

rer, at en advokat f.eks. ikke må sende fortrolige oplysninger til domstolene ved brug af digital kommunikation, f.eks. i en stævning med bilag, medmindre der er foretaget kryptering eller lignende med henblik på at sikre, at uvedkommende ikke kan læse meddelelsen. Det antages, at dette også gælder oplysninger om den pågældendes klient, selv om klienten f.eks. måtte have givet samtykke til, at oplysningerne sendes ukrypteret.

Forslaget til *stk. 3* fastlægger, hvornår en digital meddelelse må anses for at være kommet frem til retten. Det foreslås, at det afgørende er, hvornår meddelelsen kan gøres tilgængelig for retten, mens det er uden betydning, hvornår retten faktisk gør sig bekendt med indholdet. Tidspunktet for, hvornår meddelelsen kan gøres tilgængelig for retten, vil afhænge af, hvilken form for digital kommunikation, der anvendes.

Meddelelsen vil normalt være tilgængelig for retten på det tidspunkt, hvor retten kan behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i en modtagelsesanordning eller et datasystem. En meddelelse, der først er tilgængelig efter kontortids afslutning, anses først for modtaget den følgende dag. Kan modtagelsestidspunktet for en digital meddelelse ikke fastlægges som følge af problemer med rettens it-systemer eller andre lignende problemer, må meddelelsen anses for at være kommet frem på det tidspunkt, hvor meddelelsen blev afsendt, hvis der kan fremskaffes pålidelige oplysninger om afsendelsestidspunktet.

Det foreslås i *stk. 4*, at retten kan afvise en digital meddelelse, der ikke er forsynet med digital signatur eller behæftet med andre fejl, hvis meddelelsen derved er uegnet til at indgå i rettens behandling af en sag. Selv om kravet om digital signatur er knyttet til, om der i loven stilles krav om skriftlighed eller underskrift, vil det muligvis for afsenderen i visse tilfælde kunne være uklart, om der skal anvendes en digital signatur. Manglende digital signatur bør derfor i almindelighed ikke medføre, at retten afviser – og dermed ser bort fra – meddelelsen, men at retten i stedet fastsætter en frist til afhjælpning af manglen. Der kan i den forbindelse også henvises til § 349, stk. 2, om fastsættelse af en frist til at afhjælpe mangler ved en stævning.

Bestemmelsen vedrører alene »fejl«, der knytter sig til anvendelsen af digital kommunikation. Mangler ved meddelelsens indhold skal behandles efter retsplejelovens almindelige regler herom, jf. f.eks. § 349 om mangler ved en stævning.

Det foreslås endelig, at rettens afgørelse om afvisning efter anmodning fra afsenderen af den digitale

meddelelse skal træffes ved kendelse, hvilket svarer til § 349, stk. 1, om afvisning af en mangelfuld stævning.

Der henvises til lovforslagets almindelige bemærkninger punkt 2.5.

Til nr. 4 (§ 154, stk. 2)

Det foreslås præciseret, at domstolene kan anvende digital kommunikation, hvis modtageren har givet samtykke til at modtage meddelelser fra retten på denne måde, jf. *1. pkt.*

Samtykket kan både være udtrykkeligt og stiltiende og kan gives for den enkelte sag eller generelt, jf. *2. pkt.* En advokat eller anden professionel, der i sit brev-papir angiver en e-mailadresse, må normalt anses for at have givet samtykke til at modtage digital kommunikation på denne måde. Hvis en privat borger retter henvendelse til domstolene ved f.eks. en e-mail, må dette anses for at indebære et (stiltiende) samtykke til, at retten kan besvare henvendelsen på samme måde, mens der normalt ikke i sig selv vil være tale om et generelt samtykke til også i andre sammenhænge at modtage digitale meddelelser fra retten. Med hensyn til digital forkyndelse henvises til lovforslagets § 1, nr. 5-6 (forslag til § 155, nr. 2, og § 156 a), og bemærkningerne hertil.

Det foreslås samtidig i *3. pkt.* præciseret, at der ved meddelelser med fortrolige oplysninger skal anvendes kryptering eller anden forsvarlig sikring med henblik på, at uvedkommende ikke kan læse meddelelsen, jf. herom bl.a. de almindelige bemærkninger punkt 2.3. om reglerne i persondataloven.

Som anført i de almindelige bemærkninger punkt 2.3., indebærer reglerne i persondataloven, at der skal ske såkaldt stærk kryptering eller lignende, når digital kommunikation indeholder følsomme personoplysninger, jf. persondatalovens § 7 og § 8. Der skal således ske stærk kryptering mv., hvis meddelelsen indeholder oplysninger om rent private forhold, herunder racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, oplysninger om helbredsforhold, seksuelle forhold, oplysninger om strafbare forhold og væsentlige sociale problemer. Det samme gælder oplysninger om interne familieforhold, selvmord, selvmordsforsøg, ulykkestilfælde og visse andre foreningsmæssige forhold end fagforeningsmæssige tilknytningsforhold. Andre oplysninger vil kunne være fortrolige, f.eks. efter omstændighederne oplysninger om personnummer, indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold,