

selskaberne, således at disse kan sørge for, at politiet parallelt med vedkommende telefonabonnent får adgang til telefontrafikken.

Aflytning i det analoge NMT-mobiltelefonnet er i praksis blevet effektueret ved hjælp af elektronisk scanning af radiokanaler, idet der ikke er indbygget aflytningsfaciliteter i NMT-nettet. Denne form for aflytning er belagt med teknisk usikkerhed i relation til »fangning« af samtaler, ligesom det kræver store mandskabsmæssige ressourcer, idet mobiltelefonen skal være inden for rækkevidde af scanningsudstyret, og idet scanningen – af hensyn til efterforskningen – skal ske skjult. Yderligere er der i NMT-nettet installeret et EDB-baseret system, hvorefter der kan »overvåges« nogle få mobiltelefoner. Dette »automatiske« system har – foruden kapacitetsmangel – tillige bl.a. den tekniske mangel, at der alene kan ske aflytning af en samtale ad gangen.

M.h.t. aflytning i de fælleseuropæiskstandardiserede digitale mobiltelefonnet (GSM- og DCS1800-teknologierne) er de tekniske specifikationer for disse net etop udviklet med det formål at undgå (uautoriseret) aflytning.

De tekniske standarder for moderne telekommunikation udvikles i sagens natur ikke med det hovedsigte, at kommunikationen skal kunne aflyttes. Tværtimod gøres der af telesektorens interessenter et stort arbejde for at forhindre (uautoriseret) aflytning. De retshåndhævende myndigheders behov for at kunne foretage legal aflytning indgår ikke – eller i hvert fald kun perifert – i interessenternes udviklingsarbejde. Hertil kommer, at telekommunikation i vidt omfang i dag foregår på grundlag af digitale teknologier. Dette giver mulighed for ved enkle midler at kryptografere kommunikationen, hvilket i praksis umuliggør aflytning, jf. nærmere herom nedenfor.

Såfremt det, med denne udvikling, fortsat skal være muligt for politiet at aflytte telekommunikation, jf. retsplejelovens kap. 71, er det nødvendigt med en klar lovhjemmel, der pålægger udbydere af telenet, at disse udover i almindelighed at bistå politiet i forbindelse med aflytning, ved fremtidige anskaffelser af centraludstyr skal sikre, at disse er indrettet således, at aflytning er mulig.

Centraludstyr som udbydere af telenet og teletjenester allerede har anskaffet og etableret inden lovforslagets ikrafttræden er ikke omfattet af kravet om at sikre adgang til aflytning. Net- eller tjenesteudbyderen har ikke pligt til at tilpasse et »gammelt« system, så det bliver muligt at foretage aflytning.

Bestemmelsen i retsplejelovens § 786 og øvrige bestemmelser i retsplejelovens kapitel 71 regulerer ikke udtrykkeligt omkostningsspørgsmålet ved aflytninger. I praksis er omkostningerne ved aflytning blevet

fordelt således, at politiet har betalt de konkrete udgifter ved aflytningen, dvs. dels et fast beløb for etableringen – dækkende telefonmontør-løn mv.- dels de løbende udgifter forbundet ved at få telefontrafikken fra den aflyttede telefon bragt til politiets bygninger. Det fremgår udtrykkeligt af bestemmelsen at det ikke med lovforslaget er hensigten at ændre på denne praksis.

Lovforslaget indebærer imidlertid, at der allerede forud for konkrete aflytnings-situationer skal indbygges passende udstyr i telenettet, hvilket indebærer grund-investeringer af betydelig størrelse. Det fremgår af lovbestemmelsen at det ikke er hensigten, at udbydere af telenet og teletjenester skal kunne få refunderet udgifterne til denne grundlæggende opgradering, f.eks. hos politiet.

Det er endvidere hensigten med lovforslaget at give forskningsministeren hjemmel til at fastsætte nærmere regler om de tekniske krav til centraludstyr som nævnt ovenfor i det omfang, det viser sig nødvendigt at fastsætte nærmere regler herom.

Aflytningsfaciliteterne i centralerne bør, så vidt det er muligt, være baseret på fælleseuropæiske standarder. Sådanne standarder foreligger imidlertid indtil videre kun i stærkt begrænset omfang. Den efterfølgende bekendtgørelsesregulering vil i givet fald ske på grundlag af fælleseuropæiske standarder.

#### *Forholdet til kryptering*

Der findes i dag ingen dansk regulering på krypteringsområdet. Krypteringsudstyr må lovligt anvendes i Danmark og kan i dag erhverves for få tusinde kroner. Det er muligt at kryptere kommunikation »end-to-end« i hvilken som helst teletjeneste ved brug af krypteringsudstyr, der kan opstilles hos de to kommunikationsparter. Kryptering rejser dog samtidig problemer, idet moderne krypteringssystemer er så sikre, at heller ikke politi eller efterretningstjenester i alle tilfælde kan bryde dem. Anvendelsen af kryptering kan derfor reelt afskære efterforskningsmyndighedernes eksisterende mulighed for indgriben i meddelelseshemmeligheden.

Da den tekniske udvikling bevirker, at stadig større dele af telekommunikationen foregår digitalt via åbne netværk, f.eks. Internet, vil det blive mere og mere almindeligt at kryptere kommunikationen. Hertil kommer, at der fra erhvervs side er en stærkt stigende efterspørgsel efter sikker elektronisk kommunikation baseret på kryptering. Kryptering begrænser imidlertid ikke kun uvedkommendes adgang til information, men også den legale adgang, som politiet har til at foretage indgreb i meddelelseshemmeligheden i forbindelse med efterforskning af alvorlig kriminalitet.