Konventionens *artikel 16 og 17* om hastesikring af elektroniske data er behandlet særskilt nedenfor under pkt. 7.3., hvortil der henvises.

Artikel 18 vedrører parternes forpligtelse til at fastsætte regler, der giver mulighed for, at myndighederne kan pålægge en person at udlevere bestemte elektroniske data eller pålægge en serviceudbyder at udlevere kundeoplysninger.

Efter bemærkningerne til denne bestemmelse i den forklarende rapport tænkes dette indgreb alene anvendt over for tredjemænd (ikke-mistænkte), f.eks. serviceudbydere, og som et alternativ til mere indgribende indgreb, f.eks. ransagning og beslaglæggelse.

Adgangen til at foretage indgreb i meddelelseshemmeligheden er reguleret i konventionens artikel 20 og 21 om adgangen til at foretage aflytning af trafikdata og indholdsdata.

På den anførte baggrund er det Justitsministeriets opfattelse, at artikel 18 alene vedrører edition.

Forpligtelsen efter bestemmelsen må efter Justitsministeriets opfattelse anses for opfyldt ved reglerne om edition i retsplejelovens § 804, hvorefter en person, der ikke er mistænkt, kan pålægges at forevise eller udlevere genstande, hvis der er grund til at antage, at en genstand, som den pågældende har rådighed over, kan tjene som bevis, bør konfiskeres eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage.

Med henblik på at give politiet en bedre og mere effektiv adgang til abonnentoplysninger blev der i øvrigt ved lov nr. 378 af 6. juni 2002 (»anti-terrorpakken«) foretaget en ændring af § 34, stk. 5, i lov om konkurrence- og forbrugerforhold på telemarkedet, der giver politiet adgang til forsyningspligtudbyderens landsdækkende nummeroplysningstjeneste. Politiet er herved sikret direkte adgang til nummeroplysningsdata.

Artikel 19 vedrører parternes forpligtelse til at kunne ransage et edb-system og beslaglægge elektroniske data.

Forpligtelsen med hensyn til ransagning må anses for opfyldt ved bestemmelserne om ransagning i retsplejelovens § 793, jf. § 794.

Efter disse bestemmelser kan politiet under visse nærmere angivne betingelser foretage ransagning af bl.a. genstande, som en mistænkt har rådighed over, hvis den pågældende med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og ransagningen må antages at være af væsentlig betydning for efterforskningen.

Efter *artikel 19, stk. 2,* skal en ransagning kunne udstrækkes fra et edb-system til et andet, hvis de søgte elektroniske data er lovligt tilgængelige fra det første edb-system, og ransagningen heraf giver grundlag for at antage, at de søgte data er lagret i det andet system.

I dansk ret antages det om bl.a. tilfælde af denne karakter, at bestemmelserne om ransagning i retsplejelovens § 793, jf. § 794, foruden den mistænktes computer også omfatter indholdet af digitale meddelelser (f.eks. e-post), som der er adgang til fra den pågældendes computer, og som den pågældende har modtaget. Det gælder også, selv om de digitale meddelelser endnu ikke er teknisk set indhentet fra internetudbyderen eller teleselskabet, jf. betænkning nr. 1377/1999 om børneporno og IT-efterforskning, side 74-76.

En dansk ratifikation af konventionen nødvendiggør således ikke en ændring af ransagningsbestemmelserne i retsplejeloven.

For så vidt angår beslaglæggelse må forpligtelsen anses for opfyldt ved bestemmelserne om beslaglæggelse i retsplejelovens § 801, jf. § 802.

Efter disse bestemmelser kan politiet under visse nærmere angivne betingelser bl.a. beslaglægge genstande, som den mistænkte har rådighed over, hvis den pågældende med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale.

Artikel 19, stk. 4, indeholder en forpligtelse for parterne til at fastsætte regler, som skal gøre det muligt for myndighederne at forpligte en person til at give myndighederne de oplysninger, der er nødvendige for at kunne foretage ransagning og beslaglæggelse efter stk. 1 og 2.

Det følger af bemærkningerne i den forklarende rapport, at bestemmelsen tænkes anvendt under efterforskningen og over for systemadministratorer, som har en særlig viden om det edb-system, der er genstand for efterforskningen, herunder viden om hvor de relevante elektroniske data findes, eller om de sikkerhedsforanstaltninger, herunder adgangskoder, som er anvendt til at beskytte de pågældende data. En systemadministrator skal således efter bestemmelsen være forpligtet til at bistå politiet med sådanne oplysninger til brug for ransagningen af et edb-system og beslaglæggelse af elektronisk data.

Efter *artikel 19, stk. 5,* skal indgreb efter artikel 19 ske under iagttagelse af de betingelser og retssikkerhedsgarantier, der følger af konventionens artikel 14 og 15.

Af bemærkningerne til artikel 15 i den forklarende rapport fremgår, at de retssikkerhedsgarantier, der skal iagttages i national ret i forbindelse med iværksættelse af indgreb efter konventionen, bl.a. omfatter den sigtedes ret til ikke at inkriminere sig selv. Bestemmelsen i artikel 19, stk. 4, må således efter konventionen ikke anvendes til at forpligte en sigtet til at