Bestemmelsen vil efter Justitsministeriets opfattelse ikke nødvendiggøre lovændringer.

Del 2 – Særlige bestemmelser

Konventionens *artikel 29-31* samt *33* og *34* vedrører gensidig retshjælp til hastesikring af elektronisk data, hastesikring og videregivelse af trafikdata, ransagning og beslaglæggelse af elektronisk data, aflytning af trafikdata og indholdsdata, jf. artikel 16-21.

Grundlaget for danske myndigheders imødekommelse af en anmodning om retshjælp fra fremmede stater er navnlig den europæiske konvention af 20. april 1959 om gensidig retshjælp i straffesager med tilhørende tillægsprotokol af 17. marts 1978.

Hverken konventionen eller tillægsprotokollen er selvstændig inkorporeret i dansk lovgivning.

I retspraksis er det fastslået, at retsanmodninger, der har selvstændig karakter af straffeprocessuelle tvangsindgreb, f.eks. beslaglæggelse af bevismidler til brug for straffesager i udlandet, kan iværksættes med hjemmel i retsplejeloven eller dennes analogi, idet det afgørende er, om foranstaltningen vil kunne foretages i en tilsvarende straffesag her i landet, jf. ovenfor. Der kan i den forbindelse bl.a. henvises til to afgørelser, der er gengivet i Ugeskrift for Retsvæsen 1972, side 600 (Højesteret), og 1988, side 203 (Vestre Landsret).

I det omfang, der efter retsplejeloven er adgang til i en tilsvarende straffesag her i landet at foretage de indgreb, som er omfattet af konventionens artikel 16-21, vil bestemmelserne i artikel 29-31 samt 33 og 34 om gensidig retshjælp til disse indgreb således ikke nødvendiggøre lovændringer i forbindelse med en dansk ratifikation af konventionen. Om vurderingen af de lovgivningsmæssige konsekvenser af konventionens artikel 16-21 henvises til det, der er anført ovenfor.

Artikel 32 regulerer parternes mulighed for grænseoverskridende adgang til lagrede elektroniske data, hvor gensidig retshjælp ikke er påkrævet.

Bestemmelsen indebærer, at de kontraherende parters kompetente myndigheder uden at anmode om retshjælp skal kunne få adgang til offentligt tilgængelige elektroniske data (»open source«), f.eks. ved at politiet på samme måde som private skaffer sig adgang til offentligt tilgængelige hjemmesider på Internettet.

Endvidere indebærer artikel 32, at parternes kompetente myndigheder på samme måde skal kunne få adgang til elektroniske oplysninger hos en anden part, hvis den første part forinden har fået samtykke fra en person på partens eget territorium, der har lovlig adgang til de elektroniske data hos den anden part. Der kan eksempelvis være tale om, at politiet med samtykke fra indehaveren af en e-postkonto skaffer sig adgang til den pågældendes e-post, der befinder sig i en elektronisk postkasse hos en internetudbyder i et andet land.

Da bestemmelsen indebærer adgang til offentligt tilgængelige elektroniske data og til data med samtykke fra den person, der er berettiget til at videregive disse, kræver bestemmelsen efter Justitsministeriets opfattelse ikke lovændringer.

Artikel 35 vedrører udpegningen af et kontaktpunkt, der altid er tilgængeligt (24 timer i døgnet/7 dage om ugen) for at kunne yde bistand til uopsættelige efterforskningsskridt.

Der er allerede i dag hos Rigspolitichefen etableret et døgnbemandet kommunikationscenter, som yder bistand til og koordinerer uopsættelige efterforskningsskridt navnlig i forbindelse med efterforskning af IT-kriminalitet.

7.3. Justitsministeriets overvejelser om hastesikring af elektroniske data

7.3.1. Artikel 16 og 17 i Europarådets konvention om IT-kriminalitet vedrører parternes forpligtelse til at fastsætte regler om såkaldt hastesikring af elektroniske data.

Bestemmelserne omhandler hastesikring af allerede eksisterende data, som er lagret elektronisk af f.eks. en internetudbyder (»datapreservation«).

I bemærkningerne til artikel 16 og 17 i den forklarende rapport er det anført, at hastesikring af elektroniske data er et nyt vigtigt redskab i efterforskningen af lovovertrædelser, der foretages ved hjælp af informationsteknologi, herunder navnlig kriminalitet der foregår på eller ved hjælp af Internettet. Det hænger sammen med, at der ved sletning eller ændring mv. af elektroniske data er risiko for, at afgørende bevismateriale vedrørende indholdet af kommunikationen, f.eks. børnepornografisk materiale, går tabt, eller at elektroniske spor på Internettet går tabt, således at det ikke under en efterfølgende politimæssig efterforskning vil være muligt at spore den kommunikation, der har fundet sted, idet sporet ender blindt hos udbyderen.

Efter *artikel 16, stk. 1,* har parterne en forpligtelse til at fastsætte regler, hvorefter parternes kompetente myndigheder kan meddele pålæg om hurtig sikring af bestemte elektroniske data, herunder trafikdata, der er lagret ved hjælp af et edb-system, eller hvorefter der på anden lignende måde kan opnås hurtig sikring af sådanne data, navnlig hvis der er grund til at antage, at