ret. Det nærmere indhold af begrebet »lagret« synes at kunne give anledning til tvivl. Det er således ikke umiddelbart klart, om der heri ligger en forudsætning om, at den, der besidder de pågældende data, subjektivt skal have vurderet, hvilke data der skal lagres, og hvilke data der alene opbevares. Efter Justitsministeriets opfattelse kan bestemmelsen i konventionens artikel 16 henset til formålet med bestemmelsen ikke forstås således, at muligheden for hastesikring er afhængig af, om den enkelte udbyder har valgt at lagre de pågældende oplysninger eller ej. En sådan afgrænsning ville i praksis medføre, at f.eks. e-mails, der opbevares hos udbyderen, fordi modtageren endnu ikke har hentet dem, stort set aldrig kunne anses for lagrede og dermed omfattet af hastesikringspålægget. Både formålet med bestemmelsen og bemærkningerne i den forklarende rapport, jf. ovenfor, taler imod en sådan forståelse af bestemmelsen.

På den baggrund er begrebet »lagret« efter Justitsministeriets opfattelse mindre egnet som afgrænsningskriterium for, hvilke elektroniske data der kan være genstand for et pålæg om hastesikring. Det afgørende må efter Justitsministeriets opfattelse være, om de pågældende data er i udbyderens besiddelse på det tidspunkt, hvor pålægges gives, uanset om opbevaringen alene er af midlertidig karakter. Pålæg vil herefter kunne omfatte eksempelvis e-mails, der opbevares af en udbyder, uanset om denne efter aftalen med brugeren er forpligtet til at lagre disse eller alene til at opbevare korrespondancen, indtil brugeren henter de pågældende e-mails ned på sin computer.

Et pålæg om hastesikring vil derimod aldrig kunne omfatte en brugers fremtidige e-mail korrespondance, men alene allerede eksisterende data, som opbevares elektronisk.

Et pålæg om hastesikring er bagudrettet og kan omfatte alle elektroniske data i udbyderens besiddelse, uanset hvor gamle disse data måtte være. Det forudsættes imidlertid, at politiet ved anvendelse af muligheden for hastesikring i medfør af § 786 a, stk. 1, foretager en proportionalitetsafvejning, således at et pålæg alene omfatter de data, der er nødvendige for efterforskningen af den konkrete sag. Således følger det af den foreslåede § 786 a, stk. 2, at politiet skal afgrænse pålægget, såvel i relation til hvilke data, der er omfattet, som i relation til hvilken tidsmæssig udstrækning af pålægget, der er påkrævet. Ved udstedelsen af pålægget må politiet således foretage en nøje afvejning mellem på den ene side hensynet til efterforskningen og på den anden side hensynet til at begrænse pålægget mest muligt.

Politiets adgang til at meddele pålæg om hastesikring er ikke begrænset til visse kriminalitetsformer, og der gælder ikke efter bestemmelsen et kriminalitetskrav som forudsætning for at anvende bestemmelsen. Indsættelsen af et kriminalitetskrav i den foreslåede bestemmelse ville ikke være foreneligt med bestemmelsen i artikel 16, hvorefter pålæg om hastesikring skal være anvendeligt som et redskab i politiets efterforskning af kriminalitet, der foretages ved hjælp af informationsteknologi. Hertil kommer, at det må antages, at politiet vil benytte adgangen til at meddele pålæg om hastesikring på et så tidligt stadie i efterforskningen, at det på dette tidspunkt ikke vil være muligt at afgøre, om der senere vil kunne ske udlevering af oplysningerne efter betingelserne i retsplejelovens § 781 om indgreb i meddelelseshemmeligheden. Justitsministeriet forudsætter dog, at adgangen til at meddele pålæg om hastesikring ikke benyttes, hvis det på forhånd måtte stå klart for politiet, at oplysningerne ikke efterfølgende vil kunne udleveres.

Efter den foreslåede § 786 a, stk. 2, er en periode på 90 dage den maksimale tidsmæssige udstrækning af et pålæg om hastesikring. Politiet må således i hvert enkelt tilfælde nærmere vurdere, hvilken periode der inden for denne ramme er nødvendig for at varetage hensynet til en effektiv efterforskning.

Det forudsættes tillige, at politiet ikke – heller ikke inden for rammen på 90 dage – kan forlænge eller forny et pålæg om hastesikring, jf. § 786 a, stk. 2. Ved udstedelsen af pålægget må politiet således have for øje, at pålæggets tidsmæssige udstrækning begrænses mest muligt, men samtidig også, at pålægget gives for et tidsrum inden for hvilket, politiet kan nå at skabe klarhed over, hvorvidt de pågældende data skal søges udleveret, eller om dataene kan slettes.

Det er ikke i den foreslåede hastesikringsbestemmelse nærmere angivet, på hvilken måde de elektroniske data skal sikres. Det afgørende er, at autenticiteten af dataene bevares. Som eksempel på hastesikring kan nævnes »indefrysning« (dvs. at gøre de pågældende data utilgængelige for sletning eller ændring). Der kan imidlertid efter omstændighederne også ske hastesikring på anden måde, f.eks. ved kopiering.

Hastesikring i medfør af den foreslåede § 786 a, stk. 1, udgør en behandling af personoplysninger, således som dette defineres i § 3, nr. 1, i persondataloven. Det må i den forbindelse lægges til grund, at politiet som den myndighed, på hvis initiativ hastesikringen sker, og som den myndighed, der i hastesikringsperioden kan bestemme, om de sikrede data kan slettes, betragtes som dataansvarlig, jf. persondatalovens § 3, nr. 4. Dette indebærer, at Datatilsynet har