de elektroniske data er særligt udsat for at gå tabt eller blive ændret.

Bestemmelsen i artikel 16 omhandler alle typer af elektroniske data. Det gælder indholdsdata, trafikdata og øvrige elektroniske data, herunder oplysninger om navn og adresse på en internetudbyder eller et teleselskabs kunder (kundeoplysninger).

Parterne skal endvidere efter *artikel 16, stk. 2,* fastsætte regler, som forpligter den person, der er blevet meddelt et pålæg efter artikel 16, stk. 1, til midlertidigt at sikre og bevare de elektroniske data uskadt i op til 90 dage.

Det er ikke i bestemmelsen i artikel 16 nærmere angivet, hvorledes de elektroniske data skal sikres. Dette kan eksempelvis ske ved »indefrysning« (dvs. utilgængeliggørelse) af de pågældende data, men der kan efter omstændighederne også ske hastesikring af elektroniske data på anden måde, f.eks. ved kopiering.

Den pågældende skal efter *artikel 16, stk. 3,* kunne pålægges tavshedspligt i en periode, hvis længde fastlægges i medlemsstatens lovgivning, med hensyn til oplysningen om, at den pågældende har sikret de elektroniske data.

Efter artikel *16, stk. 4,* skal hastesikring ske under iagttagelse af de betingelser og retssikkerhedsgarantier, der følger af konventionens artikel 14 og 15.

Som anført ovenfor under pkt. 7.2. skal de processuelle indgreb, medmindre andet er bestemt, kunne foretages ved alle handlinger omfattet af konventionens artikel 2-11 og andre strafbare handlinger begået ved hjælp af et edb-system samt i forbindelse med indsamling af elektronisk bevismateriale for en strafbar handling, jf. artikel 14, stk. 2. Det følger i den forbindelse af bemærkningerne i den forklarende rapport til artikel 14, stk. 2, at indgrebene som udgangspunkt skal kunne foretages i forbindelse med efterforskning af alle strafbare forhold, når blot efterforskningen involverer elektronisk bevismateriale.

Hastesikring indebærer i praksis, at politiet hos en internetudbyder eller et teleselskab enten ved pålæg eller på anden måde skal kunne få hastesikret elektroniske data, således at dataene beskyttes mod f.eks. at blive ændret, forringet eller slettet og dermed eventuelt efterfølgende vil kunne udleveres til politiet.

Henvisningen til trafikdata i artikel 16, stk. 1, angiver sammenhængen mellem bestemmelserne i konventionens artikel 16 og 17.

Artikel 17 vedrører hastesikring og delvis videregivelse af trafikdata.

Artikel 17, stk. 1, litra a, indeholder en forpligtelse for de kontraherende parter til at fastsætte regler, hvorefter trafikdata, der er sikret i medfør af artikel 16, også kan sikres i tilfælde, hvor den kommunikation, som de pågældende trafikdata vedrører, involverer flere serviceudbydere.

Med henblik på at kunne identificere samtlige serviceudbydere involveret i den kommunikation, som efterforskningen angår, skal parterne efter bestemmelsen *i artikel 17, stk. 1, litra b,* i tilknytning hertil sikre videregivelse af trafikdata, der er omfattet af artikel 16, i tilstrækkeligt omfang til, at partens kompetente myndigheder eller en person udpeget af myndigheden kan identificere eventuelle andre serviceudbydere og den sti, som kommunikationen er gennemført igennem.

Efter bemærkningerne til bestemmelsen i artikel 17 i den forklarende rapport skal de kompetente myndigheder i den forbindelse nærmere angive den type trafikdata, der skal videregives af serviceudbyderen.

Bestemmelsen indebærer i praksis, at politiet i tilfælde, hvor f.eks. en persons distribution af børnepornografisk materiale sker ved anvendelse af flere internetudbydere eller teleselskaber, får mulighed for at identificere og pålægge hver enkelt udbyder eller selskab at sikre trafikdata.

Bestemmelserne i konventionens artikel 16 og 17 regulerer alene adgangen til at sikre den fortsatte, midlertidige opbevaring af visse allerede eksisterende elektroniske data hos bl.a. teleudbydere. Derimod regulerer bestemmelserne ikke spørgsmålet om, i hvilket omfang politiet kan pålægge udbydere mv. at udlevere de pågældende oplysninger.

Formålet med bestemmelserne er således at sikre, at teleudbydere mv. i en periode på op til 90 dage opbevarer oplysninger, som i forvejen er i udbyderens besiddelse, med henblik på, at oplysningerne – hvis betingelserne herfor er opfyldt – efterfølgende kan udleveres til politiet til brug for efterforskning og strafforfølgning.

7.3.2. Retsplejeloven indeholder ikke bestemmelser om hastesikring af elektroniske data. Politiet vil imidlertid efter reglerne om indgreb i meddelelseshemmeligheden og om edition kunne få udleveret elektroniske data og dermed sikre deres tilstedeværelse.

Således kan politiet efter retsplejelovens § 780, stk. 1, nr. 1, foretage indgreb i meddelelseshemmeligheden ved at aflytte telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning).

Politiet kan endvidere efter retsplejelovens § 780, stk. 1, nr. 3, foretage indgreb i meddelelseshemmeligheden ved at indhente oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet