuleret underskriftskrav, som måske oprindeligt var tiltænkt anvendelse ved brug af papirdokumenter, må forstås således, at dette krav også kan opfyldes ved brug af elektronisk signatur.

I direktivets artikel 3, stk. 7, findes en begrænset undtagelse fra dette princip, idet medlemsstaterne ved kommunikation med det offentlige har ret til at stille supplerende krav til de elektroniske signaturer. Anvendelsesområdet for undtagelsen er imidlertid ganske snævert, idet sådanne nationale særregler skal være nødvendiggjort af særlige forhold og skal være “objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende”.

Bestemmelsen om, at “avanceret elektronisk signatur” skal opfylde formkrav i national ret om elektronisk signatur, indebærer visse begrænsninger for, hvad der vil kunne fastsættes i dansk lovgivning. Reglen betyder, at der ikke vil kunne stilles krav i dansk ret om overholdelse af et strengere sikkerhedsniveau end det, der efter direktivet gælder for “avanceret elektronisk signatur”. Derimod er der ikke noget til hinder for, at man stiller mindre strenge krav på områder, hvor det er tilstrækkeligt med et lavere sikkerhedsniveau.

Direktivet indeholder i artikel 5, stk. 2, en supplerende regel om elektronisk signaturs retsvirkninger. Bestemmelsen indeholder et generelt forbud mod at nægte elektronisk signatur “retskraft og anerkendelse som bevis under retssager”, alene fordi signaturen er elektronisk eller ikke lever op til sikkerhedskravene for “avanceret elektronisk signatur”. Bestemmelsen drejer sig om alle former for elektronisk signatur, herunder signatur, som

af den ene eller anden grund ikke opfylder de krav, som skal være opfyldt for at opnå retsvirkninger efter artikel 5, stk. 1.

Den nærmere forståelse af bestemmelsen i direktivets artikel 5 drøftes nedenfor i kapitel 4.3.7.

3.2.2. Direktivet om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked

Europa-Kommissionen fremsatte endvidere i november 1998 et forslag til direktiv om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("Direktivet om elektronisk handel"). Direktivet blev vedtaget den 8. juni 2000 som Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked ("Direktivet om elektronisk handel"). Direktivet er optaget som bilag 2 til denne betænkning.

Direktivet har til formål at sikre den frie bevægelighed af "informationssamfunds-tjenester", dvs. tjenester, som mod betaling og efter individuel anmodning leveres ved brug af elektronisk udstyr til behandling og opbevaring af data. Begrebet omfatter bl.a. levering af internetforbindelser, digitale nyhedstjenester og udbud af varer og tjenester på Internettet. Direktivet indeholder bestemmelser om en lang række retlige spørgsmål, som opstår i forbindelse med erhvervsmæssige aktiviteter på Internettet.

Direktivet indeholder navnlig én bestemmelse, som har betydning for de spørgsmål, som udvalget er blevet anmodet om at overveje. Direktivets artikel 9 indeholder således en regel om, at medlemsstaternes lovgivning mv. ikke må "skabe forhindringer" for indgåelsen af kontrakter ad elektronisk vej. Bestemmelsen indebærer en pligt for medlemsstaterne til

at ændre samtlige nationale retsregler, der i praksis kan hindre, begrænse eller afholde fra anvendelsen af “elektroniske kontrakter”. Hvad der skal forstås ved en elektronisk kontrakt, er ikke præciseret i direktivet, som imidlertid indeholder nogle undtagelser, som synes at pege på, at begrebet skal fortolkes ganske bredt. Således har man fundet det nødvendigt udtrykkeligt at undtage kontrakter inden for familie- og arveretten fra bestemmelsens anvendelsesområde. Selv om sådanne dispositioner - i hvert fald i dansk ret - sædvanligvis ikke betegnes som “kontrakter”, må det på denne baggrund formentlig antages, at f.eks. bodelingsoverenskomster ville have været omfattet af bestemmelsen, hvis ikke de var blevet undtaget.

3.3. FN

3.3.1. UNCITRAL’s “Model Law on Electronic Commerce”

FN vedtog i 1996 en modellov om elektronisk handel. Modelloven, som er udarbejdet af UNCITRAL (United Nations Commission on International Trade Law), indeholder en række bestemmelser om juridisk anerkendelse af digital kommunikation, bl.a. i form af regler om fortolkningen af formkrav om skriftlighed, underskrift eller om at oplysninger fremlægges eller opbevares i original form. Modelloven og den tilhørende “Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce” er optaget som bilag 3 til betænkningen.

Bestemmelserne i modelloven er udarbejdet med henblik på anvendelse i internationale kommercielle forhold. Andre hensyn, f.eks. til forbrugerbeskyttelse og til de særlige spørgsmål af bl.a. databeskyttelsesmæssig karakter, som opstår ved kommunikation med offentlige myndigheder, har således ikke indgået i overvejelserne ved udarbejdelsen af modelloven.

Modellovens regler tager udgangspunkt i det forhold, at et papirdokument og et digital dokument ikke er det samme, og at digitale dokumenter derfor ikke kan “ligestilles” med papirdokumenter. I “Guide to enactment” anføres i paragraf 17:

“A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document.”

I paragraf 18 anføres videre:

“The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enables such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function.”

Tanken er altså den, at man ved vurderingen af, om et formkrav kan opfyldes ved digital kommunikation, skal tage udgangspunkt i de funktioner, som formkravet varetager. Kan disse funktioner udføres af digitale medier, så kan formkravet også opfyldes af disse.

For at hjælpe ved afgørelsen af, om digital kommunikation kan udføre de funktioner, som et formkrav varetager, opstiller modelloven nogle fortolkningsregler. Disse regler angiver de betingelser, som et digital dokument skal leve op til, for at det kan opfylde nogle bestemte formkrav i lovgivningen, bl.a. om skriftlighed og om underskrift.

Fortolkningsreglen vedrørende formkrav om skriftlighed findes i artikel 6:

“Article 6. Writing.

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirements therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].”

Til hjælp ved fortolkningen af bestemmelsen anføres i “Guide to Enactment”, paragraf 50:

“50. The purpose of article 6 is not to establish a requirement that, in all instances, data messages should fulfil all conceivable functions of a writing. Rather than focusing upon specific functions of a “writing”, for example, its evidentiary function in the context of tax law or its warning function in the context of civil law, article 6 focuses upon the basic notion of the information being reproduced and read.

...

The use of the word “accessible” is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word “usable” is not intended to cover only human use but also computer processing. As to the notion of “subsequent reference”, it was preferred to such notions as “durability” or “non-alterability”, which would have established too harsh standards, and to such notions as “readability” or “intelligibility”, which might constitute too subjective criteria.”

Bestemmelsen bygger altså på den grundtanke, at formkrav i lovgivningen mv. om skriftlighed kan fortolkes således, at de kan opfyldes ved brug af digitale dokumenter, blot de digitale dokumenter er tilgængelige på en sådan måde, at de er tilgængelige for senere opslag. Det blotte krav om skriftlighed antages således navnlig at have til formål at udelukke mundtlighed. Ved udformningen af bestemmelsen var man - som det fremgår af citatet - opmærksom på, at der kan forekomme tilfælde, hvor skriftlighedskravet tjener andre funktioner end blot at sikre, at der findes en optegnelse, som er tilgængelig på et senere tidspunkt. I “Guide to Enactment” paragraf 51 anføres herom:

“An enacting State may wish to exclude specifically certain types of situations, depending on the purpose of the formal requirement in question. One such type of situation may be the case of writing requirements intended to provide notice or warning of specific factual or legal risks, for example, requirements for warnings to be placed on certain types of products. Another specific exclusion might be considered, for example, in the context of formalities required pursuant to international treaty obligations of the enacting State (e.g. the requirement that a cheque be in writing pursuant to the Convention providing a Uniform Law for Cheques, Geneva, 1931), and other kinds of situations and areas of law that are beyond the power of an enacting state to change by means of a statute.”

Fortolkningsreglen vedrørende formkrav om underskrift findes i artikel 7:

“Article 7. Signature.

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

- (a) a method is used to identify that person and to indicate that person’s approval of the information contained in the data message; and*
- (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

(2) Paragraph (1) applies whether the requirements therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].”

Bestemmelsen anlægger således den samme synsvinkel på spørgsmålet om fortolkning af formkrav om underskrift som den, der anvendes i artikel 6 vedrørende skriftlighedskrav. Krav om underskrift skal som udgangspunkt anses for opfyldt af et digitalt dokument, hvis dette er forsynet med en passende sikker metode til identifikation af udstederen og som udtryk for dennes godkendelse af meddelelsen.

I “Guide to Enactment” paragraf 58 anføres, at der vil kunne opstå spørgsmål om, hvorvidt metoden i artikel 7, stk. 1, er egnet på alle områder. Det fremhæves, at en vurdering af, om metoden kan anvendes i relation til et bestemt formkrav, må afhænge af en lang række faktorer. Bl.a. nævnes, at der må lægges vægt på, hvilken funktion underskriftskravene udfylder på et givet retsområde, og på vigtigheden af de oplysninger, som findes i den digitale kommunikation.

3.3.2. UNCITRAL’s forslag til “Uniform Rules on Electronic Signatures”

Efter at have færdiggjort arbejdet med modelloven er UNCITRAL i 1996 gået i gang med at udarbejde et mere detaljeret regelsæt om anvendelsen af elektronisk signatur. Det har imidlertid vist sig vanskeligt at nå til enighed, og der forhandles stadig om det nærmere indhold af reglerne.

Ligesom modelloven om elektronisk handel drejer udkastet til “Uniform rules” sig alene om kommercielle forhold. Formålet med de foreslåede regler er bl.a. at give regler om, i hvilke tilfælde en elektronisk signatur kan opfylde formkrav i lovgivning og andre retsregler om underskrift. Bestemmelsen herom, som findes i forslagets artikel 6, er således tæt forbundet med bestemmelsen om “signature” i artikel 7 i modelloven om elektronisk handel.

Der forhandles i øjeblikket om flere forskellige formuleringer af bestemmelsen. De forskellige varianter har imidlertid det til fælles, at de giver regler om, at en digital meddelelse, der er forsynet med en elektronisk signatur, som lever op til visse sikkerhedskrav, skal “formodes at være underskrevet” (it is presumed that the data message is signed), og således opfylde formkrav om underskrift. Det skal dog overlades til medlemsstaterne at undtage bestemte formkrav, som ikke skal kunne opfyldes ved sådanne elektroniske signaturer.

Hvis der vedtages en bestemmelse af det skitserede indhold, vil dette indebære, at der gives en “genvej” til at sikre sig, at man lever op til kravene i artikel 7 i modelloven om elektronisk handel. Hvis man opfylder de sikkerhedsmæssige betingelser, vil man nemlig være sikker på, at man opfylder et formkrav om underskrift, medmindre dette direkte er undtaget.

3.4. Initiativer i andre lande

3.4.1. Sverige

Den svenske Riksdag vedtog den 2. november 2000 en ny lov om elektroniske signaturer, lag (2000:832) om kvalificerade elektroniska signaturer, som gennemfører EU-direktivet i svensk ret.

Loven indeholder navnlig regler om etablering og drift af nøglecentre og om de krav som må stilles, for at elektronisk signatur kan betegnes som sikker. I loven defineres en særlig kategori – ”kvalificerad elektronisk signatur” – som er særligt sikre, fordi sådanne signaturer skal frembringes ved brug af en sikker metode til signaturfremstilling og skal være baseret på et nøglecertifikat, som lever op til særligt høje krav.

Loven regulerer på enkelte punkter spørgsmålet om retsvirkningerne af, at man anvender elektronisk signatur. I § 17 findes følgende bestemmelse:

”17 § Om det i lag eller annan författning ställs krav på egenhändig underskrift eller motsvarande och om det är tillåtet att uppfylla kravet med elektroniska medel, skall en kvalificerad elektronisk signatur anses uppfylla kravet. Vid

kommunikation med eller mellan myndigheter kan dock användningen av elektroniska signaturer vara förenad med ytterligare krav.”

Bestemmelsen giver således de ”kvalificerede elektroniske signaturer” en vis særstilling, idet de altid skal opfylde formkrav om underskrift mv., hvis formkravet kan opfyldes ved brug af digital kommunikation.

Loven indeholder ikke andre regler om retsvirkningerne af at anvende elektronisk signatur. Således er bl.a. spørgsmålene om retsvirkningerne af at anvende elektronisk signatur efter udløbet af certifikatets gyldighedsperiode eller efter at certifikatet er blevet spærret, ikke reguleret.

Loven indeholder heller ikke regler om, hvornår formkrav om skriftlighed, underskrift eller lignende kan opfyldes ved brug af digital kommunikation. Svensk ret indeholder ikke generelle regler om anvendelsen af digital kommunikation mv. på områder med formkrav, og besvarelsen af spørgsmålet vil således afhænge af en fortolkning af de enkelte formkrav. I en betænkning fra 1996³ blev det foreslået at indføre en generel regel i den svenske forvaltningslov, som generelt skulle åbne op for at anvende digitale dokumenter med elektronisk signatur ved kommunikation med det offentlige. Forslaget er imidlertid endnu ikke blevet gennemført, og indtil nu er brugen af digital kommunikation i stedet blevet reguleret ved, at der på visse områder er blevet åbnet for brugen af digital kommunikation ved ændringer af enkelte retsregler. Bl.a. er der på told- og skatteområdet givet regler, som tillader brugen af digital kommunikation, hvor der tidligere stilledes krav om papirdokumenter.

³ SOU 1996:40 ”Elektronisk dokumenthantering”.

I en betänkning fra 1998⁴ dröftes muligheden for at gennemføre generelle regler, som "ligestiller" elektronisk signatur med håndskrevne underskrifter. Herom anføres side 183 f.:

"Den första fråga som kan ställas är om en digital signatur - om den uppfyller en viss säkerhetsnivå - generellt skall ges samma rättsverkan som en egenhändig underskrift. Det finns en fördel med en lagstiftningsmetod som har en sådan innebörd. Alla de lagar och föreskrifter som innehåller krav på underskrift kan på en gång fås att omfattas av användning av digitala signaturer genom en lagregel om jämställande med underskrift. Å andre sidan kan införandet av en sådan lagregel i ett skede där tekniken inte har prövats i större skala i öppna nätverk i transaktioner av alla möjliga slag få oanade konsekvenser.

Mot bakgrund av bl.a. de olika skälen bakom formkraven i olika författningar torde en generellt verkande reglering innebärande att digitala signaturer godtas i stället för egenhändiga namnteckningar över hela rättsområdet inte vara möjlig."

I betänkningen overvejes endvidere spørgsmålet om, hvorvidt der er grund til at give særlige regler om bevisværdien af elektronisk signatur, navnlig i relation til en indsigelse fra nøgleindehaveren om, at en signatur, som er givet "i hans navn", ikke stammer fra ham. Herom anføres (a.st. side 185 f.):

"I fråga om bevisverkan torde det för lagstiftaren enbart röra sig om att kunna uppställa bevisbörderegler, t.ex. ved förnekande av en digital signatur. Något skäl att i fråga om digitala signaturer avvika från de bevisregler som tillämpas i övrigt kan knappast sägas föreligga. Det förefaller därför inte ändamålsenligt att uppställa särskilda bevisbörderegler som avviker från vad som i dag gäller vid förfalskningsinvändningar. Någon lagreglering bör alltså inte göras beträffande bevisbördan. De fördelar som i bevishänseende kan uppnås genom strukturerade förfaranden för att åstadkomma digitala signaturer med en angiven säkerhetsnivå kan likväl bli betydande. Av betydelse ur bevishänseende är särskilt i vad mån systemen är reviderbara för det enskilda fall där t.ex. äktheten hos en digital signatur sätts i fråga."

⁴ DS 1998:14 "Digitale signaturer - en teknisk og juridisk oversikt".

3.4.2. Norge

Den norske regering har iværksat en gennemgang af norsk ret med henblik på at finde ud af, hvor der findes formkrav, der hindrer anvendelsen af digital kommunikation. I begyndelsen af 1999 blev samtlige norske ministerier således anmodet om at gennemgå lovgivningen inden for deres ressortområde for at finde de retsregler, der på den ene eller anden måde lægger hindringer i vejen for en hensigtsmæssig anvendelse af digital kommunikation. Resultaterne af gennemgangen blev i juni 2000 offentliggjort i en rapport fra det norske Nærings- og Handelsdepartement.⁵

Den norske regering har tilkendegivet, at det er dens hensigt at følge denne kortlægning op med lovændringer på de områder, hvor det er muligt og hensigtsmæssigt at anvende digital kommunikation, og hvor et formkrav hindrer dette. I forbindelse med iværksættelsen af gennemgangen anførte det norske Justisdepartement i et brev til de involverede ministerier bl.a., at der er grund til at understrege, at der på mange områder slet ikke findes retlige hindringer for anvendelsen af digital kommunikation. I den private sektor gælder som udgangspunkt princippet om aftalefrihed, og der gælder normalt hverken krav om, at aftaler skal indgås eller bevises skriftligt, og heller ikke noget krav om, at aftaler underskrives. På sådanne områder står det efter norsk ret private frit for at anvende digital kommunikation ved deres indbyrdes kommunikation. Norsk ret bygger endvidere på principperne om fri bevisførelse og fri bevisvurdering, og der er derfor heller ikke noget til hinder for at anvende digital kommunikation og elektronisk signatur som bevis under en retssag.

I brevet nævner Justisdepartementet videre, at der på de områder, hvor den norske lovgivning indeholder formkrav, nogle gange kan være tvivl om, hvorvidt disse krav kan opfyldes ved brug af digital kommunikation. Herom anføres det, at en sådan tvivl ofte

⁵ Kartleggingsprojektet - Kartlegging av bestemmelser i lover, forskrifter og instrukser som kan hindre elektronisk kommunikasjon, Nærings- og Handelsdepartementet, Oslo juni 2000.

vil kunne afklares ved, at reglen fortolkes og anvendes af domstolene, forvaltningen eller andre retsanvendende myndigheder mv. For at skabe klarhed om retsstillingen for borgere og virksomheder og for at fremme det overordnede mål om en øget anvendelse af digital kommunikation, foreslår Justisdepartementet dog, at de enkelte ministerier overvejer at ændre sådanne uklare regler, eller at man i stedet udsender en vejledning eller lignende, som forklarer, hvordan bestemmelsen skal forstås.

Som et sidste område, der skal overvejes i forbindelse med kortlægningen af formkrav i norsk lovgivning, nævner Justisdepartementet, at der også findes formkrav, som slet ikke kan opfyldes af digitale dokumenter. Om disse krav anføres det, at de ofte er udformet uden tanke på digital kommunikation og derfor kommer til at forudsætte brug af papir, uden at dette egentlig var tanken. Kortlægningen skal give et bedre overblik over, hvilke hensyn sådanne formkrav varetager, således at man får et forsvarligt grundlag for at tage stilling til, hvilke krav som bør stilles, for at digitale dokumenter kan anvendes på disse områder, og til om der findes områder, hvor papirdokumenter fortsat bør foretrækkes.

I projektrapporten har man systematiseret de forskellige typer af formkrav, som er blevet fundet ved ministeriernes gennemgang, og undersøgt om det er muligt at knytte en bestemt forståelse til de anvendte begreber som ”skriftligt”, ”underskrift” osv. Konklusionen er imidlertid blevet, at dette ikke er muligt, fordi formkravene har forskellige begrundelser og varetager forskellige formål.

I rapporten skitseres herefter 3 mulige modeller til at ”modernisere” lovgivningen:

- 1) en generel lov, som sidestiller digital og papirbaseret kommunikation,
- 2) ændring af hver bestemmelse for sig ved traditionelle ændringslove og
- 3) en ”mellemløsning”, som navnlig indebærer, at forvaltningen pålægges at tage stilling til, om lovgivningen tillader digital kommunikation, og til i rimelig grad at indrette lovgivningen således, at digital kommunikation kan anvendes.

Rapporten indeholder imidlertid ikke nogen anbefaling om, hvilken af de 3 modeller, som bør anvendes. Den norske rapport er nærmere omtalt nedenfor i kapitel 6.2.1. og 6.3.1.

På et i praksis vigtigt område, nemlig kommunikation og aftaler mellem kunder og pengeinstitutter, har man i Norge allerede indført regler, der gør det muligt at anvende digital kommunikation. I finansaftaleloven⁶ er der således i § 8 indsat en bestemmelse, der som altovervejende hovedregel gør det muligt at anvende digital kommunikation mellem kunder og pengeinstitutter.

"§ 8. Bruk af elektronisk kommunikasjon og elektroniske medier

- (1) Krav i eller i medhold af denne loven om at opplysninger eller meldinger skal gis skriftlig, er ikke til hinder for bruk av elektronisk kommunikasjon dersom kunden ønsker dette.*
- (2) Krav i eller i medhold af denne loven om at en avtale skal indgås skriftlig, er ikke til hinder for at avtalen inngås ved hjelp av et elektronisk medium dersom kunden ønsker dette, og*
 - a) avtalens innhold i sin helhet er tilgjengelig for kunden ved avtaleinngåelsen, og*
 - b) det er benyttet en betryggende metode for å autentisere inngåelsen av en avtale med det angitte innhold."*

Spørgsmålet om brug af digital kommunikation i forbindelse med oplysninger og meddelelser mellem parterne i en finansaftale drøftes nærmere i bemærkningerne til forslaget. Heri anføres, at skriftlighedskrav på dette område navnlig har til formål at sikre, at oplysninger gives på en tydelig måde og dermed i første række har til formål at udelukke, at oplysningerne gives mundtligt. Bestemmelsen i § 8, stk. 1, har på denne baggrund til formål generelt at åbne op for, at oplysninger – hvis forbrugeren ønsker det - kan gives i digital form, blot der anvendes skrifttegn.

Vedrørende spørgsmålet om digital aftaleindgåelse anføres det i bemærkningerne til lovforslaget, at krav om skriftlig aftaleindgåelse bl.a. kan begrundes ud fra hensynet til be-

⁶ Lov nr. 46 af 25. juni 1999.

vissikring. Ved indgåelse af aftaler af den art, som lovforslaget drejer sig om, er det vigtigt, at det kan bevises, hvad parterne har aftalt, og at parterne har indgået en bindende aftale. Selv om man ikke kan udelukke muligheden for fejlskrift eller forfalskning, og den traditionelle skriftlige aftaleindgåelse derfor ikke giver fuldstændig sikkerhed, vil bevishensynet normalt anses for at være tilgodeset, hvis aftalen er nedfældet på papir og underskrevet af begge parter. Loven bør imidlertid ikke foreskrive, at der altid skal anvendes papirdokumenter, når en finansaftale skal indgås. Hvis man på tilfredsstillende måde kan varetage de hensyn, som ligger bag kravet om skriftlighed, dvs. navnlig sikre beviset for indholdet af aftalen, bør det også være muligt at indgå finansaftaler på digital vis.

Selv om man altså har fundet, at digital kommunikation generelt vil kunne udfylde de funktioner, som hidtil er blevet varetaget af papirdokumenter, gælder dette dog ikke undtagelsesfrit. Kautionsaftaler er således ikke omfattet af lovens § 8, stk. 2, da man har fundet, at der her knytter sig en særlig beskyttelsesvirkning til brug af papiret. Herom anføres i bemærkningerne, at der, når en forbruger påtager sig en kautionsforpligtelse, gør sig nogle særlige hensyn gældende, som bedst varetages ved en traditionel papirbaseret aftalemodel.

3.4.3. Finland

Den finske Befolkningsregistercentral (der svarer til det danske CPR-register) blev af statsrådet den 5. februar 1998 udpeget til at skulle være et statsligt nøglecenter for elektronisk signatur i Finland. I forbindelse med statsrådets beslutning blev det endvidere bestemt, at Justitsministeriet og de øvrige ministerier inden den 30. juni 1999 skulle forberede den lovgivning, der var nødvendig for udbredelsen af digital myndighedsudøvelse i forvaltningen, herunder anvendelsen af digitale dokumenter og elektroniske signaturer, elektroniske identitetskort og nøglecenterservices.

Den finske riksdag har herefter i 1999 vedtaget forskellige ændringer i lovgivningen samt vedtaget ny lovgivning med henblik på at gøre det muligt at anvende digital kommunikation i forvaltningen. Nogle af de vigtigste ændringer i den finske lovgivning er foretaget i lov om registerforvaltningen og befolkningsdatalagen, og Riksdagen vedtog endvidere to nye love om identitetskort og om digital kommunikation i forvaltningen.

Lag om identitetskort indeholder regler om udstedelse af identitetskort til borgerne, herunder regler om udstedelse af elektroniske identitetskort til borgerne.

Lovens § 1 er formuleret således:

”Polisen utfärder på ansökan intyg över identiteten (identitetskort) för finska medborgare samt för utlänningar som är stadigvarande bosatta i Finland enligt lagen om hemkommun (201/1994) och som har införts i befolkningsdatasystemet samt vilkas identitet har kunnat konstateras på ett tillförlitligt sätt.

*Polisen kan på sökandens begäring utfärda et identitetskort som innehåller den tekniska del som behövs vid elektronisk kommunikation (elektroniskt identitets-kort). Med hjälp av et elektronisk identitetskort kan en person dessutom vid behov underteckna handlinger og meddelanden med elektronisk signatur og kryptera dem.
.....”*

Lovens § 3 indeholder regler om muligheden for, at et identitetskortet kan indeholde og anvendes som et certifikat til brug for digital kommunikation inden for forvaltningen:

”För elektroniska identitetskort kan utfärdas certifikat för användning af korten vid elektronisk kommunikation inom förvaltningen. Certifikaten utfärdas af Befolkningsregistercentralen. I 23 § befolkningsdatalagen (507/1993) finns bestämmelser om ansökningsförfarandet vid utfärdande av certifikat.

På det elektroniska identitetskortet finns, utöver vad som bestäms i 2 §, certifikatets datainnehåll enligt 20 § befolkningsdatalagen, sådana upp-gifter för identifiering af kortinnehavaren som förutsätts vid användningen av elektro-

niska identitetskort samt nödvändiga tekniska uppgifter. På det elektroniska identitetskortet antecknas även uppgift om utfärdaren av certifikaten.

På det elektroniska identitetskortet kan på kortinnehavarens begäran registreras tekniska tillämpningar eller uppgifter för olika användningsändamål.”

Det fremgår af de almindelige bemærkningerne til forslaget, at de elektroniske identitetskort, der er udstedt af staten, bl.a. kan bruges til at identificere en person, der sender data til forvaltningen i åbne net. I bemærkningerne anføres at:

”Statens elektroniska identitetskort är avsett för elektronisk kommunikation där det krävs en stark elektronisk autentisering av personen i fråga, kryptering av material som skickas eller överförs i datanätet och elektro-nisk signatur. Målet er at skapa et system som verifierar meddelandets avsändare och ursprung samt vid behov garanterar konfidentiell och oförändradinformation, tryggar meddelandets oavvislighet och verifierar transaktionens exakta tidspunkt. En lösning som baserar sig på aktivt kort möjliggör en säker användning av krypteringsmetoder som är avsedda för kryptering och dekryptering av material. Tillsammans utgör dessa basservicen inom sådan elektronisk kommunikation som sker med hjälp av statens elektroniska identitetskort

...

För ökande av den allmänna tillförligligheten inom metoden med en öppen nyckel säkerställer den som tilhandahåller certifieringstjänster att en vis person har ett visst nyckelpar som består av öppen och en privat nyckel. Den som tilhandahåller certifieringstjänster skaper certifikaten sköter uprätthållandet av dem och för vid behov in dem på en spärlista. Befolkningsregistercentralen skall tilhandahålla certifieringstjänster inom statsförvaltningen. Befolkningscentralen har emellertid inte ensamrätt att tilhandahålla certifieringstjänster inom den privata eller den offentliga sektorn. Inom den privata sektorn torde slag av certifieringstjänster för olika kundgrupper och för olika behov, t.ex. för elektronisk handel, banksektorn och informationsutbyte mellan myndigheter och medborgare”.

I lag om ändring av 23 § befolkningsdatalagen fastsattes der betingelser for Befolkningsregistercentralens udstedelse af et certifikat i forbindelse med det elektroniske identitetskort. Det fremgår af bestemmelsen, at det er det lokale politi, der modtager ansøgningen om udstedelse af et elektronisk identitetskort, og at den skal

indleveres ved personligt fremmøde. Det fremgår endvidere af § 6 i lov om identitetskort, at det elektroniske identitetskort også skal afhentes personligt.

§ 23 i befolkningsdatalagen er formuleret således:

”Befolkningsregistercentralen kan på sökandens begäran utfärda certifikat för elektroniska identitetskort som avses i lagen om identitetskort (829/1999) samt för andra kort eller tekniska anordningar som används för elektronisk kommunikation.

Ansökan om certifikat som Befolkningsregistercentralen utfärder för elektroniska identitetskort som avses i lagen om identitetskort skall personligen inlämnas til polisinrättningen i ett härad. Polisinrättningen utför därefter en identifiering av sökanden.

.....

I fråga om sådana certifikat för elektronisk kommunikation inom förvaltningen som utfärdas för andra än i 2 och 3 mom. avsedda kort eller tekniska anordningar kan Befolkningsregistercentralen med en annan myndighet, ett företag eller en sammanslutning komma överens om att ansökan personligen kan inlämnas til denna myndighet, detta företag eller denna sammanslutning för vidarebefordran til Befolkningsregistercentralen. Befolkningsregistercentralen skall härvid säkerställa att den som tar emot ansökan iakttar de krav som i personuppgiftslagen (523/1999) ställs på behandlingen av personuppgifter.

Den som tar emot ansökan skall identifiera sökanden med hjälp av en gällande, av polisen utfärdad handling som styrker identiteten och med hjälp av en kontroll av personens uppgifter i befolkningsdatasystemet på det sätt som närmare bestäms genom förordning. Om sökanden inte har någon sådan av polisen utfärdad i förordning närmare angiven handling varav identiteten fremgår eller om den finns andra särskilda skäl for att säkerställa identifieringen, utförs den identifiering som hänför sig til ansökan av polisen.”

Lag om elektronisk kommunikation i förvaltningsärenden etablerer rammerne omkring anvendelsen af digitale kommunikation med og i forvaltningen. Loven indeholder bestemmelser om myndighedernes og borgernes rettigheder, pligter og ansvar i forbindelse med digital kommunikation i forvaltningen. Loven indeholder regler om certifikater, certifikatudsteder, elektronisk signatur, opfyldelse af formkrav ved anvendelse af digital kom-

munikation mv. Loven regulerer ikke privates etablering mv. af nøglecentre, hvor der ikke foretages kommunikation med forvaltningen.

I lovens § 18 fastsættes det, at såfremt en myndighed har tilstrækkelig teknisk og økonomisk beredskab, skal der så vidt muligt tilbydes offentligheden mulighed for digital kommunikation. Det er op til myndigheden selv at beslutte, om forudsætningerne for at tilbyde digital kommunikation til borgerne er tilstede. Det skal altså ikke være en ret for borgerne at kommunikere digitalt med det offentlige.

Tilbyder myndigheden borgerne, at de kan kommunikere digitalt, og indeholder lovgivningen formkrav om skriftlighed og underskrift, skal disse formkrav anses for opfyldt, såfremt der anvendes digitale dokumenter og elektroniske signaturer. Endvidere bestemmes det i loven, hvornår et digitalt dokument anses for at være kommet frem til myndigheden.

Bestemmelserne om formkrav og ankomsttidspunktet mv. findes i lovens §§ 21 - 23

§ 21:

”Ansaret för att elektroniska meddelanden kommer fram

Elektroniska meddelanden sänds til myndigheterna på avsändarens eget ansvar.”

§ 22:

”Anhängiggörande av ärenden genom elektroniska dokument

Skall et ärende anhängiggöras skriftligen, kan det anhängiggöras också genom et elektronsik dokument som sänds til myndigheten.

Skall et ärende anhängiggöras genom undertecknad handling godkänns en elektronisk signatur som underskrift, om certifikatutfärdaren og certifikatet uppfyller kraven i 4 og 5 §.”

§ 23:

”Ankomsttidpunkten för ett elektroniskt meddelande

Ett elektronisk meddelande anses ha inkommit til en myndighet när det är tillgängligt för myndigheten i en mottagaranordning eller et datasystem på sådant sätt att meddelandet kan behandlas.

Kan det tidpunkt som avses i 1 mom. inte utredas, anses et elektroniskt meddelande ha inkommet vid den tidpunkt då det har avsänts, om det kan läggas fram tillförlitlig utredning om denna tidpunkt.”

Lag om elektronisk kommunikation i förvaltningsärenden svarer på mange områder til direktivet om en fællesskabsramme om elektroniske signaturer, men der er ikke tale om en implementering af direktivet. Direktivet var stadig under udarbejdelse, da propositionen (lovforslaget) blev fremsat for riksdagen.

3.4.4. Tyskland

Den tyske Bundestag vedtog 22. juli 1997 en lov om informations- og kommunikationstjenester, som i artikel 3 indeholder regler om digital signatur ("Signaturgesetz").

Lovens formål er at opstille generelle betingelser, under hvilke digitale signaturer kan betragtes som sikre, og som sikrer, at falske digitale signaturer eller forfalskninger af signerede data kan konstateres på troværdig vis.

Dette mål søges nået ved at tilvejebringe regler om et højt sikkerhedsniveau ved frembringelsen af signaturnøgler, ved nøglecentrenes sammenknytning af en signaturnøgle med en bestemt person, og ved kontrollen af den digitale signatur ved hjælp af den offentlige signaturnøgle. Loven og de tilhørende administrative forskrifter indeholder således en række krav til de tekniske og organisatoriske forhold omkring digital signatur.

Reglerne i den tyske lov er frivillige i den forstand, at det ikke er udelukket at anvende digitale signaturer, som ikke lever op til lovens krav. Fordelen ved at benytte en digital signatur, som opfylder lovens krav, er imidlertid, at man så vil have et særligt "kvalitetsstempel", som indikerer, at signaturen lever op til strenge sikkerhedskrav.

Den tyske lov indeholder endvidere ikke regler om retsvirkningerne af anvendelsen af digital signatur. I bemærkningerne til forslaget anføres det, at værdien af en signeret digital meddelelse som bevis for, at meddelelsen stammer fra den angivne underskriver, vil afhænge af, hvor godt den digitale signatur er sikret mod misbrug mv.

Det anføres således, at det må formodes, at domstolene - inden for rammerne af den frie bevisbedømmelse - vil tillægge digitale meddelelser, som er signeret med et produkt, der opfylder lovens strenge sikkerhedskrav, en betydelig værdi som bevis.

I de administrative forskrifter, der er udstedt i medfør af loven, er det bl.a. fastsat, at certifikater ikke kan være gældende i længere tid end højst 5 år, dog ikke i længere tid, end de anvendte algoritmer m.v. er sikre. Er de anvendte metoder f.eks. kun sikre i 3 år, gælder certifikatet kun i denne periode.

Skal den digitale meddelelse være "underskrevet" i længere tid, end den digitale signatur er sikker, skal meddelelsen forsynes med en ny digital signatur, inden den oprindelige signatur ikke længere er sikker. Med andre ord skal en digital meddelelse til enhver tid være forsynet med en digital signatur, som er sikker, for at kunne betragtes som "underskrevet". Retsvirkningen af, at man ikke overholder denne regel, er ikke angivet i bestemmelserne, som heller ikke indeholder regler om de øvrige virkninger heraf, f.eks. om der kan støttes ret på en digital signatur, efter at certifikatet er udløbet.

3.4.5. UK

Den britiske regering fremlagde i marts 1999 et dokument, som har udgjort grundlaget for en national høring om en række spørgsmål, som opstår i forbindelse med elektronisk handel⁷.

Et af de spørgsmål, som behandles i dokumentet, er om formkrav i lovgivningen om skriftlighed eller underskrift kan opfyldes ved anvendelse af digital kommunikation. Herom anføres, at det er vigtigt, at lovgivningen er ”teknologineutral”, hvorved forstås, at retsreglerne så vidt muligt ikke skal diskriminere mellem den traditionelle og den digitale måde at gøre tingene på. Det er efter britisk ret tvivlsomt, om formkrav i lovgivningen om underskrift kan opfyldes ved brug af elektronisk signatur, mens det er sikkert, at formkrav om, at information gives skriftligt, ikke kan opfyldes ved brug af digitale medier. Det anslås, at der findes op imod 40.000 bestemmelser i lovgivningen, som benytter ordene ”writing” og ”signature”.

Det anføres, at sådanne formkrav udgør hindringer for elektronisk handel og digital administration, som den britiske regering ønsker at fjerne. På den anden side er regeringen opmærksom på, at formkravene er udviklet i løbet af mange hundrede års praksis og lovgivning, og at det ikke vil være hensigtsmæssigt med et slag at ændre alle disse krav, bl.a. fordi det vil kunne have uforudsete konsekvenser på områder, hvor der på nuværende tidspunkt ikke er grundlag for at forlade papiret.

Den britiske regering foreslog derfor to metoder til at modernisere lovgivningen. Den ene model gik ud på at ændre hver enkelt formkrav ved individuel lovgivning. Det anføres, at denne model vil have den fordel, at man undgår uforudsete konsekvenser, men på den anden side vil være tidskrævende og forudsætte, at der er plads i lovgivningsprogrammet til at gennemføre alle de nødvendige lovændringer.

⁷ Department of Trade and Industri: Building confidence in electronic commerce - a consultation paper.

Den anden model gik ud på at bemyndige regeringen til at ændre lovbestemte formkrav i sekundær lovgivning (bekendtgørelser). Det anføres, at denne model har den fordel, at den gør det muligt at foretage en individuel vurdering og tilpasning af hvert enkelt formkrav uden det besvær og tidsforbrug til udarbejdelse af lovforslag, som den første model indebærer. På den anden side anføres det, at denne model indebærer en meget betydelig delegation af lovgivningskompetence til regeringen, og at det i givet fald vil være nødvendigt at opstille nogle klare rammer for, hvilke ændringer regeringen vil kunne foretage.

I det lovforslag⁸, som regeringen fremsatte efter den ovennævnte høring, og som i øjeblikket behandles i parlamentet, findes i clause 8 en bestemmelse bygget på den sidstnævnte model. Bestemmelsen indeholder en bemyndigelse for den pågældende minister til i sekundær lovgivning at ændre krav andre steder i lovgivningen med henblik på at tillade eller lette anvendelsen af digital kommunikation.

⁸ Electronic Communications Bill.

Kapitel 4. Hittidige danske overvejelser om brugen af digital kommunikation mv.

4.1. Ønsket om at fremme brugen af digital kommunikation – regeringens redegørelse til Folketinget om sikker digital kommunikation

I december 1997 fremlagde regeringen en redegørelse om sikker digital kommunikation for Folketinget, hvori der blev opstillet den overordnede målsætning at ”realisere en principiel ligestilling af digital og papirbaseret kommunikation ved at sikre mulighed for i praksis at anvende digital kommunikation på alle områder, hvor denne kan opfylde samme funktioner som papirdokumenter”.

I redegørelsen anførtes det bl.a., at der er usikkerhed om, på hvilke retsområder man kan anvende digital kommunikation, hvilket ikke er hensigtsmæssigt, når man tænker på de samfundsøkonomiske fordele ved at fremme digital kommunikation. For at undgå denne usikkerhed er der således behov for at få fastslået, på hvilke områder, i hvilket omfang, og på hvilken måde man kan anvende digital kommunikation med elektronisk signatur på områder med formkrav om underskrift eller skriftlighed.

Til brug herfor blev der lagt op til, at der skulle foretages en sortering af alle gældende formkrav, hvorefter de nødvendige ændringer af lovgivningen kunne gennemføres. Vedrørende lovgivningsmetoden ved ændring af de mange formkrav blev der peget på to modeller – frameldingsmodellen og tilmeldingsmodellen (se kapitel 4.2.) – og det anførtes, at der i forbindelse med en kommende høring over et lovforslag om digital signatur ville blive taget stilling til, hvilken af de to modeller der skulle anvendes.

4.2. Forskningsministeriets udkast til lovforslag om digital signatur fra 1998

I forlængelse af regeringens redegørelse om sikker digital kommunikation sendte Forskningsministeriet i februar 1998 et udkast til lovforslag om digital signatur i bred høring.

Lovudkastet havde som hovedformål at fremme en sikker og effektiv anvendelse af digital kommunikation. Dette formål skulle nås gennem fastsættelse af minimumskrav til nøglecentre og digitale signaturer med tilhørende nøglecertifikater.

Udkastet havde endvidere til formål at sikre lige muligheder for at anvende papirbaseret og digital kommunikation på alle områder, hvor digital kommunikation kan opfylde samme formål som den papirbaserede kommunikation, samt at forpligte offentlige myndigheder til at kunne kommunikere digitalt med alle, der ønskede det.

Lovudkastet indeholdt bl.a. regler om nøglecentres og nøgleindehaveres erstatningsansvar. Efter de foreslåede regler skulle nøglecentre hæfte på objektivet grundlag over for både nøgleindehaver og over for den, der modtager en meddelelse, der er forsynet med digital signatur. Ansvarret skulle omfatte tab, der skyldtes, at nøglecentret ikke havde overholdt de fastsatte forskrifter.

Endvidere indeholdt lovudkastet bestemmelser om spærring, udløb og anvendelsesbegrænsninger i nøglecertifikater og retsvirkningerne heraf. Reglerne gik bl.a. ud på, at der efter udløbsdatoen for et certifikat ikke skulle kunne støttes ret på den tilknyttede digitale signatur, medmindre det blev godtgjort, at signaturen var afgivet før certifikatet udløb, og det digitale dokument endvidere inden da var blevet forsynet med en ny – ikke udløbet – signatur.

Et yderligere element i lovudkastet var en forpligtelse for offentlige myndigheder til at være i stand til at modtage digital kommunikation. Derimod skulle det være frivilligt for andre, om man ønskede at modtage digital kommunikation fra offentlige myndigheder og institutioner. Hvis man ønskede dette, skulle man kunne opgive en ”officiel e-post adresse” til henholdsvis CPR-registeret og CVR-registeret.

Lovudkastets regler om muligheden for at anvende digital kommunikation på områder med formkrav var bygget således op, at der skulle vælges mellem tre forskellige modeller. Fælles for modellerne var, at de byggede på en retsregel, som ligestillede digital kommunikation og elektronisk signatur med papirdokumenter og traditionelle underskrifter. Spørgsmålet var, om denne ligestilling som udgangspunkt skulle omfattes alle retsregler med formkrav, eller om den alene skulle gælde for regler, som udtrykkeligt blev ”tilmeldt” ordningen.

Den første model – frameldingsmodellen – indebar, at alle formkrav i lovgivningen om skriftlighed mv., som udgangspunkt skulle kunne opfyldes ved brug af sikker digital kommunikation. For at et formkrav ikke skulle kunne opfyldes på denne måde, skulle den pågældende retsregel ”frameldes” ved optagelse i en bekendtgørelse, som skulle indeholde de formkrav, som (endnu) kun kunne opfyldes ved brug af papir.

Den anden model – tilmeldingsmodellen – indebar, at formkrav om skriftlighed mv. i lovgivningen kun kunne opfyldes ved brug af digital kommunikation, hvis dette blev slået fast ved optagelse af reglen på en ”positivliste” i en bekendtgørelse.

Endelig indeholdt lovudkastet en såkaldt kombinationsmodel, som indebar, at man udskød ikrafttrædelsen af frameldingsmodellen til den 1. januar 2001, men at man indtil da havde mulighed for at tilmelde de regler, man ønskede skulle kunne opfyldes ved anvendelse af sikker digital kommunikation.

Lovudkastet blev som nævnt sendt i høring, og i høringssvarene blev der fra mange sider udtrykt støtte til tanken om at regulere anvendelsen af digital signatur mv. Samtidig pegede en række af de hørte organisationer mv. imidlertid på nogle væsentlige problemer ved den valgte lovgivningsmodel. Navnlig var det et gennemgående træk i høringssvarene, at man fandt, at udkastets regler om retsvirkningerne af anvendelsen af digital signatur var problematiske, fordi de greb dybt ind i grundlæggende aftaleretlige principper.

Bl.a. blev det anført, at de foreslåede regler om spærring, udløb og anvendelsesbegrænsninger for certifikater var for vidtgående, fordi de greb ind i domstolenes frie bevisbedømmelse.

For så vidt angår hæftelses- og ansvarsreglerne mente en række af de hørte organisationer mv., at et objektivt ansvar for nøglecentre var for strengt og i praksis ville gøre det vanskeligt at få nogen til at påtage sig opgaven som nøglecenter. Ansvar – som omfattede alle typer af tab (både direkte og indirekte) – ville være meget svært for nøglecentre at overskue, og det ville næppe være muligt for nøglecentre at tegne en ansvarsforsikring, som dækkede et så vidtgående ansvar.

Vedrørende lovudkastets regler om anvendelsen af digital kommunikation på områder med lovbestemte formkrav var der fra en række af de hørte organisationer mv. støtte til ”frameldingsmodellen”, navnlig med den begrundelse, at denne model ville føre til en hurtig ”modernisering” af lovgivningen. Andre fandt imidlertid denne model for vidtrækkende og påpegede, at konsekvenserne af de foreslåede regler ikke var tænkt igennem. En lovforslag, som med et slag ændrede alle formkrav i de hidtil gældende retsregler, måtte efter nogle af de hørte myndigheder og organisationers opfattelse kræve en mere grundig undersøgelse af konsekvenserne af en sådan lovregel på de mange – og meget forskellige – berørte retsområder.

I lyset af kritikken i de fremkomne høringssvar blev det herefter besluttet at opdele problemstillingerne omkring digitale signaturer mellem Forskningsministeriet og Justitsministeriet, således at Forskningsministeriet skulle varetage opgaven med at udarbejde en regulering af nøglecentre og deres virksomhed med henblik på at få tilvejebragt de retlige rammer for udbud af certificeringstjenester mv., mens Justitsministeriet fik til opgave at vurdere spørgsmålet om behovet for at lovgive om retsvirkningerne af at anvende digital signatur samt spørgsmålet om anvendelsen af digital kommunikation i forbindelse med lovbestemte formkrav om skriftlighed mv.

Det blev senere besluttet at lade fremsættelsen af et lovforslag om nøglecentre mv. afvente udfaldet af forhandlingerne i EU om direktivforslaget om elektroniske signaturer, jf. herom ovenfor i kapitel 3.2.1.

4.3. Lov nr. 417 af 31. maj 2000 om elektroniske signaturer

Umiddelbart efter, at direktivet om elektroniske signaturer var vedtaget den 30. november 1999, sendte Forskningsministeriet den 1. december 1999 et nyt udkast til lovforslag om elektroniske signaturer i en bred høring, og et lovforslag blev herefter fremsat i Folketinget den 22. marts 2000 (nr. L 229). Lovforslaget blev vedtaget af Folketinget den 18. maj 2000 (Lov nr. 417 af 31. maj 2000). Loven er optaget som bilag 4 til denne betænkning.

I overensstemmelse med den ovenfor beskrevne opdeling af arbejdet med regulering af elektronisk signatur indeholder loven navnlig regler om udbud af certificeringstjenester og kravene til disse.

Loven bygger på et princip om teknologineutralitet, og anvendelsesområdet er således elektroniske signaturer, dvs. både digitale signaturer og eventuelle fremtidige teknikker,

som opfylder samme formål som krypteringsteknikken med offentlige nøgler, jf. herom ovenfor i kapitel 2.

I loven anvendes en bred definition af elektronisk signatur, der defineres som data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret.

Baggrunden for den brede definition er, at markedet for elektronisk signatur ligesom så mange andre dele af IT-verdenen er præget af en voldsom teknologisk udvikling. Det gør det meget vanskeligt at forudsige, hvordan dette marked vil udvikle sig, og en teknologispecifik regulering ville derfor ikke være hensigtsmæssig.

4.3.1. Lovens formål og anvendelsesområde

Loven har til formål at sikre, at der på det danske marked findes elektroniske signaturer og nøglecentre, der lever op til en række krav, der gør signaturerne sikre at bruge. Samtidig skal det sikres, at der er balance mellem de forretningsmæssige, de forbrugermæssige og de samfundsmæssige hensyn.

Ønsket er, at der udvikles og udbydes elektroniske signaturer, der har et sådant sikkerhedsniveau, at de kan anerkendes i et bredt forum og anvendes til at understøtte udbud af nye tjenesteydelser i både den private og den offentlige sektor, f.eks. i form af selvbetjeningsløsninger, elektroniske blanketter mv.

Derimod er det ikke hensigten med loven at regulere det samlede udbud af certificeringstjenester. Lovens regler om tilsynsordninger mv. er frivillige, og nøglecentre vil således også efter lovens ikrafttræden have frihed til at udbyde certifikater og elektronisk signa-

turprodukter uden at skulle underlægge sig lovens regler om tilsyn eller være tvunget til at benytte bestemte tekniske løsninger. Markedet vil med andre ord frit kunne udvikle sig, i hvilken retning det måtte ønske.

Reglerne indebærer imidlertid, at betegnelsen ”kvalificerede certifikater” forbeholdes certifikater, som lever op til visse mindstekrav, og som er udstedt af et nøglecenter, der dels lever op til bestemte kvalitetskrav og dels er undergivet et særligt strengt erstatningsansvar, hvis det begår fejl ved udstedelsen af certifikater mv. Loven indeholder også regler om de programmer mv., der benyttes til at fremstille elektronisk signatur, idet betegnelsen ”sikre signaturgenereringssystemer” anvendes til at betegne signaturnøgler mv., der lever op til visse sikkerhedskrav.

Sikkerhedskravene indebærer således en mulighed for såvel private som det offentlige for at stille krav om, at der benyttes et certifikat og en signatur, der opfylder visse minimumskrav, hvor der ved digital kommunikation er behov for sikker identifikation af afsenderen eller modtageren.

Samtidig skal loven sikre, at der er klarhed over nøglecentrets erstatningsansvar, når man som afsender benytter sig af og som modtager fæstner lid til et kvalificeret certifikat. Den valgte ansvarsmodel indebærer, at det er nøglecentrets ansvar at påvise, at nøglecentret ikke har begået fejl i forbindelse med udstedelse af certifikatet, spærring heraf eller afgivelse af oplysninger om udløbsdata og anvendelsesbegrænsninger for certifikatet.

Lovens territoriale anvendelsesområde er nøglecentre, der er etableret på dansk område. Loven stiller ikke særlige krav til nøglecentre og elektroniske signaturer med oprindelse i andre lande inden for Det Europæiske Fællesskab. Det følger imidlertid af EU-direktivet, at sådanne signaturer skal anerkendes på lige fod med signaturer, der baseres på certifikater fra danske nøglecentre.

4.3.2. Almindelige certifikater og kvalificerede certifikater

Som nævnt indeholder loven en række krav, som skal være opfyldt, for at et certifikat kan betegnes ”kvalificeret certifikat” eller lignende. Kravene omfatter både indholdet af certifikatet og de procedurer og forretningsgange, som nøglecentret anvender. Kravene skal sikre, at der skabes et tilstrækkeligt sikkerhedsniveau omkring elektroniske signaturer, der baseres på kvalificerede certifikater.

Et kvalificeret certifikat skal bl.a. indeholde oplysning om nøglecentrets navn og hjemsted, oplysninger, der giver en entydig identifikation af underskriveren (nøgleindehaveren), certifikatets gyldighedsperiode og eventuelle begrænsninger i anvendelsesområdet for certifikatet. Certifikatet skal endvidere indeholde de ”signaturverificeringsdata” (den offentlige nøgle, jf. herom ovenfor i kapitel 2), der svarer til de ”signaturgenereringsdata” (den private nøgle), som certifikatindehaveren havde i sin besiddelse, da certifikatet blev udstedt.

Et certifikat kan indeholde yderligere oplysninger, afhængigt af til hvilket formål certifikatet skal anvendes. Er der f.eks. tale om et certifikat, der alene skal bruges til kommunikation med et forsikringsselskab, kan det være hensigtsmæssigt at lade certifikatet indeholde indehaverens policenummer.

4.3.3. Krav til nøglecentre

Loven indeholder i kapitel 4 en række krav til nøglecentre, der udbyder kvalificerede certifikater. Bestemmelserne pålægger centrene løbende at træffe de juridiske, organisatoriske, tekniske, personale-, drifts- og sikkerhedsmæssige foranstaltninger, som er nødvendige for at give et sikkert og velfungerende udbud af kvalificerede certifikater.

Det kræves bl.a., at nøglecentre, der udsteder kvalificerede certifikater, skal beskæftige personale, som har den nødvendige ekspertise, erfaring og kvalifikationer. Personalet skal have sagkundskab inden for teknologien for elektroniske signaturer og indgående kendskab til korrekte sikkerhedsprocedurer, bl.a. ved kendskab til de systemer og produkter, der anvendes. Det skal med andre ord så vidt muligt undgås, at personalemæssige forhold er skyld i sikkerhedsbrud.

Nøglecentre skal til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomhed i overensstemmelse med reglerne i forslaget. Der skal være knyttet en systemrevisor, der skal være statsautoriseret revisor, til et nøglecenter. Systemrevisor skal påse, at nøglecentret overholder kravene til udbud af kvalificerede certifikater.

Nøglecentre, som udsteder kvalificerede certifikater, skal endvidere benytte betryggende procedurer til at fastslå identiteten af den person, der i certifikatet angives som indehaver af certifikatet. Loven indeholder ikke nærmere regler om, hvordan denne kontrol skal foregå, men forskningsministeren bemyndiges til at fastsætte nærmere regler herom.

Nøglecentret skal endvidere sikre sig, at den, der identificeres i certifikatet, er i besiddelse af de signaturgenereringsdata (den private nøgle), som svarer til de signaturverificeringsdata (den offentlige nøgle), som indeholdes i certifikatet. Er det centret, der leverer den private og den offentlige nøgle, skal de to nøgler endvidere være entydigt forbundne.

4.3.4. Tilsyn og anmeldelse

Nøglecentre, som udbyder kvalificerede certifikater, skal anmeldes til Telestyrelsen, som påser, at centrene overholder reglerne. Telestyrelsen kan bl.a. udstede påbud til et nøglecenter om at bringe sin virksomhed i overensstemmelse med lovens regler. Virker et påbud ikke, vil der kunne blive tale om at pålægge centret tvangsbøder.

4.3.5. Nøglecentrenes erstatningsansvar

Loven indeholder endvidere en særlig ansvarsregel for nøglecentre, der udsteder kvalificerede certifikater.

Bestemmelsen fastlægger ansvaret i visse tilfælde, hvor en person, der med rimelighed forlader sig på et certifikat, lider tab på grund af nøglecentret. Det drejer sig om tab opstået som følge af fejl og mangler i oplysningerne i et certifikat, manglende spærring af et certifikat, manglende eller fejlagtige oplysninger vedrørende udløbsdatoen eller gældende anvendelsesbegrænsninger for certifikatet samt fejl i nøglecentrets kontrol af, at indehaveren er i besiddelse af de signaturgenereringsdata (den private nøgle), som korresponderer med de signaturverificeringsdata (den offentlige nøgle), der er indeholdt i certifikatet.

Bestemmelsen indebærer, at det vil være op til nøglecentret at bevise, at det ikke har handlet uagtsomt eller forsætligt. Der er således tale om et culpaansvar med omvendt bevisbyrde eller et såkaldt præsumptionsansvar. Begrundelsen for at indføre dette skærpede ansvar for visse nøglecentre er områdets meget tekniske og komplicerede karakter. Det vil for den almindelige bruger af elektroniske signaturer være svært at bevise, om nøglecentret har begået fejl i forbindelse med sin virksomhed. Reglerne har således et forbrugerbeskyttende sigte. For at der kan pålægges nøglecentret erstatningsansvar for tab lidt hos indehaveren eller tredjemand efter bestemmelserne i loven, skal de øvrige betingelser for at pålægge et erstatningsansvar – årsagsforbindelse mv. – være opfyldt.

Dansk rets almindelige erstatningsregel – culpaeglen - skal fortsat gælde ved siden af den særlige erstatningsregel i loven, og forhold, som ikke er omfattet af det skærpede ansvar i loven, vil således fortsat skulle bedømmes efter dansk rets almindelige bestemmelser.

4.3.6. Sikre signaturgerereringssystemer

En elektronisk signatur skabes ved brug af et signaturgerereringssystem (et program mv.) og den private signaturnøgle. Loven indeholder regler om ”sikre signaturgerereringssystemer”, som er systemer, som lever op til visse sikkerhedskrav, bl.a. om, at den private nøgle med rimelig sikkerhed forbliver hemmelig, er beskyttet mod forfalskning og kan beskyttes mod uretmæssig brug.

Kravene skal anses for opfyldt, såfremt signaturgerereringssystemet opfylder almindelige standarder, som er fastsat i medfør af EU-direktivet og offentliggjort i EF-Tidende. Der vil blive udpeget et eller flere organer eller myndigheder, som her i landet skal forestå efterprøvelsen af, om signaturgerereringssystemer opfylder disse krav.

4.3.7. Anvendelse af elektronisk signatur på områder med formkrav

Loven indeholder i § 13 en bestemmelse, som drejer sig om anvendelsen af elektronisk signatur på områder, hvor der i lovgivningen stilles krav om, at digital kommunikation skal være forsynet med signatur eller lignende:

”§ 13. Bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, skal anses for opfyldt, hvis meddelelsen er forsynet med en elektronisk signatur, som er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgerereringssystem. Ved elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.”

For at bestemmelsen finder anvendelse, kræver det altså, at der i lovgivningen findes regler om, at elektroniske meddelelser skal være forsynet med signatur. Af bemærkningerne til bestemmelsen⁹ fremgår, at den ikke drejer sig om spørgsmålet om, på hvilke områder man kan anvende digital kommunikation. Om et formkrav om skriftlighed, under-

⁹ Folketingstidende 1999-2000, Tillæg A, s. 6379 f.

skrift eller lignende kan opfyldes ved brug af digital kommunikation, elektronisk signatur mv., reguleres således ikke af loven:

”Bestemmelsen har alene virkning for underskriftskrav mv., som kan opfyldes ved brug af en elektronisk signatur, og har således ikke betydning for spørgsmålet om, hvornår dette er tilfældet. På nuværende tidspunkt indeholder dansk ret ikke regler, der foreskriver anvendelse af elektroniske signaturer. Derimod findes der en del retsregler, der indeholder krav om underskrift.

Om et sådant formkrav kan opfyldes ved brug af en elektronisk signatur, skal som hidtil afgøres efter reglerne på det pågældende retsområde. Fører en fortolkning af disse regler til, at kravet kan opfyldes ved anvendelse af en elektronisk signatur, følger det imidlertid af den foreslåede bestemmelse, at en meddelelse, der er forsynet med en avanceret elektronisk signatur, som opfylder de ovenfor nævnte betingelser, ikke vil kunne afvises eller i øvrigt fratages virkning med den begrundelse, at den ikke opfylder det pågældende krav om underskrift.”

Reglen vil altså alene finde anvendelse, hvor der i national ret findes et formkrav om underskrift, signatur eller lignende, som må forstås således, at det kan opfyldes på digital vis. Et sådant krav vil enten kunne forekomme, fordi der er givet en udtrykkelig regel om, at digital kommunikation kan anvendes på et bestemt retsområde, eller fordi en regel med et generelt formuleret underskriftskrav, som måske oprindeligt var tiltænkt anvendelse ved brug af papirdokumenter, må forstås således, at dette krav også kan opfyldes ved brug af elektronisk signatur.

Efterhånden som der – bl.a. i lyset af de anbefalinger, som gives i denne betænkning – konstateres eller indføres formkrav, som kan opfyldes ved brug af digital signatur, vil en anvendelse af bestemmelsen blive aktuel.

Bestemmelsen vil lette udarbejdelsen af lovgivning på de områder, hvor man indfører formkrav om elektronisk signatur mv. I stedet for, at man i hver retsregel for sig skal fastsætte teknisk prægede bestemmelser om, hvilke krav der stilles til elektronisk signatur, vil man nemlig i langt de fleste tilfælde kunne nøjes med at henvise til, at elektronisk sig-

natur skal overholde kravene i lovens § 13. Kun hvor særlige forhold gør sig gældende, vil det være nødvendigt at fastsætte supplerende regler.

Som udgangspunkt vil det imidlertid ikke være muligt at stille krav om opfyldelse af strengere sikkerhedskrav, end hvad der følger af lovens regler om avancerede elektroniske signaturer m.v. Det skyldes, at bestemmelsen i lovens § 13 gennemfører direktivets artikel 5, stk. 1, litra a), der som udgangspunkt forbyder medlemsstaterne at opretholde eller vedtage lovgivning med signaturkrav, som ikke kan opfyldes ved brug af en signatur, der lever op til direktivets krav. Med andre ord indføres der med direktivet en art europæisk standard, som indebærer, at man, hvis man afgiver eller modtager en en signatur, der lever op til direktivets krav, kan gå ud fra, at den opfylder formkrav i lovgivningen. Som det fremgår af lovens § 13, åbner direktivet dog (i artikel 3, stk. 7) mulighed for, at der kan stilles supplerende krav ved kommunikation med offentlige myndigheder. Denne mulighed er dog betinget af, at der er et særligt behov, og at kravene er objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende.

4.4. Forskningsministeriets pilotprojekter, Det Digitale Danmark og forskningsministerens netværksredegørelse til Folketinget

4.4.1. Pilotprojekter

Forskningsministeriet bevilgede i juni 1998 15 mio. kr. til iværksættelse af i alt 9 pilotprojekter i statsligt og kommunalt regi med digitale signaturer.

Formålet med at støtte pilotprojekterne var at sikre, at det offentlige kom i gang med at bruge digital signatur, og at de nødvendige produkter og tjenester, som skal udgøre infrastrukturen til digital signatur, udvikles på markedet. Samtidig var det et mål med projekterne at sikre enighed om standarder for digital signatur i det offentlige.

Det videre mål med pilotprojekterne er, at de kan være med til at bane vejen for, at private og virksomheder kommer hurtigere i gang med at bruge digital signatur. Disse brugere kan nemlig drage fordel af den udvikling af infrastrukturen til digital signatur og de offentlige standarder, der er sket i forbindelse med projekterne.

De 9 pilotprojekter er blevet iværksat i Erhvervs- og Selskabsstyrelsen, Næstved Kommune, Ringsted Kommune, Vordingborg Kommune, EU-direktoratet, SU-styrelsen, Århus Amt, Handelshøjskolen i København og i Erhvervsfremmestyrelsen.

Efter at projekterne er blevet afsluttet i løbet af år 2000, er de ved at blive evalueret, for at den viden og de erfaringer, som er opnået i forbindelse med projekterne, kan blive anvendt i det videre arbejde med at gøre det muligt at anvende digitale signaturer.

4.4.2. Det Digitale Danmark

Udvalget for Det Digitale Danmark afgav i november 1999 en rapport "Det Digitale Danmark – omstilling til netværkssamfundet" med oplæg og anbefalinger til, hvordan regeringens fremtidige IT-politiske strategi bør formuleres.

Rapporten indeholder en række mål, som bør være retningsgivende for IT-politikken herhjemme samt en række konkrete anbefalinger hertil.

En række af de anbefalinger, som opstilles i relation til mål 2 (Danmark som e-handelsnation) og mål 3 (bedre og billigere service i den digitale forvaltning) forudsætter, at der kan skabes løsninger, hvor der er sikkerhed for, at elektroniske meddelelser, ansøgninger, indberetninger, mv. stammer fra den, som fremstår som afsenderen, og at indholdet ikke er blevet ændret undervejs.

I forhold til anvendelse af digital signatur foreslås det i rapporten, at alle unge mellem 18 og 21 år gratis tilbydes en digital signatur i perioden 2000-2003 til anvendelse bl.a. i forbindelse med uddannelse og SU.

Om sikkerhedsspørgsmålet skriver udvalget bl.a. :

”Hvis borgere og virksomheder ikke kender spillereglerne på Internettet, eller hvis de ikke stoler på, at reglerne giver den tilstrækkelige tryghed og sikkerhed, så vil det bremse IT-udviklingen – og dermed dansk deltagelse i netværkssamfundet.”

På den baggrund anbefaler udvalget, at borgerne gives IT-rettigheder. Om disse hedder det bl.a. i udvalgets rapport:

”Udformningen af borgernes IT-rettigheder skal præcisere spillereglerne i netværkssamfundet og blandt andet sikre fri kryptering uden mulighed for ulovlig aflytning.

Megen lovgivning gælder både i den fysiske og den virtuelle verden, og både i Danmark og internationalt arbejdes der på at tilpasse love og regler til netværkssamfundet. Ikke desto mindre er det på centrale områder som elektronisk handel, e-post og surfing på Internettet uklart for de fleste borgere og virksomheder, hvilke love og paragraffer der gælder fra den fysiske verden – og hvordan de skal fortolkes.

Netværkssamfundet har udstyret os med IT-værktøjer, som giver mulighed for at invadere det private rum – eksempelvis ved registrering af vores købeadfærd, overvågning og uopfordrede e-post henvendelser.

Der skal gælde helt klare regler for det elektroniske privatliv – både i forholdet mellem staten og borgerne og borgerne imellem – men også i forhold til borgerens rettigheder på et Internet, der ubesværet krydser de nationale grænser. Der er behov for, at borgerne får præciseret, hvilke rettigheder de har i netværkssamfundet. Borgernes IT-rettigheder bør blandt andet udformes på baggrund af:

- international lovgivning og aftaler
- dansk lovgivning, vejledninger og cirkulærer
- selvregulering, hvor brancheorganisationer, forbrugerorganisationer og andre lægger sig fast på garantiordninger eller mærkningsordninger, der ikke er fastlagt ved lov.

Borgernes IT-rettigheder skal i særlig grad præciseres i forhold til kryptering, lovlig og ulovlig aflytning og aflæsning, elektronisk post, elektronisk handel og elektronisk registrering.

Information om rettighederne skal ske løbende – for eksempel på en særlig hjemmeside. Endvidere skal det overvejes at stille juridisk ekspertise til rådighed for eventuelle spørgsmål om borgernes IT-rettigheder.

Et væsentligt spørgsmål er, hvordan vi fremover sikrer danske borgere og virksomheder, så de ikke mod deres vilje og viden bliver kigget over skulderen. Kryptering – det vil sige teknikker til at kode information, så den bliver uforståelig for udenforstående – er midlet til at skabe sikker kommunikation via åbne net, eksempelvis Internettet. På den anden side vil erhvervslivets og borgernes adgang til frie krypteringsprodukter svække efterforskningsmyndighedernes muligheder for at benytte aflytning som et middel i kriminalitetsbekæmpelsen.”

4.4.3. Netværksredegørelse til Folketinget

Forskningsministeren afgav i januar 2000 den første netværksredegørelse ”Omstilling til netværkssamfundet” til Folketinget.

Redegørelsen indeholder en beskrivelse af 37 af de vigtigste konkrete initiativer, som regeringen planlægger at sætte i gang på IT-området. Redegørelsen blev ved fremlæggelsen i februar 2000 bakket op af samtlige partier i Folketinget, og der er afsat væsentlige ressourcer til at gennemføre de målsætninger, som er fastlagt i redegørelsen.

De 37 initiativer skal tages inden for områderne: teleinfrastruktur, sikring af et netværkssamfund for alle, livslang læring, elektronisk handel, digital forvaltning samt IT-fyrtårne, IT-landkort og IT-tjek. Et af initiativerne i redegørelsen er udarbejdelsen af en lov om elektroniske signaturer, der som nævnt ovenfor blev vedtaget i maj 2000.

Flere af initiativerne i redegørelsen forudsætter, at der kan etableres en sikker elektronisk tovejskommunikation for, at de kan gennemføres. Inden for området digital forvaltning gælder det navnlig følgende forslag:

1. Etablering af personlig Internetadgang til det offentlige. I dette ligger, at alle danske borgere skal tilbydes en personlig Internetadgang, som vil kunne give adgang til of-

fentligt registrerede oplysninger om borgeren, et skræddersyet informationssystem samt nem, hurtig og sikker selvbetjening i forhold til offentlige myndigheder og institutioner. Målet er bedre service, mere effektivitet og større åbenhed.

2. Etablering af en offentlig informationsserver, hvor man på grundlag af allerede eksisterende offentlige registre skal give borgere og virksomheder nem og sikker adgang til de mange informationer, det offentlige har registreret om Danmark og de danske borgere. Dette er første skridt på vejen til, at borgerne kun behøver at oplyse data til det offentlige én gang.
3. Borgerne skal via Internet kunne hente, udfylde og indsende de mest almindelige borgerrettede blanketter, f.eks. til flytteanmeldelser, lægeskift m.fl.. Der skal løbende tilbydes flere blanketter på nettet, således at alle betydende blanketter kan hentes på Internet inden udgangen af 2002. En sådan blanketservice kan yderligere forbedres ved brug af elektronisk signatur, da det vil være muligt at forhåndsudfylde blanketter med personoplysninger, som myndighederne allerede er i besiddelse af, såfremt der kan ske en sikker identifikation. Tilsvarende kan borgerne gives adgang til afgive bindende oplysninger på de elektroniske blanketter med elektronisk signatur.
4. Offentlig e-handel. For at sikre så billige offentlige indkøb som muligt etableres en offentlig Internetauktionshal, hvor virksomheder kan byde på levering af varer og tjenesteydelser til det offentlige, og hvor offentlige institutioner kan gå sammen om fælles indkøb. Der udarbejdes i den forbindelse en handlingsplan for, hvornår offentlige institutioner skal overgå til elektronisk indkøb af forskellige varegrupper som eksempelvis rejser, kontorhold og IT-udstyr. Det offentliges handelspartnere skal på sigt pålægges gebyrer for papirdokumenter.

Forskningsministeriet har i foråret 1999 foretaget en kortlægning af borgernes efterspørgsel efter offentlige elektroniske tjenester.

Undersøgelsen viste bl.a., at borgerne i vid udstrækning efterspørger offentlige elektroniske tjenester, men at bekymring om sikkerhedsspørgsmål er den største barriere for borgernes anvendelse af sådanne tjenester.

Det synes således at være afgørende for den videre udbredelse af offentlige elektroniske tjenester til borgerne, at der kan skabes tillid omkring de sikkerhedsløsninger, som leveres i tilknytning hertil.

Forskningsministeriet har vurderet, at udvikling og etablering af sådanne tjenester er afgørende for det offentliges muligheder for at leve op til borgernes berettigede forventning om bedre og billigere offentlige tilbud.

Kapitel 5. Formkrav og digital kommunikation

5.1. Indledning

Udvalget har som nævnt ovenfor i kapitel 1.3. udskilt spørgsmålet om, hvorvidt formkrav i lovgivningen skaber behov for et lovgivningsinitiativ med henblik på at fremme anvendelsen af digital kommunikation og elektronisk signatur, til forlods behandling i denne delbetænkning.

Som grundlag for en nærmere vurdering af dette spørgsmål har udvalget foretaget en gennemgang af lovgivningen inden for 4 udvalgte ministerområder. Udvalgets gennemgang af lovgivningen har omfattet ca. 500 retsregler under Erhvervsministeriet, Indenrigsministeriet, Justitsministeriet og Sundhedsministeriet, der indeholder formkrav af den ene eller anden art, som på den ene eller den anden måde kan udgøre en hindring for anvendelsen af digital kommunikation.

De regler, som udvalget har gennemgået, er fundet ved søgninger i Retsinformation med angivelse af ord, som kan forventes at indgå i bestemmelser, der indeholder formkrav, jf. herom nedenfor. Udvalget har måttet afstå fra en gennemgang af den samlede lovgivning, idet en sådan gennemgang ville blive meget omfattende og næppe ville frembringe eksempler på lovgivning, som ikke allerede ville kunne fremskaffes ved en gennemgang af lovgivningen inden for de nævnte 4 ministerområder. Udvalgets gennemgang af lovgivningen har således på ingen måde tilsigtet at være udtømmende. Lovgivningen på disse 4 ministerområder må dog efter udvalgets opfattelse antages i alt væsentligt at være repræsentativ for lovgivningen på de øvrige ministerområder.

På denne baggrund finder udvalget efter at have gennemgået lovgivningen inden for de nævnte 4 ministerområder, at der herved er skabt et sådant overblik over formkrav i lov-

givningen, at udvalget har det tilstrækkelige grundlag for at fremkomme med sine konklusioner og anbefalinger om spørgsmålet.

Udvalget har anvendt to metoder til at kategorisere bestemmelserne. For det første har udvalget foretaget en inddeling efter ressortministerium, og inden for hvert ministerområde en inddeling efter de traditionelle juridiske emneområder – familieretlige regler for sig, regler inden for retsplejen for sig osv., jf. nedenfor i kapitel 5.2. Dernæst har udvalget foretaget en inddeling ”på tværs”, efter hvilket formål formkravet må antages at skulle varetage. En gennemgang af de forskellige kategorier af formkrav findes i kapitel 5.3.

5.2. Gennemgang af lovgivningen på udvalgte ministerområder

Lovgivningen inden for de udvalgte 4 ministerområder indeholder et betydeligt antal formkrav. Udvalget har som nævnt gennemgået ca. 500 retsregler, som er fundet ved søgninger i Retsinformation med angivelse af søgeord, som man kan forvente at finde i retsregler, der indeholder formkrav (”underskrift”, ”skriftlig”, ”dokument”, ”blanket”, ”papir” osv.). Der er søgt i ministeriernes hovedlove, lovbekendtgørelser og bekendtgørelser. Der er ikke søgt i cirkulærer, vejledninger mv. Udvalget har ikke foretaget en egentlig gennemlæsning af samtlige retsregler på de 4 ministeriers områder. Der findes derfor utvivlsomt flere bestemmelser indeholdende formkrav – men blot formuleret med andre ord end de mest oplagte og i andre dokumenttyper end dem, der er søgt i – inden for de 4 ministeriers område. Der er også grund til at pege på, at et formkrav ikke behøver at fremgå udtrykkeligt af lovgivningen. I nogle tilfælde følger krav om anvendelse af papirdokumenter, personligt fremmøde, underskrift o.s.v. af administrativ praksis, uden at dette kan læses ud af den pågældende bestemmelse.

5.2.1. Erhvervsministeriet

Erhvervsministeriets område omfatter navnlig næringsretlig lovgivning, bl.a. om betingelserne for at udøve en række lovregulerede erhverv, lovgivning om konkurrenceret og markedsføring, patenter, søfart mv. Under Erhvervsministeriets område falder endvidere visse forbrugerbeskyttende regler samt regler om førelsen af en række registre (vedrørende selskaber, erhvervsdrivende fonde mv.), der bl.a. vedligeholdes af Patent- og Varemærkestyrelsen samt Erhvervs- og Selskabsstyrelsen.

Formkrav på det næringsretlige område har bl.a. til formål at sikre, at der foreligger dokumentation for, at udøvere af bestemte erhverv har bestået de fornødne eksaminer, har opnået offentlig autorisation, bevilling mv. Andre formkrav inden for Erhvervsministeriets område har til formål at lette førelsen af de ovennævnte registre.

Som eksempel på et formkrav inden for Erhvervsministeriets lovgivning kan nævnes næringsloven, der indeholder regler om, at der skal løses næringsbrev for at kunne udøve visse erhverv. Af **næringslovens § 6, stk. 1**,¹⁰ fremgår det, at et næringsbrev skal ophænges på et iøjnefaldende sted :

”§ 6. Næringsdrivende, der har fast forretningssted, skal have et opslag med indehaverens navn på et sted, der er iøjnefaldende for kunderne. For næringer, der er betinget af næringsbrev, ophænges dette eller et af vedkommende myndighed udstedt duplikateksemplar.”

Et beslægtet eksempel fra det næringsretlige område drejer sig om, at der skal udfærdiges et eksamensbevis, som kan anvendes til fremvisning som bevis for, at den pågældende har bestået maskinmestereksamen, jf. **§ 6 i lov om uddannelse af maskinmestre**¹¹:

¹⁰ Lovbekendtgørelse nr. 185 af 25. marts 1988 af næringsloven.

¹¹ Lov nr. 350 af 1. juli 1988 om uddannelse af maskinmestre.

*”§ 6. Eksamenskommissionen udsteder **eksamensbevis**.*

Stk. 2. Den, der har bestået 1. årsprøve til maskinmestereksamen, kan af eksamenskommissionen få udstedt et bevis herfor. Industriministeren fastsætter nærmere regler herom.”

Som eksempel kan også nævnes **§ 8 i lov om søfartsuddannelse**¹²:

”§ 8. Søfartsstyrelsen nedsætter en eksamenskommission bestående af en formand og mindst 3 medlemmer, som alle skal have bestået skibsførereksamen og normalt have gjort tjeneste som navigatør i handelsflåden i mindst 2 år.

Stk. 2. Medlemmer af eksamenskommissionen må ikke være ansat ved eller være medlem af bestyrelsen af skoler eller kurser, der forbereder til de i § 6 omhandlede eksaminer.

*Stk. 3. Eksamenskommissionen forestår udarbejdelsen af eksamensopgaver, afholdelse af eksaminer og udstedelse af **eksamensbeviser**.”*

En række formkrav indenfor Erhvervsministeriets område har til formål at sikre, at bestemte oplysninger, f.eks. vedrørende udøvelse af et lovreguleret erhverv, opbevares i længere tid samt at de kan fremvises på anmodning, jf. bl.a. **§ 3, stk. 11, i bekendtgørelse om betryggelse ved erhvervsdykkerarbejde og om erhvervsdykkerarbejdes sikre udførelse**¹³:

”§ 3. ...

...

*Stk. 11. I forbindelse med hver dykning skal dykkeren føre en af Søfartsstyrelsen godkendt **dykkerjournal**. Hver indførsel om en dykning skal **underskrives** af dykkeren og af enten arbejdsgiveren eller af dykkerlederen. **Udskrevne** dykkerjournaler skal af dykkeren opbevares i mindst 5 år efter sidste indførsel i journalen. Hvis der for retten er rejst sag vedrørende dykkerarbejdets udførelse i det tidsrum journalen omfatter, skal den opbevares, indtil sagen endeligt er afgjort.”*

¹² Lov nr. 16 af 13. januar 1997 om søfartsuddannelse.

¹³ Bekendtgørelse nr. 30 af 15. januar 1988 om betryggelse ved erhvervsdykkerarbejde og om erhvervsdykkerarbejdes sikre udførelse.

Der findes også eksempler på formkrav, der er indsat i lovgivningen for at indskærpe alvoren og vigtigheden af et bestemt hvervs udførelse, jf. f.eks. **§ 2 i lov om translatører og tolke**¹⁴:

”§ 2. For beskikkelse som translatør og tolk betales en af Erhvervs- og Selskabsstyrelsen fastsat afgift.

*Stk. 2. Forinden **beskikkelsen udleveres**, skal den pågældende **underskrive** en højtidelig forsikring om, at han med omhu og nøjagtighed vil udføre de hverv, der betros ham, og samvittighedsfuldt opfylde sine pligter som translatør og tolk.”*

På Erhvervsministeriets område findes også eksempler på retsregler, der allerede er ændret for at muliggøre digital kommunikation. Til illustration af de overvejelser, man har gjort sig i forbindelse med sådanne ændringer kan henvises til en udtalelse af 5. maj 1994, som Patentdirektoratet (nu Patent- og Varemærkestyrelsen) afgav til Dansk EDI-råd i forbindelse med en undersøgelse om formkrav inden for de forskellige ministeriers områder:

"Generelt kan det for Patentdirektoratets område konstateres, at der adskillige steder i lovgrundlaget anvendes udtryk som "dokumenter", "skriftligt" og "underskrift". I de fleste tilfælde har lovgiver antageligvis anvendt de nævnte udtryk i overensstemmelse med den tradition, der findes på direktoratets område. Herunder bunder f.eks. kravet om skriftlighed i visse bestemmelser fortrinsvist i ønsket om, at undgå at information bliver videregivet til direktoratet i mundtlig form. Det kan således ikke generelt antages, at disse udtryk er valgt for at hindre informationsudveksling på andre medier end papir."

Bl.a. på patentområdet er en række bestemmelser blevet ændret for at muliggøre brug af elektroniske dokumenter mv.

¹⁴ Lovbekendtgørelse nr. 181 af 25. marts 1988 af lov om translatører og tolke.

I en tidligere affattelse lød **patentlovens § 8**¹⁵ således:

”§ 8. Ansøgningen om patent indleveres skriftligt til patentmyndigheden eller i de i kapitel 3 nævnte tilfælde til patentmyndigheden i fremmed stat eller til en international organisation.”

Ved lov nr. 972 af 17. december 1997 er **patentlovens § 8** imidlertid ændret således, at ordet "skriftligt" er udgået af bestemmelsen. Ændringen havde til formål at gøre det muligt at indgive patentansøgninger i elektronisk form, når de fornødne administrative forudsætninger - i form af sagsbehandlingssystemer, sikkerhedsmekanismer mv. - var opfyldt.

5.2.2. Sundhedsministeriet

Lovgivningen på Sundhedsministeriets område indeholder navnlig regler om sundhedspersonale og om det materiel mv., der benyttes i sundhedssektoren. Bestemmelser i Sundhedsministeriets lovgivning, der indeholder formkrav, er ofte regler, der omhandler autorisationer, samtykke, informationssikring, erklæringer og attester mv.

Der findes bl.a. en række formkrav, der har til formål at sikre, at patienter er indforstået med en given behandling. Dette opnås bl.a. ved krav om, at der skal foreligge et skriftligt samtykke fra patienten (eller dennes værge). Som eksempel kan nævnes **§ 23 i lov om kunstig befrugtning i forbindelse med lægelig behandling, diagnostik og forskning m.v.**¹⁶:

*”§ 23. Før behandling med kunstig befrugtning indledes, skal der indhentes **skriftligt** samtykke til behandlingen fra kvinden og dennes ægtefælle eller partner. Den behandlende læge skal påse, at samtykket fortsat er gyldigt, når behandlingen påbegyndes.”*

¹⁵ Lovbekendtgørelse nr. 824 af 13. september 1996 af patentloven.

¹⁶ Lov nr. 460 af 10. juni 1997 om kunstig befrugtning i forbindelse med lægelig behandling, diagnostik og forskning m.v.

Endvidere kan nævnes § 22 i lov om frihedsberøvelse og anden tvang i psykiatrien¹⁷:

*”§ 22. Ethvert psykokirurgisk indgreb kræver **skriftligt** samtykke fra patienten.*

Stk. 2. Psykokirurgisk indgreb må endvidere kun foretages efter forudgående godkendelse fra et lægeråd, der nedsættes af Sundhedsstyrelsen.

*Stk. 3. Er patienten ude af stand til at afgive gyldigt samtykke, kan indgrebet kun gennemføres, såfremt der over for patienten iværksættes værgemål efter værgemålslovens § 5, der omfatter personlige forhold, herunder beføjelse til at meddele samtykke til psykokirurgiske indgreb, og værgen giver **skriftligt** samtykke til indgrebet.”*

På Sundhedsministeriets område findes også formkrav, der har til formål at sikre, at information videregives til bestemte personer. Som eksempel kan nævnes kravet om, at der skal udarbejdes en skriftlig instruks, inden der foretages en rensning af røgdetektorer, som indeholder radioaktive stoffer, således at rengøringen herefter kan udføres i overensstemmelse med denne instruks, jf. §§ 14 og 26 i bekendtgørelse om røgdetektorer og forbrugerartikler indeholdende radioaktive stoffer¹⁸:

*”§ 14. Såfremt der foretages rensning af røgdetektorer skal den ansvarlige leder sørge for, at der udarbejdes en **skriftlig** instruks for rensningsarbejdet. Denne instruks skal godkendes af Sundhedsstyrelsen.*

Stk. 2. Den ansvarlige leder skal sørge for, at den i § 26, stk. 4, krævede forureningsmonitor altid fungerer, og at der udføres regelmæssig forureningskontrol”.

”§ 26. Hvis rengøring af røgdetektorer omfatter rensning af den radioaktive kilde, skal virksomheden indrette et særligt lokale til dette arbejde.

Stk. 2. Indretning og afmærkning af renselokalet skal godkendes af Sundhedsstyrelsen.

*Stk. 3. Rensning skal udføres i overensstemmelse med den af den ansvarlige leder udarbejdede **skriftlige** instruks, jf. § 14, stk. 1.*

Stk. 4. I renselokalet skal forefindes en tilstrækkelig følsom forureningsmonitor, der skal anvendes til kontrolmåling af arbejdsplads, arbejdsredskaber og lignende for evt. forurening med radioaktive stoffer.”

¹⁷ Lovbekendtgørelse nr. 849 af 2. december 1998 af lov om frihedsberøvelse og anden tvang i psykiatrien.

¹⁸ Bekendtgørelse nr. 154 af 6. marts 1990 om røgdetektorer og forbrugerartikler indeholdende radioaktive stoffer.

I Sundhedsministeriets lovgivning findes endvidere en række bestemmelser om ydelse af tilskud, såfremt en bestemt tilstand eller et bestemt forhold er til stede. For at sikre, at betingelserne for at opnå ydelsen er opfyldt, indeholder lovgivningen ofte et krav om, at der skal foreligge en skriftlig henvisning fra en læge, der attesterer, at betingelserne for at få tilskuddet mv. er opfyldt. Som eksempel kan nævnes **§ 2 i bekendtgørelse om tilskud efter sygesikringsloven til optræning af handicappede og behandling af muskellidelser på optræningscentret i Karslunde**¹⁹:

”§ 2. Tilskud til optræning, jf. § 1, stk. 1 og 2, ydes til gruppe 1-sikrede og gruppe 2-sikrede, der er bosiddende i Københavns, Roskilde og Frederiksborg Amtskommuner, i Københavns og Frederiksberg Kommuner samt i amtskommuner, hvor amtsrådet har truffet beslutning om at tiltræde overenskomsten.

Stk. 2. Tilskud til behandling af muskellidelser, jf. § 1, stk. 3, ydes til gruppe 1-sikrede og gruppe 2-sikrede, der er bosiddende i en amtskommune, hvor amtsrådet har truffet beslutning om at tiltræde overenskomsten. For Københavns og Frederiksberg Kommuner træffer magistraten henholdsvis kommunalbestyrelsen beslutning om tiltrædelse af overenskomsten.

*Stk. 3. Det er en forudsætning for ydelse af tilskud, at der foreligger en **skriftlig** henvisning fra en læge, inden optræningen eller behandlingen påbegyndes. Henvisningen skal indeholde oplysninger om diagnose, henvisningsperiode, optræningens eller behandlingens omfang samt dato for udstedelsen.”*

Fra sundhedsområdet kan endvidere nævnes en række bestemmelser om indberetning af visse oplysninger til Sundhedsstyrelsen. I nogle tilfælde gælder, at der både kræves telefonisk og skriftlig indberetning, jf. f.eks. **§§ 1 og 2 i bekendtgørelse om lægers anmeldelse af smitsomme sygdomme mv. (Til landets læger)**²⁰:

*”§ 1. Følgende sygdomme skal anmeldes telefonisk og **skriftligt**:*

- Anthrax,*
- botulisme,*
- difteri,*
- hæmorrhagisk feber (Ebola, Lassa og Marburg),*
- kolera,*
- meningokoksygdom,*

¹⁹ Bekendtgørelse nr. 882 af 17. december 1991 om tilskud efter sygesikringsloven til optræning af handicappede og behandling af muskellidelser på optræningscentret i Karslunde.

²⁰ Bekendtgørelse nr. 277 af 14. april 2000 om lægers anmeldelse af smitsomme sygdomme.

- pest,
- plettyfus,
- poliomyelitis anterior acuta,
- purulent meningitis og
- rabies.”

”§ 2. Den læge, der får en patient med en af de i § 1 nævnte sygdomme til behandling, skal straks anmelde tilfældet både telefonisk og **skriftligt**.

Stk. 2. Den telefoniske anmeldelse skal ske til embedslægeinstitutionen på patientens opholdssted.

Stk. 3. Den **skriftlige** anmeldelse foretages til

- 1) embedslægeinstitutionen på patientens opholdssted og
- 2) Statens Seruminstitut, epidemiologisk afdeling.

Stk. 4. Til den **skriftlige** anmeldelse anvendes Sundhedsstyrelsens formular nr. 1515.

Stk. 5. Der må kun anmeldes ét sygdomstilfælde på hver **formular**.

Stk. 6. Anmeldelse skal foretages, selv om tilfældet har en mild form eller ikke er fuldt udviklet (abortiv).”

5.2.3. Indenrigsministeriet

På Indenrigsministeriets område findes bl.a. regler om det danske beredskab, udlændinge- og flygtningeområdet, folkeregistreringslovgivning, tilsyn med kommuner mv. Karakteristisk for formkravene er bl.a. en række krav om personlegitimering og personregistrering.

Som eksempel på et sådant formkrav kan nævnes kravet om, at udlændinge skal være i besiddelse af pas eller anden rejselegitimation, jf. **udlændingelovens § 39²¹**:

”§ 39. En udlænding skal ved indrejse, under ophold her i landet og ved udrejse herfra være i besiddelse af pas eller andet dokument, der efter indenrigsministerens bestemmelse kan godkendes som rejselegitimation.

Stk 2. Indenrigsministeren kan fastsætte regler om, i hvilket omfang passet eller rejselegitimationen skal være påtegnet visum til indrejse i eller udrejse af landet. Indenrigsministeren kan endvidere fastsætte nærmere regler om visum, herunder om adgangen hertil, om visummets varighed og om de betingelser, der kan fastsættes for visummet.

Stk 3. Passet eller rejselegitimationen skal ved ind- og udrejse forevises for paskontrollen og under ophold her i landet på begæring forevises for offentlige myndighe-

²¹ Lovbekendtgørelse nr. 600 af 23. juni 2000 af udlændingeloven.

der. Indenrigsministeren kan bestemme, at udlændinge til stadighed skal medføre deres pas eller anden legitimation under ophold her i landet.”

Endvidere kan nævnes kravet om personligt fremmøde ved bedømmelse af en ansøgning om opholdstilladelse i medfør af **udlændingelovens § 40, stk. 1²²**:

”§ 40. En udlænding skal meddele de oplysninger, som er nødvendige til bedømmelse af, om en tilladelse i henhold til denne lov kan gives, inddrages eller bortfalde, eller om udlændingen lovligt opholder sig her i landet. Udlændingen skal efter tilsigelse give personligt møde og på begæring stille sit pas eller sin rejselegitimation til rådighed ved behandlingen af ansøgninger i henhold til loven. Andre personer, som skønnes at kunne bidrage med oplysninger til brug for sagens behandling, kan pålægges at meddele de i 1. pkt. nævnte oplysninger.”

Bestemmelsen hjemler således et krav om forevisning af pas eller lignende, jf. herom ovenfor. Derudover har der i tilknytning til bestemmelsen udviklet sig en praksis, hvorefter der - i sager, hvor ansøger ikke er repræsenteret ved en partsrepræsentant - stilles krav om, at ansøgninger om visum samt opholds- og arbejdstilladelse skal indgives ved personligt fremmøde (hos Udlændingestyrelsen eller hos det lokale politi). Der stilles endvidere krav om, at ansøgningen skal **underskrives** under det personlige fremmøde samt forsynes med billede.

I forbindelse med høringen vedrørende Forskningsministeriets udkast til lov om digital signatur i 1997 oplyste Indenrigsministeriet, at baggrunden for denne praksis er, at der er et behov for at sikre, at tilladelser efter udlændingeloven søges af og udstedes til rette vedkommende.

En række bestemmelser i Indenrigsministeriets lovgivning indeholder regler om kommunikation med borgere i andre EU-medlemsstater. For at lette denne kommunikation samt af

²² Jf. note 21.

administrative hensyn, er det ofte fastsat, at kommunikationen skal foregå skriftligt. Som eksempel kan nævnes **§ 4 i bekendtgørelse om optagelse på valglisten til Europa-Parlamentsvalg af personer, der er statsborgere i en af de øvrige medlemsstater i Den Europæiske Union**²³, hvorefter ansøgningen om optagelse på valglisten skal foretages på et ansøgningsskema, der skal være egenhændigt underskrevet af ansøgeren:

”§ 4. Kommunalbestyrelsen skal snarest muligt efter modtagelsen af en ansøgning undersøge, om den er indgivet rettidigt, jf. § 2, stk. 2 og 3, og § 1, stk. 3, jf. § 5, og i bekræftende fald tillige undersøge, om

- 1) ansøgeren senest seks uger før valgdagen henholdsvis 20.-dagen før valgdagen, jf. § 1, stk. 3, har fast bopæl i Danmark, dvs. er flyttet til Danmark og har anmeldt flytningen til folkeregistret, er statsborger i en af de øvrige medlemsstater i Den Europæiske Union og ikke er under værgemål med fratagelse af den retlige handleevne, jf. værgemålslovens § 6,*
- 2) ansøgeren er fyldt 18 år senest på valgdagen, samt om*
- 3) ansøgningsskemaet er korrekt udfyldt og egenhændigt **underskrevet** af ansøgeren, herunder om de meddelte oplysninger om fulde navn, personnummer, statsborgerskab og bopæl (adresse) i Danmark og eventuelt seneste bopæl (adresse) i hjemlandet er i overensstemmelse med oplysningerne i folkeregistret.*

*Stk. 2. Hvis ansøgningsskemaet er mangelfuldt udfyldt, og disse mangler ikke umiddelbart kan afhjælpes, eller hvis der er væsentlige uoverensstemmelser mellem oplysningerne i ansøgningsskemaet og oplysningerne i folkeregistret, skal kommunalbestyrelsen snarest muligt give ansøgeren **skriftlig** meddelelse herom med henblik på, at eventuelle mangler eller uoverensstemmelser kan blive afhjulpet henholdsvis berigtiget, eventuelt ved rettelser i folkeregistret.*

*Stk. 3. Kommunalbestyrelsen skal i forbindelse med **skriftlig** meddelelse efter stk. 2 gøre ansøgeren opmærksom på, at eventuelle mangler eller uoverensstemmelser skal være afhjulpet senest 20.dagen før valgdagen, for at ansøgeren kan optages på valglisten, jf. § 6, stk. 2.”*

Bestemmelserne om optagelse af statsborgere fra andre EU-lande på valglisten til Europa-Parlamentsvalg har en EU-retlig baggrund²⁴. Formkravene følger imidlertid ikke af EU-retten, men alene af den danske lovgivning.

²³ Bekendtgørelse nr. 80 af 31. januar 1994 om optagelse på valglisten til Europa-Parlamentsvalg af personer, der er statsborgere i en af de øvrige medlemsstater i Den Europæiske Union, som ændret ved bekendtgørelse nr. 107 af 18. februar 1999.

²⁴ Jf. Rådets direktiv 94/80 om fastsættelse af de nærmere regler for valgret og valgbarhed ved kommunale valg for unionsborgere, der har bopæl i en medlemsstat, hvor de ikke er statsborgere.

På Indenrigsministeriets område findes der endvidere en række formkrav, der skal sikre, at sagsbehandlingen ved forskellige råd og nævn sker så smidigt som muligt, og som bl.a. indebærer, at rådene og nævnene ikke nødvendigvis behøver at mødes for at træffe afgørelse i en given sag. Som eksempel kan nævnes §§ 10 og 12 i bekendtgørelse om Værnepligtsnævnet²⁵:

*”§ 10. Formanden kan på nævnets vegne bestemme, at der skal indhentes yderligere **skriftlige** indlæg og træffe bestemmelse om afslutning af den **skriftlige** forberedelse. Formanden kan bestemme, at den **skriftlige** forberedelse skal genoptages og formen herfor.”*

*”§ 12. Værnepligtsnævnets afgørelser træffes efter rådslagning på et møde eller efter formandens bestemmelse ved en **skriftlig** votering.*

***Stk. 2.** Afgørelsen træffes ved almindeligt stemmeflertal. Ved stemmelighed gør formandens stemme udslaget.*

***Stk. 3.** Afgørelserne samles i en protokol. Efter hvert møde **underskrives** protokollen af de tilstedeværende medlemmer. Ved **skriftlig** votering **underskrives** votum, der indgår i protokollen ved tilbagesendelsen. Et medlem kan kræve tilført protokollen en kort begrundelse for sit standpunkt.”*

Endvidere kan nævnes § 2 i bekendtgørelse om forretningsorden for Flygtningenævnet²⁶:

”§ 2. Ved nævnets behandling af en sag medvirker foruden formanden eller en af næstformændene 4 medlemmer, hvoraf 1 medlem udpeges af indenrigsministeren, 1 medlem beskikkes efter indstilling fra Dansk Flygtningehjælp, 1 medlem beskikkes efter indstilling fra Advokatrådet og 1 medlem beskikkes efter indstilling fra udenrigsministeren, jf. udlændingelovens § 53, stk. 2. Behandlingen er mundtlig, jf. dog lovens § 53, stk. 4-5, og § 56, stk. 4.

***Stk. 2.** Afgørelsen af, om en sag skal behandles på mundtligt eller **skriftligt** nævnsmøde, træffes ved visiteringen af sagerne, jf. § 14.”*

Regler om sagsbehandling i administrative nævn og råd på andre af de undersøgte ministerområder indeholder bestemmelser af tilsvarende indhold.

²⁵ Bekendtgørelse nr. 111 af 23. februar 1999 om Værnepligtsnævnet.

²⁶ Bekendtgørelse nr. 717 af 31. august 1995 om forretningsorden for Flygtningenævnet.

5.2.4. Justitsministeriet

Formkrav på Justitsministeriets område findes i en række ganske forskelligartede regelsæt, som bl.a. vedrører retspleje, regler om den offentlige forvaltning, person-, familie- og arveretten samt formueretten.

Reglerne på retsplejeområdet er udformet med henblik på de særlige hensyn, der skal tages til parterne og til den praktiske tilrettelæggelse af de sager, der skal føres ved domstolene. På retsplejeområdet findes et betydeligt antal formkrav.

Formkravene eksisterer bl.a. for at sikre, at alle sagens parter og/eller disses repræsentanter har mulighed for at gøre sig bekendt med det materiale, der findes i sagen. Ved sagsøgers indlevering af en stævning til retten, skal der også indleveres en genpart af stævningen, som af retten sendes til den sagsøgte, jf. **retsplejelovens § 348, stk. 3**²⁷. Ved sagsøgtes fremlæggelse af svarskrift i det første retsmøde skal der ligeledes overgives sagsøger en genpart heraf, jf. **retsplejelovens § 351**²⁸:

”§ 348. ...

Stk. 3. Med stævningen skal indleveres

1) genparter af denne,

2) genparter af de dokumenter, som sagsøgeren agter at påberåbe sig, for så vidt de er i hans besiddelse, og

3) kuvert med sagsøgtes navn og adresse som modtagerbetegnelse og med rettens navn og adresse som afsenderbetegnelse.”

”§ 351. ...

Stk. 3. Sagsøgte skal på mødet fremlægge et svarskrift eller, hvis sagen behandles ved byret, afgive en udtalelse af det i stk. 4 angivne indhold. Sagsøgte skal endvidere fremlægge de dokumenter, som han agter at påberåbe sig, for så vidt de er i hans besiddelse. Er genpart af svarskriftet eller de nævnte dokumenter ikke tidligere meddelt sagsøger, skal en genpart overgives til denne samtidig med fremlæggelsen”.

²⁷ Lovbekendtgørelse nr. 857 af 12. september 2000 af retsplejeloven.

²⁸ Jf. note 27.

*”§ 352. Retten kan undlade at indkalde til det i § 351 nævnte møde. Retten pålægger i så fald sagsøgte at indlevere **svarskrift** til retten inden en frist, der i almindelighed skal være på mindst 2 uger. Fristen regnes fra pålæggets forkyndelse eller afsendelse. Fristen kan efter anmodning forlænges.*

*Stk. 2. Med **svarskriftet** skal indleveres de **dokumenter**, som sagsøgte vil påberåbe sig, for så vidt de er i hans besiddelse. Samtidig med indleveringen til retten skal sagsøgte sende en **genpart** af svarskriftet og dokumenterne til sagsøger.”*

For at lette udførelsen af offentlige myndigheders administrative opgaver findes en række forskellige formkrav, der indebærer, at der f.eks. skal anvendes en bestemt type blanket til en ansøgning mv. Som eksempel kan nævnes **formular ved tinglysning af underpant i bilbogen**, jf. § 4, stk. 1, i bekendtgørelse om tinglysning i bilbogen²⁹:

”§ 4. Tinglysning i bilbogen af underpant sker på grundlag af et pantebrev, der skal være oprettet på Justitsministeriets pantebrevsformular ”BIL” og udformet i overensstemmelse med systematikken i bilag 1 samt reglerne i §§ 5, 6 og 7. Dog tinglyses skadesløsbreve i bilbogen på grundlag af pantebreve, der skal være oprettet på Justitsministeriets pantebrevsformular ”SKADESLØSBREV BIL” og udformet i overensstemmelse med systematikken i bilag 2 samt reglerne i §§ 5, 6 og 7.

Stk. 2. (...)”

Inden for forvaltningsrettens område findes en række bestemmelser med formkrav, der er udformet med henblik på at opnå en hensigtsmæssig administrativ opbygning og tilrettelæggelse af den offentlige forvaltning, herunder for at sikre borgerne en rimelig beskyttelse ved krav om skriftlige begrundelser for afgørelser mv.

Som eksempel på et formkrav, der skal varetage borgernes interesse i forhold til forvaltningen, kan nævnes **forvaltningslovens § 23**³⁰. Af bestemmelsen fremgår, at en borger i nogle situationer har krav på at få en skriftlig begrundelse for en mundtlig afgørelse:

*”§ 23. Den, der har fået en afgørelse meddelt mundtligt, kan forlange at få en **skriftlig begrundelse** for afgørelsen, medmindre afgørelsen fuldt ud giver den pågæl-*

²⁹ Bekendtgørelse nr. 304 af 10. maj 1993 om tinglysning i bilbogen.

³⁰ Lov nr. 571 af 19. december 1985.

dende part medhold. En begæring herom skal fremsættes over for myndigheden inden 14 dage efter, at parten har modtaget underretning om afgørelsen.

*Stk. 2. En begæring om **skriftlig** begrundelse efter stk. 1 skal besvares snarest muligt. Hvis begæringen ikke er besvaret inden 14 dage efter, at begæringen er modtaget af vedkommende myndighed, skal denne underrette parten om grunden hertil samt om, hvornår begæringen kan forventes besvaret.”*

På tinglysningsområdet gør nogle særlige hensyn sig gældende, fordi der knytter sig særlige retsvirkninger til dokumenter, der er tinglyst. Retsvirkningerne indebærer bl.a., at en erhverver, der støtter ret på et tinglyst dokument, enten får den ret, der fremgår af dokumentet, eller får erstatning fra staten. Erstatning bliver bl.a. aktuel, hvis dokumentet viser sig at være falsk, jf. tinglysningslovens § 31, jf. § 27. For at undgå falske anmeldelser er der i tinglysningsloven fastsat en række formkrav, jf. f.eks. kravet i **§ 9 i tinglysningsloven**³¹ om, at der som grundlag for tinglysning skal foreligge et dokument, sammenholdt med kravet i tinglysningslovens § 10, stk. 2, hvorefter udstederens underskrift ved skøder og pantebreve skal være bekræftet af en advokat eller to andre vitterlighedsvidner.

*”§ 9. Som grundlag for tinglysning kræves et **dokument**, der anmeldes for vedkommende dommer til tinglysning. Samtidig med dokumentet indleveres **genpart** af samme. Ved aflysning leveres genpart af **kvitteringen** samt af dertil hørende bevisligheder.”*

”§ 10. ...

Stk. 2. Ved skøder og pantebreve skal udstederens underskrift være bekræftet af en advokat eller to andre vitterlighedsvidner. Samme regel gælder det i stk. 1 nævnte samtykke. Vidnerne skal udtrykkelig bevidne underskriftens ægthed, dateringens rigtighed og udstederens myndighed. Vidnernes stilling og bopæl skal angives. Nævnte bekræftelse er dog ikke nødvendig, når dokumentet udstedes af en offentlig myndighed.”

Indenfor person-, familie- og arveretten findes en række bestemmelser, der har til formål at fastslå en persons identitet med sikkerhed, eller at fastslå at en given tilstand er indtrådt, førend en ny tilstand kan indtræde. Som eksempel kan nævnes **§ 10, stk. 7, i be-**

³¹ Lovbekendtgørelse nr. 622 af 15. september 1986 af tinglysningsloven.

kendtgørelse om ægteskabs indgåelse³², hvorefter der kræves bevis for, at en ægtefælle er afgang ved døden, førend der kan indgås et nyt ægteskab:

”§ 10. ...

*Stk. 7. Bevis for den tidligere ægtefælles død føres ved forevisning af **dødsattest** eller attest fra skifteretten. Ved dødsfald i udlandet må forevises dødsattest udstedt af vedkommende udenlandske offentlige myndighed eller indberetning fra dansk diplomatisk repræsentation i vedkommende land.*

*Stk. 8. Bevis for den tidligere ægtefælles død kan ligeledes føres ved forevisning af **udskrift af dødsformodningsdom**. Udskriften skal være forsynet med en **attest** fra vedkommende byret om, at ankestævning ikke er udtaget inden ankefristens udløb. Udskrifter af landsretsdomme skal være ledsaget af en tilsvarende **attest** fra Højesterets Justitskontor.”*

På Justitsministeriets område findes – som på de øvrige undersøgte ministerområder – en lang række formkrav, som vedrører myndighedernes sagsbehandling. Det gælder bl.a. politiområdet. Som eksempel kan nævnes **§ 1, stk. 2, i bekendtgørelse om behandling af sager om udlevering til andet nordisk land i anledning af visse beslutninger om forsorg eller behandling**³³, hvorefter en anmodning om udlevering skal være affattet skriftligt:

”§ 1. Anmodning om udlevering fremsættes af politiet i det land, hvis myndigheder søger om udlevering.

*Stk. 2. Anmodningen skal være **skriftlig** og affattet på dansk, norsk eller svensk. Den skal indeholde en redegørelse for indholdet af beslutningen om anbringelse på institution eller andet særligt opholdssted samt politiets bekræftelse af, at beslutningen kan fuldbyrdes i det land, hvor den er truffet, jfr. lovens § 1, stk. 1, og § 2.”*

Endvidere kan nævnes **§ 2 i bekendtgørelse om indretning og anlæggelse af skydebaner og feltskydningsterræner**³⁴:

³² Bekendtgørelse nr. 662 af 1. august 1995 om ægteskabs indgåelse.

³³ Bekendtgørelse nr. 500 af 29. december 1970 om behandling af sager om udlevering til andet nordisk land i anledning af visse beslutninger om forsorg eller behandling.

³⁴ Bekendtgørelse nr. 203 af 20. maj 1950 om indretning og anlæggelse af skydebaner og feltskydningsterræner.

*”§ 2. Enhver, der ønsker at indrette en skydebane, skal derom rette **skriftlig** henvendelse til politiet på det sted, hvor banen agtes anlagt. Andragendet skal indeholde nærmere oplysning om skydebanens beliggenhed, om hvem der er ejer af ejendommen, hvorpå skydebanen agtes anlagt, samt om af hvem og til hvilken art af skydning, herunder navnlig med hvilke våben og med hvilken ammunition, skydebanen skal benyttes.”*

Medieansvarsloven³⁵ indeholder i § 36 regler om genmæle, dvs. berigtigelse af oplysninger af faktisk karakter, som er blevet bragt i et massemedie. Efter bestemmelsens stk. 3 skal anmodning om genmæle fremsendes skriftligt til redaktøren for det pågældende massemedie:

”§ 36. ...

*Stk. 3. Anmodning om genmæle skal **fremsendes skriftligt** til redaktøren senest 4 uger efter offentliggørelsen af de faktiske oplysninger, der ønskes imødegået.”*

Ved en kendelse, der blev afsagt den 19. januar 2000, afviste Pressenævnet en klage over, at et massemedie ikke havde bragt et genmæle med den begrundelse, at anmodningen om genmæle var indgivet ved brug af e-mail, som efter nævnets opfattelse ikke kunne sidestilles med en skriftlig meddelelse. Afvisningen af klagen blev endvidere begrundet med, at klagen var indgivet for sent. Pressenævnet har efterfølgende oplyst, at nævnet på et plenarmøde vil drøfte det principielle spørgsmål, om elektroniske overførte meddelelser i visse sammenhænge vil kunne sidestilles med almindelige skriftlige henvendelser.

Politiet udsteder en række autorisationer og tilladelser, der på forlangende skal kunne forevises, jf. f.eks. **§ 2 i bekendtgørelse om forbud mod hold af særligt farlige hunde**³⁶, hvorefter en tilladelse til at besidde en særligt farlig hund skal forevises på forlangende:

³⁵ Lovbekendtgørelse nr. 85 af 9. februar 1998 af medieansvarsloven.

³⁶ Bekendtgørelse nr. 748 af 14. november 1991 om forbud mod hold af særligt farlige hunde.

*”§ 2. Personer, som den 1. december 1991 var ejere af de i § 1 nævnte hunde, kan dog fortsat besidde disse, såfremt der indgives anmeldelse herom til politiet senest den 1. februar 1992, og såfremt hundene forsynes med en øretatovering og steriliseres. Anmeldelse skal ske på en særlig **blanket**, der udleveres af politiet, og som på blanketten **attesterer** retten til at besidde de i § 1 nævnte hunde. Forinden indgivelse af anmeldelse til politiet, skal anmeldelsesblanketten forsynes med en **erklæring** fra en dyrlæge om, at øretatovering og sterilisation har fundet sted.
Stk. 2. Den attesterede anmeldelse skal opbevares af ejeren og skal på forlangende **forevises** politiet.”*

Justitsministeriets område indeholder en række formkrav inden for det forbrugerretlige område. Mange af disse formkrav følger i øvrigt af EU-regler. Som eksempel kan nævnes **§ 6 i lov om forbrugeraftaler, der giver brugsret til fast ejendom på timesharebasis**³⁷, hvorefter en aftale om timeshare skal udfærdiges skriftligt:

*”§ 6. Aftaler, der giver brugsret til fast ejendom på timesharebasis, skal udfærdiges **skriftligt** og **underskrives** af begge parter, og aftalen skal i det omfang, der følger af § 7, være affattet på sproget i det land, hvor forbrugeren har sin bopæl, eller hvor forbrugeren er statsborger. I modsat fald er aftalen ikke bindende for forbrugeren. Sælgeren skal i forbindelse med aftalens indgåelse udlevere en **kopi** af aftalen til forbrugeren.”*

Skriftlighedskravet følger af artikel 4 i direktiv 94/47/EF om beskyttelse af køber i forbindelse med visse aspekter ved kontrakter om brugsret til fast ejendom på timesharebasis, mens direktivet ikke indeholder et udtrykkeligt krav om, at kontrakten skal underskrives af begge parter, men dog indirekte forudsætter dette, idet køberens fortrydelsesret efter direktivet skal regnes fra den dag, hvor begge parter har underskrevet kontrakten.

Et andet eksempel findes i **lov om pakkerejser**³⁸, der også gennemfører et EF-direktiv³⁹. I henhold til lovens **§ 6** skal en aftale om en pakkerejse bekræftes skriftligt af arrangøren overfor kunden:

³⁷ Lov nr. 234 af 2. april 1997 om forbrugeraftaler, der giver brugsret til fast ejendom på timesharebasis.

³⁸ Lov nr. 472 af 30. juni 1993 om pakkerejser.

³⁹ Direktiv 90/314/EF af 13. juni 1990 om pakkerejser, herunder pakkeferier og pakketure.

*”§ 6. Arrangøren skal inden aftalens indgåelse meddele kunden aftalevilkårene samt give oplysning om bestemmelser vedrørende pas, visum, vaccinationer og lignende, som skal overholdes, for at pakkerejsen kan gennemføres. Arrangøren skal bekræfte aftalevilkårene **skriftligt** eller på anden egnet måde over for kunden, herunder udlevere **kopi** af aftalen, hvis den er indgået **skriftligt**.*

Stk. 2. Bestemmelserne i stk. 1 kan fraviges i nødvendigt omfang, hvis aftalen indgås kort før pakkerejsens påbegyndelse.”

Af bemærkningerne til bestemmelsen⁴⁰ fremgår, at man med ordene ”eller på anden egnet måde”, som også findes i artikel 4 i direktiv 90/314/EF, har villet åbne mulighed for, at oplysningerne kan gives på anden måde end ved brug af et papirdokument, f.eks. via edb.

Straffeloven⁴¹ indeholder i §§ 161-163 regler om afgivelse af urigtige erklæringer til offentlige myndigheder. Straffelovens § 163 drejer sig om urigtig erklæring eller bevidnelse til en offentlig myndighed, som den pågældende ikke har nogen viden om, og var indtil 1996 formuleret således, at den alene omfattede skriftlige erklæringer. Ved Østre Landsrets dom af 13. februar 1995 i den såkaldte Proms-sag blev det fastslået, at bestemmelsen eller dennes analogi ikke omfattede indberetninger (erklæringer), som var afgivet på edb-diskette. Herefter blev § 163 ved lov nr. 388 af 22. maj 1996 ændret til følgende ordlyd:

”§ 163. Den, som i øvrigt til brug i retsforhold, der vedkommer det offentlige, skriftligt eller ved andet læsbart medie afgiver urigtig erklæring eller bevidner noget, som den pågældende ikke har viden om, straffes med bøde, hæfte eller fængsel indtil 4 måneder.”

Af forarbejderne til bestemmelsen⁴² fremgår det bl.a., at afgrænsningen af det strafbare område beror på et visuelt kriterium, dvs. om erklæringen for afgiveren fremtræder – eller dog kan fremtræde – i læsbar form, f.eks. på et stykke papir eller på en dataskærm. Det anføres videre, at bestemmelsen f.eks. vil omfatte erklæringer mv. afgivet ved edb-

⁴⁰ Folketingstidende 1992-93 Tillæg A, sp. 9282.

⁴¹ Lovbekendtgørelse nr. 849 af 6. september 2000 af straffeloven.

⁴² Folketingstidende 1995-96, Tillæg A, s. 4076.

diskette eller andet eksternt edb-lagringsmedie, elektronisk post eller EDI ("electronic data interchange", dvs. elektronisk dataudveksling på grundlag af en på forhånd fastlagt standard for indhold og struktur). Derimod vil bestemmelsen ikke omfatte tilfælde, hvor erklæringen kun kan fremtræde i læsbar form for modtageren, f.eks. ved indtastning af oplysninger på en telefon, eller ved indtaling over telefonen til et dataanlæg, der gennem talegenkendelse kan omsætte erklæringen til læsbar form.

5.3. Inddeling efter formål

Udover en inddeling efter ministerområde har udvalget også søgt at rubricere de forskellige formkrav i kategorier afhængig af, hvilket formål kravet kan antages at varetage. I nogle tilfælde går disse formål på tværs af ministerområderne og kan således tjene til at samle en række tilsyneladende forskelligartede bestemmelser i én kategori, som kan fortolkes – og eventuelt ændres – efter samme grundlæggende principper.

5.3.1. Retsvirkninger knyttet til besiddelsen af et dokument

5.3.1.1. Negotiabilitet

I nogle tilfælde knytter der sig bestemte rettigheder til besiddelsen af et papirdokument. Der kan f.eks. være tale om, at man knytter retten til at gøre en bestemt fordring gældende til besiddelsen af et dokument. Herved lettes omsætningen. Visse dokumenter, f.eks. omsætningsgældsbreve, veksler og checks, som altid skal foreligge skriftligt, er ved lov gjort negotiable (omsættelige). Et dokument kaldes negotiabelt, hvis det er underkastet et dobbelt sæt af eksstinktionsregler, dels regler om erhververens eksstinktion af visse indsigelser fra dokumentets udsteder, dels regler om tab af tidligere indehaveres ret over dokumentet.

Ved f.eks. omsætningsgældsbreve er negotiabilitetsvirkningerne nært knyttet til **dokumentbesiddelsen**, idet retten til at gøre en fordring gældende efter reglerne i gældsbrevsloven afhænger af **indholdet og ihændehavelsen af selve dokumentet**. Erhververen opnår således som udgangspunkt den retsstilling, som fremgår af det dokument, han har i sin besiddelse.

Som eksempel kan nævnes **gældsbrevslovens § 14, stk. 1⁴⁴**:

”§ 14. Når et ihændehavergælds brev er overdraget til eje eller pant af den, der sad inde med det, og erhververen har fået gælds brevet i hænde, hindrer det ikke hans ret, at overdrageren var umyndig eller manglede ret til at råde over gælds brevet, medmindre erhververen vidste dette eller ikke har udvist den agtpågivenhed som forholdene krævede”.

Tilsvarende bestemmelser findes i bl.a. checkloven, vekselloven og aktieselskabsloven. Bestemmelserne om negotiabilitet i check- og vekselovgivningen bygger på internationale konventioner.

Søloven⁴⁵ indeholder regler om konnossementer, dvs. skriftlige erklæringer fra transportøren af, at gods, der skal transporteres med skib, er modtaget, og at godset vil blive udleveret til konnossementets indehaver på bestemmelsesstedet. Et konnossement kan være negotiabelt, men der findes også ikke-negotiable konnossementer, jf. herom nedenfor. Konnossementer skal underskrives af transportøren eller af nogen, der handler på dennes vegne, jf. sølovens § 296, stk. 3, men af bestemmelsen fremgår, at underskriften også kan være fremstillet på elektronisk vis. Af bemærkningerne til søloven⁴⁶ følger endvidere, at et konnossement ikke behøver at være et fysisk dokument. Det vil således også være muligt at udstede elektroniske konnossementer.

⁴⁴ Lovbekendtgørelse nr. 669 af 23. september 1986 af lov om gældsbreve.

⁴⁵ Lovbekendtgørelse nr. 39 af 20. januar 1998 af søloven med senere ændringer.

⁴⁶ Folketingstidende 1993-94, Tillæg A, sp. 4985 f.

Søloven indeholder ikke særlige regler om elektroniske konnossementer, og i givet fald vil disse således skulle behandles efter sølovens almindelige regler. Reglerne om negotiabilitet i søloven forudsætter i visse tilfælde, at der foreligger et fysisk dokument, jf. f.eks. sølovens § 302:

*”§ 302. Den, der **foreviser** et konnossement og ved dets tekst eller for så vidt angår ordrekonnossement ved en sammenhængende række overdragelser eller overdragelse in blanco fremtræder som retmæssig indehaver af konnossementet, er legitimeret som modtager af godset.*

*Stk. 2. Når konnossementet er udstedt i flere **eksemplarer**, er det for udlevering på bestemmelsesstedet tilstrækkeligt, at modtageren legitimerer sig med et **eksempel**. Udleveres godset andetsteds end på bestemmelsesstedet, må desuden de øvrige **eksemplarer leveres tilbage** eller sikkerhed stilles for de krav, som indehaveren måtte gøre gældende mod transportøren.”*

På værdipapirområdet har man i **værdipapirhandelsloven**⁴⁷ etableret et særskilt regelsæt, som har gjort det muligt at erstatte de hidtil anvendte papirdokumenter med registreringer på en konto i en værdipapircentral. Ordningen går ud på, at bl.a. aktier og obligationer registreres i en værdipapircentral, således at indholdet af den pågældende rettighed fastlægges ved registreringen i stedet for ved at udstede et papirdokument, jf. værdipapirhandelslovens § 59. Dispositioner over rettigheden sikres herefter mod kreditorer og mod aftaleerhververe ved registreringer i værdipapircentralen, jf. værdipapirhandelslovens § 66. Overdrages rettigheden, overføres registreringen til købers konto, og registrering af efterfølgende aftaler om overdragelse af fondsaktivet sker herefter ved, at det registreres på den nye købers konto, samtidig med at registreringen af aktivet på sælgers konto slettes. Begrænsede rettigheder, f.eks. panterrettigheder og udlæg i fondsaktiver, registreres på tilsvarende vis på ejerens konto.

Registreringen tjener som sikringsakt. Når en rettighed er registreret i en værdipapircentral, er den beskyttet mod retsforfølgning fra kreditorer og mod aftaleerhververe. Akti-

⁴⁷ Lovbekendtgørelse nr. 725 af 25. juli 2000 af lov om værdipapirhandel m.v.

ver, der er registreret i en værdipapircentral, er negotiable i den forstand, at en godtroende aftaleerhverver ikke kan mødes med andre indsigelser mod tidligere aftaleerhververs registrerede ret end falsk og voldelig tvang, jf. værdipapirhandelslovens § 69:

”§ 69. Når registrering af en aftale om rettigheder over fondsaktiver er endeligt gennemført i en værdipapircentral, kan en godtroende erhverver ifølge registreret aftale ikke mødes med nogen indsigelse mod gyldigheden af aftalen. Dog bevares den indsigelse, at aftalen er ugyldig som følge af falsk eller voldelig tvang.”

Ordningen på værdipapirområdet er et eksempel på, at man er nødt til at etablere andre sikringsakter mv. i form af registreringsordninger, når man forlader papirmediet, og dermed ikke længere – som f.eks. i den ovennævnte bestemmelse i gældsbrevslovens § 14 – kan lade retten til at gøre en fordring gældende bero på, hvem der besidder det originale papirdokument.

5.3.1.2. Dokumentation for identitet mv.

Der kan også på andre måder knytte sig særlige retsvirkninger til besiddelsen af et papirdokument. Det gælder bl.a. ved legitimationspapirer som f.eks. et pas, som benyttes til at identificere pasindehaveren, og derudover bl.a. - eventuelt ved indsættelse af eller stempling af visum i passet - giver pasindehaveren adgang til indrejse. Krav om besiddelse og forevisning af et sådant dokument kan altså være begrundet i ønsket om at sikre dokumentation for, at den pågældende har ret (tilladelse) til at foretage en bestemt handling og kan endvidere tjene til at sikre bevis for identiteten af indehaveren, jf. f.eks. **paslovens § 4**⁴⁸:

”§ 4. Enhver er i det omfang, justitsministeren bestemmer det, og efter nærmere af ham fastsatte regler, pligtig til ved indrejse til og udrejse af landet at melde sig til paskontrollen og forevise sit pas eller anden rejselegitimation”.

⁴⁸ Lovbekendtgørelse nr. 586 af 1. september 1986 af lov om pas til danske statsborgere m.v.

Krav om besiddelse og forevisning af et sådant dokument kan også være begrundet i ønsket om at sikre dokumentation for, at den pågældende har ret (tilladelse) til at foretage en bestemt handling, og kan endvidere tjene til at sikre bevis for identiteten af indehaveren, jf. f.eks. **§ 12 i bekendtgørelse om vagtvirksomhed**⁴⁹:

*”§ 12. Under udførelsen af vagtvirksomhed skal virksomhedens personale altid være i besiddelse af et **personlegitimationskort**, der udstedes af rigspolitichefen, når det er dokumenteret, at grundkursus for vagtfunktionærer eller den del af uddannelsen til sikkerhedsvagt, der giver den pågældende kvalifikationer svarende til grundkursus for vagtfunktionærer, jf. § 9, er gennemført.*

*Stk. 2. Personlegitimationskortet skal **forevises** på forlangende.*

*Stk. 3. Når et ansættelsesforhold ophører, skal vagtvirksomheden **sende** den pågældendes personlegitimationskort til den politimester (politidirektøren), der har godkendt den pågældende, senest 8 dage efter ansættelsesforholdets ophør med oplysning om fratrædelsesdatoen. Personlegitimationskort til ansatte i statslig eller kommunal myndighed, jf. § 26 a, sendes dog til rigspolitichefen.”*

Anvendelse af digitale dokumenter i forbindelse med disse typer af krav volder umiddelbart problemer, fordi reglerne er bygget op omkring nogle egenskaber – den umiddelbare læsbarhed og eksistensen af et originaldokument – som papirdokumenter besidder, men som ikke findes hos digitale dokumenter.

5.3.1.3. Dokumentation for en ret, tilstand mv.

Et formkrav kan have til formål at sikre dokumentation for, at man har ret til at disponere over et formuegode. Som eksempel herpå kan nævnes den tidligere (i kapitel 5.2.4) refererede bestemmelse **i tinglysningslovens § 9**⁵⁰:

”§ 9. Som grundlag for tinglysning kræves et dokument, der anmeldes for vedkommende dommer til tinglysning. Sam-

⁴⁹ Bekendtgørelse nr. 963 af 23. december 1986 om vagtvirksomhed som ændret ved bekendtgørelse nr. 611 af 22. juni 2000.

⁵⁰ Jf. note 31.

tidig med dokumentet indleveres genpart af samme. Ved aflysning leveres genpart af kvitteringen samt af dertil hørende bevisligheder.

*Stk. 2. Med et pantebrev skal **følge det sidst tinglyste skøde** på ejendommen. Oplyses det ved anmelderens skriftlige erklæring til dommeren, at skødet er bortkommet, eller at det af anden gyldig grund ikke kan skaffes til veje, skal der i dets sted fremlægges et offentligt dokument, der kan bestyrke pantebrevets ægthed, såsom udstederens borgerskab, ansættelsesbrev, beskikkelse el. lign.*

Stk. 3...”

Kravet om indlevering af det seneste skøde har til formål at sikre, at den anmeldte panterettighed stammer fra ejeren af ejendommen, som er den, der er berettiget til at pantsætte ejendommen. Ejeren af ejendommen vil normalt ligge inde med det seneste skøde, og indsendelse heraf giver således en vis sikkerhed for, at pantebrevet er udstedt af den rette, idet underskrifterne kan sammenlignes.

Mens et skøde hovedsagelig tjener andre formål end at virke som dokumentation, findes der også eksempler på dokumenter, der som sit hovedformål har at virke som dokumentation for en tilstand, en rettighed eller lignende. Som eksempel kan nævnes **§ 38 i lov om erstatning for atomskader (nukleare skader)**⁵¹:

*”§ 38. Ved forsendelse af nuklear substans fra eller til et anlæg her i riget henholdsvis til en modtager eller fra en afsender i en anden stat eller ved forsendelse af sådant materiale gennem riget fra eller til et anlæg i anden konventionsstat skal den ansvarlige anlægsindehaver forsyne fragtføreren med et **certifikat**, som udstedes af forsikreren eller den, som har stillet anden sikkerhed til dækning af erstatningspligten. Fragtføreren må ikke udføre transporten her i riget, forinden han har modtaget certifikatet, som på forlangende skal **forevises** for vedkommende myndigheder.”*

Nogle dokumenter indeholder en konstaterende erklæring om, at en given tilstand er indtrådt. Dokumenterne kan herefter forevises for myndigheder mv. som bevis herfor. Som eksempel på et sådant dokument kan nævnes en dødsattest, som udstedes af lægen i forbindelse med dødsfald, jf. **lov om ligsyn, obduktion og transplantation m.v. § 7**⁵²:

⁵¹ Lov nr. 332 af 19. juni 1974 om erstatning for atomskader (nukleare skader).

⁵² Lov nr. 402 af 13. juni 1990 om ligsyn, obduktion og transplantation.

”§ 7. Når ligsyn er afsluttet, skal lægen udstede dødsattest. Er dødsfaldet indberettet til politiet efter § 4, må dødsattest kun udstedes, hvis politiet meddeler, at indberetningen ikke giver anledning til retslægeligt ligsyn. Er der foretaget retslægeligt ligsyn, udstedes dødsattesten af den læge, der har deltaget heri.

Stk. 2. Liget må ikke begravnes, brændes eller føres ud af landet, førend dødsattest er udstedt. Er dødsattesten udfærdiget efter retslægeligt ligsyn, skal attesten yderligere være forsynet med politiets påtegning om, at intet er til hinder for, at liget begravnes, brændes eller føres ud af landet.”

Ud over i forbindelse med begravelse mv. anvendes dødsattester bl.a. som dokumentation i forbindelse med indgåelse af (nyt) ægteskab, jf. **§ 10, stk. 7, i bekendtgørelse om ægteskabs indgåelse**⁵³:

”§ 10. ...

...

*Stk. 7. Bevis for den tidligere ægtefælles død føres ved **forevisning af dødsattest** eller attest fra skifteretten. Ved dødsfald i udlandet må forevises **dødsattest** udstedt af vedkommende udenlandske offentlige myndighed eller indberetning fra dansk diplomatisk repræsentation i vedkommende land.”*

De tidligere nævnte bestemmelser i pasloven og næringsloven kan også placeres i denne kategori.

Ligesom for de under kapitel 5.3.1.2. nævnte identifikationsdokumenter gælder det for de her nævnte formkrav, at disse hænger tæt sammen med papirets egenskaber som bærer og formidler af information. I de nævnte eksempler er det navnlig af betydning, at papirdokumenter kan medbringes eller ophænges og forevises for den eller dem, som informationen skal videregives til.

⁵³ Jf. note 32.

5.3.2. Beskyttelses- eller advarselsfunktion (f.eks. forbrugerbeskyttelse mv.)

Krav om skriftlighed mv. kan også være givet for at beskytte en svagere part i et retsforhold. For at beskytte forbrugerne er der således på en række områder fastsat formkrav. Kravene tjener navnlig til at sikre forbrugerne adgang til at gøre sig bekendt med aftalens vilkår mv. og til at sikre bevis for indholdet af f.eks. en aftale, som indgås. Som eksempel kan nævnes **kreditaftalelovens § 8⁵⁴**:

*”§ 8. En kreditaftale skal udfærdiges **skriftligt** og indeholde de oplysninger, der er nævnt i § 9 eller § 10 og § 14, samt aftalens øvrige væsentlige vilkår.*

*Stk. 2. Forbrugeren skal i forbindelse med aftalens indgåelse have **overgivet** en genpart af kreditaftalen.”*

Der kan endvidere henvises til **§ 5 i skiltningsbekendtgørelsen⁵⁵**. Kravene i denne bestemmelse har navnlig til formål at sikre gennemsigtighed om priserne:

”§ 5. For udlån skal der i ekspeditionslokalet på et for publikum iøjnefaldende sted ved skiltning tydeligt angives

- 1) den nominelle årlige rente (d.v.s. den årlige rente inkl. renters rente),*
- 2) højeste og laveste nominelle årlige rente, hvis den pågældende udlånsform udbydes med forskellige rentesatser,*
- 3) eventuel løbende provision,*
- 4) stiftelsesomkostninger til pengeinstituttet, samt at afgifter til det offentlige ikke er angivet,*
- 5) de årlige omkostninger i procent for kreditten, og*
- 6) om der skal betales omkostninger til sikkerhedsstillelse.*

Stk. 2. (...).”

Et formkrav kan også have til formål at sikre, at oplysninger er tilgængelige et bestemt sted, jf. f.eks. kravet om at auktionsvilkår skal ophænges et iøjnefaldende sted i lokalet i **§ 13, stk. 1, i auktionslederloven⁵⁶**:

⁵⁴ Lov nr. 398 af 13. juni 1990 om kreditaftaler.

⁵⁵ Bekendtgørelse nr. 902 af 12. november 1992 om oplysning til forbrugere i ekspeditionslokaler, i annoncer m.v. om indlånsrenter, afkast af indskud på gevinstkonti samt udlånsrenter og andre kreditomkostninger i pengeinstitutter.

⁵⁶ Lovbekendtgørelse nr. 191 af 9. april 1986 af lov om offentlig auktion ved auktionsledere.

*”§ 13. Ved auktionens begyndelse oplæser auktionslederen auktionsvilkårene, som tillige skal **opslås til almindelig efterretning på et iøjnefaldende sted i lokalet** eller, hvis auktionen afholdes under åben himmel, da der, hvor den holdes eller begyndes. Når dette er iagttaget, kan de på auktionen bydende ikke påberåbe sig uvidenhed om auktionsvilkårene. Genstandene skal så vidt muligt opråbes i den rækkefølge, i hvilken de er opført i kataloget, og under iagttagelse af reglerne i § 12, stk. 2. Stk. 2. ...”*

Formkrav på forbrugerbeskyttelsesområdet kan også have til formål at sikre, at forbrugeren modtager visse oplysninger forud for indgåelsen af en aftale. Ofte stilles der således krav om, at den erhvervsdrivende skal give forbrugeren et dokument med visse oplysninger, som skal være givet på klar og tydelig vis eller lignende. Som eksempler kan anføres de i kapitel 5.2.4. nævnte bestemmelser i lov om forbrugerbeskyttelse ved erhvervelse af fast ejendom på timesharebasis og pakkerejseloven.

Forbrugerbeskyttende formkrav findes endvidere bl.a. i dørsalgsloven⁵⁷ og lov om omsætning af fast ejendom⁵⁸.

En betydelig andel af de forbrugerbeskyttende formkrav findes i lovgivning, der gennemfører EU-regler i dansk ret. Det gælder bl.a. kreditaftaleloven, dørsalgsloven, timeshareloven og pakkerejseloven.

Hvor der i nyere EU-direktiver på forbrugerbeskyttelsesområdet stilles krav om, at forbrugerne skal modtage oplysninger mv., har man benyttet den formulering, at forbrugeren skal modtage oplysningerne ”skriftligt eller på et andet varigt medium, som er til hans rådighed og tilgængeligt for ham”, jf. artikel 6, stk. 3, i forbrugerkøbsdirektivet⁵⁹ og artikel 5, stk. 1, i fjernsalgsdirektivet⁶⁰. Disse formuleringer i de nyere direktiver kan få betydning ved fortolkning af bestemmelser om krav om skriftlighed i ældre direktiver.

⁵⁷ Lovbekendtgørelse nr. 886 af 23. december 1987 af lov om visse forbrugeraftaler med senere ændringer.

⁵⁸ Lov nr. 453 af 30. juni 1993 om omsætning af fast ejendom med senere ændringer.

⁵⁹ Direktiv 99/44 af 25. maj 1999 om visse aspekter af forbruger køb og garantier i forbindelse hermed.

⁶⁰ Direktiv 97/7 af 20 maj 1997 om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg.

I den lov om ændring af dørsalgsloven m.v., som gennemfører fjernsalgsdirektivet i dansk ret⁶¹, bestemmes det i § 11 a, stk. 1, at oplysningsforpligtelsen efter direktivets artikel 5, stk. 1, skal kunne opfyldes ved, at den erhvervsdrivende giver forbrugeren oplysningerne ”læsbart på papir eller på andet læsbart medium, som forbrugeren råder over og har adgang til”. I bemærkningerne til forslaget⁶² anføres følgende om forståelsen af direktivet:

”Efter direktivet skal oplysningerne som nævnt gives ”skriftligt eller på et andet varigt medium”. Rent sprogligt synes udtrykket ”skriftligt” her at være anvendt i betydningen: ”på papir”. I den pågældende direktivbestemmelse (artikel 5) er det imidlertid særligt om oplysning om fortrydelsesretten fastsat, at denne oplysning skal gives ”skriftligt”. Kommissionen har på et møde med medlemslandene om gennemførelsen af direktivet tilkendegivet, at udtrykket efter Kommissionens opfattelse i direktivet er anvendt i betydningen ”læsbart” – altså med anvendelse af skrifttegn – idet det ikke har været tilsigtet at lægge hindringer i vejen for udbredelsen af elektronisk kommunikation på dette område.

Bestemmelsen foreslås på denne baggrund gennemført således, at det kræves, at alle de omhandlede oplysninger skal gives læsbart (med brug af bogstaver m.v.) og på papir eller et andet varigt medium.

Det fremgår ikke af direktivet, hvad der skal forstås ved ”varigt medium”, og afgørelsen af, om et medium er ”varigt” i lovens og direktivets forstand, må træffes på grundlag af en konkret vurdering. Ved vurderingen – også af eventuelle nye kommunikationsmidler, der måtte blive udbredt – bør der ud fra formålet med bestemmelsen lægges vægt på, om det er muligt for forbrugeren at opbevare (lagre) de oplysninger, han modtager direkte med det pågældende medium, på en sådan måde, at oplysningerne i en rimelig periode er tilgængelig for fremtidig reference og kan reproducere uændrede.”

⁶¹ Lov nr. 442 af 31. maj 2000 om ændring af lov om visse forbrugerftaler, markedsføringsloven og visse andre love.

⁶² Folketingstidende 1999-2000, Tillæg A, s. 5938.

5.3.3. Bevisfunktioner

5.3.3.1. Erklæringer på tro og love

Krav om skriftlighed og underskrift kan også have til formål at fastlægge (bevissikre) indholdet af en erklæring, således at den, der afgiver erklæringen, i givet fald kan straffes for at have afgivet falsk erklæring.

Afgivelse af urigtige oplysninger i skriftlige erklæringer eller på andet læsbart medie over for offentlige myndigheder er som tidligere nævnt i kapitel 5.2.4 kriminaliseret i **straffelovens § 163⁶³**:

”§ 163. Den, som i øvrigt til brug i retsforhold, der vedkommer det offentlige, skriftligt eller ved andet læsbart medie afgiver urigtig erklæring eller bevidner noget, som den pågældende ikke har viden om, straffes med bøde, hæfte eller fængsel indtil 4 måneder.”

Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet overvejer i øjeblikket, om der er behov for at modernisere straffelovens bestemmelser om dokumentfalsk mv. i lyset af den teknologiske udvikling.

I nogle tilfælde har lovgiver fundet behov for i særlig grad at indskærpe en sandhedspligt ved at stille krav om, at en erklæring afgives "på tro og love" eller lignende. Sådanne bestemmelser findes på en række forskellige retsområder og i et stort antal regler.

Jf. som eksempel **Konkurslovens § 148, stk. 2⁶⁴**:

⁶³ Jf. note 41.

⁶⁴ Lovbekendtgørelse nr. 118 af 4. februar 1997 af konkursloven.

”§ 148. ...

Stk. 2. Regnskabet skal ledsages af en kort redegørelse for boets behandling, dets indtægt og udgift. Kurator og så vidt muligt skyldneren skal ved påtegning på udkastet på tro og love erklære, at der ikke dem bekendt findes yderligere til indtægt for boet.”

Straffeloven indeholder i §§ 161-162⁶⁵ særlige straffebestemmelser om falske erklæringer på tro og love, henholdsvis om urigtige pligtmæssige erklæringer:

”§ 161. Med bøde, hæfte eller under skærpende omstændigheder med fængsel indtil 2 år straffes den, som uden for det i § 158 nævnte tilfælde for eller til en offentlig myndighed afgiver en falsk erklæring på tro og love eller på lignende højtidelig måde, hvor sådan form er påbudt eller tilstedt.

§ 162. Den, som ellers for eller til en offentlig myndighed afgiver urigtig erklæring om forhold, angående hvilke han er pligtig at afgive forklaring, straffes med bøde eller hæfte eller med fængsel indtil 4 måneder.”

Bestemmelserne gælder, uanset om erklæringen er afgivet mundtligt eller skriftligt, og vil således også finde anvendelse, hvis en sådan erklæring afgives ved brug af digitale medier. Om anvendelsen af § 162 i sådanne tilfælde anførtes i Straffelovrådets betænkning nr. 1032/1985 om datakriminalitet, s. 63-64:

”Straffelovens § 162 giver mulighed for at straffe den, som afgiver urigtig erklæring for eller til en offentlig myndighed om forhold, angående hvilke han er pligtig at afgive forklaring. Bestemmelsen stiller ikke særlige formkrav til erklæringen og vil således også kunne omfatte urigtige oplysninger, som indgives ved hjælp af datateknik.

...

Der er efter Straffelovrådets opfattelse ikke på nuværende tidspunkt påvist behov for nye bestemmelser i straffeloven om urigtige erklæringer, der afgives ved hjælp af datateknik. Sådanne erklæringer afgives i dag kun på meget begrænsede retsområder, og de pågældende myndigheder vil således have anledning til og mulighed for i forbindelse med indførelse af datateknik at tage stilling til, om der er behov for i det pågældende retsgrundlag at søge gældende straffebestemmelser om urigtige erklæringer ændret.”

⁶⁵ Jf. note 41.

Som anført ovenfor indeholder straffelovens § 163 nu en regel om straf for den, der til brug i retsforhold, der vedkommer det offentlige, skriftligt eller ”ved andet læsbart medie” afgiver urigtig erklæring eller bevidner noget, som den pågældende ikke har viden om. Ordene ”ved andet læsbart medie” er indsat i bestemmelsen ved en ændring, der ligger efter den netop citerede udtalelse af 1985 fra Straffelovrådet, nemlig ved lov nr. 388 af 22. maj 1996.

5.3.3.2. Sikkerhed for, at en meddelelse stammer fra en bestemt person, at denne person er sin fornuft mægtig mv.

Krav om underskrift eller lignende vil ofte have til formål at sikre dokumentation for, at en meddelelse stammer fra en bestemt person, og sådanne krav er meget udbredte, bl.a. på området for kommunikation mellem det offentlige på den ene side og borgere og virksomheder på den anden.

Underskriftskrav kan også udformes således, at f.eks. en ansøgning skal underskrives ”for”, dvs. i overværelse af en myndighed, og kan i så fald – ved sammenligning med underskrifter på andre dokumenter – gøre det muligt for den pågældende myndighed at kontrollere, om underskriveren er den, han eller hun udgiver sig for.

De fleste tinglysningsdokumenter skal **underskrives** egenhændigt af den, som dokumentet stammer fra. Kravet om en egenhændig underskrift har til formål at sikre tinglysningsdommeren mulighed for at påse, at dokumentet er ægte, sådan at det så vidt muligt sikres, at de rettigheder som tinglyses, er gyldige. For at øge denne sikkerhed kræves det ved

skøder og pantebreve, at udstederens underskrift bekræftes af en advokat eller 2 andre vitterlighedsvidner, jf. **tinglysningslovens § 10, stk. 2**⁶⁶:

”§ 10. ...

*Stk. 2. Ved skøder og pantebreve skal udstederens **underskrift** være bekræftet af en advokat eller to andre vitterlighedsvidner. Samme regel gælder det i stk. 1 nævnte samtykke. Vidnerne skal udtrykkelig bevidne underskriftens ægthed, dateringens rigtighed og udstederens myndighed. Vidnernes stilling og bopæl skal angives. Nævnte bekræftelse er dog ikke nødvendig, når dokumentet udstedes af en offentlig myndighed”.*

For så vidt angår testamenter stilles der også særlige krav om, at et testamente som hovedregel skal være skriftligt og underskrevet eller vedkendt af testator, enten for en notar eller for to vidner. Formkravene har til formål at sikre mod falsk samt at afskære tvivl om den rette forståelse af testamentet. Kravene kan kun fraviges under helt særlige omstændigheder, hvor der kan oprettes et ”nødtestamente”. Hvis formkravene i andre tilfælde ikke er overholdt, indebærer dette, at testamentet kan anfægtes.

Formkravene vedrørende testamenter findes i **arvelovens § 40**⁶⁷:

*”§ 40. Testamente skal oprettes **skriftligt** og underskrives eller vedkendes for en notar eller for to vidner.”*

Reglerne om nødtestamenter findes i **arvelovens § 44**:

”§ 44. Den, der på grund af sygdom eller andet nødstilfælde er forhindret i at oprette testamente i overensstemmelse med foranstående regler, kan mundtligt meddele sit testamente i samtidig nærværelse af to vidner eller oprette testamente uden vidner ved et egenhændigt skrevet og underskrevet dokument.

Stk. 2. Ved oprettelse af et mundtligt testamente finder bestemmelserne i § 42, stk. 2, og § 43, stk. 1, 2. punktum, og stk. 2 og 3, anvendelse. Vidnerne skal snarest muligt nedskrive testamentet og underskrive det således oprettede dokument.

⁶⁶ Jf. note 31.

⁶⁷ Lovbekendtgørelse nr. 584 af 1. september 1986 af arveloven.

Stk. 3. Et i medfør af stk. 1 oprettet testamente bortfalder, når der i 3 måneder ikke har været nogen hindring for at oprette testamente i overensstemmelse med § 40.”

Digital signatur har som nævnt ovenfor i kapitel 2 bl.a. til formål at sikre dokumentation for, at et elektronisk dokument stammer fra en bestemt person, og et nøglecenter vil ved udstedelse af et certifikat til en vis grad varetage samme funktioner som vitterlighedsvidnerne i de citerede bestemmelser, nemlig at indestå for identiteten af den, der har afgivet underskriften/signaturen. Nøglecentret vil dog i almindelighed ikke kunne udtale sig om signaturindehaverens evne til at handle fornuftmæssigt mv., således som det i nogle tilfælde kræves i forbindelse med vitterlighedsattestationer, men det er på den anden side ikke udelukket, at nøglecentre tilbyder at udføre også sådanne tjenesteydelser.

5.3.3.3. Bevis for, at en meddelelse er modtaget eller godkendt, eller at modtageren har været til stede på et bestemt sted

Krav om skriftlighed mv. kan også have til formål at sikre bevis for, at en person har modtaget eller set et bestemt dokument, eller at personen har været til stede på et bestemt sted. Som eksempel kan nævnes reglerne i **retsplejelovens § 155** og **§ 156⁶⁸** om forkyndelse af dokumenter under retssager mv.:

”§ 155. Forkyndelse sker ved, at den meddelelse, der skal forkyndes, med eventuelle bilag

- 1) sendes eller afleveres til den pågældende, der samtidig anmodes om at bekræfte modtagelsen på en genpart af dokumentet eller, hvis forkyndelsen foretages ved rettens eller anklagemyndighedens foranstaltning, et særligt modtagelsesbevis (brevforkyndelse),*
- 2) sendes til den pågældende i et brev med afleveringsattest (postforkyndelse) eller*
- 3) afleveres til den pågældende af en stævningsmand (stævningsmandsforkyndelse).*

⁶⁸ Jf. note 27.

§ 156. Ved brevforkyndelse anses meddelelsen for forkyndt, hvis genparten eller modtagelsesbeviset er underskrevet af den pågældende personligt (...)."

Andre formkrav har til formål at sikre, at der tilvejebringes et bevis for, at en meddelelse er set eller godkendt af en bestemt person. Som eksempel på et sådant formkrav kan nævnes **§ 20, stk. 3, i fondsloven**⁶⁹, der indeholder et krav om bestyrelsesmedlemmers underskrift af referater:

"§ 20. Formanden skal sørge for, at bestyrelsen holder møde, når dette er nødvendigt, og skal påse, at samtlige medlemmer indkaldes.

Stk. 2. Bestyrelsen er beslutningsdygtig, når halvdelen af medlemmerne eller det højere antal, som foreskrives i vedtægten, er til stede. Medmindre vedtægten bestemmer andet, træffer bestyrelsen beslutning ved simpelt stemmeflertal, og formandens stemme er i tilfælde af stemmelighed afgørende.

*Stk. 3. Over forhandlingerne i bestyrelsen skal der føres referat, der underskrives af samtlige tilstedeværende medlemmer. Et bestyrelsesmedlem eller en direktør, der ikke er enig i bestyrelsens beslutning, har ret til at få sin mening tilført referatet. Bestyrelsen skal sørge for, at referatet **opbevares forsvarligt**."*

Tilsvarende regler om underskrift af protokoller, referater mv. findes på en meget lang række andre retsområder, typisk i lovgivning om nævn og råd.

Forkyndelsesreglerne i retsplejeloven og tilsvarende bestemmelser på andre retsområder forudsætter normalt bl.a., at information er kommet frem til modtageren af et brev, når dette er afleveret i postkassen eller gennem brevsprækken mv. på den pågældendes bopæl, jf. den netop nævnte bestemmelse om postforkyndelse. Når man kan lade bl.a. forkyndelsesordningen hvile på en forudsætning herom, hænger det naturligvis sammen med, at denne i langt de fleste tilfælde holder stik.

⁶⁹ Lovbekendtgørelse nr. 698 af 11. august 1992 af lov om fonde og visse foreninger.

Det er ikke uden videre sikkert, at det samme vil være tilfældet, hvis information fremsendes via e-mail, ligesom det kan give anledning til tvivl, hvornår en e-mail kan anses for at være kommet frem til modtageren. Formkrav, som har til formål at sikre, at information kommer frem til en bestemt person, kan derfor give anledning til særlige overvejelser i relation til elektroniske dokumenter.

5.3.3.4. Fastlæggelse af tidspunktet for modtagelse

Formkrav kan også følge af et behov for at kunne fastlægge et bestemt tidspunkt for foretagelsen af en given handling eller modtagelsen af et dokument. Som eksempel kan nævnes **tinglysningslovens**⁷⁰ regler om, at et dokument skal indføres i dagbogen, og at dokumentet og genparten skal påtegnes herom med angivelse af den dato, hvor dokumentet blev indført i dagbogen.

”§ 14. ...

Stk. 2. ...

*Stk. 3. Efter indførelsen i dagbogen får dokumentet og genparten **påtegning** herom med angivelse af indførelsesdatoen. Den i dagbogen angivne dato for dokumentets indlevering anses for rigtig, medmindre der føres fuldt bevis for det modsatte. Samme regel gælder dagbogens øvrige indhold.*

Stk. 4. ...”

Tilsvarende principper gælder om fastlæggelse af tidspunktet for indlevering af konkursbegæringer og stævninger. Også ved registrering i en værdipapircentral, jf. herom ovenfor i kapitel 5.3.1.1., skal tidspunktet for anmeldelsen registreres, jf. **§ 23 i registreringsbekendtgørelsen**⁷¹:

”§ 23. Et kontoførende institut skal til enhver tid over for en værdipapircentral kunne redegøre for,

1)...

2)...

⁷⁰Jf. note 31.

⁷¹Bekendtgørelse nr. 925 af 17. oktober 1996 om registrering af fondsaktiver i en værdipapircentral.

3) på hvilket tidspunkt anmeldelse til registrering er modtaget,
...”

Fastlæggelse af modtagelsestidspunktet for et elektronisk dokument, f.eks. en e-mail, vil i situationer som de nævnte, hvor indlevering sker til en offentlig myndighed eller en anden troværdig tredjepart, kunne ske efter samme principper, som når der er tale om et papirdokument. Der opstår imidlertid nogle særlige bevisspørgsmål, når f.eks. e-mails udveksles mellem private parter, og en af parterne på et senere tidspunkt ønsker at dokumentere, hvornår – og med hvilket indhold – en meddelelse blev modtaget af ham selv eller af den anden.

5.3.3.5. Sikring af bevis over tid

Et andet bevismæssigt formål, som kan ligge bag et formkrav om skriftlighed, underskrift mv., kan være hensynet til at sikre, at det bliver muligt at bevise en given tilstand mv., også selv om der går lang tid, før behovet for at føre beviset bliver aktuelt. Som eksempel på et sådant formkrav kan nævnes kravet om, at et testamente (bortset fra de særlige nødtestamenter) skal være skriftligt, jf. **arvelovens § 40**⁷²:

*”§ 40. Testamente skal oprettes **skriftligt** og underskrives eller vedkendes for en notar eller for to vidner.”*

Et tilsvarende eksempel er kravet om, at der ved oprettelse af notartestamenter skal ske indberetning til Centralregistret for Testamenter, jf. § 17 i **bekendtgørelse om notarialforretninger**⁷³:

⁷² Jf. note 67.

⁷³ Bekendtgørelse nr. 843 af 30. november 1998 om notarialforretninger.

”§ 17. Testamenter og tilkendegivelser om forældremyndighed efter § 15 i lov om forældremyndighed og samvær, der er oprettet for en dansk notar, registreres i Centralregistret for Testamenter.”

Krav om brug af et papirdokument eller lign. kan endvidere stilles for at sikre myndighederne mulighed for at kontrollere indtægtsmæssige forhold, opkræve skatter, afgifter mv.

Som eksempel kan nævnes **lov om private bidrag til politiske partier og offentliggørelse af politiske partiers regnskaber**⁷⁴:

*”§ 5. Partiets ledelse indsender senest 12 måneder efter regnskabsårets afslutning en **bekræftet kopi** af regnskabet til Folketinget, der fremlægger regnskabet til gennemsyn for offentligheden.”*

I **bogføringsloven**⁷⁵, som indeholder regler om bogføringspligt for alle erhvervsdrivende virksomheder, samt for visse andre virksomheder, organisationer og sammenslutninger mv., findes i § 10 regler om opbevaring af regnskabsmateriale, herunder af materiale, som foreligger på elektronisk medie, på mikrofilm eller lignende:

”§ 10. Den bogføringspligtige skal opbevare regnskabsmaterialet på betryggende vis i 5 år fra udgangen af det regnskabsår, materialet vedrører. Opbevaringen skal ske på en måde, som i hele opbevaringsperioden muliggør en selvstændig og entydig fremfindning af det pågældende regnskabsmateriale.

Stk. 2. Opbevares regnskabsmaterialet på elektronisk medie, mikrofilm eller anden lignende måde, skal det uden bearbejdning, beregninger eller tilpasninger kunne udskrives i klarskrift.

...”

Den citerede bestemmelse blev indført i 1998 med henblik på at tage højde for anvendelsen af ny teknologi i bogføringen. I bemærkningerne til lovforslaget⁷⁶ anføres herom:

⁷⁴ Lov nr. 404 af 13. juni 1990 om private bidrag til politiske partier og offentliggørelse af politiske partiers regnskaber.

⁷⁵ Lov nr. 1006 af 23. december 1998 om bogføring.

⁷⁶ Folketingstidende 1998-99, Tillæg A, s. 1741 ff.

” Regnskabsmaterialet skal fortsat opbevares betryggende i 5 år, uanset det opbevares elektronisk, på mikrofilm, på papir eller på andre medier. Forslaget opstiller derfor kvalitetskrav til opbevaringen. Den bogføringspligtige må således selv om, på hvilket medium materialet opbevares, hvis blot kvalitetskravene overholdes.

...

Opbevares regnskabsmaterialet elektronisk – f.eks. ved at det scannes elektronisk – skal dette uden bearbejdning kunne udskrives i klarskrift i hele opbevaringsperioden. ... Såfremt der kræves en tidligere programversion for at kunne udskrive elektronisk lagret regnskabsmateriale i klarskrift, skal en sådan programversion også gemmes.”

Bevissspørgsmål opstår således også i forbindelse med opbevaring af digitale dokumenter, og der bliver – som det fremgår af de citerede bemærkninger til bogføringslovens § 10 – endvidere tale om nye problemstillinger. Ud over de nævnte spørgsmål om læsbarhed mv. giver det bl.a. anledning til særlige bevismæssige problemer, at en elektronisk signatur som nævnt ovenfor i kapitel 2.3. bliver mindre sikker, efterhånden som tiden går.

5.3.4. Formkrav, som har til formål at indskærpe alvor/højtidelighed

Nogle formkrav har til formål at give en bestemt handling et præg af alvor og højtidelighed, f.eks. ved et krav om underskrift på en særlig formular. Sådanne krav kan, ligesom de ovennævnte forbrugerbeskyttende bestemmelser og erklæringer på tro og love, tillige have til formål at advare om, at man nu påtager sig en forpligtelse, som i tilfælde af manglende overholdelse kan have indgribende konsekvenser. Som eksempel kan nævnes **§ 8 i rigsretsloven**⁷⁷:

*”§ 8. Hver af rigsrettens dommere afgiver **skriftlig** en højtidelig forsikring på ære og samvittighed om opmærksomt at ville følge forhandlingerne i retten og dømme således, som han finder ret og sandt at være efter loven og sagens bevisligheder.”*

⁷⁷ Lovbekendtgørelse nr. 641 af 17. september 1986 af lov om rigsretten.

Tilsvarende bestemmelser findes i andre regler om behandling af retssager, sagsbehandling i råd og nævn mv., jf. f.eks. retsplejelovens § 91⁷⁸. Om de tidligere nævnte bestemmelser, som har til formål at sikre bevis for, at et dokument er set eller godkendt af en bestemt person, se ovenfor i kapitel 5.3.3.3.

Hvis de tekniske forudsætninger er opfyldt, fordi erklæringen kan afgives i digital form, og den pågældende er i besiddelse af en elektronisk signatur, er der for så vidt ikke noget til hinder for at benytte denne metode. Det kan dog overvejes, om den særlige højtidelighed, som er tilsigtet med bl.a. de citerede bestemmelser, vil kunne opnås ved brug af elektronisk signatur. For nogle mennesker vil det måske virke mindre forpligtende at afgive en sådan erklæring i elektronisk form end ved underskrift på et papirdokument.

5.3.5. Administrativt begrundede formkrav

En meget betydelig del af de formkrav, som udvalget har gennemgået, er udfærdiget med det formål at lette det administrative arbejde for myndigheder mv. Formkravet kan f.eks. være indført for at afskære mundtlige ansøgninger og anmeldelser. Der findes således mange krav om, at en anmeldelse skal indleveres skriftligt.

Som eksempel kan nævnes **§ 7 i lov om personnavne**⁷⁹:

”§ 7. Forbeholdte navne er:

- 1) navne, der er forbeholdt efter § 7 i lov nr. 140 af 17. maj 1961 om personnavne, og*
- 2) efternavne, der tillades ved navnebevis.*

*Stk. 2. Ved **skriftlig** anmeldelse til justitsministeriet kan endvidere forbeholdes:*

- 1) efternavne, der bæres af personer med bopæl her i landet,*
- 2) navne, der udgør eller indgår i et firma, varemærke eller foreningsnavn, der*
- 3) er indregistreret her i landet, og*

⁷⁸ Jf. note 27.

⁷⁹ Lov nr. 193 af 29. april 1981 om personnavne.

4) kunstnernavne og pseudonymer, der er almindeligt kendt her i landet og anvendes af en person med bopæl her i landet.”

Formkrav om skriftlighed, brug af særlige blanketter og lignende kan således være begrundet i et ønske om at lette den videre behandling af de oplysninger, som dokumentet indeholder.

Som eksempel kan endvidere på ny nævnes **tinglysningslovens § 9, stk. 1**⁸⁰:

”§ 9. Som grundlag for tinglysning kræves et dokument, der anmeldes for vedkommende dommer til tinglysning. Samtidig med dokumentet indleveres genpart af samme. Ved aflysning leveres genpart af kvitteringen samt af dertil hørende bevisligheder”.

At der i tinglysningslovens § 9 kræves et **dokument**, betyder, at der skal foreligge en skriftlig erklæring. Tinglysningskontoret opbevarer i de fleste tilfælde en genpart af dokumentet, som skal være udfærdiget på særligt genpartsgenpapir. For nogle tinglysningsdokumenter er der - for at lette overblikket og dermed sagsbehandlingen på tinglysningskontoret - stillet krav om, at der skal anvendes særlige blanketter. Det kræves endvidere, at dokumentet skal være **underskrevet** af udstederen, jf. ovenfor.

Der findes talrige eksempler på tilsvarende bestemmelser på alle de undersøgte ministerområder.

På området for offentlige myndigheders kommunikation med borgere og virksomheder gælder der særlige regler i offentligheds- og forvaltningsloven. Justitsministeriet har i en besvarelse af et spørgsmål fra medlem af Folketinget Kristian Jensen (V)⁸¹ udtalt følgende herom:

⁸⁰ Jf. note 31.

⁸¹ Besvarelse af 8. februar 2000 af spørgsmål nr. S 1277.

” For så vidt angår kommunikation mellem borgere og den offentlige forvaltning kan det oplyses, at i det omfang, der er særlige regler om, at eksempelvis en klage til en offentlig myndighed skal indgives skriftligt, må det i princippet bero på fortolkning af lovgivningen på det enkelte område, om kravet om skriftlighed kan anses for opfyldt ved anvendelse af elektronisk post.

Når der ikke er særlige regler om fremgangsmåden ved indgivelse af klage mv., må det efter Justitsministeriets opfattelse antages, at borgeren selv kan vælge, i hvilken form klagen skal indgives. Det betyder, at borgeren frit kan vælge, om klagen skal indgives ved personlig eller telefonisk henvendelse, ved fremsendelse af brev i papirform eller ved fremsendelse af elektronisk post.

Med hensyn til spørgsmålet om formen for myndigheders meddelelse af afgørelser kan det oplyses, at der i dansk forvaltningsret ikke findes en almindelig regel om, at offentlige myndigheders afgørelser skal være skriftlige. I mange tilfælde er skriftlighed dog foreskrevet eller forudsat i lovgivningen, og god forvaltningsskik tilsiger i en række tilfælde, at afgørelserne skal meddeles i skriftlig form. Der kan i den forbindelse henvises til John Vogter: Forvaltningsloven med kommentarer (3. udg. 1999) s. 417, hvor det i tilknytning til en udtalelse fra Folketingets Ombudsmand om brug af telefax bl.a. er anført:

”Udtalelsen er særlig interessant i lyset af den tekniske udvikling, som i højere grad fører i retning af elektronisk brevveksling.

Udtalelsen må formentlig forstås således, at Folketingets Ombudsmand i hvert fald over for private borgere vil opretholde et krav om, at afgørelser meddeles i papirform, selv om den pågældende måtte være i stand til at modtage afgørelsen ad elektronisk vej.”

Den nævnte ombudsmandsudtalelse er refereret i Folketingets Ombudsmands beretning for året 1990, s. 387-388.

Der kan endvidere henvises til Forskningsministeriets vejledning om elektronisk dokumenthåndtering og forvaltningsregler (juni 1996), s. 13-18, hvor det bl.a. er anført (s. 13):

”Der er forholdsvis få formkrav i dansk forvaltningsret, som direkte hindrer brug af elektronisk kommunikation mellem myndigheder og private. Det er dog ikke ensbetydende med, at myndighederne uden videre kan bruge elektronisk kommunikation, når der er tale om kommunikation, som skaber rettigheder og pligter, eller anden form for formel kommunikation. I sådanne situationer vil brug af elektronisk kommunikation ofte forudsætte en udtrykkelig eller stiltiende aftale herom mellem myndigheden og den private part.”

Formkrav, der drejer sig om borgeres og virksomheders indberetning mv. af oplysninger til det offentlige, er som nævnt talrige, og da området endvidere er velegnet til at anvende digital kommunikation, fordi der ofte er tale om indsendelse af en stor mængde ensartede meddelelser til én eller få modtagere, er der på nogle områder allerede taget skridt til at indføre digital kommunikation. Det gælder bl.a. ved indberetning af visse forhold vedrørende selskaber mv. til Erhvervs- og Selskabsstyrelsen.

I forlængelse af finanslovsaftalen for 1999 er der endvidere taget skridt til at iværksætte en IT-handlingsplan med henblik på at tilvejebringe administrative lettelser for virksomhederne gennem anvendelse af digital kommunikation ved indberetninger og indbetalinger til offentlige myndigheder. Økonomistyrelsen har i den forbindelse lavet en undersøgelse af de offentlige myndigheders rationaliseringsgevinster herved.⁸² I undersøgelsen konkluderes det ud fra en stikprøvemæssig gennemgang af 26 blanketter fra forskellige ministerområder, at der er et betydeligt besparelspotentiale ved overgang til elektroniske indberetninger.

⁸² Undersøgelse af rationaliseringspotentialet i forbindelse med implementering af IT-handlingsplanen, Økonomistyrelsen den 8. november 1999.

Kapitel 6. Behovet for et lovgivningsinitiativ og udformningen heraf

6.1. *Er der behov for et lovgivningsinitiativ?*

Spørgsmålet om, hvorvidt der er behov for at lovgive om anvendelsen af digital kommunikation og elektronisk signatur i forbindelse med formkrav i lovgivningen, og hvordan et lovgivningsinitiativ i givet fald bør udformes, må ses i sammenhæng med, at der er en betydelig samfundsmæssig interesse i at fremme anvendelsen af informationsteknologi (IT).

Bl.a. i ”Det digitale Danmark – omstilling til netværkssamfundet” fra december 1999 og i ”.dk21 - En ny strategi for Danmarks erhvervspolitik” er der peget på behovet for en hurtig tilpasning af det danske samfund til de nye teknologiske muligheder.

Der peges på, at anvendelse af digital kommunikation i den offentlige sektor vil kunne indebære store fordele både for det offentlige, borgere og virksomheder, bl.a. i form af nye servicetilbud og enklere administration, med deraf følgende effektiviseringer og besparelser i både den offentlige og den private sektor. Hertil kommer, at elektronisk handel via Internettet m.v. i øjeblikket er ved at vinde udbredelse. Denne form for handel foregår i vidt omfang på tværs af grænser, og derfor er det nærliggende at antage, at de lande, som formår at udnytte de muligheder, som ”den ny økonomi” giver, vil kunne opleve en betydelig økonomisk vækst i de kommende år.

Senest har drøftelserne i Folketinget i februar 2000 vedrørende regeringens IT- og Telepolitiske redegørelse – omstilling til netværkssamfundet, jf. nærmere herom ovenfor i kapitel 4.4.3., vist bred opbakning til, at brugen af digital kommunikation skal fremmes mest muligt.

Der anvendes for tiden mange ressourcer på at bringe de praktiske og tekniske forudsætninger for at realisere målsætningen om at fremme brugen af digital kommunikation på plads. Således er der som opfølgning på de nævnte handlingsplaner iværksat en række projekter, bl.a. vedrørende kommunikation fra borgere og virksomheder til stat og kommuner, jf. den nærmere beskrivelse heraf ovenfor i kapitel 4.4. På andre områder, f.eks. ved kommunikation mellem pengeinstitutter og deres kunder, går udviklingen også hurtigt i retning af, at stadig flere anvender digital kommunikation.

Efter udvalgets opfattelse er der således mange gode grunde til mest muligt at fremme et initiativ, som i fornødent omfang tilpasser også lovgivningen inden for de mange forskellige livsområder til udviklingen inden for elektronisk handel og digital forvaltning mv.

I langt de fleste tilfælde er det andre forhold end indholdet af retsreglerne på det pågældende område, som afgør, om man vælger at benytte de digitale teknikker. Lovgivningens rolle i den ovenfor skitserede udvikling er således navnlig at understøtte, at informationsteknologien anvendes på en hensigtsmæssig måde. Hvor der måtte være et særligt behov for at foreskrive, at de traditionelle kommunikationsformer skal anvendes, bør lovgivningen naturligvis sætte grænser for anvendelsen af den moderne teknologi. Men hvor sådanne særlige forhold ikke foreligger, er det vigtigt, at lovgivningen ikke sætter grænser for den udvidede anvendelse af informationsteknologien, som af samfundsmæssige årsager er ønskelig. Lovgivningen skal altså kun sætte grænser for anvendelsen af informationsteknologi, hvor det er nødvendigt.

Udvalget har derfor undersøgt, om den nugældende lovgivning er i overensstemmelse hermed, eller om lovgivningen i stedet sætter unødige grænser for IT-anvendelsen. Hvis formkrav m.v. i lovgivningen udgør en unødvendig hindring for den udvikling, som samfundsmæssigt er ønskelig, er der behov for at fjerne sådanne formkrav gennem lovgivningsinitiativer.

Inden for de seneste år er der – som det bl.a. fremgår af gennemgangen ovenfor – på en række retsområder foretaget ændringer af lovgivningen med henblik på at gøre det muligt at anvende digital kommunikation. Eksempelvis blev selskabslovgivningen ændret i 1996 med henblik på at gøre det muligt at anmelde selskabsdokumenter til Erhvervs- og Selskabsstyrelsen i digital form, og i 1997 blev patentloven og en række andre love på immaterialretsområdet ændret for at gøre det muligt at indsende digitale patentansøgninger m.v. til myndighederne. En række væsentlige bestemmelser om bl.a. bogføring og arkivalier er også blevet tilpasset brugen af digitale medier.

På nogle områder er lovgivningen således allerede udtrykkeligt indrettet på brug af digital kommunikation. Udvalgets undersøgelser af lovgivningen på nogle udvalgte ministerområder har imidlertid vist, at der fortsat findes et betydeligt antal formkrav i lovgivningen - helt skønsmæssigt kan der meget vel være tale om nogle tusinde regler i love, bekendtgørelser og cirkulærer – som har et indhold, der giver anledning til at overveje, om digital kommunikation kan anvendes på det pågældende område.

Spørgsmålet er herefter, om de formkrav i lovgivningen, som ikke er blevet ændret, udgør en unødigt hindring for den udvikling, som er i gang. Det må således undersøges, om der på områder, hvor det er relevant og hensigtsmæssigt at anvende digital kommunikation, findes formkrav m.v., som må forstås således, at de er til hinder for eller begrænser mulighederne for at bruge digital kommunikation, og om de er nødvendige.

6.2. *Hvordan skal formkrav forstås?*

6.2.1. Almindelige bemærkninger

Udvalget har ovenfor i kapitel 5 gennemgået en række forskellige formkrav og søgt at kategorisere disse bl.a. på grundlag af det formål, som formkravet må antages at have, og ud-

valget har overvejet, om det på denne baggrund er muligt at udarbejde et ”katalog” over forskellige typer af formkrav med henblik på at fastlægge en bestemt forståelse af de forskellige formuleringer. Efter udvalgets opfattelse er det imidlertid ikke muligt i en sådan katalogform at fastsætte en ensartet betydning af bestemte ord eller udtryk, der bruges på flere forskellige lovgivningsområder. Selv om man har anvendt det samme ord i forskellige retsregler, er det f.eks. langt fra sikkert, at ordet har den samme betydning. At et krav om skriftlighed på ét retsområde kan eller ikke kan opfyldes ved brug af digital kommunikation, betyder således ikke nødvendigvis, at det samme også gælder et skriftlighedskrav på et andet område, jf. herom nedenfor.

Som det fremgår af gennemgangen ovenfor i kapitel 5, kan formkrav endvidere være udformet på mange forskellige måder. Et formkrav kan være formuleret ved brug af ord som ”skriftlig”, ”underskrift” eller ”blanket”, men der anvendes ofte også andre begreber eller udtryk. I nogle tilfælde fremgår et formkrav endvidere ikke af bestemmelsens ordlyd, men f.eks. af den praksis, der har udviklet sig ved administrationen af retsreglen.

Formkravene kan derfor ikke systematiseres i et begrænset antal kategorier efter de anvendte ord, og selv om man ser bort fra ordlyden af bestemmelsen og i stedet kategoriserer bestemmelserne efter det formål, som formkravet varetager, er det ikke sikkert, at alle formkrav, som på forskellige områder varetager et bestemt formål, også skal forstås på samme måde på de forskellige områder for så vidt angår muligheden for at opfylde kravet ved brug af digital kommunikation.

Også erfaringerne fra det norske ”Kartleggingsprosjekt” har vist, at det ikke lader sig gøre at opstille sådanne faste fortolkningsregler. I Norge samlede man på baggrund af en systematisk gennemgang af lovgivningen de forskellige typer af formkrav i nogle overordnede kategorier (krav om skriftlighed, krav om underskrift, krav om brug af et dokument, en original, en kopi osv.) for derefter at søge at opstille generelle retningslinier om forståelsen af de an-

vendte ord, jf. herom ovenfor i kapitel 3.4.2. Konklusjonen på den norske undersøgelse blev imidlertid at:

”Det er vanskelig å trekke noen generelle konklusjoner ut fra de begrepene som er blitt drøftet ... Etter gjennomgangen har det kommet fram at det er mange forskjellige begrunnelser for eksisterende formkrav og prosedure og at det er mange hensyn som man kan ønske å ivareta selv om ikke alle er relevante ved hvert tilfelle. På bakgrunn av dette kan ikke alle begrepene tolkes på samme måte i alle bestemmelser.”⁸³

I stedet for at forsøge at fastlægge en bestemt forståelse af de mange forskellige begreber, som anvendes i bestemmelser med formkrav, har udvalget derfor undersøgt nogle særligt hyppigt forekommende typer af formkrav (skriftlighedskrav og krav om underskrift), som kan tjene til illustration af de spørgsmål, som opstår i forbindelse med fortolkning af bestemmelser med formkrav.

6.2.2. Skriftlighedskrav

Krav om skriftlighed er blandt de hyppigst forekommende formkrav. En søgning i Retsinformation viser, at ord, som begynder med ”skriftlig” (dvs. også ord som skriftligt, skriftlighed osv.) indgår i næsten 4.000 gældende dokumenter (love, bekendtgørelser mv.). Skriftlighedskrav har da også tiltrukket sig særlig opmærksomhed i den hidtidige diskussion om behovet for at ændre lovgivningen. Som nævnt ovenfor i kapitel 4.2. har det tidligere været overvejet at indføre en generel fortolkningsregel om forståelsen af skriftlighedskrav.

Som nævnt ovenfor i kapitel 3.3.1. indeholder UNCITRAL’s ”Model law on electronic commerce” i artikel 6 en bestemmelse om forståelsen af krav om skriftlighed:

⁸³ Kartleggingsprosjektet – Kartlegging av bestemmelser i lover, forskrifter og instrukser som kan hindre elektronisk kommunikasjon, Nærings- og Handelsdepartementet, juni 2000, side 9.

“Article 6. Writing.

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].”

Bestemmelsen hviler – ligesom de øvrige bestemmelser i modelloven – på den grundtanke, at der ved vurderingen af, om et formkrav kan opfyldes ved digital kommunikation, skal tages udgangspunkt i de funktioner, som formkravet varetager. I bestemmelsen har man fokuseret på skriftlighedskravets betydning for informationens tilgængelighed. Formkrav i lovgivningen mv. om skriftlighed skal således efter modelloven som hovedregel forstås sådan, at de kan opfyldes ved brug af digitale dokumenter, blot informationen i de digitale dokumenter er tilgængelige for senere læsning.

Om fortolkningen af bestemmelser, som indeholder krav om, at information skal være skriftlig, kan det generelt anføres at disse efter ordlyden blot betyder, at der skal benyttes skrifttegn, men ikke nødvendigvis at dette skal ske ved brug af et papirdokument, og at krav om skriftlighed formentlig i mange tilfælde alene har til formål at udelukke mundtlige erklæringer og at sikre mulighed for efterfølgende at dokumentere informationsindholdet. Der kan i den forbindelse henvises til de i kapitel 5.3.2. nævnte overvejelser om forståelsen af et skriftlighedskrav i fjernsalgsdirektivet.

Hvor krav om skriftlighed eller lignende er givet for at udelukke mundtlig kommunikation, vil der efter udvalgets opfattelse som udgangspunkt ikke være noget til hinder for at forstå kravet således, at det kan opfyldes ved brug af digitale dokumenter. Krav om skriftlighed kan imidlertid have mange andre formål end at udelukke mundtlig kommunikation og at sikre, at information bliver lagret for at give mulighed for senere opslag. Blandt de formål, som er nævnt ovenfor i kapitel 5.3., er det navnlig beskyttelses- og advarselsfunktioner i bl.a. forbrugerforhold samt administrative funktioner, som bliver relevante i relation

til skriftlighedskrav. Det er ikke sikkert, at disse funktioner altid kan varetages lige så godt ved brug af digitale dokumenter, som hvis der anvendes papir.

I praksis er man ved fortolkningen af bestemmelser om skriftlighed i nogle tilfælde nået frem til, at disse ikke omfatter digitale dokumenter. Som nævnt ovenfor kom Østre Landsret i 1995 i den såkaldte Proms-sag frem til, at straffelovens § 163, som med den daværende ordlyd drejede sig om skriftlige erklæringer, ikke omfattede erklæringer, som var afgivet ved brug af datateknik. Endvidere kan der henvises til Pressenævnets afgørelse fra februar 2000 (refereret ovenfor i kapitel 5.2.4.), hvor nævnet under henvisning til affattelsen af medieansvarslovens § 36 kom frem til, at en anmodning om genmæle ikke kunne indgives ved e-mail. Nævnet har i en uddybende begrundelse for afgørelsen oplyst, at baggrunden for nævnets standpunkt er, at man ikke hidtil har ment, at der er tilvejebragt den fornødne bevismæssige sikkerhed omkring modtagelse af e-mail. Som nævnt oven for i kapitel 5.2.4. har Pressenævnet imidlertid senere meddelt, at man mere generelt vil drøfte spørgsmålet, om elektroniske overførte meddelelser i visse sammenhænge vil kunne sidestilles med almindelige skriftlige henvendelser.

6.2.3. Underskriftskrav

Krav om, at et dokument skal være forsynet med underskrift eller lignende, er også hyppigt forekommende. Retsinformation indeholder over 1.000 gældende dokumenter med sådanne krav.

Om forståelsen af bestemmelser med underskriftskrav gælder generelt, at krav om at et dokument skal være forsynet med underskrift, hidtil alene har kunnet opfyldes ved brug af de traditionelle metoder, og der har derfor ikke været grund til at overveje, om kravet også omfattede digitale teknikker. Forarbejderne til bestemmelserne er derfor af gode

grunde tavse på dette punkt, men kan eventuelt indeholde fortolkningsbidrag om formkravets baggrund og formål.

Det er efter udvalgets opfattelse også ved fortolkningen af underskriftskrav naturligt at tage udgangspunkt i de formål, som kravet varetager. Der kan således argumenteres for, at krav om underskrift eller lignende bør forstås således, at de kan opfyldes ved brug af elektronisk signatur, blot denne i tilstrækkelig grad kan varetage de pågældende formål, jf. herved artikel 7 i UNCITRAL's Model law on electronic commerce, hvorefter krav i lovgivningen om personlig underskrift i relation til digital kommunikation kan opfyldes ved, at der anvendes en passende pålidelig metode til identifikation af underskriveren og til angivelse af denne persons godkendelse af meddelelsens indhold.

Der kan imidlertid ligge mange forskellige grunde bag krav om underskrift. Underskriftskravet vil kunne have til formål at give sikkerhed for, at dokumentet stammer fra den angivne udsteder. En underskrift kan også have til formål at virke som en afslutningsfunktion, f.eks. hvor et dokument ved parternes underskrift går fra at være et kontraktsudkast til at blive en endelig aftale. Der knytter sig ofte et element af højtidelighed til afgivelsen af en underskrift, og formkravet kan derfor også have en "varslingsfunktion", fordi underskriften gør en part opmærksom på, at parten nu påtager sig forpligtelser. Et krav om underskrift giver en part bedre tid til at overveje sin handling, end hvis det talte ord er tilstrækkeligt. Underskriftskrav kan også varetage mange andre funktioner, og de her nævnte hensyn tilsigter således på ingen måde at være udtømmende. Der kan generelt henvises til gennemgangen ovenfor i kapitel 5.

I det omfang elektronisk signatur opfylder de hensyn, som ligger bag et formkrav om underskrift, taler dette efter udvalgets opfattelse som udgangspunkt for at forstå bestemmelsen således, at den kan opfyldes ved brug heraf. Det er dog i den forbindelse væsentligt at være opmærksom på, at der i forbindelse med anvendelse af elektronisk signatur opstår nogle særlige spørgsmål vedrørende sikkerhedsniveauer, holdbarhed mv., som der af go-

de grunde ikke er taget stilling til i de bestemmelser, som i dag indeholder krav om underskrift mv., og som der i nogle tilfælde vil være behov for at overveje nøje, inden man accepterer brugen af elektronisk signatur på et retsområde.

Med loven om elektronisk signatur og navnlig dennes § 13 (der er beskrevet nærmere i kapitel 4.3.7.), som indebærer, at avancerede elektroniske signaturer altid skal opfylde visse lovmæssige krav, er der taget højde for visse af disse spørgsmål. Det må forventes, at de tekniske og sikkerhedsmæssige standarder, som loven opstiller, i mange tilfælde vil give de nødvendige rammer for at anvende elektronisk signatur på et retsområde og således vil kunne åbne mulighed for en udvidende fortolkning af underskriftskrav.

Til illustration af tankegangen kan nævnes bestemmelsen i § 2, stk. 2, i lov om translatører og tolke, hvorefter den kommende translatør og tolk, forinden beskikkelsen udtaltes, skal underskrive en ”højtidelig forsikring” (bestemmelsen er omtalt i kapitel 5.2.1). Hvis (avancerede) elektroniske signaturer i praksis giver den fornødne sikkerhed for, at det digitale dokument er underskrevet af den kommende translatør og tolk og således opfylder samme formål i relation til identitetssikring som en traditionel underskrift på den afgivne erklæring, kan det anføres, at der ikke i denne henseende er nogen grund til at fortolke underskriftskravet således, at det ikke kan opfyldes ved brug heraf. Om erklæringens højtidelige karakter bevares i tilstrækkelig grad, hvis den afgives i digital form og forsynet med elektronisk signatur, er derimod umiddelbart tvivlsomt, og spørgsmålet om at erstatte den håndgjorte underskrift med elektronisk signatur måtte derfor i givet fald overvejes nærmere, før man – ved fortolkning eller ved en lovændring – tillod brug af digital kommunikation på dette område.

6.2.4. Udvalgets overvejelser om forståelsen af formkrav i lovgivningen

Som det fremgår af det anførte, er det vanskeligt at udtale sig generelt om forståelsen af formkrav om skriftlighed, underskrift mv. I nogle tilfælde er der ikke tvivl om, hvordan

et formkrav i lovgivningen skal forstås. Af en del bestemmelser fremgår det klart, at det er muligt at opfylde formkravet ved brug af digital kommunikation. Der findes på den anden side også regler, der har et indhold, som gør det klart, at dette ikke er muligt, og hvor der derfor i givet fald vil være behov for en lovændring.

Udvalgets undersøgelser har vist, at lovens tekst kun sjældent giver et klart svar på, om et formkrav kan opfyldes ved brug af digital kommunikation. Spørgsmålet er, om sådanne "uklare" lovbestemmelser med krav om f.eks. skriftlighed eller underskrift udgør en hindring for digital kommunikation, eller om de må forstås og fortolkes således, at formkravene heri også kan opfyldes ved brug af digitale medier.

Lovens motiver er sjældent til nogen hjælp til at løse dette fortolkningsspørgsmål. Mange retsregler, som indeholder formkrav, stammer fra en tid, hvor der ikke var grund til at overveje spørgsmålet om brug af digital kommunikation, og derfor er der af gode grunde hverken i bestemmelserne eller eventuelle forarbejder hertil taget stilling til denne mulighed. Men også i nyere retsregler anvendes ord som "skriftlig" og lignende i en del tilfælde, uden at det fremgår af lovens forarbejder, om hensigten med anvendelsen af udtrykket har været at udelukke brugen af digital kommunikation. I en del tilfælde har man formentlig – måske fordi man blot har genbrugt en formulering, som tidligere har været anvendt i anden lovgivning – slet ikke været opmærksom på behovet for at tage stilling til, om man på det pågældende retsområde skal kunne anvende andet end papirdokumenter, håndskrevne underskrifter o.s.v.

Ofte vil det følge af praktiske forhold, at brugen af digital kommunikation er udelukket, selv om selve retsreglen for så vidt ikke er til hinder herfor. Som eksempel kan nævnes reglen i § 3, stk. 11, i bekendtgørelse om betryggelse ved erhvervsdykkerarbejde og om erhvervsdykkerarbejdes sikre udførelse, som er beskrevet ovenfor i kapitel 5.2.1. Selv om man efter fortolkning af denne bestemmelse måtte nå frem til, at kravet om underskrift på dykkerjournalen også vil kunne opfyldes ved brug af elektronisk signatur, vil kravet om,

at udskrevne dykkerjournaler skal opbevares af dykkeren i 5 år efter sidste indførelse i journalen, imidlertid forhindre en umiddelbar anvendelse af digital kommunikation. I givet fald måtte indførelse af digital kommunikation forudsætte, at der var taget stilling til en række praktiske spørgsmål om bl.a. opbevaring af “digitale dykkerjournaler”. For at det i praksis bliver muligt at anvende digital kommunikation vil det således – uanset om lovgivningen i sig selv er til hinder derfor – ofte være nødvendigt at fastsætte nærmere regler om, hvilke tekniske formater mv. der skal anvendes, ligesom der navnlig på området for kommunikation med det offentlige vil skulle indføres IT-systemer til håndtering af digital kommunikation på de områder, hvor dette ikke i dag er muligt.

Hvor der ikke er praktiske hindringer for anvendelsen af digital kommunikation, og hvor det ikke klart fremgår af den pågældende retsregel, om denne form for kommunikation kan anvendes, er der efter udvalgets opfattelse generelt grund til at antage, at en lang række af de formkrav, som måske umiddelbart kunne se ud til at udgøre hindringer for anvendelsen af digital kommunikation, ved nærmere fortolkning vil vise sig ikke at være til hinder herfor. Forståelsen af lovgivningen ændrer sig i takt med samfundsudviklingen, og efterhånden som de tekniske forudsætninger tilvejebringes i form af en infrastruktur for afgivelse og kontrol af elektronisk signatur, og efterhånden som digital kommunikation bliver mere og mere udbredt, bliver en sådan fortolkning mere nærliggende.

Udvalget kan generelt tilslutte sig grundtanken bag UNCITRAL’s modellov om electronic commerce, hvorefter forståelsen af et formkrav må fastlægges med udgangspunkt i det eller de formål, som bestemmelsen varetager. Kan formålet varetages på tilstrækkelig vis ved brug af digital kommunikation (princippet om “funktionel ækvivalens”), bør formkravet som udgangspunkt også kunne opfyldes på denne måde.

Formålsfortolkning kan imidlertid kun tjene som rettesnor ved overvejelser om behovet for at ændre lovgivningen, men skaber ikke nødvendigvis i sig selv nærmere klarhed om forståelsen af de enkelte bestemmelser med formkrav. Denne vil afhænge af en konkret

vurdering, hvori en lang række både retlige og praktiske forhold må indgå. Som nævnt ovenfor er udvalget på baggrund af sine undersøgelser af lovgivningen af den opfattelse, at det ikke er muligt at opstille faste fortolkningsregler for forskellige typer af formkrav efter disses formål. Der kan ikke gives et generelt svar på, hvordan de mange bestemmelser med formkrav skal forstås, og på den måde skabes klarhed om, hvornår digital kommunikation kan anvendes.

I en del tilfælde vil der være en sådan tvivl om forståelsen af en retsregel, at denne tvivl i sig selv i praksis vil være til hinder for anvendelse af digital kommunikation. Selv om udvalget som anført er af den opfattelse, at mange formkrav – bl.a. i betragtning af de funktioner, som kravet varetager – kan fortolkes således, at de ikke hindrer anvendelsen af digital kommunikation, er dette endvidere ikke nødvendigvis ensbetydende med, at der ikke kan være behov for gennem regelændringer at præcisere indholdet af bestemmelserne. I nogle tilfælde, hvor det ikke på forhånd er givet, hvilket resultat man vil nå til ved fortolkning, kan det således være hensigtsmæssigt at afklare spørgsmålet gennem en lovændring. For virksomheder og borgere, som skal indrette sig efter retsreglerne, er det af stor betydning, at der skabes klarhed om reglernes indhold. Der kan således være behov for at afklare ikke blot, at et formkrav kan opfyldes ved digital kommunikation, men også at afklare på hvilke områder digital kommunikation ikke skal kunne benyttes.

Nogle formkrav er endvidere formuleret på en sådan måde, at problemet ikke kan løses ved fortolkning, idet bestemmelsens ordlyd direkte er til hinder for brug af digital kommunikation. For at løse spørgsmålet ved fortolkning, må der være uklarhed om bestemmelsens indhold. Er der ingen uklarhed, således at man ville gå ud over ”ordgrænsen” ved at lade bestemmelsen give mulighed for digital kommunikation, må problemet i stedet løses ved lovændring.

Hertil kommer, at anvendelse af digital kommunikation også på områder, hvor lovgivningen efter en nutidig forståelse for så vidt ikke er til hinder herfor, vil kunne kræve lovgiv-

ning. Ofte vil det således være nødvendigt at tage stilling til en række praktiske og tekniske forhold i den forbindelse og eventuelt udarbejde nærmere forskrifter (bekendtgørelser mv.) herom.

For at sikre, at lovgivningen ikke udgør en unødvendig hindring for en hensigtsmæssig brug af digital kommunikation, er det derfor efter udvalgets opfattelse nødvendigt systematisk at gennemgå lovgivningen for at finde frem til de bestemmelser, som ikke understøtter den ønskede udvikling. Først herefter vil der kunne tages stilling til, om de pågældende bestemmelser skal ændres, eller om problemet bør løses på anden måde, f.eks. ved at den administrative myndighed på det pågældende område fortolker og anvender bestemmelsen således, at det er muligt at anvende digital kommunikation, eller ved udstedelse af administrative forskrifter i medfør af allerede eksisterende hjemmelsbestemmelser. Det er i den forbindelse vigtigt, at den pågældende myndighed giver oplysning om sin retsopfattelse og retsanvendelse til borgere og underordnede myndigheder gennem vejledninger, tjenestebefalinger o.lign.

En sådan gennemgang af lovgivningen og et lovgivningsinitiativ bliver i øvrigt under alle omstændigheder nødvendigt som følge af artikel 9 i direktivet om elektronisk handel⁸⁴, jf. herom ovenfor i kapitel 3.2.2., idet bestemmelsen indebærer en pligt for medlemsstaterne til at gennemgå deres lovgivning for at sikre, at denne tillader brugen af ”elektroniske kontrakter”:

Art. 9. Behandling af kontrakter

1. Medlemsstaterne sikrer, at deres retssystem gør det muligt at indgå kontrakter elektronisk. Medlemsstaterne sikrer bl.a., at de juridiske krav, der gælder for aftaleindgåelsen, hverken er til hinder for anvendelsen af elektroniske kontrakter eller fører til, at sådanne kontrakter på grund af den omstændighed, at de er indgået elektronisk, mister deres retlige virkning og gyldighed.

⁸⁴ Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked.

2. Medlemsstaterne kan bestemme, at stk. 1 ikke finder anvendelse på alle eller nogle af de kontrakter, der hører ind under følgende kategorier:

- a) kontrakter, der skaber eller overfører rettigheder i fast ejendom, bortset fra udlejningsrettigheder
- b) kontrakter, der ifølge loven kræver medvirken af domstole, offentlige myndigheder eller erhverv, som udøver offentlig myndighed
- c) kontrakter om kaution og om sikkerhedsstillelse fra personer, der handler uafhængigt af deres handelsmæssige eller erhvervsmæssige virksomhed
- d) familieretlige og arveretlige aftaler.

I direktivets præambel anføres om forståelsen af bestemmelsen:

“(34) hver medlemsstat skal tilpasse sin lovgivning om krav, især formkrav, som kan hindre elektronisk indgåelse af kontrakter; der bør foretages en systematisk gennemgang af de lovgivninger, hvor en sådan tilpasning er påkrævet, og gennemgangen skal omfatte alle de nødvendige etaper og led i aftaleindgåelsen, herunder opbevaring af kontrakten; tilpasningen bør resultere i, at det bliver muligt at indgå kontrakter elektronisk; ...

...

(37) medlemsstaternes forpligtelse til at fjerne hindringer for anvendelse af elektroniske kontrakter vedrører kun hindringer, som skyldes juridiske krav, og ikke praktiske hindringer, som skyldes, at det i visse tilfælde er umuligt at anvende elektroniske midler;”

For at gennemføre bestemmelsen i dansk ret vil der således skulle foretages en gennemgang af den gældende lovgivning for at finde frem til og ændre alle regler, der forhindrer digital (elektronisk) kontraktsindgåelse. Direktivet indeholder ikke en definition af, hvad der skal forstås ved en ”elektronisk kontrakt”, men bl.a. under hensyn til listen med undtagelser i direktivets artikel 9, stk. 2, må det antages, at begrebet skal forstås bredt. Direktivet skal være gennemført i dansk ret inden den 17. januar 2002.

6.3. Valget af lovgivningsmodel

6.3.1. Indledning

Udvalget finder således, at der er behov for et lovgivningsinitiativ for at skabe klarhed over, på hvilke retsområder og under hvilke betingelser man skal kunne anvende digital kommunikation og elektronisk signatur. Spørgsmålet bliver herefter, hvorledes et sådant initiativ bør tilrettelægges.

Spørgsmålet om, hvilken metode der vil være mest hensigtsmæssig til ”modernisering” af lovgivning med formkrav mv., har tidligere været genstand for drøftelse, både herhjemme og i udlandet. I regeringens redegørelse fra december 1997 om sikker digital kommunikation, jf. kapitel 4.1., blev der således opstillet en overordnet målsætning om at gennemføre en principiel ligestilling mellem digital og papirbaseret kommunikation. Med henblik herpå blev der fremlagt to modeller – frameldingsmodellen og tilmeldingsmodellen, jf. herom nedenfor – og det blev tilkendegivet, at der var behov for at gennemgå alle formkrav i lovgivningen for at afgøre, hvilke lovkrav om skriftlighed og underskrift der bør kunne opfyldes ved brug af digital kommunikation.

På baggrund heraf og efter at der under Folketingets debat om redegørelsen i januar 1998⁸⁵ havde været bred tilslutning til tanken om en ”modernisering” af lovgivningen, blev spørgsmålet om, hvorledes et lovgivningsinitiativ vedrørende formkrav burde udformes, behandlet nærmere i Forskningsministeriets udkast til lovforslag om digital signatur fra februar 1998, jf. herom ovenfor i kapitel 4.2.

I lovudkastet lagde man sig ikke fast på nogen bestemt løsning. Forslaget var udformet således, at de hørte organisationer mv. skulle tage stilling til tre forskellige modeller. Fælles for de tre modeller var, at de ved én retsregel ville ændre en lang række bestemmelser om

⁸⁵ Folketingstidende 1997-98 (1. samling), FF, s. 3573 ff.

formkrav i lovgivningen. Det fælles, grundlæggende princip i de tre modeller – det såkaldte ”ligestillingsprincip” – gik ud på, at hvor love, lovbestemmelser eller forskrifter udstedt i medfør heraf foreskriver eller forudsætter, at en meddelelse skal afgives i skriftlig eller underskrevet form, så skulle sådanne krav anses for opfyldt, når meddelelsen var afgivet som en digital meddelelse med autoriseret digital signatur, dvs. en signatur, som opfyldte visse i lovudkastet fastsatte sikkerhedskrav.

Efter *frameldingsmodellen* skulle ligestillingsprincippet gennemføres generelt, idet det skulle gælde alle formkrav, som ikke udtrykkeligt var undtaget fra ordningen.

Tilmeldingsmodellen havde det modsatte udgangspunkt. Efter denne model skulle ligestillingsprincippet alene omfatte de formkrav, som var optaget i en bekendtgørelse herom. Modellen indebar således en hjemmel til, at den pågældende minister ved bekendtgørelse kunne fastsætte, at bestemmelser i lovgivningen om afgivelse af skriftlig eller underskrevet meddelelse skulle anses for opfyldt ved afgivelse af en digital meddelelse med autoriseret digital signatur.

Endelig gik *kombinationsmodellen* ud på indførelsen af en frameldingsmodel med udskudt ikrafttræden, således at man indtil gennemførelsen af frameldingsmodellen skulle anvende en tilmeldingsmodel.

Alle tre modeller skulle efter udkastet kombineres med en tidsfrist på ca. 3 år, inden hvilken arbejdet med at tilmelde, henholdsvis afmelde, formkravene skulle være afsluttet. Der skulle i den forbindelse iværksættes en systematisk gennemgang af samtlige gældende retsregler med henblik på at afklare, hvilke formkrav om skriftlighed og underskrift der fandtes, således at man kunne finde alle formkrav, der udgjorde hindringer for en hensigtsmæssig anvendelse af digital kommunikation.

Forskningsministeriets lovudkast blev sendt i høring til en bred kreds af organisationer og myndigheder mv., og en række af høringsinstanserne udtalte sig om spørgsmålet om anvendelse af digital kommunikation på områder med lovbestemte formkrav.

En del af de hørte organisationer mv. anførte, at man støttede frameldingsmodellen, idet man med en regel der gik ud på, at formkrav som udgangspunkt kan opfyldes ved brug af digital kommunikation, hurtigt ville få udbredt anvendelsen heraf. Nogle fandt, at kombinationsmodellen var at foretrække, fordi den gav mulighed for, at man straks kunne tilmelde de særligt egnede bestemmelser med formkrav og samtidig havde frameldingsmodellens fordele.

Andre pegede på, at der i forbindelse med en ændring af de mange formkrav i lovgivningen ville opstå en række komplekse og til dels uafklarede problemstillinger, som der var behov for at tage stilling til, før et eventuelt lovforslag blev fremsat.

Det blev også fremhævet, at den lovgivningsteknik, der var lagt op til i lovudkastet, forekom uheldig, idet man ikke ville have mulighed for at overskue de foreslåede bestemmelsers indhold og konsekvenser. Modellerne indebar således, at der skulle gennemføres en generel regel, der på én gang ændrede al bestående lovgivning med formkrav uden først at undersøge virkningerne af denne generelle regel.

Bl.a. blev det fra domstolsside anført, at arbejdet med at gennemgå samtlige regler om formkrav måtte antages at være særdeles ressourcekrævende, og at en forceret gennemførelse ville indebære en risiko for kvaliteten, samt at et stort antal bekendtgørelser om tilmelding/framelding, som det endvidere hyppigt ville være nødvendigt at ændre, antageligt ville medføre, at brugerne ville få svært ved at overskue mulighederne for anvendelse af digital kommunikation.

Spørgsmålet om valg af lovgivningsmodel til modernisering af formkrav i lovgivningen har også været overvejet i andre europæiske lande. I Sverige har man som nævnt i kapitel 3.4.1. overvejet, om det er muligt at indføre en regel, som indebærer, at alle retsregler, der indeholder krav om underskrift, kan opfyldes ved brug af digital signatur. En sådan generel ligestilling blev imidlertid afvist som umulig under henvisning til bl.a. de forskellige formål, som ligger bag formkravene⁸⁶.

I Norge har man som beskrevet i kapitel 3.4.2. iværksat en systematisk gennemgang af lovgivningen med henblik på at tilvejebringe et samlet overblik over, hvilke bestemmelser der udgør hindringer for anvendelsen af digital kommunikation. Gennemgangen har vist, at der også i norsk ret findes flere tusinde sådanne bestemmelser. I juni 2000 har Nærings- og Handelsdepartementet udsendt en projektrapport⁸⁷, der gennemgår forskellige formkrav i lovgivningen, herunder om formkravene reelt er til hinder for digital kommunikation, og om der er grund til at opretholde en given hindring. I rapporten præsenteres tre forskellige muligheder for, hvordan et lovgivningsinitiativ kan indrettes. Den første mulighed er gennemførelsen af en central lov, som omfatter alle områder og som ligestiller digital kommunikation med papirbaseret kommunikation. Den anden model går ud på at ændre hver enkelt lovregel for sig. Endelig præsenteres en ”mellemløsning”, hvorefter forvaltningen bliver pålagt at tage stilling til, om det regelsæt, de forvalter, tillader digital kommunikation, og til i rimelig grad at indrette lovgivningen, så dette bliver tilfældet. Der skal være adgang til at klage, hvis forvaltningen ikke indretter lovgivningen på digital kommunikation. I rapporten konkluderes det ikke, hvilken af de tre modeller, der bør foretrækkes, men det anføres, at flere af arbejdsgruppens medlemmer kan tilslutte sig ”mellemløsningen”.

Endelig har man i Storbritannien netop vedtaget en ”Electronic Communications Bill”, som bl.a. indebærer, at der i lovgivningen gives en generel bemyndigelse til, at den på-

⁸⁶ Ds 1998:14 ”Digitale signaturer – en teknisk og juridisk oversikt” side 183 f.

⁸⁷ Jf. note 5.

gældende minister kan ændre formkrav i lovgivningen. Forslaget indebærer således, at lovbestemmelser om, at der f.eks. skal benyttes et dokument, skal afgives underskrift eller skal afgives erklæring under ed eller med vitterlighedsattestation, vil kunne ændres administrativt.

6.3.2. Kan formkravene ændres ved én eller flere generelle regler?

Som det fremgår af gennemgangen ovenfor i kapitel 6.3.1, kan en række forskellige modeller tænkes anvendt ved tilrettelæggelsen af et lovgivningsinitiativ, som skal føre til en gennemgribende ”modernisering” af formkrav i lovgivningen.

Ved vurderingen af, hvilken af de mulige modeller der bør vælges, er der efter udvalgets opfattelse navnlig to hensyn, som bør indgå i overvejelserne om udformningen af lovgivningsinitiativet.

For det første er der som nævnt ovenfor i kapitel 6.1.1. en betydelig samfundsmæssig interesse i at fremme brugen af digital kommunikation, hvilket taler for at tilrettelægge et lovgivningsinitiativ således, at justeringen af lovgivningen til elektronisk handel og digital forvaltning m.v. kan gennemføres så hurtigt som muligt.

Dernæst bør der efter udvalgets opfattelse ved valget af lovgivningsmodel lægges vægt på, at ændringen af formkrav mv. sker på en sådan måde, at lovgivningen får den fornødne kvalitet med hensyn til bl.a. klarhed og overskuelighed for borgere og virksomheder mv.

Udvalget har herefter for det første overvejet, om det er muligt at udforme en eller flere generelle lovregler, der ændrer formkrav mv. i hele lovgivningen eller større dele heraf. En sådan model har som nævnt ovenfor i kapitel 6.3.1. tidligere været lagt frem til drøftelse herhjemme og ville i givet fald navnlig have den fordel, at den lettede lovgivningsarbejdet, fordi det ikke så ikke blev nødvendigt at ændre hver bestemmelse for sig. Reglen

kunne f.eks. udformes således, at der blev opstillet en formodning for, at visse ord i lovgivningen som ”underskrift”, ”skriftlig”, ”dokument” skulle tillægges en bestemt betydning, som også omfattede elektronisk signatur og digital kommunikation, jf. ovenfor om ”framlægningsmodellen” og ”tilmeldingsmodellen”.

Udvalget kan imidlertid ikke anbefale en sådan model, navnlig fordi udvalgets stikprøvemæssige gennemgang af bestemmelser med formkrav i lovgivningen som tidligere nævnt har vist, at disse er udformet så forskelligt og tjener så forskellige formål, at det ikke vil være muligt at formulere én regel, som på hensigtsmæssig vis ændrer et større antal formkrav. Til illustration heraf kan der henvises til, at selv om ordet skriftligt både indgår i psykiatrilovens § 22, stk. 1, om skriftligt samtykke fra patienten til ethvert psykokirurgisk indgreb og i §§ 1-2 i bekendtgørelse om lægers anmeldelse af smitsomme sygdomme mv., hvorefter en læge skriftligt skal anmelde visse bestemte sygdomme til embedslægen, varetager kravet om skriftlighed i de to bestemmelser vidt forskellige hensyn. Man risikerer derfor, at en sådan ”generel” regel kun vil kunne anvendes i forbindelse med en mindre del af formkravene.

Et formkrav kan være formuleret ved brug af ord som de nævnte, men ofte anvendes andre begreber, og i nogle tilfælde fremgår formkravet ikke direkte af bestemmelsens ordlyd, men f.eks. af dens forarbejder. En regel, som baseres på brugen af bestemte ord i de retsregler, som den skal ændre, ville således kun ramme nogle af de bestemmelser, som ønskes ændret. Vælger man på den anden side at give en sådan generel regel et bredere anvendelsesområde, f.eks. ved at tilføje ”eller lignende”, vil dette føre til usikkerhed om, hvornår bestemmelsen vil finde anvendelse.

Det vil endvidere i mange tilfælde ikke være tilstrækkeligt at knytte en bestemt betydning til et eller flere ord i en bestemmelse, der indeholder et formkrav, for at gøre det muligt at anvende digital kommunikation på det pågældende område. Ofte vil en ændret forståelse af en bestemmelse, f.eks. således at et krav om underskrift også kan opfyldes ved brug af

elektronisk signatur, gøre det nødvendigt at foretage konsekvensændringer andre steder, enten i den pågældende retsregel eller andre steder i det pågældende regelsæt. I mange tilfælde vil det være nødvendigt at ændre administrative procedurer, fastsætte regler om dokumentformater, kommunikationsformer mv., før det i praksis kan lade sig gøre at acceptere digital kommunikation.

En generel regel, som ændrer betydningen af et eller flere ord i andre retsregler, uden at der samtidig foretages de nødvendige konsekvensrettelser mv., vil således kunne få uoverskuelige konsekvenser. Hertil kommer, at der – som det fremgår af redegørelsen ovenfor i kapitel 5 – ligger mange forskellige hensyn bag udformningen af de formkrav, som udvalget har gennemgået. I nogle tilfælde kan disse hensyn varetages fuldt ud lige så godt ved brug af digital kommunikation som ved brug af papir, men dette er ikke altid tilfældet. I visse situationer kan der således være behov for en nøje afvejning af f.eks. digitale dokumenters sikkerhedsniveau eller elektronisk signaturs holdbarhed i forhold til behovene på det pågældende retsområde, før man tager stilling til, om det går an at åbne op for anvendelsen heraf. En generel regel, som med ét slag ændrer alle eller et større antal formkrav i lovgivningen, som indeholder bestemte formuleringer ("skriftligt", "underskrift" mv.), indebærer således en risiko for, at også bestemmelser som ikke er egnede dertil, vil blive omfattet af ordningen.

Endelig knytter der sig efter udvalgets opfattelse nogle principielle betænkeligheder til gennemførelsen af en eller flere generelle retsregler, der ændrer et større antal bestemmelser i lovgivningen uden nærmere at præcisere, endsige have overblik over, hvilke regler det drejer sig om, og uden at det direkte af de pågældende bestemmelser vil kunne ses, at de er blevet ændret. Som beskrevet ovenfor blev der også i nogle af høringssvarene vedrørende Forskningsministeriets lovudkast fra 1998 peget på, at en sådan ordning måtte give anledning til principielle betænkeligheder.

For det første ville en sådan model indebære, at lovgivningsmagten ikke vil have mulighed for at danne sig et overblik over konsekvenserne af den retsregel, som man vedtager.

Der findes eksempler på love af generel og tværgående karakter, der ændrer bestemmelser med et bestemt indhold. Ved lov nr. 474 af 12. juni 1996 blev der således indsat en formodningsregel i straffelovens § 26 om, at bestemmelser i lovgivningen om strafansvar for andre end enkeltpersoner omfatter enhver juridisk person. På tidspunktet for fremsættelsen af lovforslaget fandtes hjemmel til sådant ansvar i mere end 200 love, som altså blev ændret på én gang. Det kan også nævnes, at det følger af § 3, stk. 2, i lov om registreret partnerskab, at bestemmelser i dansk lovgivning, som omhandler ægteskab og ægtefæller, skal anvendes tilsvarende på registreret partnerskab og registrerede partnere. Også denne bestemmelse ændrede således generelt indholdet af al bestående lovgivning af denne karakter.

I begge tilfælde havde man imidlertid et klart overblik over, hvilke bestemmelser, der var tale om, og havde identificeret og gennemgået disse. Det samme ville ikke gælde for en model, der opstillede en formodning om en bestemt forståelse af almindeligt anvendte ord som ”underskrift”, ”dokument” mv. Regler, der indeholder disse ord, findes i alle dele af lovgivningen og drejer sig om vidt forskellige spørgsmål. Der er endvidere tale om et meget betydeligt antal regler. Konsekvenserne af gennemførelsen af en sådan generel regel ville således være nærmest umulige at overskue.

Dernæst ville en model, der ved en eller flere generelle bestemmelser ændrede en række bestemmelser andre steder i lovgivningen, have den uheldige konsekvens, at borgerne ikke ud fra den lov, der gælder på det pågældende retsområde, ville kunne se, at det er muligt at benytte digital kommunikation. Denne betænkelighed kunne i givet fald imødekommes ved i hver enkelt bestemmelse at optage en henvisning til den generelle regel, men i så fald ville der ikke være meget vundet i form af arbejdsbesparelse i forhold til at ændre formkravet direkte i hver enkelt lovbestemmelse for sig.

Selv om den beskrevne lovgivningsmodel ville have den klare fordel, at den ville kunne føre til en hurtig ændring af alle formkrav i lovgivningen, finder udvalget således, at der er væsentlige lovtekniske og principielle betænkeligheder forbundet med modellen. Dette gælder, uanset om man udformer modellen således, at den omfatter alle formkrav, som ikke udtrykkeligt undtages fra ordningen, eller om reglens virkning skal afhænge af en "tilmelding" af de pågældende bestemmelser med formkrav, jf. herom ovenfor. Med en "tilmeldingsmodel" undgås nogle af de uheldige konsekvenser, som er beskrevet ovenfor, men der vil stadig være væsentlige betænkeligheder forbundet med modellen.

Det er således ikke tilrådeligt at anvende generelle bestemmelser til en samlet ændring af lovgivningen med henblik på at tilpasse denne til brug af digital kommunikation på de områder, hvor dette er hensigtsmæssigt.

Man må derfor efter udvalgets opfattelse systematisk gennemgå lovgivningen for at finde formkrav, som bør ændres for at muliggøre en hensigtsmæssig anvendelse af digital kommunikation, og derefter ændre hvert enkelt formkrav for sig. Denne gennemgang bør foretages af de myndigheder, som administrerer de pågældende retsområder, jf. herom nedenfor.

6.3.3. Metoder til ændring af formkrav i lovgivningen

Udvalget har herefter drøftet to hovedmodeller for, hvordan gennemgangen og ændringen af bestemmelserne med formkrav bør foregå. Den første model går ud på ved en ændringslov at ændre hver enkelt lovbestemmelse, der indeholder et sådant formkrav ("særskilte lovændringer"). Efter den anden model indføres der en generel hjemmel for den pågældende minister til ved bekendtgørelse at ændre bestemmelser i lovgivningen, der indeholder formkrav, som hindrer en hensigtsmæssig anvendelse af digital kommunikation ("en generel bemyndigelseslov"). Endelig har udvalget drøftet en mellemløsning, som gør

det muligt på visse områder at anvende den førstnævnte model, mens man på andre områder går frem efter den anden.

6.3.3.1. Særskilte lovændringer

Den første model, som udvalget har overvejet, består i at følge den sædvanlige lovgivningsmetode, når en lovregel skal ændres, dvs. at der udarbejdes ændringslove, hvorved formkravene i de enkelte love ændres hver for sig. Lovgivningen bliver herved enkel at overskue. Imod modellen kan det navnlig anføres, at Folketinget vil blive belastet med en stor mængde arbejde, hvor en stor del af regelændringerne hovedsagelig vil være af administrativ karakter og formentlig tillige ukontroversielle. Udformningen af lovforslag kan også være en mere tidskrævende procedure, end når der er tale om bekendtgørelser, og der kan derfor også være en risiko for, at der med denne model vil gå noget længere tid, før lovgivningen er ændret.

For at fremme lovgivningsarbejdet mest muligt og for at undgå at belaste Folketinget med mange enkeltstående lovforslag kan det som en variant af denne model overvejes at udforme et eller flere ”samlelovforslag”, som indeholder bestemmelser om ændring af formkrav i forskellige love.

6.3.3.2. En generel bemyndigelseslov

Den anden model, som altså går ud på gennem én lov at bemyndige de enkelte ministre til at foretage de nødvendige ændringer inden for hver deres ressortområde, indebærer, at der ikke skal gennemføres lovgivning, hver gang en bestemmelse med et formkrav skal ændres, men at man i stedet kan benytte bekendtgørelsesformen, som er hurtigere.

Der er som udgangspunkt ikke noget til hinder for, at Folketinget på denne måde bemyndiger vedkommende minister til administrativt at ændre regler i lovgivningen (såkaldt

derogation)⁸⁸. Det forekommer imidlertid meget sjældent, at der i en lov gives bestemmelser, som bemyndiger til ændring af bestemmelser i anden lovgivning.

Hvis en bemyndigelseslov skal lette arbejdet med at ændre bestemmelser med formkrav i lovgivningen, må den have et bredt anvendelsesområde. Formkrav findes på mange forskellige retsområder og er udformet på mange forskellige måder, og det vil næppe være muligt på forhånd at angive, hvilke lovregler der vil kunne ændres i henhold til en sådan bemyndigelsesbestemmelse.

En generel lovregel, som bemyndiger vedkommende minister til ved bekendtgørelse at ændre et hvilket som helst formkrav i lovgivningen, vil imidlertid efter udvalgets opfattelse indebære en så vidtgående delegation af lovgivningskompetence, at det måtte give anledning til principielle betænkeligheder.

Herudover kan det indvendes, at en sådan regel vil gøre lovgivningen vanskelig at overskue for borgerne, fordi man ikke ud fra den lov, som regulerer et bestemt retsområde, vil kunne se, at der var hjemmel til at ændre loven ved bekendtgørelse. Ønskede man oplysning om, hvorvidt et formkrav var ændret i henhold til en sådan bemyndigelsesbestemmelse, ville man endvidere være henvist til at gennemgå de udstedte bekendtgørelser. Efterhånden som hjemlen blev brugt, ville en sådan gennemgang kunne blive ganske tidskrævende.

6.3.3.3. En mellemløsning

Udvalget har endelig overvejet en mellemløsning, som går ud på, at vedkommende minister bemyndiges til at ændre formkrav, der drejer sig om kommunikation fra borgere og virksomheder mv. til det offentlige (og fra én offentlig myndighed til en anden), således at

⁸⁸ Se om derogation bl.a. Ross: Dansk Statsforfatningsret II (1980), side 498 f.

det bliver muligt at anvende digital kommunikation i forhold til det offentlige, samtidig med at der gennemføres særskilte lovændringer inden for de enkelte ministerområder, eventuelt i form af samlelovforslag.

Hjemmelsbestemmelsen vedrørende ret til digital kommunikation til det offentlige forudsættes udformet således, at den gør det muligt at fastsætte regler, der giver borgere og virksomheder mv. ret til at benytte digital kommunikation i forhold til det offentlige. Derimod skal bestemmelsen ikke give hjemmel til at fastsætte bestemmelser, som udelukker muligheden for at anvende andre kommunikationsformer, f.eks. ved at fastsætte, at henvendelse alene kan ske ved brug af digital kommunikation. Formkrav for kommunikation fra borgere og virksomheder til det offentlige er talrige, og en bemyndigelsesbestemmelse på dette område vil derfor have stor praktisk betydning. Bl.a. har det vist sig i forbindelse med de pilotprojekter m.v., som Forskningsministeriet har iværksat, at der er behov for at kombinere de tekniske løsninger med tilvejebringelse af lovgivningsmæssige rammer, som muliggør digital kommunikation.

De ovenfor anførte betænkeligheder om borgernes muligheder for at indrette sig på indholdet af lovgivningen har mindre vægt på dette område, fordi modtageren af kommunikationen er en offentlig myndighed, som ofte vil være den samme, som bemyndiges til at ændre det pågældende formkrav. Er dette ikke tilfældet, f.eks. fordi formkravet drejer sig om borgernes kommunikation med kommunerne, vil det normalt være en enkel sag at inddrage den eller de pågældende myndigheder, inden reglen ændres.

Selv om reglens anvendelsesområde begrænses som anført, kan det tænkes indvendt, at der er tale om en på samme tid vidtgående og upræcis delegation af lovgivningskompetence til forvaltningen. De regler, som bemyndigelsesbestemmelsen vil finde anvendelse på, kan således næppe angives på anden måde end ved deres funktion, dvs. regler om kommunikation fra borgere og virksomheder til det offentlige, og det nærmere omfang af den foretagne delegation vil således først vise sig, efterhånden som bemyndigelsen bliver

brugt. Det kan endvidere generelt indvendes mod denne variant af bekendtgørelsesmodellen, at den gør lovgivningen vanskelig at overskue for borgerne, fordi man ikke ud fra den lov, som regulerer det pågældende retsområde, vil kunne se om et formkrav i loven kan opfyldes ved brug af digital kommunikation, jf. herom ovenfor.

Under hensyn til, at de pågældende bestemmelser med formkrav hovedsageligt drejer sig om forhold af mere formel, administrativ karakter, og da hjemmelsbestemmelsen som nævnt forudsættes udformet således, at den gør det muligt at give borgere og virksomheder ret – men ikke pligt – til at benytte digital kommunikation, finder udvalget imidlertid ikke, at de ovennævnte indvendinger har en sådan vægt, at det er udelukket at bruge denne model. Endvidere vil det også være i myndighedernes egen interesse at udbrede interessen for at kunne kommunikere digitalt.

Udvalget har overvejet også at lade bestemmelser vedrørende kommunikation fra offentlige myndigheder til virksomheder, borgere m.v. være omfattet af bestemmelsens anvendelsesområde. Herfor taler navnlig, at der ved at lade bestemmelsen omfatte al kommunikation til og fra det offentlige ville blive sikret en tidsmæssig sammenhæng i moderniseringen af lovgivningen på området. I modsat fald kunne der være risiko for, at gennemførelsen af projekter til digital forvaltning kom til at afvente gennemførelsen af lovgivning vedrørende kommunikation fra det offentlige til borgere og virksomheder, og at bekendtgørelsesmodellen derfor alligevel ikke ville føre til et hurtigere resultat.

En gennemgang af flere af de pilotprojekter vedrørende digital forvaltning, som Forskningsministeriet har ydet støtte til, har imidlertid ikke vist nogen eksempler på, at formkrav i lovgivningen vedrørende kommunikation fra det offentlige, har udgjort en reel hindring for projekternes gennemførelse. De forhindringer, som man er stødt på i projekterne, vedrører hovedsagelig situationer, hvor det offentlige som svar på en henvendelse eller ansøgning fra en borger skal fremsende et dokument, som f.eks. et pas eller et kursusbevis. Sådanne dokumenter anvendes bl.a. ved, at indehaveren efterfølgende kan fremvise

dem som bevis for en rettighed m.v., jf. herom ovenfor i kapitel 5.3.3., hvilket – i hvert fald på nuværende tidspunkt – normalt forudsætter, at dokumentet har fysisk form.

Dansk ret indeholder ikke nogen generel regel om, hvilken kommunikationsform det offentlige skal benytte ved meddelelser til private, men lige som på andre områder findes der forskellige bestemmelser i den forvaltningsretlige lovgivning, som indeholder formkrav. Således følger det af forvaltningslovens § 23, at en borger har ret til en efterfølgende skriftlig begrundelse af mundtlige afgørelser, medmindre borgeren har fået fuldt ud medhold. Ombudsmanden har flere gange under henvisning til god sagsbehandlingsskik givet udtryk for, at skriftlige henvendelser fra borgere som hovedregel bør besvares skriftligt af myndighederne.

Det vil afhænge af fortolkning af de enkelte forvaltningsretlige bestemmelser om skriftlighed mv., om disse kan opfyldes ved brug af digital kommunikation. Hvor det drejer sig om særligt indgribende afgørelser, kan dette tale for at fortolke formkravet indskrænkende. Det kan i den forbindelse nævnes, at Folketingets Ombudsmand i en sag vedrørende afskedigelse af en funktionær har fundet det tvivlsomt, om en telefaxmeddelelse opfylder funktionærlovens skriftlighedskrav⁸⁹. Afgørelsen er nærmere omtalt af John Vogter, Forvaltningsloven med kommentarer (3. udg. 1999), side 417.

I de tilfælde, hvor der ikke findes formkrav om skriftlighed mv., vil der efter udvalgets opfattelse som udgangspunkt ikke være noget til hinder for at anvende digital kommunikation fra det offentlige til borgere, hvis den pågældende har givet samtykke hertil.

Behovet for at ændre de gældende regler er derfor formentlig ikke særligt stort, og der vil endvidere efter udvalgets opfattelse knytte sig betydelige retssikkerhedsmæssige betænke-

⁸⁹ Folketingets Ombudsmands beretning for 1990, side 387-388.

ligheder ved i bekendtgørelsesform at ændre lovbestemmelser, som giver borgere mv. ret til at modtage kommunikation fra det offentlige på en bestemt måde, således at borgerne pålægges pligt til at modtage meddelelserne digitalt. Udvalget har på denne baggrund fundet, at bekendtgørelsesmodellen ikke bør omfatte kommunikation fra det offentlige. For sådanne regler vil ændring således skulle ske ved traditionelle ændringslove, evt. i form af samlelovforslag.

6.3.3.4. Udvalgets forslag

Efter udvalgets opfattelse er mellemløsningen den bedste af de tre beskrevne modeller, fordi den på et i praksis vigtigt område – kommunikation til det offentlige - gør det muligt hurtigt at komme i gang med moderniseringen af lovgivningen, samtidig med at der ikke knytter sig afgørende betænkeligheder til modellen.

For så vidt angår formkrav, som drejer sig om kommunikation fra borgere og virksomheder til det offentlige, bør der således efter udvalgets opfattelse indføres en generel lovregel, som uanset formkrav i lovgivningen gør det muligt for vedkommende minister at bestemme, at der på nærmere angivne områder kan anvendes læsbar digital kommunikation ved henvendelser til den offentlige forvaltning. Anvendelsesområdet for bestemmelsen vil navnlig være henvendelser fra borgere og virksomheder til offentlige myndigheder, f.eks. ansøgninger eller blanketter med oplysninger, og kommunikation mellem offentlige myndigheder indbyrdes.

Bestemmelsen, der f.eks. kunne indsættes i forvaltningsloven, kan udformes således:

”§ X. Hver minister kan inden for det pågældende ministerområde fastsætte bestemmelser om, at der kan anvendes digital kommunikation ved henvendelser til den offentlige forvaltning, og om de nærmere vilkår herfor.”

Hvor der i lovgivningen findes bestemmelser, som hindrer digital kommunikation, f.eks. ved krav om, at henvendelse skal ske ved brug af et papirdokument, følger det af forslaget, at vedkommende minister kan fastsætte regler om, at der skal bortses herfra. Det forudsættes, at det i givet fald klart fremgår, at den pågældende regel ændres, f.eks. ved en henvisning til bestemmelsen. Formålet med at bemyndige de enkelte ministre til at fravige formkrav i lovgivningen er at lette indførelsen af regler, der fremmer en hensigtsmæssig brug af digital kommunikation ved henvendelser til den offentlige forvaltning.

Den foreslåede regel vil imidlertid have et videre anvendelsesområde, idet der tilvejebringes en generel hjemmel for den pågældende minister til ved bekendtgørelse at bestemme, at der kan anvendes digital kommunikation ved henvendelser til offentlige myndigheder, og til at fastsætte nærmere regler om kravene til kommunikationen, f.eks. om anvendelse af bestemte dokumentformater mv. og om de nærmere vilkår herfor. Hjemmelsbestemmelsen skal gælde for samtlige ministerområder.

På områder, hvor lovgivningen ikke indeholder regler, som hindrer digital kommunikation, men hvor der på den anden side heller ikke er fastsat regler om, at denne form for kommunikation kan anvendes og på hvilke betingelser, vil sådanne regler kunne udstedes i medfør af den foreslåede bestemmelse.

Begrebet ”den offentlige forvaltning” forudsættes afgrænset på samme måde som efter offentlighedsloven og forvaltningsloven, jf. § 1 i begge love. Omfattet er navnlig henvendelser til statslige og kommunale myndigheder. Uden for bestemmelsens anvendelsesområde vil falde kommunikation med myndigheder, som ikke er den del af den offentlige forvaltning, hvilket bl.a. betyder, at bemyndigelsen ikke vil kunne anvendes til at fastsætte regler om digital kommunikation med domstolene. Det bør således selvstændigt overvejes, i hvilket omfang behovet for digital kommunikation med domstolene nødvendiggør ændringer i retsplejeloven, jf. grundlovens § 61, hvorefter den dømmende magts udøvelse kun kan ordnes ved lov.

Hjemlen foreslås endvidere begrænset til fastsættelse af regler om, at digital kommunikation kan anvendes, mens det derimod ikke i medfør af den foreslåede regel vil kunne fastsættes, at henvendelse skal ske på denne måde. Det vil således ikke kunne fastsættes, at henvendelse ikke kan ske ved brug af f.eks. papirdokumenter.

Bestemmelsen vil navnlig kunne anvendes til at give regler om brug af læsbar digital kommunikation, dvs. meddelelser, hvis meningsindhold består af bogstaver mv. og som kan gøres læselige for modtageren ved gengivelse på en skærm, udskrift på papir mv., men det vil efter omstændighederne også kunne komme på tale at tillade brug af andre digitale medier, f.eks. indsendelse af video- eller lydoptagelser.

Udvalget finder, at formkrav, som ikke drejer sig om henvendelser til den offentlige forvaltning, kun bør ændres ved særskilte lovændringer. Det drejer sig dels om henvendelser fra den offentlige forvaltning til borgere og virksomheder mv., dels om kommunikation, som ikke involverer den offentlige forvaltning, men som foregår mellem borgere og virksomheder indbyrdes. Som anført ovenfor vil der efter udvalgets opfattelse normalt ikke være noget til hinder for, at der anvendes digital kommunikation fra det offentlige til borgere og virksomheder, hvis modtageren har givet samtykke hertil.

Efter udvalgets opfattelse er den foreslåede model for udformningen af et lovgivningsinitiativ udtryk for en balanceret afvejning mellem hensynet til, at initiativet gennemføres hurtigst muligt, og hensynet til, at almindelige lovgivningsprincipper om klarhed og retssikkerhed tilgodeses.

Lov om elektroniske signaturer og de tilhørende bekendtgørelser udgør nu den lovmæssige ramme for udbud af kvalificerede certifikater med krav om overholdelse af en række tekniske og sikkerhedsmæssige krav. Etablering af et tilsyn med nøglecentre og fastsættelsen

af det særlige erstatningsansvar for nøglecentre vil samtidig bidrage til at skabe klarhed over de juridiske forhold omkring anvendelsen af elektroniske signaturer.

Udvalget vurderer, at en systematisk gennemgang af lovgivningen fulgt op af en modernisering af de formkrav, som forhindrer brug af digital kommunikation, vil udgøre en vigtig brik til understøttelse af de forskellige elektroniske initiativer i den offentlige sektor og inden for den elektroniske handel i almindelighed, som i dag er under udvikling.

Regeringen har som nævnt oven for i kapitel 4 og kapitel 6.1.1 lagt op til, at der i de kommende år skal satses på at opbygge en moderne digital forvaltning. I øjeblikket arbejdes der for eksempel med at give borgere og virksomheder mulighed for at indberette en lang række oplysninger via Internettet, at indsende ansøgninger, at søge aktindsigt og at søge informationer via Internettet, ligesom også offentlige myndigheder skal kunne foretage en lang række indkøb fra private leverandører via auktionshaller på Internettet.

Endelig er der efter udvalgets opfattelse grund til at fremhæve, at mange eksisterende formkrav ikke vil være til hinder for anvendelse af digital kommunikation. Der vil derfor være mange tilfælde, hvor der allerede i dag er mulighed for at gå i gang med udviklingen af nye elektroniske serviceydelser, hvori brugere af elektroniske signaturer indgår, uden at man behøver vente på, at moderniseringen af formkrav gennemføres.

6.3.4. Tilrettelæggelsen af det videre arbejde

Der findes som nævnt et betydeligt antal formkrav i lovgivningen, og en systematisk gennemgang og ændring af disse er en ganske omfattende opgave. I lyset af den samfundsmæssige interesse i at tilvejebringe en lovgivning, som understøtter brugen af digital kommunikation, har udvalget overvejet forskellige måder, hvorpå en ændring af de mange formkrav kan foretages, således at arbejdet fremmes mest muligt. En hurtig gennemgang

af lovgivningen vil i øvrigt også være nødvendig for at finde formkrav, som hindrer anvendelsen af ”elektroniske kontrakter”, jf. ovenfor i kapitel 3.2.2. om direktivet om visse retlige aspekter af elektronisk handel i det indre marked. Sådanne krav skal være fjernet inden den 17. januar 2002.

Vurderingen af de enkelte bestemmelser med formkrav forudsætter et indgående kendskab til de øvrige regler på det pågældende retsområde. Udarbejdelse af forslag om ændring af en bestemmelse i lovgivningen forudsætter et kendskab til baggrunden for den pågældende bestemmelse og til retsområdet i øvrigt, som det pågældende ressortministerium i almindelighed besidder. Der vil også kunne blive behov for at inddrage berørte organisationer, myndigheder mv. i arbejdet med at ændre lovreglerne, hvilket bør ske gennem det ministerium, som har det generelle ansvar for det pågældende retsområde.

Udvalget finder på denne baggrund, at det bør være de enkelte ressortministerier, der får til opgave at gennemgå hver deres ressortområde med henblik på at finde frem til og udarbejde forslag til ændring af formkrav, som hindrer en hensigtsmæssig anvendelse af digital kommunikation.

At ansvaret for at ”modernisere” lovgivningen bør overlades til de enkelte ministerier, udelukker ikke, at der samtidig etableres nogle overordnede rammer for arbejdet. Tværtimod er der efter udvalgets opfattelse flere forhold, der taler for at gøre dette.

Det vil være nødvendigt at koordinere de ændringer, som de enkelte ministerier overvejer at gennemføre, uanset om disse sker ved bekendtgørelse eller ved ændringslove, fordi man ellers bl.a. risikerer, at der på områder, som er reguleret i flere ministeriers lovgivning, ikke gennemføres alle de ændringer, som er nødvendige for at gøre digital kommunikation attraktiv at benytte for borgere og virksomheder. Hvis f.eks. kun nogle oplysninger i en sag kan fremsendes digitalt til en kommune, mens andre skal indsendes ved brug af papirdokumenter, vil dette kunne betyde, at muligheden for digital kommunikation ikke

bliver benyttet. Det er også vigtigt, at reglerne og mulighederne for digital kommunikation så vidt muligt udformes på samme måde, så lovgivningen får et ensartet præg og bliver lettere at anvende for borgerne

Det er ikke udvalgets opgave at tage stilling til, hvordan denne koordination nærmere skal gennemføres. Det vil som ovenfor anført i et vist omfang kunne vise sig hensigtsmæssigt at udarbejde samlelovforslag med ændringer af love på de forskellige ministerområder. Herved vil der kunne sikres den fornødne sammenhæng mellem ændringerne på de forskellige ministerområder, ligesom det vil være lettere for både borgere, virksomheder og myndigheder at overskue ændringerne.

Bekendtgørelser i medfør af den bemyndigelsesbestemmelse, som udvalget har foreslået indsat i f.eks. forvaltningsloven, vil skulle udstedes af hver enkelt minister, men der kan også her være behov for at koordinere arbejdet.

Der er grund til at fremhæve, at det ikke er nogen let opgave, som efter udvalgets forslag pålægges de enkelte ministerier. Der er ganske mange regler i lovgivningen, som indeholder formkrav af den ene eller anden art, som ministerierne skal gennemgå og eventuelt udarbejde ændringer eller forslag til ændringer i. Mængden af regler, der skal vurderes, kan dog svinge fra det ene ministerium til det andet.

For at formkrav i lovgivningen ikke skal være en unødigt hindring for brug af sikker digital kommunikation, er det vigtigt, at arbejdet med denne gennemgang gives høj prioritet, således at man hurtigt kommer i gang med at gennemgå reglerne inden for de enkelte ministerområder.

Det er således vigtigt, at arbejdet hermed sættes hurtigt i gang, således at de nødvendige regelændringer eller lovforslag hurtigst muligt kommer ”på plads”. Kun herved kan det

sikres, at man hurtigt opnår de fordele for borgerne og samfundet som helhed, som digital kommunikation vil kunne indebære.

6.4. Retningslinier ved ændring af formkrav

6.4.1. Indledning

Udvalget har afslutningsvis overvejet, om det er muligt at opstille nogle generelle retningslinier, som de enkelte ministerier kan følge, når de gennemgår og i givet fald udarbejder forslag til ændring af lovgivningen på hver deres ressortområde.

Bestemmelser med formkrav er imidlertid som tidligere fremhævet meget forskellige, og det er derfor ikke muligt at opstille egentlige lovgivningsmodeller i form af faste formuleringer eller lignende, som man generelt kan anvende ved ændring af formkrav. Udvalget har på denne baggrund valgt i stedet at fremhæve nogle overordnede synspunkter, som kan tjene til inspiration ved de enkelte ministeriers videre arbejde.

Selv om der ikke kan opstilles et fast skema for, hvordan lovgivningen bør ændres, er der dog efter udvalgets opfattelse behov for, at der så vidt muligt anvendes en ensartet fremgangsmåde, når formkravene på de forskellige retsområder ændres. Dette vil kunne sikres, hvis der som foreslået ovenfor udpeges én eller flere myndigheder, som får til opgave at koordinere lovgivningsinitiativet.

6.4.2. Gennemgang af lovgivningen

Den første opgave for de involverede ministerier vil gå ud på at finde de bestemmelser på det pågældende ressortområde, som udelukker brug af digital kommunikation eller giver anledning til tvivl om, hvorvidt det er muligt at anvende digital kommunikation. Tvivl om

forståelsen af en bestemmelse kan i sig selv udgøre en hindring for brug af digital kommunikation, og undersøgelsen kan derfor ikke begrænses til alene at dreje sig om at finde de bestemmelser, som direkte forhindrer brug af digital kommunikation, men må også rettes mod bestemmelser, der ikke utvivlsomt tillader denne form for kommunikation.

I mange tilfælde vil man efter udvalgets opfattelse ved fortolkning kunne nå frem til, at en bestemmelse, hvis forståelse giver anledning til tvivl, f.eks. fordi den blot foreskriver, at information skal indsendes skriftligt, kan opfyldes også ved brug af digital kommunikation, jf. herom ovenfor i kapitel 6.2.4. I så fald kan problemet løses uden lovgivning, men der vil formentlig ofte være behov for at skabe klarhed om forståelsen af bestemmelsen for borgere og virksomheder mv. Retter bestemmelsen sig mod en snæver kreds af brugere, vil tvivlen kunne afhjælpes ved henvendelse direkte til de pågældende. I andre tilfælde kan der blive tale om udsendelse af en cirkulæreskrivelse til de berørte myndigheder, information i pressen o.s.v.

6.4.3. Hvilke bestemmelser skal ændres?

For så vidt angår de bestemmelser, som herefter findes at udgøre reelle hindringer for anvendelse af digital kommunikation, må det overvejes, om det vil være hensigtsmæssigt at tillade brug af digitale medier på de pågældende områder. Vurderingen heraf vil afhænge af en lang række forskellige forhold af både praktisk, retlig og økonomisk karakter, som det enkelte ministerium, eventuelt efter drøftelse med andre involverede parter, vil være nærmest til at tage stilling til. I det følgende gives der en oversigt over nogle af de spørgsmål, som formentlig oftest vil opstå.

6.4.3.1. Kan formålet opfyldes ved digital kommunikation?

Efter udvalgets opfattelse vil der ofte være grund til at lade overvejelserne om at ændre et formkrav tage udgangspunkt i de formål, som den pågældende bestemmelse varetager. Som nævnt ovenfor i kapitel 2.2. og 2.3.4. er der en række lighedspunkter mellem digitale dokumenter og papirdokumenter og mellem elektronisk signatur og traditionelle underskrifter, men der er også en række væsentlige forskelle. Spørgsmålet vil være, om disse forskelle har betydning på det pågældende retsområde. Kan formålet opfyldes på tilfredsstillende vis ved brug af digitale medier, vil dette tale for at tillade denne kommunikationsform.

I nogle tilfælde vil forskellene mellem papirmediet og det digitale medie betyde, at formålet med de pågældende regler ikke kan opnås ved brug af digitale dokumenter. Det kan f.eks. være tilfældet med regler om negotiable dokumenter, identitetspapirer m.v., jf. herom ovenfor i kapitel 5.3. I så fald må formkravet bevares.

I andre tilfælde vil forskellene mellem papirdokumenter og digitale medier give anledning til tvivl om, hvorvidt det vil være hensigtsmæssigt at tillade digital kommunikation på det pågældende område, fordi formålet ikke kan opfyldes på helt samme måde, når der ikke benyttes et papirdokument. Selv om digital kommunikation ikke fuldt ud opfylder formålene bag et formkrav, behøver det imidlertid ikke nødvendigvis at betyde, at anvendelsen heraf er udelukket. I nogle tilfælde vil overvejelserne om at ændre formkravet således kunne give anledning til mere grundlæggende at overveje et formkravs berettigelse. Det kan være, at man med mindre indgribende midler kan opnå en fuldt ud tilfredsstillende sikkerhed mv., og at der derfor generelt kan gennemføres en lempelse, som gør det muligt også at anvende digital kommunikation.

6.4.3.2. Behov for identifikation af afsenderen

Tvivl om, hvorvidt digital kommunikation opfylder de nødvendige krav til at kunne anvendes på et retsområde, vil formentlig navnlig opstå i de tilfælde, hvor reglerne har til formål at sikre afsenderens identitet, f.eks. ved et krav om underskrift.

Der er som nævnt ovenfor gennemført lovgivning om elektronisk signatur, etableret en infrastruktur til udstedelse af certifikater mv. og gennemført forsøgsprojekter, netop med henblik på at gøre det muligt at anvende digital kommunikation med sikkerhed for afsenderens identitet.

Endnu er det dog kun meget få, der er i besiddelse af en elektronisk signatur, og derfor kan det på nuværende tidspunkt være vanskeligt at vurdere, om signaturerne på alle retsområder vil give den fornødne sikkerhed. Det må dog forventes, at elektroniske signaturer, der lever op til EU-direktivet, jf. herom ovenfor i kapitel 3.2.1., i langt de fleste tilfælde vil give en tilstrækkelig identifikation af afsenderen og sikkerhed for, at meddelelsen ikke er ændret efter afsendelsen. Noget andet er, at netop den manglende udbredelse kan gøre det vanskeligt på nuværende tidspunkt at basere en løsning på elektronisk signatur. Dette problem er dog antagelig kun midlertidigt, idet det forventes, at signaturløsninger i løbet af få år vil være almindeligt udbredte.

6.4.3.3. Administrative og økonomiske forhold

Ofte vil det være de økonomiske og administrative konsekvenser, som afgør, om der bliver taget skridt til at ændre en retsregel, så den ikke længere hindrer brug af digital kommunikation. En regelændring vil sjældent kunne stå alene, idet der ofte vil skulle foretages en række praktiske skridt for at muliggøre digital kommunikation. I mange tilfælde vil det

formentlig være de praktiske snarere end de retlige forhold, som udgør den egentlige hindring for brug af digitale medier.

De fleste af de formkrav, udvalget har gennemgået, drejer sig om kommunikation med det offentlige, og her vil det i givet fald være nødvendigt at indrette kommunikationsløsninger, journaliserings- og arkiveringssystemer mv. på digital kommunikation. Om udgifterne hertil står i rimeligt forhold til de fordele, som knytter sig til brug af digital kommunikation, vil afhænge af mange forhold. Økonomistyrelsens rapport ”Undersøgelse af rationaliseringspotentialer i forbindelse med implementering af IT-handlingsplanen” indeholder en redegørelse for udgifter og mulige rationaliseringsgevinster ved indførelse af elektroniske blanketter m.v. i det offentlige.

6.4.3.4. Arkivering og bevisspørgsmål

Endelig vil der ofte være grund til at overveje behovet for at opbevare de digitale dokumenter og de bevismæssige spørgsmål, som vil kunne opstå, når information ikke længere findes i papirdokumenter.

Breve mv. kan normalt uden videre fremfindes (i original eller kopi) og anvendes som dokumentation for indholdet af den information, som er blevet udvekslet, f.eks. i forbindelse med behandling af en ansøgning, indgåelse af en aftale osv. Kommer det til en retssag, kan dokumenterne fremlægges som bevis.

Som nærmere beskrevet ovenfor i kapitel 2.2. og 2.3.4. gælder det samme ikke altid for digitale dokumenter og elektroniske signaturer. Elektronisk signatur har en begrænset ”holdbarhed”, og formater for både signaturer og digitale dokumenter ændrer sig løbende. Hvis digitale meddelelser skal kunne læses og benyttes som bevis, også når der er gået nogen tid, vil der således skulle benyttes særlige sikkerhedsmekanismer.

Problemstillingen er navnlig af praktisk karakter. Oftest vil modtageren af den digitale kommunikation således selv have behov for at kunne fremfinde og læse de digitale dokumenter på et senere tidspunkt, og i så fald opstår der dels spørgsmål om indretning af passende arkiveringssystemer, dels spørgsmål om, hvor længe dokumenterne skal kunne læses.

I nogle tilfælde vil indretningen af systemer til opbevaring af digitale dokumenter m.v. få en retlig karakter, fordi meddelelsen skal benyttes som bevis i forbindelse med en retssag eller lignende. I så fald må det digitale dokument udskrives, og der vil kunne opstå spørgsmål om, hvorvidt udskriften svarer til den oprindelige meddelelse, eller om der er sket ændringer.

Den danske civilproces bygger på principper om fri bevisførelse og fri bevisbedømmelse. Der gælder således som udgangspunkt ikke retlige grænser for, hvad der kan benyttes som bevis, og det er op til den enkelte dommer at vurdere betydningen af de beviser, som bliver fremlagt. Der er således ikke noget til hinder for at benytte digitale dokumenter og elektronisk signatur som bevis under en retssag, men det er på den anden side ikke på forhånd muligt at give et generelt svar på, hvilken bevisværdi der knytter sig hertil. Dette vil afhænge af en række forhold, hvor bl.a. kvaliteten af de anvendte signaturløsninger og sikkerhedsmekanismerne i forbindelse med opbevaring og udskrift af de digitale dokumenter vil kunne blive tillagt vægt.

For en grundig behandling af disse spørgsmål og anvisninger om, hvordan journaliseringssystemer mv. indrettes med henblik på at sikre en høj bevisværdi, kan der henvises til to vejledninger fra IT-sikkerhedsrådet: ”Digitale dokumenters bevisværdi” og ”Praktisk brug af kryptering og digital signatur”⁹⁰.

⁹⁰ Digitale dokumenters bevisværdi – Introduktion og vejledning med bilag, IT-sikkerhedsrådet, december 1998, og Praktisk brug af kryptering og digital signatur – en vejledning fra IT-sikkerhedsrådet, maj 2000.

6.4.4. Metode ved ændring af reglerne

Som nævnt i indledningen kan der ikke opstilles generelle modeller eller angives særlige formuleringer, som skal anvendes, når man ændrer retsregler, som hindrer brug af digitale medier. Hver bestemmelse må vurderes og ændres for sig og i overensstemmelse med almindelige principper for udformning af lovforslag og administrative forskrifter mv.

Ved ændring af formkrav med henblik på at muliggøre brug af digital kommunikation opstår der dog nogle særlige spørgsmål, som der kan være grund til at fremhæve her. Navnlig er der grund til at være opmærksom på, at en ændring af selve den bestemmelse, som hindrer brug af digital kommunikation, ofte ikke i sig selv vil være tilstrækkelig. Drejer reglen sig om kommunikation til offentlige myndigheder, vil der ofte være behov for at fastsætte nærmere regler om, hvordan kommunikationen skal foregå, bl.a. med henblik på at sikre, at meddelelserne kan læses af myndigheden.

Det bør således indgå i overvejelserne om udformningen af lovændringen, om der er behov for at fastsætte regler om tekniske forhold i forbindelse med indførelsen af muligheden for at anvende digital kommunikation, herunder eventuelt hvilke formater mv. der skal anvendes.

Sådanne spørgsmål er af praktisk karakter, og som følge af den tekniske udvikling vil der kunne være behov for relativt hyppige ændringer af regler herom. Det mest hensigtsmæssige vil derfor normalt være ikke at fastsætte regler herom i selve lovteksten, men i stedet i administrative forskrifter. I de fleste tilfælde vil der derfor skulle indsættes en bemyndigelsesbestemmelse – eller foretages ændringer i en allerede eksisterende bemyndigelsesbestemmelse – således at vedkommende minister får adgang til administrativt at fastsætte nærmere regler om den digitale kommunikation. I nogle tilfælde kan det blive aktuelt at fastsætte nærmere regler om dokumentformater mv., brug af elektronisk signatur, angivelse af bestemte e-mail adresser eller lignende, hvortil kommunikationen skal sendes osv.

Som et eksempel på denne fremgangsmåde kan nævnes lov nr. 972 af 17. december 1997 om ændring af patentloven, lov om brugsmodeller og lov om mønstre. Loven havde bl.a. til formål at gøre det muligt at indlevere ansøgninger mv. til patentmyndighederne i digital form, og derfor blev ordet ”skriftlig” fjernet fra bl.a. brugsmodellovens § 7, stk. 2, samtidig med at erhvervsministeren blev bemyndiget til at fastsætte nærmere regler om kommunikationen, jf. bl.a. brugsmodellovens § 46, stk. 3:

”Erhvervsministeren kan fastsætte bestemmelser om udveksling af elektroniske data med patentmyndigheden.”

Drejer formkravet sig om henvendelser til den offentlige forvaltning, vil en bemyndigelsesbestemmelse som beskrevet i kapitel 6.3.3.4. i givet fald indeholde den fornødne hjemmel for vedkommende minister til at fastsætte nærmere regler vedrørende disse mere tekniske spørgsmål, og i sådanne tilfælde bliver det derfor ikke nødvendigt at indsætte en bemyndigelsesbestemmelse i den pågældende lov.

Ud over spørgsmålet om udstedelse af administrative forskrifter vil en ændring af et formkrav ofte også give anledning til overvejelser om behovet for eventuelle konsekvensændringer andre steder i lovgivningen. Ofte vil et formkrav på et område hænge sammen med anden lovgivning på en måde, der gør, at den ønskede effekt kun opnås ved samtidige ændringer heri. Som nævnt i kapitel 6.3.4. vil det ofte være nødvendigt at ændre flere regelsæt for at gøre det attraktivt at anvende digital kommunikation. Kan en ansøgning f.eks. indsendes digitalt, mens de nødvendige bilag fortsat skal indsendes eller afleveres på papir, vil det formentlig i praksis betyde, at også ansøgningerne fortsat bliver indsendt på papir.

Et andet særligt spørgsmål opstår i relation til formkrav, der drejer sig om underskrift eller lignende, og hvor der i øvrigt er grund til at overveje at fastsætte regler om, at den digitale kommunikation skal være forsynet med elektronisk signatur.

Hidtil har der normalt ikke været brug for at fastsætte nærmere regler om, hvad der skal til for, at der foreligger en underskrift. I nogle tilfælde har man i lovgivningen udelukket brug af blyant, men ellers er den ene underskrift som udgangspunkt lige så god som den anden, når det drejer sig om at opfylde et formkrav.

Til forskel herfra vil der – bl.a. som følge af elektroniske signaturers teknisk komplicerede karakter, den løbende udvikling og de forskellige sikkerhedsniveauer afhængigt af den anvendte teknik – være behov for at fastsætte nærmere regler om, hvad der skal til for at opfylde et formkrav i lovgivningen om brug af elektronisk signatur.

For at lette lovgivningsarbejdet og for så vidt muligt at sikre en ensartet lovgivning, som endvidere overholder kravene i EU-direktivet om en fællesskabsramme for elektroniske signaturer og visse certificeringstjenester, indeholder lov om elektroniske signaturer i § 13 en bestemmelse, som giver formkrav om signatur mv. et bestemt indhold:

”§ 13. Bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, skal anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgenereringssystem. Ved elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.”

Bestemmelsen, som er nærmere omtalt ovenfor i kapitel 4.3.7., virker som en ”udfyldningsregel”, som giver formkrav om signatur et bestemt indhold. Indsætter man f.eks. følgende bestemmelse i lovgivningen:

”§ X. Ansøgninger kan indgives i digital form og skal i så fald være forsynet med elektronisk signatur.”

vil det følge af § 13 i lov om elektroniske signaturer, at formkravet om elektronisk signatur er opfyldt, hvis der er anvendt en avanceret elektronisk signatur, som er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgenereringssystem. Begreberne avanceret elektronisk signatur og kvalificeret certifikat er nærmere defineret i henholdsvis § 3, nr. 2, og § 4 i lov om elektroniske signaturer.

Normalt vil det således alene være nødvendigt at fastsætte nærmere regler om formater m.v. for den elektroniske signatur, hvis man vil tillade brug af signaturer, som ikke lever op til kravene i § 13 i lov om elektroniske signaturer. For at lette overblikket over bestemmelsens indhold for borgere og virksomheder mv., kan det dog være hensigtsmæssigt at indsætte en henvisning til lov om elektroniske signaturer, f.eks. således:

”§ X. Ansøgninger kan indgives i digital form og skal i så fald være forsynet med elektronisk signatur, jf. § 13 i lov om elektroniske signaturer.”

Som udgangspunkt vil der ikke kunne stilles krav om opfyldelse af strengere sikkerhedskrav, end hvad der følger af lovens regler om avancerede elektroniske signaturer mv. Ved kommunikation til og fra en offentlig myndighed kan der, som det fremgår af bestemmelsen, stilles strengere krav, men dette forudsætter, at der er et særligt behov herfor, og at de strengere krav er objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende, og de må kun være affødt af den pågældende anvendelses særlige karakter. Kravene må ikke hindre grænseoverskridende tjenesteydelser til borgerne.

Oftere vil det formentlig kunne komme på tale at overveje at tillade brug af elektroniske signaturer, som ikke lever op til (alle) de krav, der stilles i § 13 i lov om elektroniske signaturer. Selv om en elektronisk signatur ikke er lige så sikker som en signatur, der lever op til kravene i § 13, behøver dette således ikke at betyde, at den ikke kan anvendes. Selv om det måske kan være en nærliggende tanke at kræve en så høj grad af sikkerhed m.v. som muligt, ville en sådan fremgangsmåde i nogle tilfælde føre til, at der blev stillet alt for høje sikkerheds-

krav i forhold til det reelle behov på det pågældende område, hvilket i givet fald ville udgøre en unødigt hindring for brugen af digital kommunikation på det pågældende retsområde. Der er derfor grund til, at ministerierne nøje overvejer de reelle sikkerhedsbehov m.v., når reglerne om digital kommunikation udformes, med henblik på i givet fald at udforme kravene således, at de også kan opfyldes ved brug af andre typer af elektronisk signatur end dem, der er reguleret i lov om elektronisk signatur, og måske i nogle tilfælde uden brug af elektronisk signatur.

B I L A G 1

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 1999/93/EF

af 13. december 1999

om en fællesskabsramme for elektroniske signaturer

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 47, stk. 2, artikel 55 og 95,

under henvisning til forslag fra Kommissionen ⁽¹⁾,

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg ⁽²⁾,

under henvisning til udtalelse fra Regionsudvalget ⁽³⁾,

i henhold til fremgangsmåden i traktatens artikel 251 ⁽⁴⁾, og

ud fra følgende betragtninger:

- (1) Kommissionen forelagde den 16. april 1997 Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget en meddelelse med titlen »Et europæisk initiativ inden for elektronisk handel«;
- (2) Kommissionen forelagde den 8. oktober 1997 Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget en meddelelse med titlen »Sikkerhed og tillid i elektronisk kommunikation — Imod europæiske rammer for digitale signaturer og kryptering«;
- (3) Rådet opfordrede den 1. december 1997 Kommissionen til snarest muligt at forelægge Europa-Parlamentet og Rådet et forslag til direktiv om digitale signaturer;
- (4) elektronisk kommunikation og handel nødvendiggør elektroniske signaturer og dertil knyttede tjenesteydelser til autentifikation af data; forskellige regler for retlig anerkendelse af elektroniske signaturer og akkreditering af certificeringstjenesteudbydere i medlemsstaterne kan skabe betydelige hindringer for anvendelse af elektronisk kommunikation og elektronisk handel; en klar fællesskabsramme vedrørende betingelserne for elektroniske signaturer vil derimod styrke tilliden til og den generelle accept af de nye teknologier; medlemsstaternes lovgivning bør ikke udgøre en hindring for den frie bevægelighed for varer og tjenesteydelser i det indre marked;
- (5) elektronisk signatur-produkters interoperabilitet bør fremmes; efter traktatens artikel 14 indebærer det indre marked et område med fri bevægelighed for varer, specifikke væsentlige krav til elektronisk signatur-produkter skal opfyldes for at sikre fri bevægelighed på det indre marked og opbygge tilliden til elektroniske signaturer, jf.

dog Rådets forordning (EF) nr. 3381/94 af 19. december 1994 om en fællesskabsordning for kontrol med udførsel af varer med dobbelt anvendelse ⁽⁵⁾ og afgørelse 94/942/FUSP af 19. december 1994 om en fælles aktion vedtaget af Rådet vedrørende kontrol med udførslen af varer med dobbelt anvendelse ⁽⁶⁾;

- (6) dette direktiv harmoniserer ikke levering af tjenesteydelser med hensyn til informationens fortrolige karakter, hvis disse ydelser er omfattet af nationale bestemmelser med »ordre public« eller offentlig sikkerhed;
- (7) det indre marked sikrer den fri bevægelighed for personer, hvorfor unionsborgere og andre, der er bosat i EU, i stigende omfang har behov for kontakt med myndigheder i andre medlemsstater end den, hvori de er bosiddende; elektronisk kommunikation vil kunne blive til stor nytte i den forbindelse;
- (8) den hastige teknologiske udvikling og Internettets globale karakter nødvendiggør, at den valgte metode er åben for forskellige teknologier og tjenester til elektronisk autentifikation af data;
- (9) elektroniske signaturer vil blive anvendt i mange forskellige situationer og i forbindelse med meget forskellige applikationer, hvilket vil resultere i en lang række nye tjenesteydelser og produkter i relation til elektroniske signaturer; definitionen af sådanne produkter og tjenesteydelser bør ikke begrænses til udstedelse og forvaltning af certifikater, men bør også omfatte alle andre tjenesteydelser eller produkter, der anvender eller understøtter elektroniske signaturer, såsom registreringstjenester, tidsstempeling, katalogtjenester, databehandlingstjenester eller konsulenttjenester i forbindelse med elektroniske signaturer;
- (10) det indre marked giver certificeringstjenesteudbydere mulighed for at udvikle deres aktiviteter hen over grænserne med henblik på at øge deres konkurrenceevne og dermed tilbyde forbrugere og erhvervsliv nye muligheder for sikker elektronisk informationsudveksling og handel uden hensyn til grænser; certificeringstjenesteudbydere bør for at stimulere udbuddet af certificeringstjenesteydelser via åbne net i hele Fællesskabet frit kunne tilbyde deres tjenesteydelser uden forudgående autorisation; ved forudgående autorisation forstås ikke alene enhver

⁽¹⁾ EFT C 325 af 23.10.1998, s. 5.

⁽²⁾ EFT C 40 af 15.2.1999, s. 29.

⁽³⁾ EFT C 93 af 6.4.1999, s. 33.

⁽⁴⁾ Europa-Parlamentets udtalelse af 13. januar 1999 (EFT C 104 af 14.4.1999, s. 49), Rådets fælles holdning af 28. juni 1999 (EFT C 243 af 27.8.1999, s. 33), Europa-Parlamentets afgørelse af 27. oktober 1999 (endnu ikke offentliggjort i EFT) og Rådets afgørelse af 30. november 1999 (endnu ikke offentliggjort i EFT).

⁽⁵⁾ EFT L 367 af 31.12.1994, s. 1. Forordningen er ændret ved forordning (EF) nr. 837/95 (EFT L 90 af 21.4.1995, s. 1).

⁽⁶⁾ EFT L 367 af 31.12.1994, s. 8. Afgørelsen er senest ændret ved afgørelse 1999/193/FUSP (EFT L 73 af 19.3.1999, s. 1).

tilladelse, hvis udstedelse forudsætter, at de nationale myndigheder træffer en afgørelse, inden certificeringstjenesteudbyderen kan udbyde sine certificeringstjenester, men også enhver anden foranstaltning med samme virkning;

- (11) frivillige akkrediteringsordninger, hvis sigte er et tjenesteydelsesudbud på et mere avanceret niveau, kunne være den rette ramme for certificeringstjenesteudbydere til at udvikle deres tjenester yderligere i retning af det tillids-, sikkerheds- og kvalitetsniveau, som et marked i hastig udvikling kræver; sådanne ordninger bør anspore udviklingen af optimal praksis blandt certificeringstjenesteudbydere; det bør stå certificeringstjenesteudbydere frit for, om de ønsker at tilslutte sig og nyde godt af sådanne ordninger;
- (12) certificeringstjenesterne bør kunne udbydes enten af et offentligt organ eller en fysisk eller juridisk person oprettet i overensstemmelse med national ret; medlemsstaterne bør ikke forhindre certificeringstjenesteudbydere i at holde sig uden for sådanne akkrediteringsordninger; det bør sikres, at frivillige akkrediteringsordninger ikke svækker konkurrencen blandt certificeringstjenester;
- (13) medlemsstaterne kan selv fastsætte, hvordan de vil sikre overvågningen af overholdelsen af direktivets bestemmelser; dette direktiv er ikke til hinder for indførelsen af overvågningssystemer, der baseres på den private sektor; direktivet forpligter ikke certificeringstjenesteudbydere til at ansøge om at blive overvåget i henhold til en gældende akkrediteringsordning;
- (14) det er vigtigt at finde den rigtige balance mellem forbrugernes og erhvervslivets behov;
- (15) bilag III omfatter krav til sikre signaturgenereringssystemer med henblik på at sikre, at avancerede elektroniske signaturer fungerer hensigtsmæssigt; det omfatter ikke det samlede omgivende miljø, som systemerne opererer i; for at det indre marked kan fungere efter hensigten, er det påkrævet, at Kommissionen og medlemsstaterne handler hurtigt med henblik på at muliggøre udpegelsen af de organer, der skal foretage overensstemmelsesvurderingen af sikre signatursystemer, jf. bilag III; for at imødekomme markedets behov bør overensstemmelsesvurderingen være rettidig og effektiv;
- (16) dette direktiv bidrager til anvendelse og retlig anerkendelse af elektroniske signaturer i Fællesskabet; der er ikke behov for lovfæstede rammebestemmelser for elektroniske signaturer, der udelukkende anvendes inden for systemer, som er baseret på frivillige privatretlige aftaler mellem et afgrænset antal deltagere; parternes frihed til indbyrdes at aftale, på hvilke betingelser de vil acceptere elektronisk signerede data, bør respekteres i det omfang, national ret tillader det; elektroniske signaturer, der anvendes i sådanne systemer, bør ikke nægtes retlig gyldighed og anerkendelse som bevis under retssager;
- (17) det er ikke dette direktivs mål at harmonisere national aftaleret, herunder især regler om kontraktindgåelse og -opfyldelse eller andre ikke-aftaleretlige formkrav vedrørende underskrifter; derfor bør bestemmelserne om elektroniske signaturers retsvirkninger ikke bevare formkrav til indgåelse af kontrakter eller regler til bestemmelse af, hvor en kontrakt er indgået, som er fastsat i national ret;
- (18) opbevaring og kopiering af signaturgenereringsdata vil kunne udgøre en alvorlig trussel mod elektroniske signaturers juridiske gyldighed;
- (19) elektroniske signaturer vil blive anvendt i den offentlige sektor inden for nationale forvaltninger og fællesskabsforvaltninger samt i kommunikationen mellem disse og med borgere og erhvervslivet, for eksempel i forbindelse med offentlige indkøb, beskatning, social sikkerhed, sundheds- og retsvæsenet;
- (20) harmoniserede kriterier vedrørende retsvirkningen af elektroniske signaturer vil gøre det muligt at bevare en sammenhængende retlig ramme i hele Fællesskabet; der er i de nationale lovgivninger fastlagt forskellige krav for at anse håndskrevne underskrifter for juridisk gyldige; certifikater kan anvendes til at certificere identiteten af en person, der underskriver elektronisk; avancerede elektroniske signaturer, som er baseret på kvalificerede certifikater, tilsigter at skabe et højt sikkerhedsniveau; avancerede elektroniske signaturer, som er baseret på kvalificerede certifikater, og som er genereret af et sikkert signaturgenereringssystem, kan kun betragtes som retligt ligestillede med håndskrevne underskrifter, hvis kravene til håndskrevne underskrifter er opfyldt;
- (21) for at bidrage til at gøre elektroniske certificeringsmetoder almindeligt accepteret bør det sikres, at elektroniske signaturer kan anvendes som bevis ved retshandlinger i alle medlemsstater; den retlige anerkendelse af elektroniske signaturer bør hvile på objektive kriterier og ikke afhænge af den berørte certificeringstjenesteudbyders eventuelle akkreditering; fastlæggelsen af de retsområder, hvor der kan anvendes elektroniske dokumenter og elektroniske signaturer, reguleres i national lovgivning; dette direktiv indskrænker ikke nationale domstoles kompetence til at træffe afgørelse om, hvorvidt kravene i dette direktiv er overholdt, og berører ikke nationale bestemmelser om domstolenes fri bevisbedømmelse;
- (22) certificeringstjenesteudbydere, der udbyder certificeringstjenester til offentligheden, er underkastet nationale erstatningsansvarsregler;
- (23) udviklingen i international elektronisk handel kræver grænseoverskridende ordninger, der involverer tredjelande; for at sikre global interoperabilitet kan det være hensigtsmæssigt at indgå aftaler med tredjelande om multilaterale regler for gensidig anerkendelse af certificeringstjenester;

- (24) med henblik på at øge brugeles tillid til elektronisk kommunikation og elektronisk handel skal certificeringstjenesteudbydere overholde lovgivningen om databeskyttelse og privatlivets fred;
- (25) bestemmelserne om brug af pseudonymer i certifikater bør ikke være til hinder for, at medlemsstaterne kan håndhæve krav om identifikation af personer i henhold til Fællesskabets lovgivning eller national lovgivning;
- (26) de nødvendige gennemførelsesforanstaltninger til dette direktiv vedtages i overensstemmelse med Rådets afgørelse 1999/468/EF af 28. juni 1999 om fastsættelse af de nærmere vilkår for udøvelsen af de gennemførelsesbeføjelser, der tillægges Kommissionen ⁽¹⁾;
- (27) Kommissionen bør foretage en vurdering af dette direktiv to år efter dets gennemførelse bl.a. med henblik på at sikre, at hverken den teknologiske udvikling eller juridiske ændringer bliver til hinder for opfyldelsen af målene i dette direktiv; Kommissionen bør undersøge virkningerne af beslægtede tekniske områder og forelægge Europa-Parlamentet og Rådet en rapport herom;
- (28) målsætningen om at skabe en harmoniseret retlig ramme for udbud af elektroniske signaturer og beslægtede tjenester kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor i overensstemmelse med subsidiaritets- og proportionalitetsprincipperne som omhandlet i traktatens artikel 5 bedre gennemføres af Fællesskabet; dette direktiv går ikke ud over, hvad der er nødvendigt for at nå dette mål —
- 2) »avanceret elektronisk signatur«: en elektronisk signatur, som opfylder følgende krav:
- a) den er entydigt knyttet til underskriveren
 - b) den kan identificere underskriveren
 - c) den genereres med midler, som underskriveren kan bevare den fulde kontrol med, og
 - d) den er knyttet til de data, som den vedrører, på en sådan måde, at en hvilken som helst senere ændring af disse data kan opdages
- 3) »underskriver«: en person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af den fysiske eller juridiske person eller det organ, som vedkommende repræsenterer
- 4) »signaturgenereringsdata«: unikke data, som f.eks. koder eller private krypteringsnøgler, som anvendes af underskriveren til generering af en elektronisk signatur
- 5) »signaturgenereringssystem«: konfigureret software eller hardware til behandling af signaturgenereringsdata
- 6) »sikkert signaturgenereringssystem«: et signaturgenereringssystem, der opfylder kravene i bilag III
- 7) »signaturverificeringsdata«: data, som f.eks. koder eller offentlige krypteringsnøgler, der anvendes til kontrol af den elektroniske signatur
- 8) »signaturverificeringssystem«: konfigureret software eller hardware til behandling af signaturverificeringsdata
- 9) »certifikat«: en elektronisk attestering, som knytter signaturverificeringsdata til en person og bekræfter denne persons identitet
- 10) »kvalificeret certifikat«: et certifikat, som opfylder kravene i bilag I og leveres af en certificeringstjenesteudbyder, som opfylder kravene i bilag II
- 11) »certificeringstjenesteudbyder«: et organ eller en fysisk eller juridisk person, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektroniske signaturer
- 12) »elektronisk signatur-produkt«: hardware eller software eller relevante komponenter heraf, som er beregnet til at blive brugt af en certificeringstjenesteudbyder til levering af tjenesteydelser i forbindelse med elektronisk signatur eller beregnet til at blive brugt i forbindelse med generering eller verificering af elektroniske signaturer
- 13) »frivillig akkreditering«: enhver tilladelse, der fastsætter rettigheder og forpligtelser, der er særlige for certificeringstjenester, og som efter anmodning fra den pågældende certificeringstjenesteudbyder tildeles denne af det offentlige eller private organ, der har til opgave at udarbejde og føre tilsyn med overholdelsen af sådanne rettigheder og forpligtelser, og hvor certificeringstjenesteudbyderen ikke er berettiget til at udøve de rettigheder, som tilladelsen giver, før denne har modtaget organets afgørelse.

UDSTEDT FØLGENDE DIREKTIV:

Artikel 1

Anvendelsesområde

Formålet med dette direktiv er at lette brugen af elektroniske signaturer og bidrage til disses retlige anerkendelse. Det fastlægger en retlig ramme for elektroniske signaturer og visse certificeringstjenester, for at det indre marked kan fungere efter hensigten.

Det omfatter ikke aspekter i forbindelse med kontraktens indgåelse og gyldighed eller andre retlige forpligtelser, som ifølge national ret eller fællesskabsret er undergivet formkrav, og det berører heller ikke de regler og begrænsninger, der efter national ret eller fællesskabsret gælder for anvendelsen af dokumenter.

Artikel 2

Definitioner

I dette direktiv forstås ved:

- 1) »elektronisk signatur«: data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes som en autentifikationsmetode

⁽¹⁾ EFT L 184 af 17.7.1999, s. 23.

Artikel 3

Markedsadgang

1. Medlemsstaterne må ikke gøre udbud af certificeringstjenesteydelser afhængigt af forudgående autorisation.

2. Med forbehold af stk. 1 kan medlemsstaterne indføre eller opretholde frivillige akkrediteringsordninger med henblik på at højne niveauet for ydelse af certificeringstjenester. Alle vilkår i forbindelse med sådanne ordninger skal være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende. Medlemsstaterne kan ikke af årsager, der falder ind under dette direktivs anvendelsesområde, begrænse antallet af akkrediterede certificeringstjenesteudbydere.

3. Medlemsstaterne sikrer, at der indføres et passende system til kontrol af certificeringstjenesteudbydere, der er etableret på deres område, og som udbyder kvalificerede certifikater til offentligheden.

4. Egnede offentlige eller private organer, som udpeges af medlemsstaterne, afgør, om sikre signaturgeringssystemer opfylder kravene i bilag III. Kommissionen fastlægger efter proceduren i artikel 9 kriterier, ud fra hvilke medlemsstaterne afgør, om et organ er egnet til at blive udpeget.

Medlemsstaterne anerkender de afgørelser, som de organer, der er nævnt i første afsnit, træffer for så vidt angår opfyldelsen af kravene i bilag III.

5. Kommissionen kan efter proceduren i artikel 9 fastsætte og i *De Europæiske Fællesskabers Tidende* offentliggøre referencenumre på almindeligt anerkendte standarder for elektroniske signatur-produkter. Medlemsstaterne formoder, at et elektronisk signatur-produkt overholder kravene i bilag II, litra f), og bilag III, hvis det overholder sådanne standarder.

6. Medlemsstaterne og Kommissionen samarbejder med henblik på at fremme udviklingen og brugen af signaturverificeringssystemer på baggrund af anbefalingerne vedrørende signaturverificering i bilag IV og under hensyn til forbrugernes interesser.

7. Medlemsstaterne kan gøre anvendelse af elektroniske signaturer i den offentlige sektor afhængig af opfyldelsen af eventuelle supplerende krav. Sådanne krav skal være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende, og må kun være affødt af den pågældende anvendelses særlige karakter. Kravene må ikke hindre grænseoverskridende tjenesteydelser til borgerne.

Artikel 4

Principper vedrørende det indre marked

1. Medlemsstaterne anvender de nationale bestemmelser, som de vedtager i henhold til dette direktiv, på certificeringstjenesteudbydere, der er etableret på deres område, og på disses tjenesteydelser. Medlemsstaterne kan ikke på områder, der er

omfattet af dette direktiv, pålægge ydelse af certificeringstjenester med oprindelse i en anden medlemsstat begrænsninger.

2. Medlemsstaterne sikrer fri bevægelighed inden for det indre marked for elektroniske signatur-produkter, der overholder bestemmelserne i dette direktiv.

Artikel 5

Retsvirkninger af elektroniske signaturer

1. Medlemsstaterne sikrer, at avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, og som er genereret af et sikkert signaturgeringssystem,

a) opfylder retskravene til en signatur i forbindelse med data i elektronisk form, på samme måde som en håndskreven underskrift opfylder disse krav i forbindelse med papirbaserede data, og

b) kan godtages som bevismateriale under retssager.

2. Medlemsstaterne sikrer, at en elektronisk signatur ikke nægtes retlig gyldighed og anerkendelse som bevis under retssager alene af den grund, at den

— er i elektronisk form, eller

— ikke er baseret på et kvalificeret certifikat, eller

— ikke er baseret på et kvalificeret certifikat udstedt af en akkrediteret certificeringstjenesteudbyder, eller

— ikke er genereret af et sikkert signaturgeringssystem.

Artikel 6

Erstatningsansvar

1. Medlemsstaterne sikrer som et minimum, at en certificeringstjenesteudbyder, der udsteder et certifikat som kvalificeret certifikat til offentligheden, eller som garanterer et sådant certifikat over for offentligheden, ifalder erstatningsansvar for tab, der påføres ethvert organ eller enhver fysisk eller juridisk person, som med rimelighed forlader sig på certifikatet for så vidt angår:

a) korrektheden af alle oplysningerne i det kvalificerede certifikat på udstedelsestidspunktet og certifikatets indhold af alle de for et kvalificeret certifikat foreskrevne angivelser

b) sikkerhed for, at den i det kvalificerede certifikat identificerede underskriver på udstedelsestidspunktet var i besiddelse af de signaturgeringsdata, der svarer til de i certifikatet indeholdte eller omhandlede signaturverificeringsdata

c) sikkerhed for, at signaturgerings- og signaturverificeringsdataene kan anvendes komplementært med hinanden i de tilfælde, hvor det er certificeringstjenesteudbyderen, der genererer begge datasæt,

medmindre certificeringstjenesteudbyderen kan bevise, at han ikke har handlet uagtsomt.

2. Medlemsstaterne sikrer som et minimum, at en certificeringstjenesteudbyder, der har udstedt et certifikat som et kvalificeret certifikat til offentligheden, er erstatningsansvarlig for tab, der påføres ethvert organ eller enhver fysisk eller juridisk person, som med rimelighed forlader sig på certifikatet, for så vidt angår manglende registrering af tilbagekaldelse af certifikatet, medmindre certificeringstjenesteudbyderen kan bevise, at han ikke har handlet uagtsomt.

3. Medlemsstaterne sikrer, at en certificeringstjenesteudbyder i et kvalificeret certifikat kan anføre begrænsninger i dette certifikats anvendelsesområde, idet disse begrænsninger skal være tydelige for tredjeparter. Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes brug af et kvalificeret certifikat, som overskrider begrænsningerne i dets anvendelsesområde.

4. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen i et kvalificeret certifikat kan sætte en beløbsgrænse for de transaktioner, som certifikatet kan anvendes til, og at denne beløbsgrænse er tydelig for tredjeparter.

Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes en overskridelse af denne beløbsgrænse.

5. Stk. 1-4 berører ikke Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler⁽¹⁾.

Artikel 7

Internationale aspekter

1. Medlemsstaterne sikrer, at certifikater, der er udstedt som kvalificerede certifikater til offentligheden af en certificeringstjenesteudbyder, der er etableret i et tredjeland, anses for at være retligt ligestillede med certifikater, der er udstedt af en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet:

- a) hvis certificeringstjenesteudbyderen opfylder kravene i dette direktiv og er akkrediteret under en frivillig akkrediteringsordning i en medlemsstat, eller
- b) hvis en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet, og som opfylder kravene i dette direktiv, garanterer certifikatet, eller
- c) hvis certifikatet eller certificeringstjenesteudbyderen er anerkendt i henhold til en bilateral eller multilateral aftale mellem Fællesskabet og tredjelande eller internationale organisationer.

2. For at lette grænseoverskridende certificeringstjenester med tredjelande og retlig anerkendelse af avancerede elektroniske signaturer med oprindelse i tredjelande fremsætter Kommissionen i givet fald forslag med henblik på den faktiske implementering af standarder og internationale aftaler om certificeringstjenester. Kommissionen forelægger, hvis det er nødvendigt, Rådet forslag til passende mandater til forhandling af bilaterale og multilaterale aftaler med tredjelande og internationale organisationer. Rådet træffer afgørelse med kvalificeret flertal.

⁽¹⁾ EFT L 95 af 21.4.1993, s. 29.

3. Når Kommissionen underrettes om vanskeligheder, som EF-virksomheder støder på ved markedsføringen i tredjelande, kan den om nødvendigt forelægge forslag til Rådet til et passende mandat med henblik på forhandling af tilsvarende rettigheder for EF-virksomheder i disse tredjelande. Rådet træffer afgørelse med kvalificeret flertal.

Foranstaltninger, der træffes i henhold til dette stykke, berører ikke Fællesskabets og medlemsstaternes forpligtelser i henhold til relevante internationale aftaler.

Artikel 8

Databeskyttelse

1. Medlemsstaterne sikrer, at certificeringstjenesteudbyderne og de nationale akkrediterings- og tilsynsorganer opfylder kravene i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger⁽²⁾.

2. Medlemsstaterne sikrer, at den certificeringstjenesteudbyder, der udsteder certifikatet til offentligheden, kun har tilladelse til at opnå persondata direkte fra den registrerede eller med den registreredes udtrykkelige tilladelse og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat. Data må ikke indsamles eller behandles til noget andet formål uden den registreredes udtrykkelige samtykke.

3. Uden at den retsvirkning, der tillægges pseudonymer i henhold til den nationale lovgivning dermed foregribes, må medlemsstaterne ikke forhindre, at certificeringstjenesteudbyderen på certifikatet anfører et pseudonym i stedet for underskriverens navn.

Artikel 9

Udvalg

1. Kommissionen bistås af et elektronisk signatur-udvalg, i det følgende benævnt »udvalget«.

2. Når der henvises til dette stykke, anvendes artikel 4 og 7 i afgørelse 1999/468/EF under overholdelse af bestemmelserne i afgørelsens artikel 8.

Den frist, der er omhandlet i artikel 4, stk. 3, i afgørelse 1999/468/EF, fastsættes til tre måneder.

3. Udvalget vedtager selv sin forretningsorden.

Artikel 10

Udvalgets hverv

Udvalget skal efter proceduren i artikel 9, stk. 2, præcisere de krav, der er fastlagt i bilagene, de kriterier, som er omhandlet i artikel 3, stk. 4, samt de alment anerkendte standarder for elektroniske signatur-produkter, der er indført og offentliggjort i henhold til artikel 3, stk. 5.

⁽²⁾ EFT L 281 af 23.11.1995, s. 31.

Artikel 11

Meddelelse

1. Medlemsstaterne meddeler Kommissionen og de øvrige medlemsstater følgende:

- a) oplysninger om frivillige nationale akkrediteringsordninger, herunder alle supplerende krav i henhold til artikel 3, stk. 7
- b) navn og adresse på nationale akkrediterings- og tilsynsorganer og på de organer, som er omhandlet i artikel 3, stk. 4
- c) navn og adresse på alle akkrediterede nationale certificeringstjenesteudbydere.

2. Medlemsstaterne meddeler alle oplysninger i henhold til stk. 1 samt ændringer heraf så hurtigt som muligt.

Artikel 12

Revision

1. Kommissionen foretager en vurdering af, hvordan dette direktiv fungerer, og aflægger rapport herom til Europa-Parlamentet og Rådet senest den 19. juli 2003.

2. I vurderingen tages der bl.a. stilling til, om direktivets anvendelsesområde bør ændres under hensyn til den teknologiske, markedsmæssige og retlige udvikling. Rapporten skal på grundlag af de indhøstede erfaringer navnlig omfatte en bedømmelse af harmoniseringsaspekterne. Rapporten ledsages om fornødent af forslag til retsfor skrifter.

Artikel 13

Gennemførelse

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv

inden den 19. juli 2001. De underretter straks Kommissionen herom.

Disse love og administrative bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastlægges af medlemsstaterne.

2. Medlemsstaterne meddeler Kommissionen de væsentligste nationale retsfor skrifter, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 14

Ikrafttræden

Dette direktiv træder i kraft på dagen for offentliggørelsen i *De Europæiske Fællesskabers Tidende*.

Artikel 15

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 13. december 1999.

På Europa-Parlamentets vegne

N. FONTAINE

Formand

På Rådets vegne

S. HASSI

Formand

BILAG I

Krav til kvalificerede certifikater

Kvalificerede certifikater skal indeholde:

- a) angivelse af, at certifikatet er udstedt som et kvalificeret certifikat
- b) den udstedende certificeringstjenesteudbyders identifikation og den stat som vedkommende er etableret i
- c) underskriverens navn eller pseudonym; i sidstnævnte tilfælde skal det fremgå, at der er tale om et pseudonym
- d) særlige oplysninger om underskriveren, der tilføjes, hvis det er relevant, afhængigt af formålet med certifikatet
- e) de signaturverificeringsdata, som svarer til de signaturgenereringsdata, som er under underskriverens kontrol
- f) certifikatets ikrafttrædelses- og udløbsdato
- g) certifikatets identifikationskode
- h) den udstedende certificeringstjenesteudbyders avancerede elektroniske signatur
- i) eventuelle begrænsninger i certifikatets anvendelsesområde, og
- j) eventuelle beløbsmæssige begrænsninger med hensyn til de transaktioner, for hvilke certifikatet kan anvendes.

BILAG II

Krav til certificeringstjenesteudbydere, der udsteder kvalificerede certifikater

Certificeringstjenesteudbydere

- a) skal udvise den fornødne pålidelighed til at kunne udbyde certificeringstjenester
- b) skal sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste
- c) skal sikre, at det er muligt at fastslå datoen og tidspunktet for udstedelsen eller tilbagekaldelsen af et certifikat
- d) skal med hensigtsmæssige midler og i overensstemmelse med national ret kontrollere identiteten og eventuelt særlige forhold i forbindelse med de personer, til hvem der udstedes kvalificerede certifikater
- e) skal beskæftige personale med den ekspertviden og de erfaringer og kvalifikationer, som de tilbudte tjenesteydelser kræver, navnlig ledelseskompetence, sagkundskab inden for elektronisk signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer; de skal også anvende adækvate administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder
- f) skal anvende pålidelige systemer og produkter, som er beskyttet mod ændringer, og som garanterer de af disse systemer og produkter understøttede processers tekniske og kryptografiske sikkerhed
- g) skal træffe foranstaltninger imod forfalskning af certifikater, og, hvis certificeringstjenesteudbyderen genererer signaturgenereringsdata, garantere disse datas fortrolighed under genereringsprocessen
- h) skal til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomheden i overensstemmelse med dette direktivs krav, navnlig til at bære erstatningsansvaret, f.eks. ved at tegne en passende forsikring
- i) skal registrere alle relevante oplysninger om kvalificerede certifikater i en rimelig periode, navnlig for at kunne fremlægge bevis for certificering, når det er påkrævet i retssager. Denne registrering kan ske elektronisk
- j) må ikke opbevare eller kopiere de personers signaturgenereringsdata, som certificeringstjenesteudbyderen har tilbudt nøglehåndteringstjenester
- k) skal, inden de indgår i et kontraktforhold med en person, der søger at opnå et certifikat fra dem til støtte for sin elektroniske signatur, gennem et bestandigt kommunikationsmedium underrette denne person om de nøjagtige vilkår for anvendelsen af certifikatet, herunder eventuelle begrænsninger i brugen heraf, eksistensen af en eventuel frivillig akkrediteringsordning og procedurer for klager og bilæggelse af tvister. Sådanne oplysninger, som kan sendes elektronisk, skal gives skriftligt og i et umiddelbart forståeligt sprog. De relevante dele af disse oplysninger skal efter anmodning også stilles til rådighed for tredjemand, der forlader sig på certifikatet
- l) skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form, således at
 - kun bemyndigede personer kan foretage tilføjelser og ændringer
 - oplysningernes ægthed kan kontrolleres
 - certifikaterne kun er offentligt tilgængelige i de tilfælde, hvor indehaveren har givet sit samtykke, og
 - eventuelle tekniske ændringer, som bringer disse sikkerhedskrav i fare, er synlige for operatøren.

BILAG III

Krav til sikre elektroniske signaturgerereringssystemer

1. Sikre signaturgerereringssystemer skal ved hjælp af passende og tekniske og proceduremæssige midler i det mindste sikre, at:
 - a) signaturgerereringsdata, der anvendes til signaturgererering, i praksis kun kan fremtræde én gang, og at de med rimelig sikkerhed forbliver hemmelige
 - b) signaturgerereringsdata, der anvendes til signaturgererering, med rimelig sikkerhed ikke kan udledes, og at signaturen er beskyttet mod forfalskning under anvendelse af eksisterende teknologi
 - c) signaturgerereringsdata, der anvendes til signaturgererering, på pålidelig vis kan beskyttes af den retmæssige underskriver mod andres brug.
2. Sikre signaturgerereringssystemer må ikke ændre de data, som skal underskrives, eller hindre, at disse data vises for underskriveren forud for signaturprocessen.

BILAG IV

Anbefalinger vedrørende signaturverificering

I løbet af signaturverificeringsprocessen bør der skabes rimelig sikkerhed for, at:

- a) de data, der anvendes til verificering af signaturen, svarer til de data, som vises kontrolløren
- b) signaturen verificeres på pålidelig vis, og at resultatet af denne verificering vises korrekt
- c) kontrolløren om nødvendigt på pålidelig vis kan fastslå indholdet af de underskrevne data
- d) certifikatets ægthed og gyldighed, som kræves på tidspunktet for signaturverificeringen, verificeres på pålidelig vis
- e) resultatet af verificeringen og underskriverens identitet vises på korrekt vis
- f) anvendelsen af pseudonym klart fremgår
- g) eventuelle sikkerhedsrelevante ændringer kan spores.

B I L A G 2

I

(Retsakter hvis offentliggørelse er obligatorisk)

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 2000/31/EF

af 8. juni 2000

om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel,
i det indre marked
(»Direktivet om elektronisk handel«)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE
UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske
Fællesskab, særlig artikel 47, stk. 2, artikel 55 og artikel 95,

under henvisning til forslag fra Kommissionen⁽¹⁾,

under henvisning til udtalelse fra Det Økonomiske og Sociale
Udvalg⁽²⁾,

i henhold til fremgangsmåden i traktatens artikel 251⁽³⁾, og

ud fra følgende betragtninger:

- (1) Den Europæiske Union har som mål at skabe stadig tættere bånd mellem de europæiske stater og folk for at sikre økonomiske og sociale fremskridt; i henhold til traktatens artikel 14, stk. 2, indebærer det indre marked et område uden indre grænser med fri bevægelighed for varer og tjenesteydelser samt fri etableringsret; udviklingen af informationssamfundstjenester i et område uden indre grænser er afgørende for fjernelsen af de barrierer, der deler de europæiske folk.
- (2) Udviklingen af den elektroniske handel i informations-samfundet indebærer store muligheder for beskæftigelsen i Fællesskabet, især i de små og mellemstore virksomheder, og vil stimulere den økonomiske vækst og de europæiske virksomheders investeringer i innovation, samtidig med at den også kan øge den europæiske industris konkurrenceevne, hvis Internettet gøres tilgængeligt for alle.

- (3) Fællesskabsretten og Fællesskabets retsorden har stor betydning for at gøre det muligt for Europas borgere og aktører fuldt ud og uden hensyn til grænser at udnytte de muligheder, der er forbundet med elektronisk handel; dette direktiv har således til formål at sikre et højt lovgivningsmæssigt integrationsniveau i Fællesskabet på området, så der opstår et reelt område uden indre grænser for informationssamfundstjenester.

- (4) Det er vigtigt at sikre, at elektronisk handel kan udnytte det indre marked fuldt ud og derfor, at der opnås et højt integrationsniveau i Fællesskabet, således som det er tilfældet i forbindelse med Rådets direktiv 89/552/EØF af 3. oktober 1989 om samordning af visse love og administrative bestemmelser i medlemsstaterne vedrørende udøvelse af tv-radiospredningsvirksomhed⁽⁴⁾.

- (5) Udviklingen af informationssamfundstjenester i Fællesskabet hæmmes af en række retlige hindringer for et velfungerende indre marked, hvilket gør udøvelsen af etableringsfriheden og den frie udveksling af tjenesteydelser mindre attraktiv; hindringerne skyldes, at de nationale lovgivninger er forskellige, og at der hersker retsikkerhed med hensyn til, hvilke nationale regler der finder anvendelse på sådanne tjenester; da lovgivningerne på de pågældende områder ikke er koordineret eller tilpasset hinanden, kan hindringerne efter De Europæiske Fællesskabers Domstols retspraksis være berettigede; der hersker retsikkerhed med hensyn til, i hvilket omfang medlemsstaterne kan føre kontrol med tjenester fra en anden medlemsstat.

⁽¹⁾ EFT C 30 af 5.2.1999, s. 4.

⁽²⁾ EFT C 169 af 16.6.1999, s. 36.

⁽³⁾ Europa-Parlamentets udtalelse af 6.5.1999 (EFT C 279 af 1.10.1999, s. 389), Rådets fælles holdning af 28.2.2000 (EFT C 128 af 8.5.2000, s. 32) og Europa-Parlamentets afgørelse af 4.5.2000 (endnu ikke offentliggjort i EFT).

⁽⁴⁾ EFT L 298 af 17.10.1989, s. 23. Direktivet er senest ændret ved Europa-Parlamentets og Rådets direktiv 97/36/EF (EFT L 202 af 30.7.1997, s. 60).

- (6) Af hensyn til Fællesskabets mål og på baggrund af traktatens artikel 43 og 49 og den afledte fællesskabsret bør disse hindringer fjernes gennem koordinering af visse nationale lovgivninger og præcisering på fællesskabsplan af visse juridiske begreber, i det omfang det er nødvendigt for et velfungerende indre marked; da dette direktiv kun vedrører visse specifikke spørgsmål, som giver anledning til problemer for det indre marked, overholder direktivet fuldt ud kravet i traktatens artikel 5 overensstemmelse med subsidiaritetsprincippet.
- (7) For at sikre retssikkerhed og forbrugernes tillid er det nødvendigt, at dette direktiv fastsætter en klar og generel ramme for visse retlige aspekter af elektronisk handel i det indre marked.
- (8) Formålet med dette direktiv er at skabe en retlig ramme for at sikre fri bevægelighed for informationssamfundstjenester mellem medlemsstaterne og ikke at harmonisere det strafferetlige område som sådant.
- (9) Den frie bevægelighed for informationssamfundstjenester kan i mange tilfælde i fællesskabsretten også være et særligt udtryk for et mere generelt princip, nemlig ytringsfriheden som defineret i artikel 10, stk. 1, i konventionen til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, der er ratificeret af alle medlemsstaterne; derfor må direktiver om levering af informationssamfundstjenester sikre, at denne virksomhed kan udøves frit i lyset af nævnte artikel og kun med forbehold af de begrænsninger, der er omhandlet i nævnte artikels stk. 2 og i traktatens artikel 46, stk. 1; det er ikke hensigten med dette direktiv at anfægte nationale grundlæggende regler og principper for ytringsfriheden.
- (10) I overensstemmelse med proportionalitetsprincippet begrænses dette direktiv til de foranstaltninger, som er strengt nødvendige for at opnå et velfungerende indre marked; hvor det er nødvendigt, at foranstaltninger træffes på fællesskabsplan, og for at sikre et område reelt uden indre grænser for elektronisk handel, skal direktivet sikre en høj grad af beskyttelse af almene hensyn og især beskyttelse af mindreårige, den menneskelige værdighed, forbrugernes og folkesundheden; i henhold til traktatens artikel 152 indgår sundhedsbeskyttelse som et væsentligt led i Fællesskabets politik på andre områder.
- (11) Dette direktiv berører ikke det niveau for beskyttelse af især folkesundheden og forbrugernes interesser, som er fastlagt ved Fællesskabets retsakter, bl.a. Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår⁽¹⁾ og Europa-Parlamentets og Rådets direktiv 97/7/EF af 20. maj 1997 om forbrugerbeskyttelse i forbindelse med aftaler vedrørende fjernsalg⁽²⁾ indeholder væsentlige regler om forbrugerbeskyttelse i kontraktforhold; disse direktiver finder også fuldt ud anvendelse på informationssamfundstjenester; denne gældende fællesskabsret, som fuldt ud finder anvendelse på informationssamfundstjenester, omfatter navnlig også Rådets direktiv 84/450/EØF af 10. september 1984 om vildledende og sammenlignende reklame⁽³⁾, Rådets direktiv 87/102/EØF af 22. december 1986 om indbyrdes tilnærmelse af medlemsstaternes love og administrative bestemmelser om forbrugercredit⁽⁴⁾, Rådets direktiv 93/22/EØF af 10. maj 1993 om investeringsservice i forbindelse med værdipapirer⁽⁵⁾, Rådets direktiv 90/314/EØF af 13. juni 1990 om pakkerejser, herunder pakkeferier og pakketure⁽⁶⁾, Europa-Parlamentets og Rådets direktiv 98/6/EF af 16. februar 1998 om angivelse af priser på forbrugsvarer⁽⁷⁾, Rådets direktiv 92/59/EØF af 29. juni 1992 om produktsikkerhed i almindelighed⁽⁸⁾, Europa-Parlamentets og Rådets direktiv 94/47/EF af 26. oktober 1994 om beskyttelse af køber i forbindelse med visse aspekter ved kontrakter om brugsret til fast ejendom på timesharebasis⁽⁹⁾, Europa-Parlamentets og Rådets direktiv 98/27/EF af 19. maj 1998 om søgsmål med påstand om forbud på området beskyttelse af forbrugernes interesser⁽¹⁰⁾, Rådets direktiv 85/374/EØF af 25. juli 1985 om tilnærmelse af medlemsstaternes administrativt eller ved lov fastsatte bestemmelser om produktansvar⁽¹¹⁾, Europa-Parlamentets og Rådets direktiv 1999/44/EF af 25. maj 1999 om visse aspekter af forbrugerbetaling og garantier i forbindelse hermed⁽¹²⁾, Europa-Parlamentets og Rådets kommende direktiv om fjernsalg af finansielle tjenesteydelser til forbrugere og Rådets direktiv 92/28/EØF af 31. marts 1992 om reklame for lægemidler⁽¹³⁾; nærværende direktiv bør ikke berøre Europa-Parlamentets og Rådets direktiv 98/43/EF af 6. juli 1998 om indbyrdes tilnærmelse af medlemsstaternes love og

(1) EFT L 95 af 21.4.1993, s. 29.

(2) EFT L 144 af 4.6.1997, s. 19.

(3) EFT L 250 af 19.9.1984, s. 17. Direktivet er ændret ved Europa-Parlamentets og Rådets direktiv 97/55/EF (EFT L 290 af 23.10.1997, s. 18).

(4) EFT L 42 af 12.2.1987, s. 48. Direktivet er senest ændret ved Europa-Parlamentets og Rådets direktiv 98/7/EF (EFT L 101 af 1.4.1998, s. 17).

(5) EFT L 141 af 11.6.1993, s. 27. Direktivet er senest ændret ved Europa-Parlamentets og Rådets direktiv 97/9/EF (EFT L 84 af 26.3.1997, s. 22).

(6) EFT L 158 af 23.6.1990, s. 59.

(7) EFT L 80 af 18.3.1998, s. 27.

(8) EFT L 228 af 11.8.1992, s. 24.

(9) EFT L 280 af 29.10.1994, s. 83.

(10) EFT L 166 af 11.6.1998, s. 51. Direktivet er ændret ved direktiv 1999/44/EF (EFT L 171 af 7.7.1999, s. 12).

(11) EFT L 210 af 7.8.1985, s. 29. Direktivet er ændret ved direktiv 1999/34/EF (EFT L 141 af 4.6.1999, s. 20).

(12) EFT L 171 af 7.7.1999, s. 12.

(13) EFT L 113 af 30.4.1992, s. 13.

- administrative bestemmelser om reklame for tobaksvarer og sponsoring til fordel for disse⁽¹⁾, der er vedtaget inden for rammerne af det indre marked, og heller ikke direktiver om beskyttelse af folkesundheden; nærværende direktiv supplerer de informationskrav, der er fastlagt i ovennævnte direktiver og navnlig i direktiv 97/7/EF.
- (12) Det er nødvendigt at holde visse former for aktiviteter uden for dette direktivs anvendelsesområde, da den frie bevægelighed for tjenesteydelser ikke på nuværende tidspunkt kan sikres i henhold til traktaten eller gældende afledt ret; dette berører ikke eventuelle retsakter, som vil være nødvendige for et velfungerende indre marked; skatter og afgifter, især moms, som pålægges en stor del af de tjenesteydelser, der er omhandlet i dette direktiv, skal holdes uden for direktivets anvendelsesområde.
- (13) Dette direktiv tager ikke sigte på at fastlægge bestemmelser om afgiftsmæssige forpligtelser og foregriber ikke udarbejdelsen af fællesskabsinstrumenter om de afgiftsmæssige aspekter af elektronisk handel.
- (14) For beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger gælder alene bestemmelserne i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger⁽²⁾ og i Europa-Parlamentets og Rådets direktiv 97/66/EF af 15. december 1997 om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren⁽³⁾, som fuldt ud finder anvendelse på informationssamfundstjenester; disse direktiver opstiller allerede en fællesskabsretlig ramme inden for personoplysninger, og det er derfor ikke nødvendigt at behandle dette spørgsmål i nærværende direktiv for at sikre, at det indre marked fungerer efter hensigten, især med hensyn til den frie bevægelighed for personoplysninger mellem medlemsstaterne; nærværende direktiv bør gennemføres og anvendes i fuld overensstemmelse med principperne om beskyttelse af personoplysninger, især hvad angår uopfordret kommerciel kommunikation og reglerne om formidleransvar; direktivet kan ikke forhindre anonym brug af åbne netværk som f.eks. Internettet.
- (15) Fortrolig behandling af meddelelser er sikret ved artikel 5 i direktiv 97/66/EF; medlemsstaterne skal i medfør af nævnte direktiv forbyde enhver form for opfangning eller overvågning af sådanne meddelelser af andre end afsenderen og modtageren, bortset fra tilfælde, hvor det er tilladt ifølge loven.
- (16) Udelukkelsen af spil fra anvendelsesområdet for dette direktiv gælder kun hasardspil, lotteri og væddemål, som indebærer, at der gøres en indsats med penge; dette omfatter ikke salgsfremmende konkurrencer eller spil, hvor formålet er at fremme salget af varer eller tjenesteydelser, og hvor der i givet fald kun skal ske betaling i tilfælde af køb af de varer eller tjenesteydelser, som der reklameres for.
- (17) En definition af informationssamfundstjenester findes allerede i fællesskabsretten i Europa-Parlamentets og Rådets direktiv 98/34/EF af 22. juni 1998 om en informationsprocedure med hensyn til tekniske standarder og forskrifter samt forskrifter for informationssamfundstjenester⁽⁴⁾ og i Europa-Parlamentets og Rådets direktiv 98/84/EF af 20. november 1998 om retlig beskyttelse af adgangsstyrede og adgangsstyrede tjenester⁽⁵⁾; denne definition omfatter enhver tjeneste, der normalt leveres mod betaling, og som teleformidles ved hjælp af elektronisk databehandlingsudstyr (herunder digital komprimering) og dataoplagringsudstyr på individuel anmodning af en tjenestemodtager; de tjenester, der henvises til i den vejledende liste i bilag V til direktiv 98/34/EF, og som ikke indebærer databehandling og -oplagring, er ikke omfattet af denne definition.
- (18) Informationssamfundstjenester omfatter en lang række økonomiske aktiviteter, som finder sted online; disse aktiviteter kan navnlig bestå i onlinesalg af varer; aktiviteter som levering af varer som sådan eller af tjenesteydelser offline er ikke omfattet; informationssamfundstjenester er ikke kun begrænset til tjenester, der giver mulighed for onlineindgåelse af kontrakter, men omfatter også, når der er tale om erhvervsmæssig virksomhed, tjenester, som modtageren ikke yder vederlag for, f.eks. tjenester som består i at tilbyde onlineinformation eller kommerciel kommunikation, eller tjenester, som leverer redskaber til at søge, få adgang til og hente data; informationssamfundstjenester omfatter også tjenester, der består i at udsende information via kommunikationsnetværk, give adgang til et kommunikationsnetværk eller være vært for information, som leveres af tjenestemodtageren; tv-radiospredning i den betydning, hvori ordet anvendes i direktiv 89/552/EØF, og radiospredning er ikke informationssamfundstjenester, da de ikke leveres på individuel anmodning; derimod er tjenester, som udsendes punkt til punkt, som f.eks. video on demand eller fremsendelse af kommerciel kommunikation via elektronisk post, informationssamfundstjenester; f.eks. er fysiske personers anvendelse af elektronisk post eller tilsvarende individuel kommunikation uden for deres handelsmæssige eller erhvervsmæssige virksomhed, herunder anvendelse til indgåelse af kontrakter mellem sådanne personer, ikke

(1) EFT L 213 af 30.7.1998, s. 9.

(2) EFT L 281 af 23.11.1995, s. 31.

(3) EFT L 24 af 30.1.1998, s. 1.

(4) EFT L 204 af 21.7.1998, s. 37. Direktivet er ændret ved direktiv 98/48/EF (EFT L 217 af 5.8.1998, s. 18).

(5) EFT L 320 af 28.11.1998, s. 54.

nogen informationssamfundstjeneste; kontraktforholdet mellem en arbejdstager og dennes arbejdsgiver er ikke nogen informationssamfundstjeneste; aktiviteter, der ifølge deres natur ikke kan udføres på afstand og ved hjælp af elektroniske midler såsom lovpligtig revision af selskabsregnskaber eller lægelige vurderinger, der kræver fysisk undersøgelse af patienten, er ikke informationssamfundstjenester.

- (19) Tjenesteyderens etableringssted skal fastlægges i overensstemmelse med Domstolens retspraksis, ifølge hvilken begrebet etableringssted forudsætter, at der rent faktisk udøves erhvervsmæssig virksomhed ved hjælp af en fast indretning i et ikke nærmere angivet tidsrum; dette krav er også opfyldt, når en virksomhed er oprettet for et bestemt tidsrum; etableringsstedet for en virksomhed, der leverer tjenester via en Internet-hjemmeside (website), er ikke det sted, hvor den benyttede teknologi befinder sig, eller det sted, hvor Internet-hjemmesiden er tilgængelig, men det sted, hvor virksomheden udøver sin erhvervsmæssige virksomhed; når en tjenesteyder har flere etableringssteder, er det vigtigt at få fastlagt, fra hvilket etableringssted den pågældende tjeneste leveres; når det er vanskeligt at afgøre, fra hvilket af etableringsstederne en given tjeneste leveres, er det det sted, hvor centret for tjenesteyderens aktiviteter vedrørende denne bestemte tjeneste befinder sig.
- (20) Definitionen på en »tjenestemodtager« omfatter alle former for benyttelse af informationssamfundstjenester både af personer, der giver oplysninger på åbne netværk som f.eks. Internettet, og af personer, der søger oplysninger på Internettet af private eller erhvervsmæssige årsager.
- (21) Anvendelsesområdet for det koordinerede område berører ikke fremtidig fællesskabsharmonisering af informationssamfundstjenester og fremtidig lovgivning, der vedtages på nationalt plan i overensstemmelse med fællesskabsretten; det koordinerede område omfatter kun krav til onlineaktiviteter som f.eks. onlineinformation, online-reklame, onlineshopping og onlineindgåelse af kontrakter og vedrører ikke medlemsstaternes lovbestemte krav til varer som f.eks. sikkerhedskrav, mærkningskrav eller produktansvar eller medlemsstaternes krav til levering eller transport af varer, herunder distribution af lægemidler; det koordinerede område omfatter ikke offentlige myndigheders udøvelse af forkøbsret til visse varer som f.eks. kunstværker.
- (22) Informationssamfundstjenester bør kontrolleres på det sted, hvor tjenesterne udføres, for at sikre en effektiv beskyttelse af almene hensyn; der skal derfor være

sikkerhed for, at den kompetente myndighed yder denne beskyttelse ikke alene for borgerne i det pågældende land, men for alle Fællesskabets borgere; for at fremme den gensidige tillid mellem medlemsstaterne er det absolut nødvendigt, at det klart præciseres, at ansvaret påhviler oprindelseslandet; for effektivt at sikre den frie udveksling af tjenesteydelser og for at skabe retssikkerhed for tjenesteyderne og -modtagerne bør informationssamfundstjenester principielt være underlagt retssystemet i den medlemsstat, hvor tjenesteyderen er etableret.

- (23) Dette direktiv har hverken til formål at opstille yderligere internationale privatretlige regler om lovkonflikter eller at berøre retternes kompetence; bestemmelser om lovvalg i den internationale privatret indskrænker ikke adgangen til at levere informationssamfundstjenester som fastsat i dette direktiv.
- (24) I forbindelse med dette direktiv er det til trods for princippet om kontrol ved kilden af informationssamfundstjenester tilladt, at medlemsstaterne under de omstændigheder, der er fastlagt i dette direktiv, iværksætter foranstaltninger til begrænsning af den frie bevægelighed for informationssamfundstjenester.
- (25) Nationale domstole, herunder civile domstole, der behandler privatretlige tvister, kan træffe foranstaltninger med henblik på at fravige adgangen til at levere informationssamfundstjenester i overensstemmelse med dette direktiv.
- (26) Medlemsstaterne kan i overensstemmelse med betingelserne i dette direktiv anvende deres nationale strafferet og strafferetspleje, når de træffer efterforskningsforanstaltninger og andre foranstaltninger, der er nødvendige for afsløring og retsforfølgning af lovovertrædelser, uden at det er nødvendigt at meddele Kommissionen disse foranstaltninger.
- (27) Nærværende direktiv bidrager sammen med Europa-Parlamentets og Rådets kommende direktiv om fjernsalg af finansielle tjenesteydelser til forbrugerne til at etablere en retlig ramme for onlinelevering af finansielle tjenesteydelser; nærværende direktiv foregriber ikke fremtidige initiativer inden for finansielle tjenesteydelser navnlig med hensyn til harmonisering af adfældsregler på området; medlemsstaternes mulighed ifølge nærværende direktiv for under visse omstændigheder at indskrænke adgangen til at levere informationssamfundstjenester for at beskytte forbrugerne dækker også foranstaltninger vedrørende finansielle tjenesteydelser, navnlig foranstaltninger der tager sigte på at beskytte investorer.

- (28) Medlemsstaternes forpligtelse til ikke at underlægge adgangen til aktiviteten »leverandør af informationssamfundstjenester« krav om forudgående godkendelse gælder ikke posttjenester, som er omfattet af Europa-Parlamentets og Rådets direktiv 97/67/EF af 15. december 1997 om fælles regler for udvikling af Fællesskabets indre marked for posttjenester og forbedring af disse tjenesters kvalitet⁽¹⁾, og som består i fysisk levering af en udskrift af en elektronisk postmeddelelse, og berører ikke frivillige godkendelsesordninger især for ydere af signaturcertifikationstjenester.
- (29) Kommerciel kommunikation er af afgørende betydning for finansieringen af informationssamfundstjenester og for udviklingen af et stort udbud af nye gratis tjenester; af hensyn til forbrugerne og god forretningsskik skal kommerciel kommunikation, herunder rabatter, tilbud og salgsfremmende konkurrencer eller spil, overholde en række krav om gennemsækelighed; disse krav berører ikke direktiv 97/7/EF; nærværende direktiv berører ikke gældende direktiver om kommerciel kommunikation, navnlig direktiv 98/43/EF.
- (30) Fremsendelse af uopfordret kommerciel kommunikation via elektronisk post kan være uønsket af forbrugerne og leverandørerne af informationssamfundstjenester og kan være en hindring for, at interaktive netværk kan være velfungerende; spørgsmålet om modtagerens samtykke i visse tilfælde af uopfordret kommerciel kommunikation behandles ikke i dette direktiv, men er allerede behandlet, især i direktiv 97/7/EF og 97/66/EF; i medlemsstater, som tillader uopfordret kommerciel kommunikation via elektronisk post, bør industriers passende filtreringsinitiativer (industry filtering initiatives) fremmes og lettes; derudover er det nødvendigt, at uopfordret kommerciel kommunikation under alle omstændigheder klart kan identificeres som sådan for at forbedre gennemsækeligheden og gøre det lettere for sådanne initiativer at fungere; uopfordret kommerciel kommunikation via elektronisk post bør ikke resultere i ekstra udgifter for modtageren.
- (31) Medlemsstater, som tillader, at tjenesteydere, der er etableret på deres område, sender uopfordret kommerciel kommunikation via elektronisk post til en modtager uden dennes forudgående samtykke, skal sikre, at tjenesteyderne regelmæssigt konsulterer og respekterer »opt-out-registre«, hvor fysiske personer, der ikke ønsker at modtage sådan kommerciel kommunikation, kan registrere sig.
- (32) For at fjerne barrierer for udviklingen af grænseoverskridende tjenester i Fællesskabet, som udøvere af lovregulerede erhverv kan tilbyde på Internettet, er det nødvendigt, at det på fællesskabsplan sikres, at de faglige regler, der er fastsat for at beskytte bl.a. forbrugerne eller folkesundheden, overholdes; adfærdskodekser på fællesskabsplan er det bedste middel til opstilling af etiske regler for kommerciel kommunikation; der bør tilskyndes til udarbejdelse eller i givet fald til tilpasning af sådanne regler med forbehold af faglige organisationers og sammenslutningers uafhængighed.
- (33) Dette direktiv supplerer fællesskabslovgivningen og den nationale lovgivning om lovregulerede erhverv, hvorved der opretholdes et samlet regelsæt på dette område.
- (34) Hver medlemsstat skal tilpasse sin lovgivning om krav, især formkrav som kan hindre elektronisk indgåelse af kontrakter, der bør foretages en systematisk gennemgang af de lovgivninger, hvor en sådan tilpasning er påkrævet, og gennemgangen skal omfatte alle de nødvendige etaper og led i aftaleindgåelsen, herunder opbevaring af kontrakten; tilpasningen bør resultere i, at det bliver muligt at indgå kontrakter elektronisk; retsvirkningen af elektroniske signaturer er reguleret i Europa-Parlamentets og Rådets direktiv 1999/93/EF af 19. december 1999 om en fællesskabsramme for elektroniske signaturer⁽²⁾; en tjenesteyders modtagelsesbekræftelse kan bestå i onlinelevering af den tjeneste, der leveres mod vederlag.
- (35) Dette direktiv berører ikke medlemsstaternes mulighed for at opretholde eller fastsætte generelle eller specifikke juridiske krav til kontrakter, der kan indgås elektronisk, især krav til sikre elektroniske signaturer.
- (36) Medlemsstaterne kan opretholde begrænsninger for anvendelse af elektroniske kontrakter i forbindelse med kontrakter, der ifølge loven kræver medvirken af domstole, offentlige myndigheder eller erhverv, som udøver offentlig myndighed; denne mulighed omfatter også kontrakter, der kræver medvirken af domstole, offentlige myndigheder eller erhverv, som udøver offentlig myndighed, for at få virkning over for tredjemand, samt kontrakter, der ifølge loven kræver en notars certification eller attestering.
- (37) Medlemsstaternes forpligtelse til at fjerne hindringer for anvendelse af elektroniske kontrakter vedrører kun hindringer, som skyldes juridiske krav, og ikke praktiske hindringer, som skyldes, at det i visse tilfælde er umuligt at anvende elektroniske midler.

(1) EFT L 15 af 21.1.1998, s. 14.

(2) EFT L 13 af 19.1.2000, s. 12.

- (38) Medlemsstaternes forpligtelse til at fjerne hindringer for anvendelse af elektroniske kontrakter skal opfyldes i overensstemmelse med de juridiske krav, der ifølge fællesskabsretten gælder i forbindelse med kontrakter.
- (39) Undtagelser fra bestemmelserne vedrørende kontrakter i forbindelse med oplysninger eller ordreafgivelse, der udelukkende indgås med elektronisk post eller med tilsvarende individuel kommunikation som fastsat i dette direktiv, bør ikke give leverandører af informationssamfundstjenester mulighed for at omgå disse bestemmelser.
- (40) Både eksisterende og nye forskelle i medlemsstaternes lovgivning eller retspraksis med hensyn til tjenesteydernes ansvar, når de optræder som formidlere, er til hinder for et velfungerende indre marked, især fordi de hindrer udviklingen af grænseoverskridende tjenester og medfører konkurrencefordrejning; tjenesteyderne har i visse tilfælde pligt til at handle for at forhindre ulovlig virksomhed eller bringe den til ophør; dette direktivs bestemmelser bør udgøre det rette grundlag for at udarbejde hurtige og pålidelige ordninger, som gør det muligt at fjerne ulovlig information og at hindre adgangen til den; sådanne ordninger bør udarbejdes ved frivillige aftaler mellem alle berørte parter og fremmes af medlemsstaterne; alle de parter, som deltager i levering af informationssamfundstjenester, har interesse i at vedtage og anvende sådanne ordninger; ansvarsbestemmelserne i dette direktiv bør ikke være til hinder for, at de forskellige berørte parter udvikler og faktisk gennemfører tekniske beskyttelses- og identifikationssystemer samt tekniske overvågningsinstrumenter, som er muliggjort af den digitale teknik, inden for de grænser, der er fastsat i direktiv 95/46/EF og 97/66/EF.
- (41) Dette direktiv skaber balance mellem de berørte interesser og indfører principper, som aftaler og normer inden for denne sektor kan baseres på.
- (42) De fritagelser for ansvar, der er fastlagt i dette direktiv, omfatter kun de tilfælde, hvor en informationssamfundstjenesteyders aktivitet er begrænset til den tekniske drift af og indrømmelse af adgang til et kommunikationsnet, hvor informationer, som er stillet til rådighed af tredjemand, transmitteres eller oplagres midlertidigt med det ene formål at gøre transmissionen mere effektiv; denne aktivitet er udelukkende teknisk, automatisk og passiv, hvilket indebærer, at leverandøren af informationssamfundstjenesten hverken har kendskab til eller kontrol over de informationer, der transmitteres eller oplagres.
- (43) En tjenesteyder kan fritages for ansvar for ren viderefremstilling (»mere conduit«) og for caching (automatisk, mellemliggende og midlertidig oplagring), hvis den pågældende på ingen måde er involveret i de informationer, der transmitteres; dette forudsætter bl.a., at den pågældende ikke ændrer de informationer, der transmitteres; dette krav omfatter ikke tekniske manipulationer, der finder sted i løbet af transmissionen, da disse ikke ændrer de transmitterede informationers integritet.
- (44) En tjenesteyder, der bevidst samarbejder med en tjenestemodtager om at begå ulovlige handlinger, overskrider grænserne for ren viderefremstilling eller caching, og den pågældende kan som følge heraf ikke omfattes af de ansvarsfritagelser, der er fastsat for denne form for aktiviteter.
- (45) De begrænsninger i formidleransvaret for tjenesteydere, der fastsættes i dette direktiv, påvirker ikke muligheden for at anvende forskellige former for foreløbige retsmidler; sådanne foreløbige retsmidler kan navnlig bestå i afgørelser fra domstole eller administrative myndigheder, hvori det kræves, at eventuelle overtrædelser bringes til ophør eller forhindres, herunder at ulovlige informationer fjernes, eller at adgangen til dem hindres.
- (46) For at blive omfattet af en ansvarsbegrænsning skal en leverandør af en informationssamfundstjeneste, som består i oplagring af information, når han har fået konkret kendskab til ulovlige aktiviteter, straks tage skridt til at fjerne informationen eller hindre adgangen til den; fjernelsen af informationen eller hindringen af adgangen til den skal foretages under overholdelse af ytringsfriheden og de procedurer, der er fastlagt på nationalt plan med henblik herpå; dette direktiv berører ikke medlemsstaternes mulighed for at fastsætte specifikke krav, som skal opfyldes straks, inden informationen fjernes, eller adgangen til den hindres.
- (47) Kun i forbindelse med generelle forpligtelser kan medlemsstaterne ikke pålægge tjenesteyderne overvågningsforpligtelser; dette vedrører ikke overvågningsforpligtelser i særlige tilfælde og berører navnlig ikke de nationale myndigheders bekendtgørelser i henhold til national lovgivning.
- (48) Dette direktiv berører ikke medlemsstaternes mulighed for at pålægge tjenesteydere, som oplagrer oplysninger, der er fremsendt af modtagere af deres tjeneste, pligt til en sådan agtpågivenhed, som med rimelighed kan forventes af dem, og som der er fastsat bestemmelser om i den nationale lovgivning, med henblik på at afsløre og forhindre visse former for ulovlige aktiviteter.
- (49) Medlemsstaterne og Kommissionen tilskynder til, at der udarbejdes adfærdskodekser; dette ændrer ikke ved sådanne kodekseres frivillige karakter og de berørte parters mulighed for frit at afgøre, om de vil tilslutte sig dem.

- (50) Det er vigtigt, at forslaget til direktivet om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet og nærværende direktiv træder i kraft nogenlunde samtidig med henblik på at opstille et klart regelsæt for spørgsmålet om formidleransvar for overtrædelser af ophavsret og beslægtede rettigheder på fællesskabsplan.
- (51) Hver medlemsstat bør i givet fald tilpasse lovgivning, som kan hindre anvendelsen af regler om udenretslig bilæggelse af tvister ad elektronisk vej; resultatet af denne tilpasning skal være, at det reelt og faktisk bliver muligt retligt og i praksis at få sådanne regler til at fungere, også på tværs af grænserne.
- (52) Den faktiske udøvelse af frihederne i det indre marked kræver, at de, der har lidt skade, sikres reel adgang til instrumenter til bilæggelse af tvister; de skader, der kan opstå i forbindelse med informationssamfundstjenester, er kendetegnet både ved det hurtige tempo, hvori de opstår, og ved deres geografiske udstrækning; som følge af disse særlige kendetegn og nødvendigheden af at påse, at de nationale myndigheder ikke bringer den gensidige tillid i fare, som de skal have til hinanden, opstilles der i dette direktiv det krav, at medlemsstaterne skal sikre, at der er adgang til passende former for søgsmål; medlemsstaterne bør undersøge, om der er behov for at give hensigtsmæssig elektronisk adgang til søgsmål.
- (53) Direktiv 98/27/EF, som finder anvendelse på informationssamfundstjenester, omfatter en mekanisme vedrørende foranstaltninger med henblik på forbud, der tager sigte på beskyttelse af forbrugernes kollektive interesser; denne mekanisme vil bidrage til fri bevægelighed for informationssamfundstjenester ved at sikre et højt forbrugerbeskyttelsesniveau.
- (54) Sanktionerne i henhold til dette direktiv berører ikke andre mulige sanktioner eller retsmidler i medfør af national lovgivning; medlemsstaterne er ikke forpligtet til at fastsætte strafferetlige sanktioner for overtrædelse af nationale bestemmelser, der er udstedt i henhold til dette direktiv.
- (55) Dette direktiv berører ikke den lov, der finder anvendelse på kontraktlige forpligtelser i forbindelse med forbruger-aftaler; dette direktiv kan derfor ikke berøve forbrugeren den beskyttelse, som ydes gennem de ufravigelige regler for kontraktmæssige forpligtelser, der findes i lovgivningen i den medlemsstat, hvor forbrugeren har sin sædvanlige bopæl.
- (56) Hvad angår undtagelsen i dette direktiv, bør kontraktforpligtelser i forbruger-aftaler fortolkes som omfattende oplysninger om de væsentlige elementer i aftaleindholdet, herunder forbrugerrettighederne, som har afgørende betydning for beslutningen om at indgå en aftale.
- (57) Ifølge Domstolens faste retspraksis bevarer en medlemsstat retten til at træffe foranstaltninger over for en tjenesteyder, der er etableret i en anden medlemsstat, men hvis aktivitet udelukkende eller hovedsagelig er rettet mod førstnævnte medlemsstats territorium, såfremt etableringen har fundet sted med det formål at omgå den lovgivning, som tjenesteyderen ville være underlagt, hvis han var etableret på førstnævnte medlemsstats territorium.
- (58) Direktivet bør ikke finde anvendelse på tjenester, der leveres af tjenesteydere etableret i tredjelande; henset til den elektroniske handels globale dimension bør det imidlertid sikres, at Fællesskabets bestemmelser er i overensstemmelse med de internationale regler; dette direktiv berører ikke resultaterne af drøftelser om retlige aspekter i internationale organisationer (bl.a. WTO, OECD og Uncitral).
- (59) Til trods for den elektroniske kommunikations globale karakter er det nødvendigt at koordinere de nationale regulerende foranstaltninger inden for Den Europæiske Union for at undgå en opsplitning af det indre marked og for at få etableret en hensigtsmæssig regulerende ramme på europæisk plan; en sådan koordinering bør også bidrage til at fastlægge en stærk, fælles forhandlingsposition i internationale fora.
- (60) For ikke at hindre udviklingen af elektronisk handel er det nødvendigt, at den retlige ramme er klar, enkel og konsekvent og i overensstemmelse med de regler, som gælder internationalt, så den europæiske industris konkurrenceevne ikke skades, og så innovationen i denne sektor ikke hindres.
- (61) Hvis markedet skal fungere effektivt elektronisk i en global sammenhæng, er det påkrævet, at Den Europæiske Union og de vigtigste områder uden for Europa konsulterer hinanden med henblik på at tilpasse deres lovgivninger og procedurer.
- (62) Samarbejdet med tredjelande om elektronisk handel bør styrkes, især med ansøgerlandene, udviklingslandene og Den Europæiske Unions andre handelspartnere.

(63) Vedtagelsen af dette direktiv hindrer ikke, at medlemsstaterne tager hensyn til de forskellige sociale, samfundsmæssige og kulturelle virkninger af informationssamfundets opståen; den bør især ikke gribe ind i de foranstaltninger, som medlemsstaterne måtte vedtage i henhold til fællesskabsretten for at nå sociale, kulturelle og demokratiske mål under hensyn til deres sproglige mangfoldighed, de nationale og regionale særpræg samt deres kulturarv og for at sikre og opretholde offentlig adgang til så mange informationssamfundstjenester som muligt; udviklingen af informationssamfundet skal under alle omstændigheder sikre Fællesskabets borgere adgang til den europæiske kulturarv i et digitalt miljø.

(64) Medlemsstaterne råder med elektronisk kommunikation over et glimrende middel til at levere offentlige tjenester på det kulturelle, uddannelsesmæssige og sproglige område.

(65) Rådet understregede i sin resolution af 19. januar 1999 om forbrugerdimensionen i informationssamfundet⁽¹⁾, at forbrugerbeskyttelse fortjener særlig opmærksomhed i denne forbindelse; Kommissionen vil undersøge, hvorvidt beskyttelsen i henhold til gældende lovgivning om forbrugerbeskyttelse er utilstrækkelig i forbindelse med informationssamfundet, og vil i givet fald identificere eventuelle mangler i denne lovgivning og de aspekter, hvor supplerende foranstaltninger måtte vise sig nødvendige; Kommissionen bør i givet fald udarbejde specifikke supplerende forslag med henblik på afhjælpning af de mangler, den måtte have påvist.

UDSTEDT FØLGENDE DIREKTIV:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Formål og anvendelsesområde

1. Dette direktiv har til formål at bidrage til et velfungerende indre marked ved at sikre fri bevægelighed for informations-samfundstjenester mellem medlemsstaterne.

2. Ved dette direktiv foretages der, i det omfang det er nødvendigt for at nå det i stk. 1 omhandlede mål, en tilnærmelse af visse nationale bestemmelser om informationssamfundstjenester, som vedrører det indre marked, tjenesteydernes

etablering, kommerciel kommunikation, elektroniske kontrakter, formidleransvar, adfærdskodekser, udenretslig bilæggelse af tvister, klageadgang og samarbejde mellem medlemsstaterne.

3. Dette direktiv supplerer den fællesskabsret, der finder anvendelse på informationssamfundstjenester, uden at det berører det niveau for beskyttelse af især folkesundheden og forbrugernes interesser, der er fastlagt ved Fællesskabets retsakter og den nationale lovgivning til gennemførelse heraf, forudsat at det ikke begrænser adgangen til at levere informationssamfundstjenester.

4. Dette direktiv indfører ikke nye internationale privatretlige regler og berører ikke domstolenes kompetence.

5. Dette direktiv finder ikke anvendelse på:

- a) beskatningsområdet
- b) spørgsmål, der vedrører informationssamfundstjenester omfattet af direktiv 95/46/EF og 97/66/EF
- c) spørgsmål, der vedrører aftaler eller praksis reguleret ved kartellovgivningen
- d) følgende aktiviteter inden for informationssamfundstjenester:

— notarvirksomhed eller lignende virksomhed, i det omfang den er direkte og specifikt forbundet med udøvelse af offentlig myndighed

— repræsentation og forsvar af en klient i retten

— spil, som indebærer, at der gøres en indsats med penge i hasardspil, herunder lotteri og væddemål.

6. Dette direktiv berører ikke foranstaltninger, som er truffet på fællesskabsplan eller på nationalt plan i overensstemmelse med fællesskabsretten, for at fremme kulturel og sproglig mangfoldighed og for at sikre pluralismen.

Artikel 2

Definitioner

I dette direktiv forstås ved:

- a) "informationssamfundstjenester": tjenester som defineret i artikel 1, nr. 2, i direktiv 98/34/EF som ændret ved direktiv 98/48/EF

⁽¹⁾ EFT C 23 af 28.1.1999, s. 1.

b) »tjenesteyder«: enhver fysisk eller juridiske person, som leverer en informationssamfundstjeneste

c) »etableret tjenesteyder«: en tjenesteyder, som faktisk udøver erhvervmæssig virksomhed i et ikke nærmere angivet tidsrum ved hjælp af en fast indretning. Det forhold, at der findes og anvendes tekniske og teknologiske hjælpemidler, som benyttes til at levere tjenesten, medfører ikke i sig selv, at tjenesteyderen er etableret

d) »tjenestemodtager«: enhver fysisk eller juridisk person, som, uanset om det er til erhvervmæssig eller anden brug, anvender en informationssamfundstjeneste, bl.a. for at søge information eller gøre information tilgængelig

e) »forbruger«: en fysisk person, der ikke handler som led i sin handelsmæssige eller erhvervmæssige virksomhed

f) »kommerciel kommunikation«: alle former for kommunikation bestemt til direkte eller indirekte at fremme afsætningen af varer eller tjenester eller til etablering af et image for en virksomhed, en organisation eller en person, som udøver handels-, industri- eller håndværksvirksomhed eller et lovreguleret erhverv. Nedenstående udgør ikke i sig selv kommerciel kommunikation:

— information, som gør det muligt at få direkte adgang til denne virksomheds, organisations eller persons aktiviteter, herunder et domænenavn eller en e-postadresse

— kommunikation vedrørende en virksomheds, organisations eller persons varer, tjenester eller image udarbejdet uafhængigt af denne, især uden finansiell modydelse

g) »lovreguleret erhverv«: ethvert erhverv som omhandlet enten i artikel 1, litra d), i Rådets direktiv 89/48/EØF af 21. december 1988 om indførelse af en generel ordning for gensidig anerkendelse af eksamensbeviser for erhvervs-kompetencegivende videregående uddannelser af mindst tre års varighed⁽¹⁾ eller i artikel 1, litra f), i Rådets direktiv 92/51/EØF af 18. juni 1992 om anden generelle ordning for anerkendelse af erhvervsuddannelser til supplering af direktiv 89/48/EØF⁽²⁾

h) »koordineret område«: de krav, der i medlemsstaterne retssystemer er fastsat for leverandører af informationssamfundstjenester eller for informationssamfundstjenester, uanset om de er generelle eller specifikt fastsat for disse.

i) Det koordinerede område vedrører krav, som tjenesteyderen skal opfylde:

— når han påbegynder aktivitet som leverandør af informationssamfundstjenester, f.eks. krav til kvalifikationer, tilladelse og underretningsordninger

— når han udøver aktivitet som leverandør af informationssamfundstjenester, f.eks. krav til tjenesteyderens adfærd, krav til kvaliteten eller indholdet af tjenesten, herunder krav, som gælder i forbindelse med reklamer og kontrakter, eller krav vedrørende tjenesteyderens ansvar.

ii) Det koordinerede område omfatter ikke krav som f.eks.:

— krav til varer som sådan

— krav til levering af varer

— krav til tjenester, som ikke ydes elektronisk.

Artikel 3

Det indre marked

1. Hver medlemsstat påser, at de informationssamfundstjenester, som leveres af en tjenesteyder etableret på medlemsstatens territorium, er i overensstemmelse med de nationale bestemmelser, der finder anvendelse i denne medlemsstat inden for det koordinerede område.

2. Medlemsstaterne må ikke af grunde, der henhører under det koordinerede område, begrænse adgangen til at levere informationssamfundstjenester fra en anden medlemsstat.

3. Stk. 1 og 2 finder ikke anvendelse på de områder, der er nævnt i bilaget.

4. Medlemsstaterne kan træffe foranstaltninger til fravigelse af stk. 2 for en bestemt informationssamfundstjeneste, hvis følgende betingelser er opfyldt:

a) foranstaltningerne skal:

i) være nødvendige af en af følgende grunde:

— ufravigelige retsgrundsætninger, især forebyggelse, efterforskning, afsløring og retsforfølgning af lovovertrædelser, herunder beskyttelsen af mindreårige og bekæmpelsen af enhver tilskyndelse til had på grund af race, køn, religion eller nationalitet, og krænkelse af enkeltpersoners værdighed

— beskyttelse af folkesundheden

⁽¹⁾ EFT L 19 af 24.1.1989, s. 16.

⁽²⁾ EFT L 209 af 24.7.1992, s. 25. Direktivet er senest ændret ved Kommissionens direktiv 97/38/EF (EFT L 184 af 12.7.1997, s. 31).

- den offentlige sikkerhed, herunder national sikkerhed og forsvar
- beskyttelse af forbrugere, herunder investorer
- ii) træffes over for en informationssamfundstjeneste, som krænker de i nr. i) omhandlede mål, eller som udgør en alvorlig og tungvejende risiko for en krænkelse af disse mål
- iii) stå i et rimeligt forhold til disse mål
- b) uden at det berører retssager, herunder forudgående retsmøder og handlinger, der udføres i forbindelse med efterforskning af kriminalsager, skal medlemsstaten, inden den træffer de pågældende foranstaltninger:
 - have opfordret den i stk. 1 omhandlede medlemsstat til at træffe foranstaltninger, og denne medlemsstat har ikke truffet disse foranstaltninger, eller de har ikke været tilstrækkelige
 - have meddelt Kommissionen og den i stk. 1 omhandlede medlemsstat, at den har til hensigt at træffe sådanne foranstaltninger.

5. Medlemsstaterne kan i hastende tilfælde fravige betingelserne i stk. 4, litra b). Foranstaltningerne skal i så fald snarest muligt meddeles Kommissionen og den i stk. 1 omhandlede medlemsstat med angivelse af grundene til, at medlemsstaten finder, at der er tale om et hastende tilfælde.

6. Uden at dette berører medlemsstatens mulighed for at anvende de pågældende foranstaltninger, skal Kommissionen hurtigst muligt undersøge, om de anmeldte foranstaltninger er i overensstemmelse med fællesskabsretten; kommer Kommission til den konklusion, at foranstaltningerne ikke er i overensstemmelse med fællesskabsretten, skal den anmode den pågældende medlemsstat om at undlade at træffe de påtænkte foranstaltninger eller om straks at bringe allerede trufne foranstaltninger til ophør.

KAPITEL II

PRINCIPPER

Afdeling 1: Krav vedrørende etablering og oplysninger

Artikel 4

Princippet om, at der ikke kræves forhåndsgodkendelse

1. Medlemsstaterne sikrer, at en tjenesteyder for at påbegynde og udøve aktivitet som leverandør af informationssamfundstjenester ikke skal opfylde noget krav om forudgående godkendelse eller noget andet tilsvarende krav.

2. Stk. 1 berører ikke godkendelsesordninger, som ikke specifikt og udelukkende vedrører informationssamfundstjenester, eller som er omfattet af Europa-Parlamentets og Rådets direktiv 97/13/EF af 10. april 1997 om ensartede principper for generelle tilladelser og individuelle tilladelser for teletjenester⁽¹⁾.

Artikel 5

Generel oplysningspligt

1. Ud over andre informationskrav, som er fastlagt i fællesskabsretten, sikrer medlemsstaterne, at tjenesteyderen giver tjenestemodtagerne og de kompetente myndigheder let, umiddelbar og vedvarende adgang til som minimum følgende oplysninger:

- a) tjenesteyderens navn
- b) den fysiske adresse, hvor tjenesteyderen er etableret
- c) nærmere oplysninger, som gør det muligt hurtigt at kontakte tjenesteyderen og at kommunikere direkte og konkret med denne, herunder tjenesteyderens e-postadresse
- d) hvis tjenesteyderen er optaget i et handelsregister eller et lignende offentligt register, det register, hvor tjenesteyderen er registreret, og vedkommendes registreringsnummer eller tilsvarende identifikationsmidler i dette register
- e) hvis den pågældende aktivitet er omfattet af en godkendelsesordning, nærmere oplysninger om den relevante tilsynsmyndighed
- f) med hensyn til lovregulerede erhverv:
 - enhver erhvervssammenslutning eller tilsvarende institution, hvor tjenesteyderen er registreret
 - erhvervsbetegnelsen og den medlemsstat, hvor den er givet
 - en henvisning til de faglige regler, der gælder i etableringsmedlemsstaten, og hvorledes der kan fås adgang til dem
- g) hvis tjenesteyderen udøver momspligtig virksomhed, det identifikationsnummer, der er omhandlet i artikel 22, stk. 1, i Rådets sjette direktiv (77/388/EØF) af 17. maj 1977 om harmonisering af medlemsstaternes lovgivning om omsætningsafgifter — Det fælles merværdiafgiftssystem: ensartet beregningsgrundlag⁽²⁾.

⁽¹⁾ EFT L 117 af 7.5.1997, s. 15.

⁽²⁾ EFT L 145 af 13.6.1977, s. 1. Direktivet er senest ændret ved direktiv 1999/85/EF (EFT L 277 af 28.10.1999, s. 34).

2. Ud over andre informationskrav, som er fastlagt i fællesskabsretten, sikrer medlemsstaterne som minimum, at priser angives klart og utvetydigt, når der i forbindelse med informationssamfundstjenester angives priser, og især at det anføres, om de er inklusive afgifter og leveringsomkostninger.

Afdeling 2: Kommerciel kommunikation

Artikel 6

Oplysningspligt

Ud over andre informationskrav, som er fastlagt i fællesskabsretten, sikrer medlemsstaterne, at kommerciel kommunikation, som er en del af eller udgør en informationssamfundstjeneste, mindst overholder følgende betingelser:

- den kommercielle kommunikation skal klart kunne identificeres som sådan
- den fysiske eller juridiske person, på hvis vegne den kommercielle kommunikation foretages, skal klart kunne identificeres
- reklametilbud som f.eks. rabatter, præmier og tilgift skal, når de er tilladt i den medlemsstat, hvor tjenesteyderen er etableret, klart kunne identificeres som sådanne, og betingelserne for at opnå dem skal være let tilgængelige og fremlægges klart og utvetydigt
- salgsfremmende konkurrencer eller spil skal, når de er tilladt i den medlemsstat, hvor tjenesteyderen er etableret, klart kunne identificeres som sådanne, og betingelserne for deltagelse skal være let tilgængelige og fremlægges klart og utvetydigt.

Artikel 7

Uopfordret kommerciel kommunikation

1. Ud over andre krav, som er fastlagt i fællesskabsretten, sikrer medlemsstater, som tillader uopfordret kommerciel kommunikation via elektronisk post, at sådan kommerciel kommunikation fra en tjenesteyder, der er etableret på deres område, klart og utvetydigt er angivet som sådan, når modtageren modtager den.

2. Med forbehold af direktiv 97/7/EF og direktiv 97/66/EF træffer medlemsstaterne foranstaltninger for at sikre, at tjenesteydere, som fremsender uopfordret kommerciel kommunikation via elektronisk post, respekterer og regelmæssigt konsulterer »opt-out«-registre, hvor fysiske personer, der ikke ønsker at modtage sådan kommerciel kommunikation, kan registrere sig.

Artikel 8

Lovregulerede erhverv

1. Medlemsstaterne sikrer, at anvendelsen af kommerciel kommunikation, der er en del af eller udgør en informations-samfundstjeneste, som leveres af et medlem af et lovreguleret erhverv, er tilladt under overholdelse af faglige regler om især uafhængighed, værdighed, faglig etik samt tavshedspligt og loyalitet over for klienter og fagfæller.

2. Med forbehold af faglige sammenslutningers og organisationers uafhængighed tilskynder medlemsstaterne og Kommissionen faglige sammenslutninger og organisationer til at udarbejde adfærdskodekser på fællesskabsplan for nærmere at fastslå, hvilke oplysninger der kan gives med henblik på kommerciel kommunikation i overensstemmelse med stk. 1.

3. Ved udarbejdelsen af forslag til fællesskabsinitiativer, som måtte blive nødvendige for at sikre, at det indre marked fungerer tilfredsstillende med hensyn til de oplysninger, der er omhandlet i stk. 2, skal Kommissionen tage behørigt hensyn til de adfærdskodekser, der gælder på fællesskabsplan, og handle i tæt samarbejde med de relevante faglige sammenslutninger og organisationer.

4. Dette direktiv supplerer Fællesskabets direktiver om adgang til og udøvelse af lovreguleret erhvervsmæssig virksomhed.

Afdeling 3: Kontrakter, der er indgået elektronisk

Artikel 9

Behandling af kontrakter

1. Medlemsstaterne sikrer, at deres retssystem gør det muligt at indgå kontrakter elektronisk. Medlemsstaterne sikrer bl.a., at de juridiske krav, der gælder for aftaleindgåelsen, hverken er til hinder for anvendelsen af elektroniske kontrakter eller fører til, at sådanne kontrakter på grund af den omstændighed, at de er indgået elektronisk, mister deres retlige virkning og gyldighed.

2. Medlemsstaterne kan bestemme, at stk. 1 ikke finder anvendelse på alle eller nogle af de kontrakter, der hører ind under følgende kategorier:

- kontrakter, der skaber eller overfører rettigheder i fast ejendom, bortset fra udlejningsrettigheder

- b) kontrakter, der ifølge loven kræver medvirken af domstole, offentlige myndigheder eller erhverv, som udøver offentlig myndighed
- c) kontrakter om kaution og om sikkerhedsstillelse fra personer, der handler uafhængigt af deres handelsmæssige eller erhvervsmæssige virksomhed
- d) familieretlige og arveretlige aftaler.

3. Medlemsstaterne meddeler Kommissionen, hvilke af de i stk. 2 omhandlede kontraktkategorier de ikke lader stk. 1 finde anvendelse på. Medlemsstaterne forelægger hvert femte år Kommissionen en rapport om anvendelsen af stk. 2, hvori de forklarer, hvorfor de anser det for nødvendigt at opretholde den i stk. 2, litra b), omhandlede kategori, som de ikke lader stk. 1 finde anvendelse på.

Artikel 10

Oplysningspligt

1. Foruden anden information, der kræves ifølge fælleskabslovgivningen, sikrer medlemsstaterne, medmindre andet er aftalt i handelskøb, at tjenesteyderen mindst oplyser nedenstående klart, forståeligt og utvetydigt, inden ordren afgives af tjenestemodtageren:

- a) de forskellige tekniske led i forbindelse med kontraktens indgåelse
- b) oplysninger om, hvorvidt den indgående kontrakt opbevares af tjenesteyderen, samt om den vil være tilgængelig
- c) de tekniske midler til at finde og rette indtastningsfejl, inden ordren afgives
- d) de sprog, kontrakten kan indgås på.

2. Medlemsstaterne sikrer, at tjenesteydere, medmindre andet er aftalt i handelskøb, angiver, hvilke relevante adfærdskodekser de følger, samt hvordan disse kodekser kan konsulteres elektronisk.

3. Kontraktbetingelser og generelle betingelser skal stilles til rådighed for modtageren på en sådan måde, at vedkommende kan oplagre og gengive dem.

4. Stk. 1 og 2 finder ikke anvendelse på kontrakter, der indgås udelukkende ved udveksling af elektronisk post eller lignende individuel kommunikation.

Artikel 11

Ordreafgivelse

1. Medlemsstaterne sikrer, at nedenstående principper finder anvendelse, når tjenestemodtageren afgiver sin ordre elektronisk, medmindre andet er aftalt i handelskøb:

- tjenesteyderen skal bekræfte modtagelsen af tjenestemodtagerens ordre uden unødigt forsinkelse og elektronisk
- orden og bekræftelsen af dens modtagelse anses for modtaget, når parterne, som de er adresseret til, har adgang til dem.

2. Medlemsstaterne sikrer, at tjenesteyderen, medmindre andet er aftalt i handelskøb, stiller hensigtsmæssige, effektive og tilgængelige tekniske midler til at finde og rette indtastningsfejl til rådighed for tjenestemodtageren, inden ordren afgives.

3. Stk. 1, første led, og stk. 2 finder ikke anvendelse på kontrakter, der indgås udelukkende ved udveksling af elektronisk post eller lignende individuel kommunikation.

Afdeling 4: Formidleransvar for tjenesteydere

Artikel 12

Ren videreformidling («Mere conduit»)

1. Ved levering af en informationssamfundstjeneste i form af transmission på et kommunikationsnet af information, der leveres af en tjenestemodtager, eller levering af adgang til et kommunikationsnet sikrer medlemsstaterne, at tjenesteyderen ikke er ansvarlig for den transmitterede information, forudsat at tjenesteyderen:

- a) ikke selv iværksætter transmissionen
- b) ikke udvælger modtageren af transmissionen, og
- c) ikke udvælger og ikke ændrer den transmitterede information.

2. Den i stk. 1 omhandlede transmission og levering af adgang omfatter automatisk, mellemliggende og kortvarig oplagring af transmitteret information, forudsat at denne oplagring udelukkende tjener til udførelse af transmission på kommunikationsnettet, og dens varighed ikke overstiger den tid, der med rimelighed kan antages at være nødvendig til transmissionen.

3. Denne artikel berører ikke en domstols eller en administrativ myndigheds mulighed for i overensstemmelse med medlemsstaternes retssystem at kræve, at en tjenesteyder bringer en overtrædelse til ophør eller forhindrer den.

Artikel 13

Caching

1. Medlemsstaterne sikrer, at tjenesteyderen i tilfælde af levering af en informationssamfundstjeneste, der består i transmission på et kommunikationsnet af information, som leveres af en tjenestemodtager, ikke pådrager sig ansvar for automatisk, mellemliggende og midlertidig oplagring af denne information foretaget alene med det formål at gøre senere transmission af informationen til andre tjenestemodtagere efter disses anmodning mere effektiv, forudsat:

- a) at tjenesteyderen ikke ændrer informationen
- b) at tjenesteyderen overholder betingelserne for adgang til informationen
- c) at tjenesteyderen overholder reglerne om ajourføring af informationen, angivet på en måde, der er almindelig anerkendt og anvendt af industrien
- d) at tjenesteyderen ikke foretager indgreb i den lovlige anvendelse af teknologi, som er almindelig anerkendt og anvendt af industrien, med det formål at skaffe sig data om anvendelsen af informationen, og
- e) at tjenesteyderen straks tager skridt til at fjerne den information, han har oplagret, eller til at hindre adgangen til den, når han får konkret kendskab til, at informationen er blevet fjernet fra nettet eller adgangen til den hindret, eller at en domstol eller en administrativ myndighed har krævet informationen fjernet eller adgangen til den hindret.

2. Denne artikel berører ikke en domstols eller en administrativ myndigheds muligheder for i overensstemmelse med medlemsstaternes retssystem at kræve, at en tjenesteyder bringer en overtrædelse til ophør eller forhindrer den.

Artikel 14

Oplagring (»Hosting«)

1. Medlemsstaterne sikrer, at tjenesteyderen i tilfælde af levering af en informationssamfundstjeneste, som består i oplagring af information leveret af en tjenestemodtager, ikke pådrager sig ansvar for information oplagret på anmodning af en tjenestemodtager, forudsat:

- a) at tjenesteyderen ikke har konkret kendskab til den ulovlige aktivitet eller information og, for så vidt angår erstatningskrav, ikke har kendskab til forhold eller omstændigheder, hvoraf den ulovlige aktivitet eller information fremgår, eller

- b) at tjenesteyderen fra det øjeblik, hvor han får et sådant kendskab, straks tager skridt til at fjerne informationen eller hindre adgangen til den.

2. Stk. 1 finder ikke anvendelse, når tjenestemodtageren handler under tjenesteyderens myndighed eller kontrol.

3. Denne artikel berører ikke en domstols eller en administrativ myndigheds muligheder for i overensstemmelse med medlemsstaternes retssystemer at kræve, at en tjenesteyder bringer en overtrædelse til ophør eller forhindrer den, eller medlemsstaternes muligheder for at fastlægge procedurer for at fjerne information eller hindre adgangen til den.

Artikel 15

Ingen generel overvågningsforpligtelse

1. Med hensyn til levering af de i artikel 12, 13 og 14 omhandlede tjenester må medlemsstaterne ikke pålægge tjenesteyderne en generel forpligtelse til at overvåge den information, de fremsender eller oplagrer, eller en generel forpligtelse til aktivt at undersøge forhold eller omstændigheder, der tyder på ulovlig virksomhed.

2. Medlemsstaterne kan kræve, at leverandører af informationssamfundstjenester straks underretter de kompetente offentlige myndigheder om påståede ulovlige aktiviteter, der udøves, eller information, der leveres af deres tjenestemodtagere, eller at de på anmodning giver de kompetente myndigheder oplysninger, som gør det muligt at identificere de tjenestemodtagere, de har oplagingsaftaler med.

KAPITEL III

IVÆRKSÆTTELSE

Artikel 16

Adfærdskodekser

1. Medlemsstaterne og Kommissionen tilskynder til:

- a) at handels-, erhvervs- og forbrugersammenslutningerne og -organisationerne på fællesskabsplan udarbejder adfærdskodekser med henblik på en hensigtsmæssig gennemførelse af artikel 5-15
- b) at udkast til adfærdskodekser på nationalt eller fællesskabsplan frivilligt sendes til Kommissionen.
- c) at der er elektronisk adgang til adfærdskodekserne på fællesskabssprogene

- d) at handels-, erhvervs- og forbrugersammenslutningerne og -organisationerne forelægger medlemsstaterne og Kommissionen evalueringer af anvendelsen af deres adfærdskodekser og disses indvirkning på praksis, brug og sædvaner i forbindelse med elektronisk handel
- e) at der udarbejdes adfærdskodekser vedrørende beskyttelse af mindreårige og den menneskelige værdighed.

2. Medlemsstaterne og Kommissionen opfordrer til, at forbrugersammenslutningerne eller -organisationerne inddrages i udarbejdelsen og iværksættelsen af adfærdskodekser, der vedrører deres interesseområder, og som udarbejdes i overensstemmelse med stk. 1, litra a). Foreninger, der repræsenterer synshandicappede og andre handicappede, bør i behørigt omfang høres, så der kan tages hensyn til deres særlige behov.

Artikel 17

Udenretslig bilæggelse af tvister

1. Medlemsstaterne drager omsorg for, at deres lovgivning i tilfælde af uenighed mellem en leverandør af en informations-samfundstjeneste og en tjenestemodtager ikke er til hinder for anvendelsen af ordninger for udenretslig bilæggelse af tvister i henhold til national lovgivning, herunder ad hensigtsmæssig elektronisk vej.
2. Medlemsstaterne tilskynder organerne for udenretslig bilæggelse af tvister, navnlig tvister i forbrugerforhold, til at handle på en måde, der giver parterne passende proceduremæssig sikkerhed.
3. Medlemsstaterne tilskynder organerne for udenretslig bilæggelse af tvister til at holde Kommissionen underrettet om de væsentlige afgørelser, de træffer vedrørende informations-samfundstjenester, og om alle andre oplysninger om praksis, brug og sædvaner i forbindelse med elektronisk handel.

Artikel 18

Søgsmålsadgang

1. Medlemsstaterne drager omsorg for, at indgivelse af søgsmål i henhold til national ret vedrørende aktiviteter i forbindelse med informations-samfundstjenester kan føre til hurtig vedtagelse af forholdsregler, herunder foreløbige forholdsregler, for at bringe den påståede overtrædelse til ophør og hindre, at der opstår yderligere skade for de berørte interesser.
2. I bilaget til direktiv 98/27/EF tilføjes følgende punkt:

11. Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8. juni 2000 om visse retlige aspekter af informa-

tionssamfundstjenester, navnlig elektronisk handel, i det indre marked («Direktivet om elektronisk handel») (EFT L 178 af 17.7.2000, s. 1).

Artikel 19

Samarbejde

1. Medlemsstaterne sørger for at råde over tilstrækkelige kontrol- og undersøgelsesmidler til en effektiv iværksættelse af dette direktiv, og de drager omsorg for, at tjenesteyderne giver dem de nødvendige oplysninger.

2. Medlemsstaterne samarbejder med de øvrige medlemsstater; de udpeger med henblik herpå et eller flere kontaktpunkter, og nærmere oplysninger om disse meddeles de øvrige medlemsstater og Kommissionen.

3. Medlemsstaterne yder hurtigst muligt og i overensstemmelse med national lovgivning den bistand og giver de oplysninger, som en anden medlemsstat eller Kommissionen anmoder om, herunder ad hensigtsmæssig elektronisk vej.

4. Medlemsstaterne opretter kontaktpunkter, hvortil der som et minimum er elektronisk adgang, og til hvilke tjenestemodtagere og tjenesteydere kan henvende sig:

- a) for at få generelle oplysninger om deres rettigheder og pligter i kontraktforhold samt om de klage- og retsmidler, der er til rådighed i tilfælde af tvister, herunder praktiske forhold i forbindelse med anvendelsen af sådanne mekanismer
- b) for at få nærmere oplysninger om de myndigheder, sammenslutninger eller organisationer, hos hvilke de kan få yderligere oplysninger eller praktisk bistand.

5. Medlemsstaterne tilskynder til, at Kommissionen underrettes om alle væsentlige administrative eller retlige afgørelser på deres område i tvister om informations-samfundstjenester samt om praksis, brug og sædvaner i forbindelse med elektronisk handel. Kommissionen meddeler de øvrige medlemsstater disse afgørelser.

Artikel 20

Sanktioner

Medlemsstaterne fastsætter de sanktioner, der skal finde anvendelse ved overtrædelse af de nationale bestemmelser, der udstedes i henhold til dette direktiv, og træffer alle de foranstaltninger, der er nødvendige for at sikre gennemførelsen af dem. De således fastsatte sanktioner skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

KAPITEL IV

AFSLUTTENDE BESTEMMELSER

Artikel 21

Revision

1. Inden den 17. juli 2003 og derefter hvert andet år forelægger Kommissionen Europa-Parlamentet, Rådet og Det Økonomiske og Sociale Udvalg en rapport om anvendelsen af dette direktiv tillige med eventuelle forslag til dets tilpasning til den retlige, tekniske og økonomiske udvikling inden for informationssamfundstjenester, navnlig med henblik på kriminalitetsforebyggelse, beskyttelse af mindreårige, forbrugerbeskyttelse samt på, at det indre marked fungerer korrekt.

2. Rapporten skal i sin undersøgelse af behovet for tilpasning af dette direktiv navnlig analysere behovet for forslag vedrørende det erstatningsansvar, der påhviler tjenesteudbydere af hyperlinks og søgemaskiner, procedurer for fjernelse af ulovligt indhold («notice and take down procedures») og pålæggelse af ansvar efter nedtagelse af indhold. Rapporten skal også analysere behovet for yderligere betingelser for fritagelse for ansvar, som omhandlet i artikel 12 og 13, i lyset af den tekniske udvikling og muligheden for at anvende det indre markeds principper på uopfordret kommerciel kommunikation via elektronisk post.

Artikel 22

Gennemførelse

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv inden den 17. januar 2002. De underretter straks Kommissionen herom.

2. De i stk. 1 nævnte love og bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

Artikel 23

Ikrafttræden

Dette direktiv træder i kraft på dagen for offentliggørelsen i *De Europæiske Fællesskabers Tidende*.

Artikel 24

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Luxembourg, den 8. juni 2000.

På Europa-Parlamentets vegne

På Rådets vegne

N. FONTAINE

G. d'OLIVEIRA MARTINS

Formand

Formand

BILAG

UNDTAGELSER FRA ARTIKEL 3

De i artikel 3, stk. 3, omhandlede områder, som artikel 3, stk. 1 og 2, ikke finder anvendelse på:

- ophavsret og beslægtede rettigheder, rettigheder som omhandlet i direktiv 87/54/EØF⁽¹⁾ og i direktiv 96/9/EF⁽²⁾, samt industrielle ejendomsrettigheder
- udstedelse af elektroniske penge af institutter, for hvilke medlemsstaterne har anvendt en af undtagelserne i artikel 8, stk. 1, i direktiv 2000/46/EF⁽³⁾
- artikel 44, stk. 2, i direktiv 85/611/EØF⁽⁴⁾
- artikel 30 og afsnit IV i direktiv 92/49/EØF⁽⁵⁾, afsnit IV i direktiv 92/96/EØF⁽⁶⁾, artikel 7 og 8 i direktiv 88/357/EØF⁽⁷⁾ og artikel 4 i direktiv 90/619/EØF⁽⁸⁾
- parternes ret til frit at vælge den lov, der skal anvendes på deres kontrakt
- kontraktforpligtelser i forbindelse med forbrugerkontrakter
- den formelle gyldighed af kontrakter, der etablerer eller overfører rettigheder i fast ejendom, når sådanne kontrakter er underkastet ufravigelige formkrav ifølge retten i den medlemsstat, hvor den faste ejendom er beliggende
- tilladeligheden af uopfordret kommerciel kommunikation via elektronisk post.

⁽¹⁾ EFT L 24 af 27.1.1987, s. 36.

⁽²⁾ EFT L 77 af 27.3.1996, s. 20.

⁽³⁾ Endnu ikke offentliggjort i EFT.

⁽⁴⁾ EFT L 375 af 31.12.1985, s. 3. Direktivet er senest ændret ved direktiv 95/26/EF (EFT L 168 af 18.7.1995, s. 7).

⁽⁵⁾ EFT L 228 af 11.8.1992, s. 1. Direktivet er senest ændret ved direktiv 95/26/EF.

⁽⁶⁾ EFT L 360 af 9.12.1992, s. 1. Direktivet er senest ændret ved direktiv 95/26/EF.

⁽⁷⁾ EFT L 172 af 4.7.1988, s. 1. Direktivet er senest ændret ved direktiv 92/49/EF.

⁽⁸⁾ EFT L 330 af 29.11.1990, s. 50. Direktivet er senest ændret ved direktiv 92/96/EF.

B I L A G 3

UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT

1996

with additional article 5 bis as adopted in 1998

UNITED NATIONS

CONTENTS

GENERAL ASSEMBLY RESOLUTION 51/162 OF 16 DECEMBER 1996
UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

Part one. Electronic commerce in general

Chapter I. General provisions

- Article 1. Sphere of application
- Article 2. Definitions
- Article 3. Interpretation
- Article 4. Variation by agreement

Chapter II. Application of legal requirements to data messages

- Article 5. Legal recognition of data messages
- Article 5 bis. Incorporation by reference
- Article 6. Writing
- Article 7. Signature
- Article 8. Original
- Article 9. Admissibility and evidential weight of data messages
- Article 10. Retention of data messages

Chapter III. Communication of data messages

- Article 11. Formation and validity of contracts
- Article 12. Recognition by parties of data messages
- Article 13. Attribution of data messages
- Article 14. Acknowledgement of receipt
- Article 15. Time and place of dispatch and receipt of data messages

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

- Article 16. Actions related to contracts of carriage of goods
- Article 17. Transport documents

Paragraphs

GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE	1-150
Purpose of this Guide	1
I. Introduction to the Model Law	2-23
A. Objectives	2-6
B. Scope	7-10
C. Structure	11-12
D. A "framework" law to be supplemented by technical regulations	13-14
E. The "functional-equivalent" approach	15-18
F. Default rules and mandatory law	19-21
G. Assistance from UNCITRAL secretariat	22-23
II. Article-by-article remarks	24-122
Part one. Electronic commerce in general	24-107
Chapter I. General provisions	24-45
Article 1. Sphere of application	24-29
Article 2. Definitions	30-40
Article 3. Interpretation	41-43
Article 4. Variation by agreement	44-45
Chapter II. Application of legal requirements to data messages	46-75
Article 5. Legal recognition of data messages	46
Article 5bis. Incorporation by reference	46-1 - 46-7
Article 6. Writing	47-52
Article 7. Signature	53-61
Article 8. Original	62-69
Article 9. Admissibility and evidential weight of data messages	70-71
Article 10. Retention of data messages	72-75
Chapter III. Communication of data messages	76-107
Article 11. Formation and validity of contracts	76-80

Article 12. Recognition by parties of data messages	81-82
Article 13. Attribution of data messages	83-92
Article 14. Acknowledgement of receipt	93-99
Article 15. Time and place of dispatch and receipt of data messages	100-107
Part two. Electronic commerce in specific areas	108-122
Chapter I. Carriage of goods	110-122
Article 16. Actions related to contracts of carriage of goods	111-112
Article 17. Transport documents	113-122
III. History and background of the Model Law	123-150

Resolution adopted by the General Assembly
[on the report of the Sixth Committee (A/51/628)]
*51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on
International Trade Law*

The General Assembly,

Recalling its resolution 2205 (XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law, with a mandate to further the progressive harmonization and unification of the law of international trade and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade,

Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information,

Recalling the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session, in 1985,⁽¹⁾ and paragraph 5(b) of General Assembly resolution 40/71 of 11 December 1985, in which the Assembly called upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission,⁽¹⁾ so as to ensure legal security in the context of the widest possible use of automated data processing in international trade,

Convinced that the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations,

Noting that the Model Law on Electronic Commerce was adopted by the Commission at its twenty-ninth session after consideration of the observations of Governments and interested organizations,

Believing that the adoption of the Model Law on Electronic Commerce by the Commission will assist all States significantly in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such

legislation where none currently exists,

1. *Expresses* its appreciation to the United Nations Commission on International Trade Law for completing and adopting the Model Law on Electronic Commerce contained in the annex to the present resolution and for preparing the Guide to Enactment of the Model Law;
2. *Recommends* that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;
3. *Recommends* also that all efforts be made to ensure that the Model Law, together with the Guide, become generally known and available.

*85th plenary meeting
16 December 1996*

UNCITRAL Model Law on Electronic Commerce

[Original: Arabic, Chinese, English, French, Russian, Spanish]

Part one. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application*

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

* The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

** This Law does not override any rule of law intended for the protection of consumers.

*** The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies to any kind of information in the form of a data message, except in the following situations: [...]."

**** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road

Article 2. Definitions

For the purposes of this Law:

- (a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;
- (b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;
- (c) "Originator" of a data message means a person by whom, or on whose behalf, the

data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

(d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

Chapter II. Application of legal requirements to data messages

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 5 bis. Incorporation by reference

(as adopted by the Commission at its thirty-first session, in June 1998)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: [...].

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in

which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Chapter III. Communication of data messages

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) The provisions of this article do not apply to the following: [...].

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

- (b) by an information system programmed by, or on behalf of, the originator to operate automatically.
- (3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
- (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
 - (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.
- (4) Paragraph (3) does not apply:
- (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
 - (b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.
- (5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.
- (6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

- (1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.
- (2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by
- (a) any communication by the addressee, automated or otherwise, or
 - (b) any conduct of the addressee,
- sufficient to indicate to the originator that the data message has been received.
- (3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or,

where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: [...].

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

- (a) (i) furnishing the marks, number, quantity or weight of goods;
- (ii) stating or declaring the nature or value of goods;
- (iii) issuing a receipt for goods;
- (iv) confirming that goods have been loaded;
- (b) (i) notifying a person of terms and conditions of the contract;
- (ii) giving instructions to a carrier;
- (c) (i) claiming delivery of goods;
- (ii) authorizing release of goods;
- (iii) giving notice of loss of, or damage to, goods;
- (d) giving any other notice or statement in connection with the performance of the contract;
- (e) undertaking to deliver goods to a named person or a person authorized to claim delivery;
- (f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;
- (g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

(7) The provisions of this article do not apply to the following: [...].

* * * * *

Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

Purpose of this guide

1. In preparing and adopting the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"), the United Nations Commission on International Trade Law (UNCITRAL) was mindful that the Model Law would be a more effective tool for States modernizing their legislation if background and explanatory information would be provided to executive branches of Governments and legislators to assist them in using the Model Law. The Commission was also aware of the likelihood that the Model Law would be used in a number of States with limited familiarity with the type of communication techniques considered in the Model Law. This Guide, much of which is drawn from the travaux préparatoires of the Model Law, is also intended to be helpful to users of electronic means of communication as well as to scholars in that area. In the preparation of the Model Law, it was assumed that the draft Model Law would be accompanied by such a guide. For example, it was decided in respect of a number of issues not to settle them in the draft Model Law but to address them in the Guide so as to provide guidance to States enacting the draft Model Law. The information presented in this Guide is intended to explain why the provisions in the Model Law have been included as essential basic features of a statutory device designed to achieve the objectives of the Model Law. Such information might assist States also in considering which, if any, of the provisions of the Model Law might have to be varied to take into account particular national circumstances.

I. INTRODUCTION TO THE MODEL LAW

A. Objectives

2. The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions has been increasing rapidly

and is expected to develop further as technical supports such as information highways and the INTERNET become more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. The purpose of the Model Law is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce". The principles expressed in the Model Law are also intended to be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce.

3. The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce. In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents. While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists no legislation dealing with electronic commerce as a whole. This may result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Moreover, while sound laws and practices are necessary in all countries where the use of EDI and electronic mail is becoming widespread, this need is also felt in many countries with respect to such communication techniques as telecopy and telex.

4. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. Disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may contribute to limiting the extent to which businesses may access international markets.

5. Furthermore, at an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those States parties to such international instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

6. The objectives of the Model Law, which include enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law in its national legislation for those situations where parties opt to use electronic means of communication, an enacting State would create a media-neutral environment.

B. Scope

7. The title of the Model Law refers to "electronic commerce". While a definition of "electronic data interchange (EDI)" is provided in article 2, the Model Law does not specify the meaning of "electronic commerce". In preparing the Model Law, the Commission decided that, in addressing the subject matter before it, it would have in mind a broad notion of EDI, covering a variety of trade-related uses of EDI that might be referred to broadly under the rubric of "electronic commerce" (see A/CN.9/360, paras. 28-29), although other descriptive terms could also be used. Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the INTERNET. It was also noted that, in certain circumstances, the notion of "electronic commerce" might cover the use of techniques such as telex and telecopy.

8. It should be noted that, while the Model Law was drafted with constant reference to the more modern communication techniques, e.g., EDI and electronic mail, the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy. There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. A data message may be initiated as an oral communication and end up in the form of a telecopy, or it may start as a telecopy and end up as an EDI message. A characteristic of electronic commerce is that it covers programmable messages, the computer programming of which is the essential difference between such messages and traditional paper-based documents. Such situations are intended to be covered by the Model Law, based on a consideration of the users' need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably. More generally, it may be noted that, as a matter of principle, no communication technique is excluded from the scope of the Model Law since future technical developments need to be accommodated.

9. The objectives of the Model Law are best served by the widest possible application of the Model Law. Thus, although there is provision made in the Model Law for exclusion of certain situations from the scope of articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well decide not to enact in its legislation substantial restrictions on the scope of application of the Model Law.

10. The Model Law should be regarded as a balanced and discrete set of rules, which are recommended to be enacted as a single statute. Depending on the situation in each enacting State, however, the Model Law could be implemented in various ways, either as a single statute or in several pieces of legislation (see below, para. 143).

C. Structure

11. The Model Law is divided into two parts; one dealing with electronic commerce in general and the other one dealing with electronic commerce in specific areas. It should be noted that part two of the Model Law, which deals with electronic commerce in specific areas, is composed of a chapter I only, dealing with electronic commerce as it applies to the carriage of goods. Other aspects of electronic commerce might need to be dealt with in the future, and the Model Law can be regarded as an open-ended instrument, to be complemented by future work.

12. UNCITRAL intends to continue monitoring the technical, legal and commercial developments that underline the Model Law. It might, should it regard it advisable, decide to add new model provisions to the Model Law or modify the existing ones.

D. A "framework" law to be supplemented by technical regulations

13. The Model Law is intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances. However, it is a "framework" law that does not itself set forth all the rules and regulations that may be necessary to implement those techniques in an enacting State. Moreover, the Model Law is not intended to cover every aspect of the use of electronic commerce. Accordingly, an enacting State may wish to issue regulations to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Model Law. It is recommended that, should it decide to issue such regulation, an enacting State should give particular attention to the need to maintain the beneficial flexibility of the provisions in the Model Law.

14. It should be noted that the techniques for recording and communicating information considered in the Model Law, beyond raising matters of procedure that may need to be addressed in the implementing technical regulations, may raise certain legal questions the answers to which will not necessarily be found in the Model Law, but rather in other bodies of law. Such other

bodies of law may include, for example, the applicable administrative, contract, criminal and judicial-procedure law, which the Model Law is not intended to deal with.

E. The "functional-equivalent" approach

15. The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. In the preparation of the Model Law, consideration was given to the possibility of dealing with impediments to the use of electronic commerce posed by such requirements in national laws by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques. Such an approach is used in a number of existing legal instruments, e.g., article 7 of the UNCITRAL Model Law on International Commercial Arbitration and article 13 of the United Nations Convention on Contracts for the International Sale of Goods. It was observed that the Model Law should permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. At the same time, it was said that the electronic fulfilment of writing requirements might in some cases necessitate the development of new rules. This was due to one of many distinctions between EDI messages and paper-based documents, namely, that the latter were readable by the human eye, while the former were not so readable unless reduced to paper or displayed on a screen.

16. The Model Law thus relies on a new approach, sometimes referred to as the "functional equivalent approach", which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

17. A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document. That is why the Model Law adopted a flexible standard, taking into account the various layers of existing requirements in a paper-based environment: when adopting the "functional-equivalent" approach, attention was given to the existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and unalterability with respect to paper-based documents. For example, the requirement that data be presented in written form (which constitutes a "threshold requirement") is not to be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act".

18. The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function. It should be noted that the functional-equivalent approach has been taken in articles 6 to 8 of the Model Law with respect to the concepts of "writing", "signature" and "original" but not with respect to other legal concepts dealt with in the Model Law. For example, article 10 does not attempt to create a functional equivalent of existing storage requirements.

F. Default rules and mandatory law

19. The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to most of the legal difficulties raised by the use of modern means of communication are sought within contracts. The Model Law embodies the principle of party autonomy in article 4 with respect to the provisions contained in chapter III of part one. Chapter III of part one contains a set of rules of the kind that would typically be found in agreements between parties, e.g., interchange agreements or "system rules". It should be noted that the notion of "system rules" might cover two different categories of rules, namely, general terms provided by communication networks and specific rules that might be included in those general terms to deal with bilateral relationships between originators and addressees of data messages. Article 4 (and the notion of "agreement" therein) is intended to encompass both categories of "system rules".

20. The rules contained in chapter III of part one may be used by parties as a basis for concluding such agreements. They may also be used to supplement the terms of agreements in cases of gaps or omissions in contractual stipulations. In addition, they may be regarded as setting a basic standard for situations where data messages are exchanged without a previous agreement being entered into by the communicating parties, e.g., in the context of open-networks communications.

21. The provisions contained in chapter II of part one are of a different nature. One of the main purposes of the Model Law is to facilitate the use of modern communication techniques and to provide certainty with the use of such techniques where obstacles or uncertainty resulting from statutory provisions could not be avoided by contractual stipulations. The provisions contained in chapter II may, to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy. The provisions contained in chapter II should be regarded as stating the minimum acceptable form requirement and are, for that reason, of a mandatory nature, unless expressly stated otherwise in those provisions. The indication that such form requirements are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

G. Assistance from UNCITRAL secretariat

22. In line with its training and assistance activities, the UNCITRAL secretariat may provide technical consultations for Governments preparing legislation based on the UNCITRAL Model Law on Electronic Commerce, as it may for Governments considering legislation based on other UNCITRAL model laws, or considering adhesion to one of the international trade law conventions prepared by UNCITRAL.

23. Further information concerning the Model Law as well as the Guide and other model laws and conventions developed by UNCITRAL, may be obtained from the secretariat at the address below. The secretariat welcomes comments concerning the Model Law and the Guide, as well as information concerning enactment of legislation based on the Model Law.

International Trade Law Branch
Office of Legal Affairs
United Nations Vienna International Centre
P.O. Box 500
A-1400, Vienna, Austria
Telephone: (43-1) 26060-4060 or 4061
Telefax: (43-1) 26060-5813 or (43-1) 2692669
Telex: 135612 uno a
E-mail: uncitral@unov.un.or.at
Internet Home Page: <http://www.un.or.at/uncitral>

II. ARTICLE-BY-ARTICLE REMARKS

Part one. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application

24. The purpose of article 1, which is to be read in conjunction with the definition of "data message" in article 2(a), is to delineate the scope of application of the Model Law. The approach used in the Model Law is to provide in principle for the coverage of all factual situations where information is generated, stored or communicated, irrespective of the medium on which such information may be affixed. It was felt during the preparation of the Model Law that exclusion of any form or medium by way of a limitation in the scope of the Model Law might result in practical difficulties and would run counter to the purpose of providing truly "media-neutral" rules. However, the focus of the Model Law is on "paperless" means of communication and, except to the extent expressly provided by the Model Law, the Model Law is not intended to alter traditional rules on paper-based communications.

25. Moreover, it was felt that the Model Law should contain an indication that its focus was on the types of situations encountered in the commercial area and that it had been prepared against the background of trade relationships. For that reason, article 1 refers to "commercial activities" and provides, in footnote ****, indications as to what is meant thereby. Such indications, which may be particularly useful for those countries where there does not exist a discrete body of commercial law, are modelled, for reasons of consistency, on the footnote to article 1 of the UNCITRAL Model Law on International Commercial Arbitration. In certain countries, the use of footnotes in a statutory text would not be regarded as acceptable legislative practice. National authorities enacting the Model Law might thus consider the possible inclusion of the text of footnotes in the body of the Law itself.

26. The Model Law applies to all kinds of data messages that might be generated, stored or communicated, and nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic commerce outside the commercial sphere. For example, while the focus of the Model Law is not on the relationships between users of electronic commerce and public authorities, the Model Law is not intended to be inapplicable to such relationships. Footnote *** provides for alternative wordings, for possible use by enacting States that would consider it appropriate to extend the scope of the Model Law beyond the commercial sphere.

27. Some countries have special consumer protection laws that may govern certain aspects of the use of information systems. With respect to such consumer legislation, as was the case with previous UNCITRAL instruments (e.g., the UNCITRAL Model Law on International Credit Transfers), it was felt that an indication should be given that the Model Law had been drafted without special attention being given to issues that might arise in the context of consumer protection. At the same time, it was felt that there was no reason why situations involving consumers should be excluded from the scope of the Model Law by way of a general provision, particularly since the provisions of the Model Law might be found appropriate for consumer protection, depending on legislation in each enacting State. Footnote ** thus recognizes that any such consumer protection law may take precedence over the provisions in the Model Law. Legislators may wish to consider whether the piece of legislation enacting the Model Law should apply to consumers. The question of which individuals or corporate bodies would be regarded as "consumers" is left to applicable law outside the Model Law.

28. Another possible limitation of the scope of the Model Law is contained in the first footnote. In principle, the Model Law applies to both international and domestic uses of data messages. Footnote * is intended for use by enacting States that might wish to limit the applicability of the Model Law to international cases. It indicates a possible test of internationality for use by those States as a possible criterion for distinguishing international cases from domestic ones. It should be noted, however, that in some jurisdictions, particularly in federal States, considerable difficulties might arise in distinguishing international trade from domestic trade. The Model Law

should not be interpreted as encouraging enacting States to limit its applicability to international cases.

29. It is recommended that application of the Model Law be made as wide as possible. Particular caution should be used in excluding the application of the Model Law by way of a limitation of its scope to international uses of data messages, since such a limitation may be seen as not fully achieving the objectives of the Model Law. Furthermore, the variety of procedures available under the Model Law (particularly articles 6 to 8) to limit the use of data messages if necessary (e.g., for purposes of public policy) may make it less necessary to limit the scope of the Model Law. As the Model Law contains a number of articles (articles 6, 7, 8, 11, 12, 15 and 17) that allow a degree of flexibility to enacting States to limit the scope of application of specific aspects of the Model Law, a narrowing of the scope of application of the text to international trade should not be necessary. Moreover, dividing communications in international trade into purely domestic and international parts might be difficult in practice. The legal certainty to be provided by the Model Law is necessary for both domestic and international trade, and a duality of regimes governing the use of electronic means of recording and communication of data might create a serious obstacle to the use of such means.

References⁽²⁾

A/50/17, paras. 213-219;
A/CN.9/407, paras. 37-40;
A/CN.9/406, paras. 80-85; A/CN.9/WG.IV/WP.62, article 1;
A/CN.9/390, paras. 21-43; A/CN.9/WG.IV/WP.60, article 1;
A/CN.9/387, paras. 15-28; A/CN.9/WG.IV/WP.57, article 1;
A/CN.9/373, paras. 21-25 and 29-33; A/CN.9/WG.IV/WP.55, paras. 15-20.

Article 2. Definitions

"Data message"

30. The notion of "data message" is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of "message" includes the notion of "record". However, a definition of "record" in line with the characteristic elements of "writing" in article 6 may be added in jurisdictions where that would appear to be necessary.

31. The reference to "similar means" is intended to reflect the fact that the Model Law was not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments. The aim of the definition of "data message" is to encompass all types of messages that are generated, stored, or communicated in essentially paperless form. For that purpose, all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means listed in the definition are intended to be covered by the reference to "similar means", although, for example, "electronic" and "optical" means of communication might not be, strictly speaking, similar. For the purposes of the Model Law, the word "similar" connotes "functionally equivalent".

32. The definition of "data message" is also intended to cover the case of revocation or amendment. A data message is presumed to have a fixed information content but it may be revoked or amended by another data message.

"Electronic Data Interchange (EDI)"

33. The definition of EDI is drawn from the definition adopted by the Working Party on Facilitation of International Trade Procedures (WP.4) of the Economic Commission for Europe, which is the United Nations body responsible for the development of UN/EDIFACT technical standards.

34. The Model Law does not settle the question whether the definition of EDI necessarily implies that EDI messages are communicated electronically from computer to computer, or whether that

definition, while primarily covering situations where data messages are communicated through a telecommunications system, would also cover exceptional or incidental types of situation where data structured in the form of an EDI message would be communicated by means that do not involve telecommunications systems, for example, the case where magnetic disks containing EDI messages would be delivered to the addressee by courier. However, irrespective of whether digital data transferred manually is covered by the definition of "EDI", it should be regarded as covered by the definition of "data message" under the Model Law.

"Originator" and "Addressee"

35. In most legal systems, the notion of "person" is used to designate the subjects of rights and obligations and should be interpreted as covering both natural persons and corporate bodies or other legal entities. Data messages that are generated automatically by computers without direct human intervention are intended to be covered by subparagraph (c) . However, the Model Law should not be misinterpreted as allowing for a computer to be made the subject of rights and obligations. Data messages that are generated automatically by computers without direct human intervention should be regarded as "originating" from the legal entity on behalf of which the computer is operated. Questions relevant to agency that might arise in that context are to be settled under rules outside the Model Law.

36. The "addressee" under the Model Law is the person with whom the originator intends to communicate by transmitting the data message, as opposed to any person who might receive, forward or copy the data message in the course of transmission. The "originator" is the person who generated the data message even if that message was transmitted by another person. The definition of "addressee" contrasts with the definition of "originator", which is not focused on intent. It should be noted that, under the definitions of "originator" and "addressee" in the Model Law, the originator and the addressee of a given data message could be the same person, for example in the case where the data message was intended for storage by its author. However, the addressee who stores a message transmitted by an originator is not itself intended to be covered by the definition of "originator".

37. The definition of "originator" should cover not only the situation where information is generated and communicated, but also the situation where such information is generated and stored without being communicated. However, the definition of "originator" is intended to eliminate the possibility that a recipient who merely stores a data message might be regarded as an originator.

"Intermediary"

38. The focus of the Model Law is on the relationship between the originator and the addressee, and not on the relationship between either the originator or the addressee and any intermediary. However, the Model Law does not ignore the paramount importance of intermediaries in the field of electronic communications. In addition, the notion of "intermediary" is needed in the Model Law to establish the necessary distinction between originators or addressees and third parties.

39. The definition of "intermediary" is intended to cover both professional and non-professional intermediaries, i.e., any person (other than the originator and the addressee) who performs any of the functions of an intermediary. The main functions of an intermediary are listed in subparagraph (e) , namely receiving, transmitting or storing data messages on behalf of another person. Additional "value-added services" may be performed by network operators and other intermediaries, such as formatting, translating, recording, authenticating, certifying and preserving data messages and providing security services for electronic transactions. "Intermediary" under the Model Law is defined not as a generic category but with respect to each data message, thus recognizing that the same person could be the originator or addressee of one data message and an intermediary with respect to another data message. The Model Law, which is focused on the relationships between originators and addressees, does not, in general, deal with the rights and obligations of intermediaries.

"Information system"

40. The definition of "information system" is intended to cover the entire range of technical means used for transmitting, receiving and storing information. For example, depending on the factual situation, the notion of "information system" could be indicating a communications network, and in other instances could include an electronic mailbox or even a telecopier. The Model Law does not address the question of whether the information system is located on the premises of the addressee or on other premises, since location of information systems is not an operative criterion under the Model Law.

References

A/51/17, paras. 116-138;
A/CN.9/407, paras. 41-52;
A/CN.9/406, paras. 132-156; A/CN.9/WG.IV/WP.62, article 2;
A/CN.9/390, paras. 44-65; A/CN.9/WG.IV/WP.60, article 2;
A/CN.9/387, paras. 29-52; A/CN.9/WG.IV/WP.57, article 2;
A/CN.9/373, paras. 11-20, 26-28 and 35-36; A/CN.9/WG.IV/WP.55, paras. 23-26;
A/CN.9/360, paras. 29-31; A/CN.9/WG.IV/WP.53, paras. 25-33.

Article 3. Interpretation

41. Article 3 is inspired by article 7 of the United Nations Convention on Contracts for the International Sale of Goods. It is intended to provide guidance for interpretation of the Model Law by courts and other national or local authorities. The expected effect of article 3 is to limit the extent to which a uniform text, once incorporated in local legislation, would be interpreted only by reference to the concepts of local law.

42. The purpose of paragraph (1) is to draw the attention of courts and other national authorities to the fact that the provisions of the Model Law (or the provisions of the instrument implementing the Model Law), while enacted as part of domestic legislation and therefore domestic in character, should be interpreted with reference to its international origin in order to ensure uniformity in the interpretation of the Model Law in various countries.

43. As to the general principles on which the Model Law is based, the following non-exhaustive list may be considered: (1) to facilitate electronic commerce among and within nations; (2) to validate transactions entered into by means of new information technologies; (3) to promote and encourage the implementation of new information technologies; (4) to promote the uniformity of law; and (5) to support commercial practice. While the general purpose of the Model Law is to facilitate the use of electronic means of communication, it should not be construed in any way as imposing their use.

References

A/50/17, paras. 220-224;
A/CN.9/407, paras. 53-54;
A/CN.9/406, paras. 86-87; A/CN.9/WG.IV/WP.62, article 3;
A/CN.9/390, paras. 66-73; A/CN.9/WG.IV/WP.60, article 3;
A/CN.9/387, paras. 53-58; A/CN.9/WG.IV/WP.57, article 3;
A/CN.9/373, paras. 38-42; A/CN.9/WG.IV/WP.55, paras. 30-31.

Article 4. Variation by agreement

44. The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to the legal difficulties raised by the use of modern means of communication are mostly sought within contracts. The Model Law is thus intended to support the principle of party autonomy. However, that principle is embodied only with respect to the provisions of the Model Law contained in chapter III of part one. The reason for such a limitation is that the provisions contained in chapter II of part one may, to some extent, be regarded as a collection of exceptions to well-established rules regarding the form of legal transactions. Such well-established rules are normally of a mandatory nature since they generally reflect decisions of public policy. An unqualified statement regarding the freedom of parties to derogate from the

Model Law might thus be misinterpreted as allowing parties, through a derogation to the Model Law, to derogate from mandatory rules adopted for reasons of public policy. The provisions contained in chapter II of part one should be regarded as stating the minimum acceptable form requirement and are, for that reason, to be regarded as mandatory, unless expressly stated otherwise. The indication that such form requirements are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

45. Article 4 is intended to apply not only in the context of relationships between originators and addressees of data messages but also in the context of relationships involving intermediaries. Thus, the provisions of chapter III of part one could be varied either by bilateral or multilateral agreements between the parties, or by system rules agreed to by the parties. However, the text expressly limits party autonomy to rights and obligations arising as between parties so as not to suggest any implication as to the rights and obligations of third parties.

References

A/51/17, paras. 68, 90 to 93, 110, 137, 188 and 207 (article 10);
A/50/17, paras. 271-274 (article 10);
A/CN.9/407, para. 85;
A/CN.9/406, paras. 88-89; A/CN.9/WG.IV/WP.62, article 5;
A/CN.9/390, paras. 74-78; A/CN.9/WG.IV/WP.60, article 5;
A/CN.9/387, paras. 62-65; A/CN.9/WG.IV/WP.57, article 5;
A/CN.9/373, para. 37; A/CN.9/WG.IV/WP.55, paras. 27-29.

Chapter II. Application of legal requirements to data messages

Article 5. Legal recognition of data messages

46. Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is intended to apply notwithstanding any statutory requirements for a "writing" or an original. That fundamental principle is intended to find general application and its scope should not be limited to evidence or other matters covered in chapter II. It should be noted, however, that such a principle is not intended to override any of the requirements contained in articles 6 to 10. By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.

References

A/51/17, paras. 92 and 97 (article 4);
A/50/17, paras. 225-227 (article 4);
A/CN.9/407, para. 55;
A/CN.9/406, paras. 91-94; A/CN.9/WG.IV/WP. 62, article 5 *bis*;
A/CN.9/390, paras. 79-87;
A/CN.9/WG.IV/WP. 60, article 5 *bis*;
A/CN.9/387, paras. 93-94.

Article 5 bis. Incorporation by reference

46-1. Article 5 *bis* was adopted by the Commission at its thirty-first session, in June 1998. It is intended to provide guidance as to how legislation aimed at facilitating the use of electronic commerce might deal with the situation where certain terms and conditions, although not stated in full but merely referred to in a data message, might need to be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of that data message. Such recognition is acceptable under the laws of many States with respect to conventional paper

communications, usually with some rules of law providing safeguards, for example rules on consumer protection. The expression "incorporation by reference" is often used as a concise means of describing situations where a document refers generically to provisions which are detailed elsewhere, rather than reproducing them in full.

46-2. In an electronic environment, incorporation by reference is often regarded as essential to widespread use of electronic data interchange (EDI), electronic mail, digital certificates and other forms of electronic commerce. For example, electronic communications are typically structured in such a way that large numbers of messages are exchanged, with each message containing brief information, and relying much more frequently than paper documents on reference to information accessible elsewhere. In electronic communications, practitioners should not have imposed upon them an obligation to overload their data messages with quantities of free text when they can take advantage of extrinsic sources of information, such as databases, code lists or glossaries, by making use of abbreviations, codes and other references to such information.

46-3. Standards for incorporating data messages by reference into other data messages may also be essential to the use of public key certificates, because these certificates are generally brief records with rigidly prescribed contents that are finite in size. The trusted third party which issues the certificate, however, is likely to require the inclusion of relevant contractual terms limiting its liability. The scope, purpose and effect of a certificate in commercial practice, therefore, would be ambiguous and uncertain without external terms being incorporated by reference. This is the case especially in the context of international communications involving diverse parties who follow varied trade practices and customs.

46-4. The establishment of standards for incorporating data messages by reference into other data messages is critical to the growth of a computer-based trade infrastructure. Without the legal certainty fostered by such standards, there might be a significant risk that the application of traditional tests for determining the enforceability of terms that seek to be incorporated by reference might be ineffective when applied to corresponding electronic commerce terms because of the differences between traditional and electronic commerce mechanisms.

46-5. While electronic commerce relies heavily on the mechanism of incorporation by reference, the accessibility of the full text of the information being referred to may be considerably improved by the use of electronic communications. For example, a message may have embedded in it uniform resource locators (URLs), which direct the reader to the referenced document. Such URLs can provide "hypertext links" allowing the reader to use a pointing device (such as a mouse) to select a key word associated with a URL. The referenced text would then be displayed. In assessing the accessibility of the referenced text, factors to be considered may include: availability (hours of operation of the repository and ease of access); cost of access; integrity (verification of content, authentication of sender, and mechanism for communication error correction); and the extent to which that term is subject to later amendment (notice of updates; notice of policy of amendment).

46-6. One aim of article 5 *bis* is to facilitate incorporation by reference in an electronic context by removing the uncertainty prevailing in many jurisdictions as to whether the provisions dealing with traditional incorporation by reference are applicable to incorporation by reference in an electronic environment. However, in enacting article 5 *bis*, attention should be given to avoid introducing more restrictive requirements with respect to incorporation by reference in electronic commerce than might already apply in paper-based trade.

46-7. Another aim of the provision is to recognize that consumer-protection or other national or international law of a mandatory nature (e.g., rules protecting weaker parties in the context of contracts of adhesion) should not be interfered with. That result could also be achieved by validating incorporation by reference in an electronic environment "to the extent permitted by law", or by listing the rules of law that remain unaffected by article 5 *bis*. Article 5 *bis* is not to be interpreted as creating a specific legal regime for incorporation by reference in an electronic environment. Rather, by establishing a principle of non-discrimination, it is to be construed as making the domestic rules applicable to incorporation by reference in a paper-based environment equally applicable to incorporation by reference for the purposes of electronic commerce. For example, in a number of jurisdictions, existing rules of mandatory law only validate incorporation

by reference provided that the following three conditions are met: (a) the reference clause should be inserted in the data message; (b) the document being referred to, e.g., general terms and conditions, should actually be known to the party against whom the reference document might be relied upon; and (c) the reference document should be accepted, in addition to being known, by that party.

References

- | | |
|--|-------------------------------------|
| A/53/17, paras. 212-221; | A/CN.9/407, paras. 100-105 and 117; |
| A/CN.9/450; | A/CN.9/WG.IV/WP.66; |
| A/CN.9/446, paras. 14-24; | A/CN.9/WG.IV/WP.65; |
| A/CN.9/WG.IV/WP.74; | A/CN.9/406, paras. 90 and 178-179; |
| A/52/17, paras. 248-250; | A/CN.9/WG.IV/WP.55, para. 109-113; |
| A/CN.9/437, paras. 151-155; | A/CN.9/360, paras. 90-95; |
| A/CN.9/WG.IV/WP. 71, paras 77-93; | A/CN.9/WG.IV/WP.53, paras. 77-78; |
| A/51/17, paras. 222-223; | A/CN.9/350, paras. 95-96; |
| A/CN.9/421, paras. 109 and 114; | A/CN.9/333, paras. 66-68. |
| A/CN.9/WG.IV/WP.69, paras. 30, 53, 59-60 and 91; | |

Article 6. Writing

47. Article 6 is intended to define the basic standard to be met by a data message in order to be considered as meeting a requirement (which may result from statute, regulation or judge-made law) that information be retained or presented "in writing" (or that the information be contained in a "document" or other paper-based instrument). It may be noted that article 6 is part of a set of three articles (articles 6, 7 and 8), which share the same structure and should be read together.

48. In the preparation of the Model Law, particular attention was paid to the functions traditionally performed by various kinds of "writings" in a paper-based environment. For example, the following non-exhaustive list indicates reasons why national laws require the use of "writings": (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) to help the parties be aware of the consequences of their entering into a contract; (3) to provide that a document would be legible by all; (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (5) to allow for the reproduction of a document so that each party would hold a copy of the same data; (6) to allow for the authentication of data by means of a signature; (7) to provide that a document would be in a form acceptable to public authorities and courts; (8) to finalize the intent of the author of the "writing" and provide a record of that intent; (9) to allow for the easy storage of data in a tangible form; (10) to facilitate control and sub-sequent audit for accounting, tax or regulatory purposes; and (11) to bring legal rights and obligations into existence in those cases where a "writing" was required for validity purposes.

49. However, in the preparation of the Model Law, it was found that it would be inappropriate to adopt an overly comprehensive notion of the functions performed by writing. Existing requirements that data be presented in written form often combine the requirement of a "writing" with concepts distinct from writing, such as signature and original. Thus, when adopting a functional approach, attention should be given to the fact that the requirement of a "writing" should be considered as the lowest layer in a hierarchy of form requirements, which provide distinct levels of reliability, traceability and unalterability with respect to paper documents. The requirement that data be presented in written form (which can be described as a "threshold

requirement") should thus not be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act". For example, under certain national laws, a written document that is neither dated nor signed, and the author of which either is not identified in the written document or is identified by a mere letterhead, would be regarded as a "writing" although it might be of little evidential weight in the absence of other evidence (e.g., testimony) regarding the authorship of the document. In addition, the notion of unalterability should not be considered as built into the concept of writing as an absolute requirement since a "writing" in pencil might still be considered a "writing" under certain existing legal definitions. Taking into account the way in which such issues as integrity of the data and protection against fraud are dealt with in a paper-based environment, a fraudulent document would nonetheless be regarded as a "writing". In general, notions such as "evidence" and "intent of the parties to bind themselves" are to be tied to the more general issues of reliability and authentication of the data and should not be included in the definition of a "writing".

50. The purpose of article 6 is not to establish a requirement that, in all instances, data messages should fulfil all conceivable functions of a writing. Rather than focusing upon specific functions of a "writing", for example, its evidentiary function in the context of tax law or its warning function in the context of civil law, article 6 focuses upon the basic notion of the information being reproduced and read. That notion is expressed in article 6 in terms that were found to provide an objective criterion, namely that the information in a data message must be accessible so as to be usable for subsequent reference. The use of the word "accessible" is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word "usable" is not intended to cover only human use but also computer processing. As to the notion of "subsequent reference", it was preferred to such notions as "durability" or "non-alterability", which would have established too harsh standards, and to such notions as "readability" or "intelligibility", which might constitute too subjective criteria.

51. The principle embodied in paragraph (3) of articles 6 and 7, and in paragraph (4) of article 8, is that an enacting State may exclude from the application of those articles certain situations to be specified in the legislation enacting the Model Law. An enacting State may wish to exclude specifically certain types of situations, depending in particular on the purpose of the formal requirement in question. One such type of situation may be the case of writing requirements intended to provide notice or warning of specific factual or legal risks, for example, requirements for warnings to be placed on certain types of products. Another specific exclusion might be considered, for example, in the context of formalities required pursuant to international treaty obligations of the enacting State (e.g., the requirement that a cheque be in writing pursuant to the Convention providing a Uniform Law for Cheques, Geneva, 1931) and other kinds of situations and areas of law that are beyond the power of the enacting State to change by means of a statute.

52. Paragraph (3) was included with a view to enhancing the acceptability of the Model Law. It recognizes that the matter of specifying exclusions should be left to enacting States, an approach that would take better account of differences in national circumstances. However, it should be noted that the objectives of the Model Law would not be achieved if paragraph (3) were used to establish blanket exceptions, and the opportunity provided by paragraph (3) in that respect should be avoided. Numerous exclusions from the scope of articles 6 to 8 would raise needless obstacles to the development of modern communication techniques, since what the Model Law contains are very fundamental principles and approaches that are expected to find general application.

References

- A/51/17, paras. 180-181 and 185-187 (article 5);
- A/50/17, paras. 228-241 (article 5);
- A/CN.9/407, paras. 56-63;
- A/CN.9/406, paras. 95-101; A/CN.9/WG.IV/WP.62, article 6;
- A/CN.9/390, paras. 88-96; A/CN.9/WG.IV/WP.60, article 6;
- A/CN.9/387, paras. 66-80; A/CN.9/WG.IV/WP.57, article 6; A/CN.9/WG.IV/WP.58, annex;
- A/CN.9/373, paras. 45-62; A/CN.9/WG.IV/WP.55, paras. 36-49;
- A/CN.9/360, paras. 32-43; A/CN.9/WG.IV/WP.53, paras. 37-45;
- A/CN.9/350, paras. 68-78;
- A/CN.9/333, paras. 20-28;

Article 7. Signature

53. Article 7 is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the Model Law, the following functions of a signature were considered: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text; the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place.

54. It may be noted that, alongside the traditional handwritten signature, there exist various types of procedures (e.g., stamping, perforation), sometimes also referred to as "signatures", which provide various levels of certainty. For example, in some countries, there exists a general requirement that contracts for the sale of goods above a certain amount should be "signed" in order to be enforceable. However, the concept of a signature adopted in that context is such that a stamp, perforation or even a typewritten signature or a printed letterhead might be regarded as sufficient to fulfil the signature requirement. At the other end of the spectrum, there exist requirements that combine the traditional handwritten signature with additional security procedures such as the confirmation of the signature by witnesses.

55. It might be desirable to develop functional equivalents for the various types and levels of signature requirements in existence. Such an approach would increase the level of certainty as to the degree of legal recognition that could be expected from the use of the various means of authentication used in electronic commerce practice as substitutes for "signatures". However, the notion of signature is intimately linked to the use of paper. Furthermore, any attempt to develop rules on standards and procedures to be used as substitutes for specific instances of "signatures" might create the risk of tying the legal framework provided by the Model Law to a given state of technical development.

56. With a view to ensuring that a message that was required to be authenticated should not be denied legal value for the sole reason that it was not authenticated in a manner peculiar to paper documents, article 7 adopts a comprehensive approach. It establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements which currently present barriers to electronic commerce. Article 7 focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document. Paragraph (1)(a) establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.

57. Paragraph (1)(b) establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph (1)(a). The method used under paragraph (1)(a) should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all the circumstances, including any agreement between the originator and the addressee of the data message.

58. In determining whether the method used under paragraph (1) is appropriate, legal, technical and commercial factors that may be taken into account include the following: (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance

and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor.

59. Article 7 does not introduce a distinction between the situation in which users of electronic commerce are linked by a communication agreement and the situation in which parties had no prior contractual relationship regarding the use of electronic commerce. Thus, article 7 may be regarded as establishing a basic standard of authentication for data messages that might be exchanged in the absence of a prior contractual relationship and, at the same time, to provide guidance as to what might constitute an appropriate substitute for a signature if the parties used electronic communications in the context of a communication agreement. The Model Law is thus intended to provide useful guidance both in a context where national laws would leave the question of authentication of data messages entirely to the discretion of the parties and in a context where requirements for signature, which were usually set by mandatory provisions of national law, should not be made subject to alteration by agreement of the parties.

60. The notion of an "agreement between the originator and the addressee of a data message" is to be interpreted as covering not only bilateral or multilateral agreements concluded between parties exchanging directly data messages (e.g., "trading partners agreements", "communication agreements" or "interchange agreements") but also agreements involving intermediaries such as networks (e.g., "third-party service agreements"). Agreements concluded between users of electronic commerce and networks may incorporate "system rules", i.e., administrative and technical rules and procedures to be applied when communicating data messages. However, a possible agreement between originators and addressees of data messages as to the use of a method of authentication is not conclusive evidence of whether that method is reliable or not.

61. It should be noted that, under the Model Law, the mere signing of a data message by means of a functional equivalent of a handwritten signature is not intended, in and of itself, to confer legal validity on the data message. Whether a data message that fulfilled the requirement of a signature has legal validity is to be settled under the law applicable outside the Model Law.

References

A/51/17, paras. 180-181 and 185-187 (article 6);
A/50/17, paras. 242-248 (article 6);
A/CN.9/407, paras. 64-70;
A/CN.9/406, paras. 102-105; A/CN.9/WG.IV/WP.62, article 7;
A/CN.9/390, paras. 97-109; A/CN.9/WG.IV/WP.60, article 7;
A/CN.9/387, paras. 81-90; A/CN.9/WG.IV/WP.57, article 7; A/CN.9/WG.IV/WP.58, annex;
A/CN.9/373, paras. 63-76; A/CN.9/WG.IV/WP.55, paras. 50-63;
A/CN.9/360, paras. 71-75; A/CN.9/WG.IV/WP.53, paras. 61-66;
A/CN.9/350, paras. 86-89;
A/CN.9/333, paras. 50-59;
A/CN.9/265, paras. 49-58 and 79-80.

Article 8. Original

62. If "original" were defined as a medium on which information was fixed for the first time, it would be impossible to speak of "original" data messages, since the addressee of a data message would always receive a copy thereof. However, article 8 should be put in a different context. The notion of "original" in article 8 is useful since in practice many disputes relate to the question of originality of documents, and in electronic commerce the requirement for presentation of originals constitutes one of the main obstacles that the Model Law attempts to remove. Although in some jurisdictions the concepts of "writing", "original" and "signature" may overlap, the Model Law approaches them as three separate and distinct concepts. Article 8 is also useful in clarifying the notions of "writing" and "original", in particular in view of their importance for purposes of evidence.

63. Article 8 is pertinent to documents of title and negotiable instruments, in which the notion of uniqueness of an original is particularly relevant. However, attention is drawn to the fact that the Model Law is not intended only to apply to documents of title and negotiable instruments, or to such areas of law where special requirements exist with respect to registration or notarization of "writings", e.g., family matters or the sale of real estate. Examples of documents that might require an "original" are trade documents such as weight certificates, agricultural certificates, quality or quantity certificates, inspection reports, insurance certificates, etc. While such documents are not negotiable or used to transfer rights or title, it is essential that they be transmitted unchanged, that is in their "original" form, so that other parties in international commerce may have confidence in their contents. In a paper-based environment, these types of document are usually only accepted if they are "original" to lessen the chance that they be altered, which would be difficult to detect in copies. Various technical means are available to certify the contents of a data message to confirm its "originality". Without this functional equivalent of originality, the sale of goods using electronic commerce would be hampered since the issuers of such documents would be required to retransmit their data message each and every time the goods are sold, or the parties would be forced to use paper documents to supplement the electronic commerce transaction.

64. Article 8 should be regarded as stating the minimum acceptable form requirement to be met by a data message for it to be regarded as the functional equivalent of an original. The provisions of article 8 should be regarded as mandatory, to the same extent that existing provisions regarding the use of paper-based original documents would be regarded as mandatory. The indication that the form requirements stated in article 8 are to be regarded as the "minimum acceptable" should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

65. Article 8 emphasizes the importance of the integrity of the information for its originality and sets out criteria to be taken into account when assessing integrity by reference to systematic recording of the information, assurance that the information was recorded without lacunae and protection of the data against alteration. It links the concept of originality to a method of authentication and puts the focus on the method of authentication to be followed in order to meet the requirement. It is based on the following elements: a simple criterion as to "integrity" of the data; a description of the elements to be taken into account in assessing the integrity; and an element of flexibility, i.e., a reference to circumstances.

66. As regards the words "the time when it was first generated in its final form" in paragraph (1)(a), it should be noted that the provision is intended to encompass the situation where information was first composed as a paper document and subsequently transferred on to a computer. In such a situation, paragraph (1)(a) is to be interpreted as requiring assurances that the information has remained complete and unaltered from the time when it was composed as a paper document onwards, and not only as from the time when it was translated into electronic form. However, where several drafts were created and stored before the final message was composed, paragraph (1)(a) should not be misinterpreted as requiring assurance as to the integrity of the drafts.

67. Paragraph (3)(a) sets forth the criteria for assessing integrity, taking care to except necessary additions to the first (or "original") data message such as endorsements, certifications, notarizations, etc. from other alterations. As long as the contents of a data message remain complete and unaltered, necessary additions to that data message would not affect its "originality". Thus when an electronic certificate is added to the end of an "original" data message to attest to the "originality" of that data message, or when data is automatically added by computer systems at the start and the finish of a data message in order to transmit it, such additions would be considered as if they were a supplemental piece of paper with an "original" piece of paper, or the envelope and stamp used to send that "original" piece of paper.

68. As in other articles of chapter II of part one, the words "the law" in the opening phrase of article 8 are to be understood as encompassing not only statutory or regulatory law but also judicially-created law and other procedural law. In certain common law countries, where the words "the law" would normally be interpreted as referring to common law rules, as opposed to

statutory requirements, it should be noted that, in the context of the Model Law, the words "the law" are intended to encompass those various sources of law. However, "the law", as used in the Model Law, is not meant to include areas of law that have not become part of the law of a State and are sometimes, somewhat imprecisely, referred to by expressions such as "lex mercatoria" or "law merchant".

69. Paragraph (4), as was the case with similar provisions in articles 6 and 7, was included with a view to enhancing the acceptability of the Model Law. It recognizes that the matter of specifying exclusions should be left to enacting States, an approach that would take better account of differences in national circumstances. However, it should be noted that the objectives of the Model Law would not be achieved if paragraph (4) were used to establish blanket exceptions. Numerous exclusions from the scope of articles 6 to 8 would raise needless obstacles to the development of modern communication techniques, since what the Model Law contains are very fundamental principles and approaches that are expected to find general application.

References

A/51/17, paras. 180-181 and 185-187 (article 7);
A/50/17, paras. 249-255 (article 7);
A/CN.9/407, paras. 71-79;
A/CN.9/406, paras. 106-110; A/CN.9/WG.IV/WP.62, article 8;
A/CN.9/390, paras. 110-133; A/CN.9/WG.IV/WP.60, article 8;
A/CN.9/387, paras. 91-97; A/CN.9/WG.IV/WP.57, article 8; A/CN.9/WG.IV/WP.58, annex;
A/CN.9/373, paras. 77-96;
A/CN.9/WG.IV/WP.55, paras. 64-70;
A/CN.9/360, paras. 60-70; A/CN.9/WG.IV/WP.53, paras. 56-60;
A/CN.9/350, paras. 84-85;
A/CN.9/265, paras. 43-48.

Article 9. Admissibility and evidential weight of data messages

70. The purpose of article 9 is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value. With respect to admissibility, paragraph (1), establishing that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, puts emphasis on the general principle stated in article 4 and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdictions. The term "best evidence" is a term understood in, and necessary for, certain common law jurisdictions. However, the notion of "best evidence" could raise a great deal of uncertainty in legal systems in which such a rule is unknown. States in which the term would be regarded as meaningless and potentially misleading may wish to enact the Model Law without the reference to the "best evidence" rule contained in paragraph (1).

71. As regards the assessment of the evidential weight of a data message, paragraph (2) provides useful guidance as to how the evidential value of data messages should be assessed (e.g., depending on whether they were generated, stored or communicated in a reliable manner).

References

A/50/17, paras. 256-263 (article 8);
A/CN.9/407, paras. 80-81;
A/CN.9/406, paras. 111-113; A/CN.9/WG.IV/WP.62, article 9;
A/CN.9/390, paras. 139-143; A/CN.9/WG.IV/WP.60, article 9;
A/CN.9/387, paras. 98-109; A/CN.9/WG.IV/WP.57, article 9; A/CN.9/WG.IV/WP.58, annex;
A/CN.9/373, paras. 97-108; A/CN.9/WG.IV/WP.55, paras. 71-81;
A/CN.9/360, paras. 44-59; A/CN.9/WG.IV/WP.53, paras. 46-55;
A/CN.9/350, paras. 79-83 and 90-91;
A/CN.9/333, paras. 29-41;
A/CN.9/265, paras. 27-48.

Article 10. Retention of data messages

72. Article 10 establishes a set of alternative rules for existing requirements regarding the storage of information (e.g., for accounting or tax purposes) that may constitute obstacles to the development of modern trade.

73. Paragraph (1) is intended to set out the conditions under which the obligation to store data messages that might exist under the applicable law would be met. Subparagraph (a) reproduces the conditions established under article 6 for a data message to satisfy a rule which prescribes the presentation of a "writing". Subparagraph (b) emphasizes that the message does not need to be retained unaltered as long as the information stored accurately reflects the data message as it was sent. It would not be appropriate to require that information should be stored unaltered, since usually messages are decoded, compressed or converted in order to be stored.

74. Subparagraph (c) is intended to cover all the information that may need to be stored, which includes, apart from the message itself, certain transmittal information that may be necessary for the identification of the message. Subparagraph (c), by imposing the retention of the transmittal information associated with the data message, is creating a standard that is higher than most standards existing under national laws as to the storage of paper-based communications. However, it should not be understood as imposing an obligation to retain transmittal information additional to the information contained in the data message when it was generated, stored or transmitted, or information contained in a separate data message, such as an acknowledgement of receipt. Moreover, while some transmittal information is important and has to be stored, other transmittal information can be exempted without the integrity of the data message being compromised. That is the reason why subparagraph (c) establishes a distinction between those elements of transmittal information that are important for the identification of the message and the very few elements of transmittal information covered in paragraph (2) (e.g., communication protocols), which are of no value with regard to the data message and which, typically, would automatically be stripped out of an incoming data message by the receiving computer before the data message actually entered the information system of the addressee.

75. In practice, storage of information, and especially storage of transmittal information, may often be carried out by someone other than the originator or the addressee, such as an intermediary. Nevertheless, it is intended that the person obligated to retain certain transmittal information cannot escape meeting that obligation simply because, for example, the communications system operated by that other person does not retain the required information. This is intended to discourage bad practice or wilful misconduct. Paragraph (3) provides that in meeting its obligations under paragraph (1), an addressee or originator may use the services of any third party, not just an intermediary.

References

A/51/17, paras. 185-187 (article 9);
A/50/17, paras. 264-270 (article 9);
A/CN.9/407, paras. 82-84;
A/CN.9/406, paras. 59-72; A/CN.9/WG.IV/WP.60, article 14;
A/CN.9/387, paras. 164-168;
A/CN.9/WG.IV/WP.57, article 14;
A/CN.9/373, paras. 123-125; A/CN.9/WG.IV/WP.55, para. 94.

Chapter III. Communication of data messages

Article 11. Formation and validity of contracts

76. Article 11 is not intended to interfere with the law on formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed. In certain countries, a provision along the lines of paragraph (1) might be regarded as merely stating the obvious, namely that an offer and an acceptance, as any other expression of will, can be communicated by any means, including data messages. However, the provision is needed in view of the remaining uncertainties in a

considerable number of countries as to whether contracts can validly be concluded by electronic means. Such uncertainties may stem from the fact that, in certain cases, the data messages expressing offer and acceptance are generated by computers without immediate human intervention, thus raising doubts as to the expression of intent by the parties. Another reason for such uncertainties is inherent in the mode of communication and results from the absence of a paper document.

77. It may also be noted that paragraph (1) reinforces, in the context of contract formation, a principle already embodied in other articles of the Model Law, such as articles 5, 9 and 13, all of which establish the legal effectiveness of data messages. However, paragraph (1) is needed since the fact that electronic messages may have legal value as evidence and produce a number of effects, including those provided in articles 9 and 13, does not necessarily mean that they can be used for the purpose of concluding valid contracts.

78. Paragraph (1) covers not merely the cases in which both the offer and the acceptance are communicated by electronic means but also cases in which only the offer or only the acceptance is communicated electronically. As to the time and place of formation of contracts in cases where an offer or the acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to contract formation. It was felt that such a provision might exceed the aim of the Model Law, which should be limited to providing that electronic communications would achieve the same degree of legal certainty as paper-based communications. The combination of existing rules on the formation of contracts with the provisions contained in article 15 is designed to dispel uncertainty as to the time and place of formation of contracts in cases where the offer or the acceptance are exchanged electronically.

79. The words "unless otherwise stated by the parties", which merely restate, in the context of contract formation, the recognition of party autonomy expressed in article 4, are intended to make it clear that the purpose of the Model Law is not to impose the use of electronic means of communication on parties who rely on the use of paper-based communication to conclude contracts. Thus, article 11 should not be interpreted as restricting in any way party autonomy with respect to parties not involved in the use of electronic communication.

80. During the preparation of paragraph (1), it was felt that the provision might have the harmful effect of overruling otherwise applicable provisions of national law, which might prescribe specific formalities for the formation of certain contracts. Such forms include notarization and other requirements for "writings", and might respond to considerations of public policy, such as the need to protect certain parties or to warn them against specific risks. For that reason, paragraph (2) provides that an enacting State can exclude the application of paragraph (1) in certain instances to be specified in the legislation enacting the Model Law.

References

A/51/17, paras. 89-94 (article 13);
A/CN.9/407, para. 93;
A/CN.9/406, paras. 34-41; A/CN.9/WG.IV/WP.60, article 12;
A/CN.9/387, paras. 145-151; A/CN.9/WG.IV/WP.57, article 12;
A/CN.9/373, paras. 126-133; A/CN.9/WG.IV/WP.55, paras. 95-102;
A/CN.9/360, paras. 76-86; A/CN.9/WG.IV/WP.53, paras. 67-73;
A/CN.9/350, paras. 93-96;
A/CN.9/333, paras. 60-68.

Article 12. Recognition by parties of data messages

81. Article 12 was added at a late stage in the preparation of the Model Law, in recognition of the fact that article 11 was limited to dealing with data messages that were geared to the conclusion of a contract, but that the draft Model Law did not contain specific provisions on data messages that related not to the conclusion of contracts but to the performance of contractual obligations (e.g., notice of defective goods, an offer to pay, notice of place where a contract would be performed, recognition of debt). Since modern means of communication are used in a context of legal

uncertainty, in the absence of specific legislation in most countries, it was felt appropriate for the Model Law not only to establish the general principle that the use of electronic communication should not be discriminated against, as expressed in article 5, but also to include specific illustrations of that principle. Contract formation is but one of the areas where such an illustration is useful and the legal validity of unilateral expressions of will, as well as other notices or statements that may be issued in the form of data messages, also needs to be mentioned.

82. As is the case with article 11, article 12 is not to impose the use of electronic means of communication but to validate such use, subject to contrary agreement by the parties. Thus, article 12 should not be used as a basis to impose on the addressee the legal consequences of a message, if the use of a non-paper-based method for its transmission comes as a surprise to the addressee.

References

A/51/17, paras. 95-99 (new article 13 *bis*).

Article 13. Attribution of data messages

83. Article 13 has its origin in article 5 of the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order. Article 13 is intended to apply where there is a question as to whether a data message was really sent by the person who is indicated as being the originator. In the case of a paper-based communication the problem would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorized person may have sent the message but the authentication by code, encryption or the like would be accurate. The purpose of article 13 is not to assign responsibility. It deals rather with attribution of data messages by establishing a presumption that under certain circumstances a data message would be considered as a message of the originator, and goes on to qualify that presumption in case the addressee knew or ought to have known that the data message was not that of the originator.

84. Paragraph (1) recalls the principle that an originator is bound by a data message if it has effectively sent that message. Paragraph (2) refers to the situation where the message was sent by a person other than the originator who had the authority to act on behalf of the originator. Paragraph (2) is not intended to displace the domestic law of agency, and the question as to whether the other person did in fact and in law have the authority to act on behalf of the originator is left to the appropriate legal rules outside the Model Law.

85. Paragraph (3) deals with two kinds of situations, in which the addressee could rely on a data message as being that of the originator: firstly, situations in which the addressee properly applied an authentication procedure previously agreed to by the originator; and secondly, situations in which the data message resulted from the actions of a person who, by virtue of its relationship with the originator, had access to the originator's authentication procedures. By stating that the addressee "is entitled to regard a data as being that of the originator", paragraph (3) read in conjunction with paragraph (4)(a) is intended to indicate that the addressee could act on the assumption that the data message is that of the originator up to the point in time it received notice from the originator that the data message was not that of the originator, or up to the point in time when it knew or should have known that the data message was not that of the originator.

86. Under paragraph (3)(a) , if the addressee applies any authentication procedures previously agreed to by the originator and such application results in the proper verification of the originator as the source of the message, the message is presumed to be that of the originator. That covers not only the situation where an authentication procedure has been agreed upon by the originator and the addressee but also situations where an originator, unilaterally or as a result of an agreement with an intermediary, identified a procedure and agreed to be bound by a data message that met the requirements corresponding to that procedure. Thus, agreements that became effective not through direct agreement between the originator and the addressee but through the participation of third-party service providers are intended to be covered by paragraph (3)(a) . However, it should be noted that paragraph (3)(a) applies only when the communication between the originator and the addressee is based on a previous agreement, but that it does not apply in an open environment.

87. The effect of paragraph (3)(b) , read in conjunction with paragraph (4)(b) , is that the originator or the addressee, as the case may be, is responsible for any unauthorized data message that can be shown to have been sent as a result of negligence of that party.

88. Paragraph (4)(a) should not be misinterpreted as relieving the originator from the consequences of sending a data message, with retroactive effect, irrespective of whether the addressee had acted on the assumption that the data message was that of the originator. Paragraph (4) is not intended to provide that receipt of a notice under subparagraph (a) would nullify the original message retroactively. Under subparagraph (a) , the originator is released from the binding effect of the message after the time notice is received and not before that time. Moreover, paragraph (4) should not be read as allowing the originator to avoid being bound by the data message by sending notice to the addressee under subparagraph (a) , in a case where the message had, in fact, been sent by the originator and the addressee properly applied agreed or reasonable authentication procedures. If the addressee can prove that the message is that of the originator, paragraph (1) would apply and not paragraph (4)(a) . As to the meaning of "reasonable time", the notice should be such as to give the addressee sufficient time to react. For example, in the case of just-in-time supply, the addressee should be given time to adjust its production chain.

89. With respect to paragraph (4)(b) , it should be noted that the Model Law could lead to the result that the addressee would be entitled to rely on a data message under paragraph (3)(a) if it had properly applied the agreed authentication procedures, even if it knew that the data message was not that of the originator. It was generally felt when preparing the Model Law that the risk that such a situation could arise should be accepted, in view of the need for preserving the reliability of agreed authentication procedures.

90. Paragraph (5) is intended to preclude the originator from disavowing the message once it was sent, unless the addressee knew, or should have known, that the data message was not that of the originator. In addition, paragraph (5) is intended to deal with errors in the content of the message arising from errors in transmission.

91. Paragraph (6) deals with the issue of erroneous duplication of data messages, an issue of considerable practical importance. It establishes the standard of care to be applied by the addressee to distinguish an erroneous duplicate of a data message from a separate data message.

92. Early drafts of article 13 contained an additional paragraph, expressing the principle that the attribution of authorship of a data message to the originator should not interfere with the legal consequences of that message, which should be determined by other applicable rules of national law. It was later felt that it was not necessary to express that principle in the Model Law but that it should be mentioned in this Guide.

References

A/51/17, paras. 189-194 (article 11);
A/50/17, paras. 275-303 (article 11);
A/CN.9/407, paras. 86-89;
A/CN.9/406, paras. 114-131; A/CN.9/WG.IV/WP.62, article 10;
A/CN.9/390, paras. 144-153; A/CN.9/WG.IV/WP.60, article 10;
A/CN.9/387, paras. 110-132; A/CN.9/WG.IV/WP.57, article 10;
A/CN.9/373, paras. 109-115; A/CN.9/WG.IV/WP.55, paras. 82-86.

Article 14. Acknowledgement of receipt

93. The use of functional acknowledgements is a business decision to be made by users of electronic commerce; the Model Law does not intend to impose the use of any such procedure. However, taking into account the commercial value of a system of acknowledgement of receipt and the widespread use of such systems in the context of electronic commerce, it was felt that the Model Law should address a number of legal issues arising from the use of acknowledgement procedures. It should be noted that the notion of "acknowledgement" is sometimes used to cover a

variety of procedures, ranging from a mere acknowledgement of receipt of an unspecified message to an expression of agreement with the content of a specific data message. In many instances, the procedure of "acknowledgement" would parallel the system known as "return receipt requested" in postal systems. Acknowledgements of receipt may be required in a variety of instruments, e.g., in the data message itself, in bilateral or multilateral communication agreements, or in "system rules". It should be borne in mind that variety among acknowledgement procedures implies variety of the related costs. The provisions of article 14 are based on the assumption that acknowledgement procedures are to be used at the discretion of the originator. Article 14 is not intended to deal with the legal consequences that may flow from sending an acknowledgement of receipt, apart from establishing receipt of the data message. For example, where an originator sends an offer in a data message and requests acknowledgement of receipt, the acknowledgement of receipt simply evidences that the offer has been received. Whether or not sending that acknowledgement amounted to accepting the offer is not dealt with by the Model Law but by contract law outside the Model Law.

94. The purpose of paragraph (2) is to validate acknowledgement by any communication or conduct of the addressee (e.g., the shipment of the goods as an acknowledgement of receipt of a purchase order) where the originator has not agreed with the addressee that the acknowledgement should be in a particular form. The situation where an acknowledgement has been unilaterally requested by the originator to be given in a specific form is not expressly addressed by article 14, which may entail as a possible consequence that a unilateral requirement by the originator as to the form of acknowledgements would not affect the right of the addressee to acknowledge receipt by any communication or conduct sufficient to indicate to the originator that the message had been received. Such a possible interpretation of paragraph (2) makes it particularly necessary to emphasize in the Model Law the distinction to be drawn between the effects of an acknowledgement of receipt of a data message and any communication in response to the content of that data message, a reason why paragraph (7) is needed.

95. Paragraph (3), which deals with the situation where the originator has stated that the data message is conditional on receipt of an acknowledgement, applies whether or not the originator has specified that the acknowledgement should be received by a certain time.

96. The purpose of paragraph (4) is to deal with the more common situation where an acknowledgement is requested, without any statement being made by the originator that the data message is of no effect until an acknowledgement has been received. Such a provision is needed to establish the point in time when the originator of a data message who has requested an acknowledgement of receipt is relieved from any legal implication of sending that data message if the requested acknowledgement has not been received. An example of a factual situation where a provision along the lines of paragraph (4) would be particularly useful would be that the originator of an offer to contract who has not received the requested acknowledgement from the addressee of the offer may need to know the point in time after which it is free to transfer the offer to another party. It may be noted that the provision does not create any obligation binding on the originator, but merely establishes means by which the originator, if it so wishes, can clarify its status in cases where it has not received the requested acknowledgement. It may also be noted that the provision does not create any obligation binding on the addressee of the data message, who would, in most circumstances, be free to rely or not to rely on any given data message, provided that it would bear the risk of the data message being unreliable for lack of an acknowledgement of receipt. The addressee, however, is protected since the originator who does not receive a requested acknowledgement may not automatically treat the data message as though it had never been transmitted, without giving further notice to the addressee. The procedure described under paragraph (4) is purely at the discretion of the originator. For example, where the originator sent a data message which under the agreement between the parties had to be received by a certain time, and the originator requested an acknowledgement of receipt, the addressee could not deny the legal effectiveness of the message simply by withholding the requested acknowledgement.

97. The rebuttable presumption established in paragraph (5) is needed to create certainty and would be particularly useful in the context of electronic communication between parties that are not linked by a trading-partners agreement. The second sentence of paragraph (5) should be read in conjunction with paragraph (5) of article 13, which establishes the conditions under which, in case of an inconsistency between the text of the data message as sent and the text as received, the

text as received prevails.

98. Paragraph (6) corresponds to a certain type of acknowledgement, for example, an EDIFACT message establishing that the data message received is syntactically correct, i.e., that it can be processed by the receiving computer. The reference to technical requirements, which is to be construed primarily as a reference to "data syntax" in the context of EDI communications, may be less relevant in the context of the use of other means of communication, such as telegram or telex. In addition to mere consistency with the rules of "data syntax", technical requirements set forth in applicable standards may include, for example, the use of procedures verifying the integrity of the contents of data messages.

99. Paragraph (7) is intended to dispel uncertainties that might exist as to the legal effect of an acknowledgement of receipt. For example, paragraph (7) indicates that an acknowledgement of receipt should not be confused with any communication related to the contents of the acknowledged message.

References

A/51/17, paras. 63-88 (article 12);
A/CN.9/407, paras. 90-92;
A/CN.9/406, paras. 15-33; A/CN.9/WG.IV/WP.60, article 11;
A/CN.9/387, paras. 133-144; A/CN.9/WG.IV/WP.57, article 11;
A/CN.9/373, paras. 116-122; A/CN.9/WG.IV/WP.55, paras. 87-93;
A/CN.9/360, para. 125; A/CN.9/WG.IV/WP.53, paras. 80-81;
A/CN.9/350, para. 92;
A/CN.9/333, paras. 48-49.

Article 15. Time and place of dispatch and receipt of data messages

100. Article 15 results from the recognition that, for the operation of many existing rules of law, it is important to ascertain the time and place of receipt of information. The use of electronic communication techniques makes those difficult to ascertain. It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change. The Model Law is thus intended to reflect the fact that the location of information systems is irrelevant and sets forth a more objective criterion, namely, the place of business of the parties. In that connection, it should be noted that article 15 is not intended to establish a conflict-of-laws rule.

101. Paragraph (1) defines the time of dispatch of a data message as the time when the data message enters an information system outside the control of the originator, which may be the information system of an intermediary or an information system of the addressee. The concept of "dispatch" refers to the commencement of the electronic transmission of the data message. Where "dispatch" already has an established meaning, article 15 is intended to supplement national rules on dispatch and not to displace them. If dispatch occurs when the data message reaches an information system of the addressee, dispatch under paragraph (1) and receipt under paragraph (2) are simultaneous, except where the data message is sent to an information system of the addressee that is not the information system designated by the addressee under paragraph (2)(a) .

102. Paragraph (2), the purpose of which is to define the time of receipt of a data message, addresses the situation where the addressee unilaterally designates a specific information system for the receipt of a message (in which case the designated system may or may not be an information system of the addressee), and the data message reaches an information system of the addressee that is not the designated system. In such a situation, receipt is deemed to occur when the data message is retrieved by the addressee. By "designated information system", the Model Law is intended to cover a system that has been specifically designated by a party, for instance in the case where an offer expressly specifies the address to which acceptance should be sent. The mere indication of an electronic mail or telecopy address on a letterhead or other document should not be regarded as express designation of one or more information systems.

103. Attention is drawn to the notion of "entry" into an information system, which is used for both the definition of dispatch and that of receipt of a data message. A data message enters an information system at the time when it becomes available for processing within that information system. Whether a data message which enters an information system is intelligible or usable by the addressee is outside the purview of the Model Law. The Model Law does not intend to overrule provisions of national law under which receipt of a message may occur at the time when the message enters the sphere of the addressee, irrespective of whether the message is intelligible or usable by the addressee. Nor is the Model Law intended to run counter to trade usages, under which certain encoded messages are deemed to be received even before they are usable by, or intelligible for, the addressee. It was felt that the Model Law should not create a more stringent requirement than currently exists in a paper-based environment, where a message can be considered to be received even if it is not intelligible for the addressee or not intended to be intelligible to the addressee (e.g., where encrypted data is transmitted to a depository for the sole purpose of retention in the context of intellectual property rights protection).

104. A data message should not be considered to be dispatched if it merely reached the information system of the addressee but failed to enter it. It may be noted that the Model Law does not expressly address the question of possible malfunctioning of information systems as a basis for liability. In particular, where the information system of the addressee does not function at all or functions improperly or, while functioning properly, cannot be entered into by the data message (e.g., in the case of a telecopier that is constantly occupied), dispatch under the Model Law does not occur. It was felt during the preparation of the Model Law that the addressee should not be placed under the burdensome obligation to maintain its information system functioning at all times by way of a general provision.

105. The purpose of paragraph (4) is to deal with the place of receipt of a data message. The principal reason for including a rule on the place of receipt of a data message is to address a circumstance characteristic of electronic commerce that might not be treated adequately under existing law, namely, that very often the information system of the addressee where the data message is received, or from which the data message is retrieved, is located in a jurisdiction other than that in which the addressee itself is located. Thus, the rationale behind the provision is to ensure that the location of an information system is not the determinant element, and that there is some reasonable connection between the addressee and what is deemed to be the place of receipt, and that that place can be readily ascertained by the originator. The Model Law does not contain specific provisions as to how the designation of an information system should be made, or whether a change could be made after such a designation by the addressee.

106. Paragraph (4), which contains a reference to the "underlying transaction", is intended to refer to both actual and contemplated underlying transactions. References to "place of business", "principal place of business" and "place of habitual residence" were adopted to bring the text in line with article 10 of the United Nations Convention on Contracts for the International Sale of Goods.

107. The effect of paragraph (4) is to introduce a distinction between the deemed place of receipt and the place actually reached by a data message at the time of its receipt under paragraph (2). That distinction is not to be interpreted as apportioning risks between the originator and the addressee in case of damage or loss of a data message between the time of its receipt under paragraph (2) and the time when it reached its place of receipt under paragraph (4). Paragraph (4) merely establishes an irrebuttable presumption regarding a legal fact, to be used where another body of law (e.g., on formation of contracts or conflict of laws) require determination of the place of receipt of a data message. However, it was felt during the preparation of the Model Law that introducing a deemed place of receipt, as distinct from the place actually reached by that data message at the time of its receipt, would be inappropriate outside the context of computerized transmissions (e.g., in the context of telegram or telex). The provision was thus limited in scope to cover only computerized transmissions of data messages. A further limitation is contained in paragraph (5), which reproduces a provision already included in articles 6, 7, 8, 11 and 12 (see above, para. 69).

A/51/17, paras. 100-115 (article 14);
A/CN.9/407, paras. 94-99;
A/CN.9/406, paras. 42-58; A/CN.9/WG.IV/WP.60, article 13;
A/CN.9/387, paras. 152-163; A/CN.9/WG.IV/WP.57, article 13;
A/CN.9/373, paras. 134-146; A/CN.9/WG.IV/WP.55, paras. 103-108;
A/CN.9/360, paras. 87-89; A/CN.9/WG.IV/WP.53, paras. 74-76;
A/CN.9/350, paras. 97-100;
A/CN.9/333, paras. 69-75.

Part two. Electronic commerce in specific areas

108. As distinct from the basic rules applicable to electronic commerce in general, which appear as part one of the Model Law, part two contains rules of a more specific nature. In preparing the Model Law, the Commission agreed that such rules dealing with specific uses of electronic commerce should appear in the Model Law in a way that reflected both the specific nature of the provisions and their legal status, which should be the same as that of the general provisions contained in part one of the Model Law. While the Commission, when adopting the Model Law, only considered such specific provisions in the context of transport documents, it was agreed that such provisions should appear as chapter I of part two of the Model Law. It was felt that adopting such an open-ended structure would make it easier to add further specific provisions to the Model Law, as the need might arise, in the form of additional chapters in part two.

109. The adoption of a specific set of rules dealing with specific uses of electronic commerce, such as the use of EDI messages as substitutes for transport documents does not imply that the other provisions of the Model Law are not applicable to such documents. In particular, the provisions of part two, such as articles 16 and 17 concerning transfer of rights in goods, presuppose that the guarantees of reliability and authenticity contained in articles 6 to 8 of the Model Law are also applicable to electronic equivalents to transport documents. Part two of the Model Law does not in any way limit or restrict the field of application of the general provisions of the Model Law.

Chapter I. Carriage of goods

110. In preparing the Model Law, the Commission noted that the carriage of goods was the context in which electronic communications were most likely to be used and in which a legal framework facilitating the use of such communications was most urgently needed. Articles 16 and 17 contain provisions that apply equally to non-negotiable transport documents and to transfer of rights in goods by way of transferable bills of lading. The principles embodied in articles 16 and 17 are applicable not only to maritime transport but also to transport of goods by other means, such as road, railroad and air transport.

Article 16. Actions related to contracts of carriage of goods

111. Article 16, which establishes the scope of chapter I of part two of the Model Law, is broadly drafted. It would encompass a wide variety of documents used in the context of the carriage of goods, including, for example, charter-parties. In the preparation of the Model Law, the Commission found that, by dealing comprehensively with contracts of carriage of goods, article 16 was consistent with the need to cover all transport documents, whether negotiable or non-negotiable, without excluding any specific document such as charter-parties. It was pointed out that, if an enacting State did not wish chapter I of part two to apply to a particular kind of document or contract, for example if the inclusion of such documents as charter-parties in the scope of that chapter was regarded as inappropriate under the legislation of an enacting State, that State could make use of the exclusion clause contained in paragraph (7) of article 17.

112. Article 16 is of an illustrative nature and, although the actions mentioned therein are more common in maritime trade, they are not exclusive to such type of trade and could be performed in connection with air transport or multimodal carriage of goods.

References

A/51/17, paras. 139-172 and 198-204 (draft article x);
A/CN.9/421, paras. 53-103; A/CN.9/WG.IV/WP.69, paras. 82-95;
A/50/17, paras. 307-309;
A/CN.9/407, paras. 106-118; A/CN.9/WG.IV/WP.67, annex; A/CN.9/WG.IV/WP.66, annex II;
A/49/17, paras. 198, 199 and 201;
A/CN.9/390, para. 155-158.

Article 17. Transport documents

113. Paragraphs (1) and (2) are derived from article 6. In the context of transport documents, it is necessary to establish not only functional equivalents of written information about the actions referred to in article 16, but also functional equivalents of the performance of such actions through the use of paper documents. Functional equivalents are particularly needed for the transfer of rights and obligations by transfer of written documents. For example, paragraphs (1) and (2) are intended to replace both the requirement for a written contract of carriage and the requirements for endorsement and transfer of possession of a bill of lading. It was felt in the preparation of the Model Law that the focus of the provision on the actions referred to in article 16 should be expressed clearly, particularly in view of the difficulties that might exist, in certain countries, for recognizing the transmission of a data message as functionally equivalent to the physical transfer of goods, or to the transfer of a document of title representing the goods.

114. The reference to "one or more data messages" in paragraphs (1), (3) and (6) is not intended to be interpreted differently from the reference to "a data message" in the other provisions of the Model Law, which should also be understood as covering equally the situation where only one data message is generated and the situation where more than one data message is generated as support of a given piece of information. A more detailed wording was adopted in article 17 merely to reflect the fact that, in the context of transfer of rights through data messages, some of the functions traditionally performed through the single transmission of a paper bill of lading would necessarily imply the transmission of more than one data message and that such a fact, in itself, should entail no negative consequence as to the acceptability of electronic commerce in that area.

115. Paragraph (3), in combination with paragraph (4), is intended to ensure that a right can be conveyed to one person only, and that it would not be possible for more than one person at any point in time to lay claim to it. The effect of the two paragraphs is to introduce a requirement which may be referred to as the "guarantee of singularity". If procedures are made available to enable a right or obligation to be conveyed by electronic methods instead of by using a paper document, it is necessary that the guarantee of singularity be one of the essential features of such procedures. Technical security devices providing such a guarantee of singularity would almost necessarily be built into any communication system offered to the trading communities and would need to demonstrate their reliability. However, there is also a need to overcome requirements of law that the guarantee of singularity be demonstrated, for example in the case where paper documents such as bills of lading are traditionally used. A provision along the lines of paragraph (3) is thus necessary to permit the use of electronic communication instead of paper documents.

116. The words "one person and no other person" should not be interpreted as excluding situations where more than one person might jointly hold title to the goods. For example, the reference to "one person" is not intended to exclude joint ownership of rights in the goods or other rights embodied in a bill of lading.

117. The notion that a data message should be "unique" may need to be further clarified, since it may lend itself to misinterpretation. On the one hand, all data messages are necessarily unique, even if they duplicate an earlier data message, since each data message is sent at a different time from any earlier data message sent to the same person. If a data message is sent to a different person, it is even more obviously unique, even though it might be transferring the same right or obligation. Yet, all but the first transfer might be fraudulent. On the other hand, if "unique" is interpreted as referring to a data message of a unique kind, or a transfer of a unique kind, then in that sense no data message is unique, and no transfer by means of a data message is unique. Having considered the risk of such misinterpretation, the Commission decided to retain the reference to the concepts of uniqueness of the data message and uniqueness of the transfer for the

purposes of article 17, in view of the fact that the notions of "uniqueness" or "singularity" of transport documents were not unknown to practitioners of transport law and users of transport documents. It was decided, however, that this Guide should clarify that the words "a reliable method is used to render such data message or messages unique" should be interpreted as referring to the use of a reliable method to secure that data messages purporting to convey any right or obligation of a person might not be used by, or on behalf of, that person inconsistently with any other data messages by which the right or obligation was conveyed by or on behalf of that person.

118. Paragraph (5) is a necessary complement to the guarantee of singularity contained in paragraph (3). The need for security is an overriding consideration and it is essential to ensure not only that a method is used that gives reasonable assurance that the same data message is not multiplied, but also that no two media can be simultaneously used for the same purpose. Paragraph (5) addresses the fundamental need to avoid the risk of duplicate transport documents. The use of multiple forms of communication for different purposes, e.g., paper-based communications for ancillary messages and electronic communications for bills of lading, does not pose a problem. However, it is essential for the operation of any system relying on electronic equivalents of bills of lading to avoid the possibility that the same rights could at any given time be embodied both in data messages and in a paper document. Paragraph (5) also envisages the situation where a party having initially agreed to engage in electronic communications has to switch to paper communications where it later becomes unable to sustain electronic communications.

119. The reference to "terminating" the use of data messages is open to interpretation. In particular, the Model Law does not provide information as to who would effect the termination. Should an enacting State decide to provide additional information in that respect, it might wish to indicate, for example, that, since electronic commerce is usually based on the agreement of the parties, a decision to "drop down" to paper communications should also be subject to the agreement of all interested parties. Otherwise, the originator would be given the power to choose unilaterally the means of communication. Alternatively, an enacting State might wish to provide that, since paragraph (5) would have to be applied by the bearer of a bill of lading, it should be up to the bearer to decide whether it preferred to exercise its rights on the basis of a paper bill of lading or on the basis of the electronic equivalent of such a document, and to bear the costs for its decision.

120. Paragraph (5), while expressly dealing with the situation where the use of data messages is replaced by the use of a paper document, is not intended to exclude the reverse situation. The switch from data messages to a paper document should not affect any right that might exist to surrender the paper document to the issuer and start again using data messages.

121. The purpose of paragraph (6) is to deal directly with the application of certain laws to contracts for the carriage of goods by sea. For example, under the Hague and Hague-Visby Rules, a contract of carriage means a contract that is covered by a bill of lading. Use of a bill of lading or similar document of title results in the Hague and Hague-Visby Rules applying compulsorily to a contract of carriage. Those rules would not automatically apply to contracts effected by one or more data message. Thus, a provision such as paragraph (6) is needed to ensure that the application of those rules is not excluded by the mere fact that data messages are used instead of a bill of lading in paper form. While paragraph (1) ensures that data messages are effective means for carrying out any of the actions listed in article 16, that provision does not deal with the substantive rules of law that might apply to a contract contained in, or evidenced by, data messages.

122. As to the meaning of the phrase "that rule shall not be inapplicable" in paragraph (6), a simpler way of expressing the same idea might have been to provide that rules applicable to contracts of carriage evidenced by paper documents should also apply to contracts of carriage evidenced by data messages. However, given the broad scope of application of article 17, which covers not only bills of lading but also a variety of other transport documents, such a simplified provision might have had the undesirable effect of extending the applicability of rules such as the Hamburg Rules and the Hague-Visby Rules to contracts to which such rules were never intended to apply. The Commission felt that the adopted wording was more suited to overcome the

obstacle resulting from the fact that the Hague-Visby Rules and other rules compulsorily applicable to bills of lading would not automatically apply to contracts of carriage evidenced by data messages, without inadvertently extending the application of such rules to other types of contracts.

References

A/51/17, paras. 139-172 and 198-204 (draft article x);
A/CN.9/421, paras. 53-103; A/CN.9/WG.IV/WP.69, paras 82-95;
A/50/17, paras. 307-309
A/CN.9/407, paras. 106-118 A/CN.9/WG.IV/WP.67, annex; A/CN.9/WG.IV/WP.66, annex II;
A/49/17, paras. 198, 199 and 201;
A/CN.9/390, para. 155-158.

III. HISTORY AND BACKGROUND OF THE MODEL LAW

123. The UNCITRAL Model Law on Electronic Commerce was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996 in furtherance of its mandate to promote the harmonization and unification of international trade law, so as to remove unnecessary obstacles to international trade caused by inadequacies and divergences in the law affecting trade. Over the past quarter of a century, UNCITRAL, whose membership consists of States from all regions and of all levels of economic development, has implemented its mandate by formulating international conventions (the United Nations Conventions on Contracts for the International Sale of Goods, on the Limitation Period in the International Sale of Goods, on the Carriage of Goods by Sea, 1978 ("Hamburg Rules"), on the Liability of Operators of Transport Terminals in International Trade, on International Bills of Exchange and International Promissory Notes, and on Independent Guarantees and Stand-by Letters of Credit), model laws (the UNCITRAL Model Laws on International Commercial Arbitration, on International Credit Transfers and on Procurement of Goods, Construction and Services), the UNCITRAL Arbitration Rules, the UNCITRAL Conciliation Rules, and legal guides (on construction contracts, countertrade transactions and electronic funds transfers).

124. The Model Law was prepared in response to a major change in the means by which communications are made between parties using computerized or other modern techniques in doing business (sometimes referred to as "trading partners"). The Model Law is intended to serve as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of commercial relationships involving the use of computerized or other modern communication techniques, and for the establishment of relevant legislation where none presently exists. The text of the Model Law, as reproduced above, is set forth in annex I to the report of UNCITRAL on the work of its twenty-ninth session.⁽³⁾

125. The Commission, at its seventeenth session (1984), considered a report of the Secretary-General entitled "Legal aspects of automatic data processing" (A/CN.9/254), which identified several legal issues relating to the legal value of computer records, the requirement of a "writing", authentication, general conditions, liability and bills of lading. The Commission took note of a report of the Working Party on Facilitation of International Trade Procedures (WP.4), which is jointly sponsored by the Economic Commission for Europe and the United Nations Conference on Trade and Development, and is responsible for the development of UN/EDIFACT standard messages. That report suggested that, since the legal problems arising in this field were essentially those of international trade law, the Commission as the core legal body in the field of international trade law appeared to be the appropriate central forum to undertake and coordinate the necessary action.⁽⁴⁾ The Commission decided to place the subject of the legal implications of automatic data processing to the flow of international trade on its programme of work as a priority item.⁽⁵⁾

126. At its eighteenth session (1985), the Commission had before it a report by the Secretariat entitled "Legal value of computer records" (A/CN.9/265). That report came to the conclusion that, on a global level, there were fewer problems in the use of data stored in computers as evidence in litigation than might have been expected. It noted that a more serious legal obstacle to the use of computers and computer-to-computer telecommunications in international trade arose out of

requirements that documents had to be signed or be in paper form. After discussion of the report, the Commission adopted the following recommendation, which expresses some of the principles on which the Model Law is based:

"The United Nations Commission on International Trade Law,

"*Noting* that the use of automatic data processing (ADP) is about to become firmly established throughout the world in many phases of domestic and international trade as well as in administrative services,

"*Noting* also that legal rules based upon pre-ADP paper-based means of documenting international trade may create an obstacle to such use of ADP in that they lead to legal insecurity or impede the efficient use of ADP where its use is otherwise justified,

"*Noting* further with appreciation the efforts of the Council of Europe, the Customs Co-operation Council and the United Nations Economic Commission for Europe to overcome obstacles to the use of ADP in international trade arising out of these legal rules,

"*Considering* at the same time that there is no need for a unification of the rules of evidence regarding the use of computer records in international trade, in view of the experience showing that substantial differences in the rules of evidence as they apply to the paper-based system of documentation have caused so far no noticeable harm to the development of international trade,

"*Considering* also that the developments in the use of ADP are creating a desirability in a number of legal systems for an adaptation of existing legal rules to these developments, having due regard, however, to the need to encourage the employment of such ADP means that would provide the same or greater reliability as paper-based documentation,

"1. *Recommends* to Governments:

"(a) to review the legal rules affecting the use of computer records as evidence in litigation in order to eliminate unnecessary obstacles to their admission, to be assured that the rules are consistent with developments in technology, and to provide appropriate means for a court to evaluate the credibility of the data contained in those records;

"(b) to review legal requirements that certain trade transactions or trade related documents be in writing, whether the written form is a condition to the enforceability or to the validity of the transaction or document, with a view to permitting, where appropriate, the transaction or document to be recorded and transmitted in computer-readable form;

"(c) to review legal requirements of a handwritten signature or other paper-based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication;

"(d) to review legal requirements that documents for submission to governments be in writing and manually signed with a view to permitting, where appropriate, such documents to be submitted in computer-readable form to those administrative services which have acquired the necessary equipment and established the necessary procedures;

"2. *Recommends* to international organizations elaborating legal texts related to trade to take account of the present Recommendation in adopting such texts and,

where appropriate, to consider modifying existing legal texts in line with the present Recommendation."⁽⁶⁾

127. That recommendation (hereinafter referred to as the "1985 UNCITRAL Recommendation") was endorsed by the General Assembly in resolution 40/71, paragraph 5(b), of 11 December 1985 as follows:

"The General Assembly,

"... Calls upon Governments and international organizations to take action, where appropriate, in conformity with the Commission's recommendation so as to ensure legal security in the context of the widest possible use of automated data processing in international trade; ...".⁽⁷⁾

128. As was pointed out in several documents and meetings involving the international electronic commerce community, e.g. in meetings of WP. 4, there was a general feeling that, in spite of the efforts made through the 1985 UNCITRAL Recommendation, little progress had been made to achieve the removal of the mandatory requirements in national legislation regarding the use of paper and handwritten signatures. It has been suggested by the Norwegian Committee on Trade Procedures (NORPRO) in a letter to the Secretariat that "one reason for this could be that the 1985 UNCITRAL Recommendation advises on the need for legal update, but does not give any indication of how it could be done". In this vein, the Commission considered what follow-up action to the 1985 UNCITRAL Recommendation could usefully be taken so as to enhance the needed modernization of legislation. The decision by UNCITRAL to formulate model legislation on legal issues of electronic data interchange and related means of communication may be regarded as a consequence of the process that led to the adoption by the Commission of the 1985 UNCITRAL Recommendation.

129. At its twenty-first session (1988), the Commission considered a proposal to examine the need to provide for the legal principles that would apply to the formation of international commercial contracts by electronic means. It was noted that there existed no refined legal structure for the important and rapidly growing field of formation of contracts by electronic means and that future work in that area could help to fill a legal vacuum and to reduce uncertainties and difficulties encountered in practice. The Commission requested the Secretariat to prepare a preliminary study on the topic.⁽⁸⁾

130. At its twenty-third session (1990), the Commission had before it a report entitled "Preliminary study of legal issues related to the formation of contracts by electronic means" (A/CN.9/333). The report summarized work that had been undertaken in the European Communities and in the United States of America on the requirement of a "writing" as well as other issues that had been identified as arising in the formation of contracts by electronic means. The efforts to overcome some of those problems by the use of model communication agreements were also discussed.⁽⁹⁾

131. At its twenty-fourth session (1991), the Commission had before it a report entitled "Electronic Data Interchange" (A/CN.9/350). The report described the current activities in the various organizations involved in the legal issues of electronic data interchange (EDI) and analysed the contents of a number of standard interchange agreements already developed or then being developed. It pointed out that such documents varied considerably according to the various needs of the different categories of users they were intended to serve and that the variety of contractual arrangements had sometimes been described as hindering the development of a satisfactory legal framework for the business use of electronic commerce. It suggested that there was a need for a general framework that would identify the issues and provide a set of legal principles and basic legal rules governing communication through electronic commerce. It concluded that such a basic framework could, to a certain extent, be created by contractual arrangements between parties to an electronic commerce relationship and that the existing contractual frameworks that were proposed to the community of users of electronic commerce were often incomplete, mutually incompatible, and inappropriate for international use since they relied to a large extent upon the structures of local law.

132. With a view to achieving the harmonization of basic rules for the promotion of electronic commerce in international trade, the report suggested that the Commission might wish to consider the desirability of preparing a standard communication agreement for use in international trade. It pointed out that work by the Commission in this field would be of particular importance since it would involve participation of all legal systems, including those of developing countries that were already or would soon be confronted with the issues of electronic commerce.

133. The Commission was agreed that the legal issues of electronic commerce would become increasingly important as the use of electronic commerce developed and that it should undertake work in that field. There was wide support for the suggestion that the Commission should undertake the preparation of a set of legal principles and basic legal rules governing communication through electronic commerce.⁽¹⁰⁾ The Commission came to the conclusion that it would be premature to engage immediately in the preparation of a standard communication agreement and that it might be preferable to monitor developments in other organizations, particularly the Commission of the European Communities and the Economic Commission for Europe. It was pointed out that high-speed electronic commerce required a new examination of basic contract issues such as offer and acceptance, and that consideration should be given to legal implications of the role of central data managers in international commercial law.

134. After deliberation, the Commission decided that a session of the Working Group on International Payments would be devoted to identifying the legal issues involved and to considering possible statutory provisions, and that the Working Group would report to the Commission on the desirability and feasibility of undertaking further work such as the preparation of a standard communication agreement.⁽¹¹⁾

135. The Working Group on International Payments, at its twenty-fourth session, recommended that the Commission should undertake work towards establishing uniform legal rules on electronic commerce. It was agreed that the goals of such work should be to facilitate the increased use of electronic commerce and to meet the need for statutory provisions to be developed in the field of electronic commerce, particularly with respect to such issues as formation of contracts; risk and liability of commercial partners and third-party service providers involved in electronic commerce relationships; extended definitions of "writing" and "original" to be used in an electronic commerce environment; and issues of negotiability and documents of title (A/CN.9/360).

136. While it was generally felt that it was desirable to seek the high degree of legal certainty and harmonization provided by the detailed provisions of a uniform law, it was also felt that care should be taken to preserve a flexible approach to some issues where legislative action might be premature or inappropriate. As an example of such an issue, it was stated that it might be fruitless to attempt to provide legislative unification of the rules on evidence that may apply to electronic commerce messaging (ibid., para. 130). It was agreed that no decision should be taken at that early stage as to the final form or the final content of the legal rules to be prepared. In line with the flexible approach to be taken, it was noted that situations might arise where the preparation of model contractual clauses would be regarded as an appropriate way of addressing specific issues (ibid., para. 132).

137. The Commission, at its twenty-fifth session (1992), endorsed the recommendation contained in the report of the Working Group (ibid., paras. 129-133) and entrusted the preparation of legal rules on electronic commerce (which was then referred to as "electronic data interchange" or "EDI") to the Working Group on International Payments, which it renamed the Working Group on Electronic Data Interchange.⁽¹²⁾

138. The Working Group devoted its twenty-fifth to twenty-eighth sessions to the preparation of legal rules applicable to "electronic data interchange (EDI) and other modern means of communication" (reports of those sessions are found in documents A/CN.9/373, 387, 390 and 406).⁽¹³⁾

139. The Working Group carried out its task on the basis of background working papers prepared by the Secretariat on possible issues to be included in the Model Law. Those background papers included A/CN.9/WG.IV/WP.53 (Possible issues to be included in the programme of future work on the legal aspects of EDI) and A/CN.9/WG.IV/WP.55 (Outline of possible uniform rules on the legal aspects of electronic data interchange). The draft articles of the Model Law were submitted by the Secretariat in documents A/CN.9/WG.IV/WP.57, 60 and 62. The Working Group also had before it a proposal by the United Kingdom of Great Britain and Northern Ireland relating to the possible contents of the draft Model Law (A/CN.9/WG.IV/WP.58).

140. The Working Group noted that, while practical solutions to the legal difficulties raised by the use of electronic commerce were often sought within contracts (A/CN.9/WG.IV/WP.53, paras. 35-36), the contractual approach to electronic commerce was developed not only because of its intrinsic advantages such as its flexibility, but also for lack of specific provisions of statutory or case law. The contractual approach was found to be limited in that it could not overcome any of the legal obstacles to the use of electronic commerce that might result from mandatory provisions of applicable statutory or case law. In that respect, one difficulty inherent in the use of communication agreements resulted from uncertainty as to the weight that would be carried by some contractual stipulations in case of litigation. Another limitation to the contractual approach resulted from the fact that parties to a contract could not effectively regulate the rights and obligations of third parties. At least for those parties not participating in the contractual arrangement, statutory law based on a model law or an international convention seemed to be needed (see A/CN.9/350, para. 107).

141. The Working Group considered preparing uniform rules with the aim of eliminating the legal obstacles to, and uncertainties in, the use of modern communication techniques, where effective removal of such obstacles and uncertainties could only be achieved by statutory provisions. One purpose of the uniform rules was to enable potential electronic commerce users to establish a legally secure electronic commerce relationship by way of a communication agreement within a closed network. The second purpose of the uniform rules was to support the use of electronic commerce outside such a closed network, i.e., in an open environment. However, the aim of the uniform rules was to enable, and not to impose, the use of EDI and related means of communication. Moreover, the aim of the uniform rules was not to deal with electronic commerce relationships from a technical perspective but rather to create a legal environment that would be as secure as possible, so as to facilitate the use of electronic commerce between communicating parties.

142. As to the form of the uniform rules, the Working Group was agreed that it should proceed with its work on the assumption that the uniform rules should be prepared in the form of statutory provisions. While it was agreed that the form of the text should be that of a "model law", it was felt, at first, that, owing to the special nature of the legal text being prepared, a more flexible term than "model law" needed to be found. It was observed that the title should reflect that the text contained a variety of provisions relating to existing rules scattered throughout various parts of the national laws in an enacting State. It was thus a possibility that enacting States would not incorporate the text as a whole and that the provisions of such a "model law" might not appear together in any one particular place in the national law. The text could be described, in the parlance of one legal system, as a "miscellaneous statute amendment act". The Working Group agreed that this special nature of the text would be better reflected by the use of the term "model statutory provisions". The view was also expressed that the nature and purpose of the "model statutory provisions" could be explained in an introduction or guidelines accompanying the text.

143. At its twenty-eighth session, however, the Working Group reviewed its earlier decision to formulate a legal text in the form of "model statutory provisions" (A/CN.9/390, para. 16). It was widely felt that the use of the term "model statutory provisions" might raise uncertainties as to the legal nature of the instrument. While some support was expressed for the retention of the term "model statutory provisions", the widely prevailing view was that the term "model law" should be preferred. It was widely felt that, as a result of the course taken by the Working Group as its work progressed towards the completion of the text, the model statutory provisions could be regarded as a balanced and discrete set of rules, which could also be implemented as a whole in a single instrument (A/CN.9/406, para. 75). Depending on the situation in each enacting State, however,

the Model Law could be implemented in various ways, either as a single statute or in various pieces of legislation.

144. The text of the draft Model Law as approved by the Working Group at its twenty-eighth session was sent to all Governments and to interested international organizations for comment. The comments received were reproduced in document A/CN.9/409 and Add.1-4. The text of the draft articles of the Model Law as presented to the Commission by the Working Group was contained in the annex to document A/CN.9/406.

145. At its twenty-eighth session (1995), the Commission adopted the text of articles 1 and 3 to 11 of the draft Model Law and, for lack of sufficient time, did not complete its review of the draft Model Law, which was placed on the agenda of the twenty-ninth session of the Commission.⁽¹⁴⁾

146. The Commission, at its twenty-eighth session,⁽¹⁵⁾ recalled that, at its twenty-seventh session (1994), general support had been expressed in favour of a recommendation made by the Working Group that preliminary work should be undertaken on the issue of negotiability and transferability of rights in goods in a computer-based environment as soon as the preparation of the Model Law had been completed.⁽¹⁶⁾ It was noted that, on that basis, a preliminary debate with respect to future work to be undertaken in the field of electronic data interchange had been held in the context of the twenty-ninth session of the Working Group (for the report on that debate, see A/CN.9/407, paras. 106-118). At that session, the Working Group also considered proposals by the International Chamber of Commerce (A/CN.9/WG.IV/WP.65) and the United Kingdom of Great Britain and Northern Ireland (A/CN.9/WG.IV/WP.66) relating to the possible inclusion in the draft Model Law of additional provisions to the effect of ensuring that certain terms and conditions that might be incorporated in a data message by means of a mere reference would be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of the data message (for the report on the discussion, see A/CN.9/407, paras. 100-105). It was agreed that the issue of incorporation by reference might need to be considered in the context of future work on negotiability and transferability of rights in goods (A/CN.9/407, para. 103). The Commission endorsed the recommendation made by the Working Group that the Secretariat should be entrusted with the preparation of a background study on negotiability and transferability of EDI transport documents, with particular emphasis on EDI maritime transport documents, taking into account the views expressed and the suggestions made at the twenty-ninth session of the Working Group.⁽¹⁷⁾

147. On the basis of the study prepared by the Secretariat (A/CN.9/WG.IV/WP.69), the Working Group, at its thirtieth session, discussed the issues of transferability of rights in the context of transport documents and approved the text of draft statutory provisions dealing with the specific issues of contracts of carriage of goods involving the use of data messages (for the report on that session, see A/CN.9/421). The text of those draft provisions as presented to the Commission by the Working Group for final review and possible addition as part II of the Model Law was contained in the annex to document A/CN.9/421.

148. In preparing the Model Law, the Working Group noted that it would be useful to provide in a commentary additional information concerning the Model Law. In particular, at the twenty-eighth session of the Working Group, during which the text of the draft Model Law was finalized for submission to the Commission, there was general support for a suggestion that the draft Model Law should be accompanied by a guide to assist States in enacting and applying the draft Model Law. The guide, much of which could be drawn from the *travaux préparatoires*

of the draft Model Law, would also be helpful to users of electronic means of communication as well as to scholars in that area. The Working Group noted that, during its deliberations at that session, it had proceeded on the assumption that the draft Model Law would be accompanied by a guide. For example, the Working Group had decided in respect of a number of issues not to settle them in the draft Model Law but to address them in the guide so as to provide guidance to States enacting the draft Model Law. The Secretariat was requested to prepare a draft and submit it to the Working Group for consideration at its twenty-ninth session (A/CN.9/406, para. 177).

149. At its twenty-ninth session, the Working Group discussed the draft Guide to Enactment of the Model Law (hereinafter referred to as "the draft Guide") as set forth in a note prepared by the Secretariat (A/CN.9/WG.IV/WP.64). The Secretariat was requested to prepare a revised version of the draft Guide reflecting the decisions made by the Working Group and taking into account the various views, suggestions and concerns that had been expressed at that session. At its twenty-eighth session, the Commission placed the draft Guide to Enactment of the Model Law on the agenda of its twenty-ninth session.⁽¹⁸⁾

150. At its twenty-ninth session (1996), the Commission, after consideration of the text of the draft Model Law as revised by the drafting group, adopted the following decision at its 605th meeting, on 12 June 1996:

"The United Nations Commission on International Trade Law,

"Recalling its mandate under General Assembly resolution 2205 (XXI) of 17 December 1966 to further the progressive harmonization and unification of the law of international trade, and in that respect to bear in mind the interests of all peoples, and in particular those of developing countries, in the extensive development of international trade,

"Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based forms of communication and storage of information,

"Recalling the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session, in 1985, and paragraph 5(b) of General Assembly resolution 40/71 of 11 December 1985 calling upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission⁽¹⁹⁾ so as to ensure legal security in the context of the widest possible use of automated data processing in international trade,

"Being of the opinion that the establishment of a model law facilitating the use of electronic commerce, and acceptable to States with different legal, social and economic systems, contributes to the development of harmonious international economic relations,

"Being convinced that the UNCITRAL Model Law on Electronic Commerce will significantly assist all States in enhancing their legislation governing the use of alternatives to paper-based forms of communication and storage of information, and in formulating such legislation where none currently exists,

"1. Adopts the UNCITRAL Model Law on Electronic Commerce as it appears in annex I to the report on the current session;

"2. Requests the Secretary-General to transmit the text of the UNCITRAL Model Law on Electronic Commerce, together with the Guide to Enactment of the Model Law prepared by the Secretariat, to Governments and other interested bodies;

"3. Recommends that all States give favourable consideration to the UNCITRAL Model Law on Electronic Commerce when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based forms of communication and storage of information."⁽²⁰⁾

1. See *Official Records of the General Assembly, Fortieth Session, Supplement No. 17*

(A/40/17), chap. VI, sect. B.

2. Reference materials listed by symbols in this Guide belong to the following three categories of documents:

A/50/17 and A/51/17 are the reports of UNCITRAL to the General Assembly on the work of its twenty-eighth and twenty-ninth sessions, held in 1995 and 1996, respectively;

A/CN.9/... documents are reports and notes discussed by UNCITRAL in the context of its annual session, including reports presented by the Working Group to the Commission;

A/CN.9/WG.IV/... documents are working papers considered by the UNCITRAL Working Group on Electronic Commerce (formerly known as the UNCITRAL Working Group on Electronic Data Interchange) in the preparation of the Model Law.

3. Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), Annex I.

4. "Legal aspects of automatic trade data interchange" (TRADE/WP.4/R.185/Rev.1). The report submitted to the Working Party is reproduced in A/CN.9/238, annex.

5. Official Records of the General Assembly, Thirty-ninth Session, Supplement No. 17 (A/39/17), para. 136.

6. Official Records of the General Assembly, Fortieth Session, Supplement No. 17 (A/40/17), para. 360.

7. Resolution 40/71 was reproduced in United Nations Commission on International Trade Law Yearbook, 1985, vol. XVI, Part One, D. (United Nations publication, Sales No. E.87.V.4).

8. Official Records of the General Assembly, Forty-third Session, Supplement No. 17 (A/43/17), paras. 46 and 47, and ibid., Forty-fourth Session, Supplement No. 17 (A/44/17), para. 289.

9. Ibid., Forty-fifth Session, Supplement No. 17 (A/45/17), paras. 38 to 40.

10. It may be noted that the Model Law is not intended to provide a comprehensive set of rules governing all aspects of electronic commerce. The main purpose of the Model Law is to adapt existing statutory requirements so that they would no longer constitute obstacles to the use of paperless means of communication and storage of information.

11. Official Records of the General Assembly, Forty-sixth Session, Supplement No. 17 (A/46/17), paras. 311 to 317.

12. Ibid., Forty-seventh Session, Supplement No. 17 (A/47/17), paras. 141 to 148.

13. The notion of "EDI and related means of communication" as used by the Working Group is not to be construed as a reference to narrowly defined EDI under article 2(b) of the Model Law but to a variety of trade-related uses of modern communication techniques that was later referred to broadly under the rubric of "electronic commerce". The Model Law is not intended only for application in the context of existing communication techniques but rather as a set of flexible rules that should accommodate foreseeable technical developments. It should also be emphasized that the purpose of the Model Law is not only to establish rules for the movement of information communicated by means of data messages but equally to deal with the storage of information in data messages that are not intended for communication.

14. Official Records of the General Assembly, Fiftieth Session, Supplement No. 17 (A/50/17),

para. 306.

15. Ibid., para. 307.

16. Ibid., Forty-ninth Session, Supplement No. 17 (A/49/17), para. 201.

17. Ibid., Fiftieth Session, Supplement No. 17 (A/50/17), para. 309.

18. Ibid., para. 306.

19. Ibid., Fortieth Session, Supplement No. 17 (A/40/17), paras. 354 - 360.

20. Ibid., Fifty-first Session, Supplement No. 17 (A/51/17), para. 209.

B I L A G 4

Lov om elektroniske signaturer¹⁾

VI MARGRETHE DEN ANDEN, af Guds Nåde Danmarks Dronning, gør vitterligt:
Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

Kapitel 1

Formål og anvendelsesområde

§ 1. Lovens formål er at fremme en sikker og effektiv anvendelse af elektronisk kommunikation gennem fastsættelse af krav til visse elektroniske signaturer og til nøglecentre, der udsteder certifikater til elektroniske signaturer.

§ 2. Loven finder anvendelse på nøglecentre etableret i Danmark, der udsteder kvalificerede certifikater til offentligheden, jf. dog § 12.

Stk. 2. Loven finder desuden anvendelse på efterprøvelse af, at signaturgenereringssystemer overholder de opstillede krav til sikre signaturgenereringssystemer.

Kapitel 2

Definitioner

§ 3. I denne lov forstås ved:

- 1) Elektronisk signatur: Data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et signaturgenereringssystem, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret.
- 2) Avanceret elektronisk signatur: En elektronisk signatur, der
 - a) entydigt er knyttet til underskriveren,

- b) gør det muligt at identificere underskriveren,
- c) skabes med midler, som kun underskriveren har kontrol over, og som
- d) er knyttet til de data, den vedrører på en sådan måde, at enhver efterfølgende ændring af disse data kan opdages.
- 3) Underskriver: En fysisk person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af en anden fysisk eller juridisk person.
- 4) Signaturgenereringsdata: Unikke data, som for eksempel en kode eller en privat krypteringsnøgle, som anvendes til at fremstille en elektronisk signatur.
- 5) Signaturgenereringssystem: Et software- eller hardwarebaseret system til behandling og opbevaring af signaturgenereringsdata.
- 6) Signaturverificeringsdata: Unikke data, som for eksempel en kode eller en offentlig krypteringsnøgle, som anvendes til at verificere en elektronisk signatur.
- 7) Signaturverificeringssystem: Et software- eller hardwarebaseret system til behandling af signaturverificeringsdata.
- 8) Certifikat: En elektronisk attest, som knytter bestemte signaturverificeringsdata til underskriveren og bekræfter dennes identitet.
- 9) Nøglecenter: En fysisk eller juridisk person, der udsteder certifikater.

¹⁾ Loven indeholder bestemmelser, der gennemfører Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EF-Tidende 2000 nr. L 13, s. 12).

Kapitel 3

Kvalificerede certifikater

§ 4. Betegnelsen kvalificerede certifikater eller betegnelser, der er egnede til at fremkalde det indtryk, at der er tale om kvalificerede certifikater, må kun anvendes om certifikater, der opfylder de i stk. 2 og 3 nævnte krav, og som udstedes af et nøglecenter, der opfylder bestemmelserne i kapitel 4 samt regler fastsat i medfør heraf.

Stk. 2. Et kvalificeret certifikat skal indeholde:

- 1) En angivelse af, at certifikatet er udstedt som et kvalificeret certifikat.
- 2) Nøglecentrets navn og hjemsted.
- 3) Underskriverens navn eller pseudonym med angivelse af, at der er tale om et pseudonym.
- 4) Eventuelle yderligere oplysninger om underskriveren, for så vidt det er nødvendigt for anvendelsen af certifikatet, herunder oplysninger, der sikrer en entydig identifikation af underskriveren.
- 5) Certifikatets gyldighedsperiode.
- 6) En tydelig angivelse af eventuelle begrænsninger i certifikatets anvendelsesområde (formålsbegrænsninger).
- 7) En tydelig angivelse af eventuelle begrænsninger med hensyn til de transaktionsbeløb, certifikatet kan anvendes til (beløbsbegrænsninger).
- 8) Certifikatets identifikationskode.
- 9) De signaturverificeringsdata, der svarer til de signaturgenereringsdata, som var under underskriverens kontrol på udstedelsestidspunktet.

Stk. 3. Et kvalificeret certifikat skal være underskrevet med nøglecentrets avancerede elektroniske signatur.

Kapitel 4

Krav til nøglecentres virksomhed

§ 5. Et nøglecenter skal træffe de foranstaltninger, som er nødvendige for et sikkert, pålideligt og velfungerende udbud af kvalificerede certifikater. Nøglecentret skal herunder

- 1) anvende betryggende administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder,
- 2) beskæftige personale med den fornødne ekspertise, erfaring og kvalifikation, herunder personale med sagkundskab inden for elektronisk signaturteknologi og indgående

kendskab til korrekte sikkerhedsprocedurer i forbindelse hermed,

- 3) anvende pålidelige systemer og produkter, som er beskyttet imod uautoriserede ændringer, og som sikrer den tekniske og kryptografiske sikkerhed af de processer, som disse systemer og produkter understøtter,
- 4) træffe foranstaltninger mod eventuelle muligheder for forfalskning af certifikaterne og
- 5) til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomhed i overensstemmelse med bestemmelserne i denne lov, herunder til at opfylde erstatningsmæssige forpligtelser i henhold til loven.

Stk. 2. Nøglecentre, der udsteder kvalificerede certifikater, skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen i nøglecentret. Telestyrelsen kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor.

Stk. 3. Forskningsministeren fastsætter nærmere regler om kravene i stk. 1.

§ 6. Nøglecentre skal fastsætte og anvende betryggende procedurer til at kontrollere identiteten og andre forhold vedrørende underskriveren forud for udstedelsen af certifikatet.

Stk. 2. Oplysninger om procedurerne som nævnt i stk. 1 skal være offentligt tilgængelige.

Stk. 3. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1 og 2.

§ 7. Et nøglecenter skal ved udstedelse af et kvalificeret certifikat sikre, at underskriveren på tidspunktet for udstedelsen er i besiddelse af de signaturgenereringsdata, som korresponderer med de signaturverificeringsdata, der er indeholdt i certifikatet.

Stk. 2. Ved udstedelse af kvalificerede certifikater, hvor det er nøglecentret, der leverer signaturgenereringsdata og signaturverificeringsdata, må der kun anvendes signaturgenereringsdata og signaturverificeringsdata, som hører sammen på en unik måde. Nøglecentret skal sikre signaturgenereringsdataenes fortrolighed under genereringsprocessen.

Stk. 3. Et nøglecenter skal fastlægge procedurer for udstedelse af certifikater, der gør det muligt at fastslå dato og tidspunkt for udstedelsen.

§ 8. Ved indgåelse af en aftale om udstedelse af et kvalificeret certifikat skal nøglecentret skriftligt oplyse underskriveren om:

- 1) Vilkårene for anvendelsen af certifikatet, herunder eventuelle formåls- eller beløbsbegrænsninger.
- 2) Eventuelle krav til underskriverens opbevaring og beskyttelse af signaturgenereringsdataene.
- 3) Underskriverens omkostninger ved erhvervelse og anvendelse af certifikatet og brug af nøglecentrets øvrige tjenester.
- 4) Hvorvidt nøglecentret er tilknyttet en frivillig akkrediteringsordning.
- 5) Procedurer for behandling af klager og bilæggelse af tvister.

Stk. 2. Kontraktsvilkårene kan afgives elektronisk, forudsat at det sker i en for modtageren umiddelbart læsbar form.

Stk. 3. De relevante dele af de i stk. 1 nævnte oplysninger skal på anmodning stilles til rådighed for tredjemand, der forlader sig på et kvalificeret certifikat.

Stk. 4. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

§ 9. Nøglecentre skal sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste, som giver mulighed for, at det kan undersøges, om et kvalificeret certifikat er spærret, hvilken gyldighedsperiode certifikatet har, og om certifikatet indeholder formåls- eller beløbsbegrænsninger.

Stk. 2. Et nøglecenter skal spærre et certifikat straks efter at have modtaget anmodning fra underskriveren herom, eller hvis forholdene i øvrigt tilsiger dette.

Stk. 3. Oplysninger efter stk. 1 skal være umiddelbart tilgængelige.

Stk. 4. Et kvalificeret certifikat må kun gøres offentligt tilgængeligt, hvis underskriveren har givet samtykke hertil.

Stk. 5. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

§ 10. Et nøglecenter skal registrere og opbevare alle relevante oplysninger om certifikaterne i en rimelig periode, dog mindst seks år.

Stk. 2. Et nøglecenter skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form.

Stk. 3. Nøglecentre må ikke opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til.

Stk. 4. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1 og 2.

Kapitel 5

Erstatningsansvar

§ 11. Nøglecentre, der udsteder kvalificerede certifikater til offentligheden, eller som over for offentligheden indestår for sådanne certifikater udstedt af et andet nøglecenter, er ansvarlig for tab hos den, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes,

- 1) at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet,
- 2) at certifikatet ikke indeholder alle oplysninger som krævet i henhold til § 4,
- 3) manglende spærring af certifikatet, jf. § 9, stk. 2,
- 4) manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. § 9, stk. 1 og 3, eller
- 5) tilsidesættelse af § 7.

Stk. 2. Et nøglecenter pådrager sig erstatningsansvar efter stk. 1, medmindre nøglecentret kan godtgøre, at nøglecentret ikke har handlet uagtsomt eller forsætligt.

Stk. 3. Et nøglecenter er ikke ansvarlig for

- 1) tab opstået som følge af anvendelse af et kvalificeret certifikat uden for de formålsbegrænsninger, som gælder for certifikatet, eller for
- 2) tab opstået som følge af en overskridelse af de beløbsbegrænsninger, som gælder for certifikatet,

forudsat at de pågældende begrænsninger tydeligt fremgår af certifikatet, jf. § 4, og på forespørgsel oplyses, jf. § 9, stk. 1 og 3.

Stk. 4. Stk. 1-3 kan ikke ved forudgående aftale fraviges til skade for skadelidte.

Stk. 5. Stk. 1-3 finder ikke anvendelse, i det omfang tabet dækkes efter lov om visse betalingsmidler.

Kapitel 6

Supplerende krav til behandling af personoplysninger

§ 12. Et nøglecenter må kun indsamle personoplysninger i forbindelse med nøglecentervirksomheden direkte fra den registrerede eller med den registreredes udtrykkelige samtykke og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat.

Stk. 2. Personoplysninger indsamlet i medfør af stk. 1 må ikke behandles eller videregives til andet formål end nævnt i stk. 1 uden den registreredes udtrykkelige samtykke hertil.

Kapitel 7

Elektronisk signatur og formkrav

§ 13. Bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, skal anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgenereringssystem. Ved elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.

Kapitel 8

Sikre signaturgenereringssystemer

§ 14. Ved et sikkert signaturgenereringssystem forstås et signaturgenereringssystem, der ved hjælp af procedurer og tekniske midler sikrer, at signaturgenereringsdata, der anvendes til at skabe en elektronisk signatur,

- 1) i praksis kun kan fremtræde en gang,
- 2) med rimelig sikkerhed forbliver hemmelige og ikke kan udledes,
- 3) er beskyttet mod forfalskning og
- 4) på pålidelig vis kan beskyttes af underskriveren mod andres uretmæssige brug.

Stk. 2. Et sikkert signaturgenereringssystem må ikke indrettes således, at det ændrer de data, som en elektronisk signatur knyttes til, eller hindrer, at disse data forevises for underskriveren forud for signeringen.

Stk. 3. De i stk. 1 og 2 nævnte krav skal anses for opfyldt, såfremt et signaturgenereringssystem overholder almindeligt anerkendte standarder for sådanne systemer, som Kommissionen har fastsat og offentliggjort i EF-Tidende i overensstemmelse med proceduren i artikel 9 i Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer.

§ 15. Forskningsministeren udpeger et eller flere egnede organer eller myndigheder, som kan medvirke til at efterprøve, om signaturgenereringssystemer opfylder kravene til sikre signaturgenereringssystemer, jf. § 14, stk. 1 og 2, og fastsætter nærmere regler om procedurerne for

denne efterprøvelse samt om betaling af gebyr for efterprøvelsen.

Stk. 2. Et signaturgenereringssystem, der betegnes som et sikkert signaturgenereringssystem, må først markedsføres eller anvendes til at fremstille avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, når det er blevet efterprøvet, jf. stk. 1.

Stk. 3. Med en efterprøvelse efter stk. 1 lige-stilles en efterprøvelse af et sikkert signaturgenereringssystem foretaget af et organ eller en myndighed i et andet land inden for Det Europæiske Økonomiske Samarbejde (EØS).

Kapitel 9

Tilsyn

§ 16. Nøglecentre skal senest samtidig med, at udstedelse af kvalificerede certifikater påbegyndes, foretage anmeldelse til Telestyrelsen.

Stk. 2. Anmeldelsen skal indeholde oplysning om

- 1) nøglecentrets navn og hjemsted,
- 2) selskabsform, såfremt nøglecentret drives som selskab,
- 3) nøglecentrets ledelse og systemrevisor.

Stk. 3. Ændringer i forhold, der er anmeldt i henhold til stk. 2, skal anmeldes inden 8 dage efter, at ændringen er sket.

Stk. 4. Telestyrelsen kan fastsætte nærmere regler om, hvilke yderligere oplysninger anmeldelsen skal indeholde.

§ 17. Nøglecentret skal samtidig med anmeldelse efter § 16 indsende en rapport til Telestyrelsen.

Stk. 2. Rapporten skal indeholde

- 1) en beskrivelse af nøglecentrets virksomhed og systemer,
- 2) en erklæring fra nøglecentrets ledelse om, hvorvidt nøglecentrets samlede data-, system- og driftssikkerhed må anses for betryggende og i overensstemmelse med denne lovs regler samt regler fastsat i medfør heraf, og
- 3) en erklæring fra systemrevisor, jf. § 5, stk. 2, om, hvorvidt nøglecentrets samlede data-, system- og driftssikkerhed efter systemrevisors opfattelse må anses for betryggende og i overensstemmelse med denne lovs regler samt regler fastsat i medfør heraf.

Stk. 3. Nøglecentret skal årligt udarbejde en opdateret rapport. Telestyrelsen fastsætter en

frist for, hvornår rapporten senest skal indsendes til Telestyrelsen.

Stk. 4. Telestyrelsen kan fastsætte nærmere regler vedrørende indholdet af nøglecentrets rapporter samt om systemrevisionens gennemførelse i nøglecentre.

§ 18. Telestyrelsen påser overholdelsen af denne lov og bestemmelser udstedt i medfør af loven.

Stk. 2. Telestyrelsen kan påbyde et nøglecenter at

- 1) foretage anmeldelse til Telestyrelsen, jf. § 16,
- 2) indsende rapporter til Telestyrelsen, jf. § 17,
- 3) bringe forhold vedrørende nøglecentrets virksomhed i overensstemmelse med loven eller bestemmelser udstedt i medfør af loven.

Stk. 3. Telestyrelsen fastsætter en tidsfrist for opfyldelse af påbud efter stk. 2.

Stk. 4. Telestyrelsen kan pålægge et nøglecenter tvangsbøder med henblik på at gennemtvinge påbud efter stk. 2, § 19, stk. 1, eller § 20.

Stk. 5. Telestyrelsen kan kræve, at der gennemføres en ekstraordinær systemrevision af et nøglecenter. Telestyrelsen udpeger den systemrevisor, som skal udføre den ekstraordinære systemrevision. Nøglecentret kan pålægges at betale for den ekstraordinære systemrevisions udførelse.

Stk. 6. Telestyrelsen kan fratage et nøglecenter retten til at anvende betegnelsen kvalificerede certifikater, jf. § 4, hvis nøglecentret

- 1) trods pålæg af tvangsbøder undlader at efterkomme Telestyrelsens påbud efter stk. 2, § 19, stk. 1, eller § 20,
- 2) groft eller i gentagne tilfælde har overtrådt lovens regler eller regler fastsat i medfør heraf eller
- 3) anmelder betalingsstandsning eller kommer under konkurs.

Stk. 7. Telestyrelsens afgørelse efter stk. 6 kan af nøglecentret forlanges indbragt for domstolene. Anmodning herom skal være modtaget i Telestyrelsen senest 4 uger efter, at afgørelsen er blevet meddelt nøglecentret. Telestyrelsen anlægger sag mod nøglecentret efter reglerne i den borgerlige retsplejes former.

Stk. 8. Anmodning om sagsanlæg har ikke opsættende virkning, men retten kan ved kendelse bestemme, at det pågældende nøglecenter under sagens behandling skal have adgang til at udstede

de kvalificerede certifikater. Ankes en dom, hvorved fratagelsen af adgangen til at udstede kvalificerede certifikater ikke findes lovlig, kan den ret, der har afsagt dommen, eller den ret, hvortil sagen er indbragt, bestemme, at nøglecentret ikke må udstede kvalificerede certifikater under ankesagens behandling.

§ 19. Telestyrelsen kan af nøglecentre kræve meddelt alle oplysninger, som findes nødvendige for tilsynet efter § 18, herunder til afgørelse af, om en fysisk eller juridisk person er omfattet af dette tilsyn.

Stk. 2. Nøglecentret og systemrevisor skal straks meddele Telestyrelsen oplysning om forhold, der er af afgørende betydning for nøglecentrets fortsatte virksomhed.

§ 20. Telestyrelsen kan pålægge nøglecentret inden for en fastsat frist at vælge en ny systemrevisor, jf. § 5, stk. 2, såfremt den fungerende systemrevisor findes åbenbart uegnet til sit hverv.

Stk. 2. Telestyrelsen kan pålægge systemrevisor at give oplysninger om nøglecentrets forhold uden accept fra nøglecentret.

Stk. 3. Ved revisorskifte skal nøglecentret og den eller de fratrådte systemrevisorer hver især give Telestyrelsen en redegørelse. Telestyrelsen kan give påbud om at efterkomme 1. pkt.

§ 21. Telestyrelsens afgørelser efter denne lov eller bestemmelser, der er fastsat i medfør heraf, kan ikke indbringes for anden administrativ myndighed.

§ 22. Forskningsministeren kan fastsætte regler om, at udgifterne ved Telestyrelsens tilsyn afholdes af de nøglecentre, der udsteder kvalificerede certifikater.

Kapitel 10

Internationale forhold

§ 23. Kvalificerede certifikater udstedt af et nøglecenter etableret i et land uden for Det Europæiske Økonomiske Samarbejde (EØS), skal anerkendes på samme måde som kvalificerede certifikater udstedt af nøglecentre etableret i et land inden for Det Europæiske Økonomiske Samarbejde (EØS) såfremt

- 1) nøglecentret opfylder kravene i denne lov og er tilsluttet en frivillig akkrediteringsordning i en medlemsstat eller

31. maj 2000.

2585

Nr. 417.

- 2) et nøglecenter etableret i en medlemsstat, der opfylder kravene i denne lov, indestår for certifikater udstedt af det pågældende nøglecenter eller
- 3) certifikatet eller nøglecentret er anerkendt i henhold til en bilateral eller multilateral aftale mellem Fællesskabet og tredjelande eller internationale organisationer.
- 3) overtræder påbud eller afgørelser fra Telestyrelsen i medfør af § 18, stk. 2 og 6, og § 19, stk. 1.
- Stk. 2.* Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.
- Stk. 3.* Forældelsesfristen for strafansvar efter stk. 1 og 2 er 5 år.

Kapitel 11
Strafansvar

§ 24. Medmindre strengere straf er forskyldt efter anden lovgivning, straffes med bøde den, der

- 1) overtræder § 9, stk. 4, § 10, stk. 3, § 12 eller § 15, stk. 2,
- 2) afgiver urigtige eller vildledende oplysninger til Telestyrelsen eller

Kapitel 12
Ikrafttrædelse m.v.

§ 25. Loven træder i kraft den 1. oktober 2000.

§ 26. Loven gælder ikke for Grønland og Færøerne, men kan ved kongelig anordning sættes i kraft for disse landsdele med de afvigelser, som de særlige grønlandske og færøske forhold tilsiger.

Givet på Christiansborg Slot, den 31. maj 2000

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Birte Weiss