

at der i almindelighed skal være tale om efterforskning af en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover, jf. retsplejelovens § 781, stk. 1. Endvidere skal proportionalitetskravet i § 782 være opfyldt. Kravet om »bestemte grunde« skal ikke være opfyldt ved udvidet teleoplysning, men der er omvendt kun adgang til disse oplysninger, når mistanken vedrører en forbrydelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier, jf. § 781, stk. 5.

Denne del af forslaget giver således ikke politiet adgang til oplysninger i videre omfang end i dag. Forslaget skal alene sikre, at de pågældende oplysninger rent faktisk findes, hvis der bliver brug for dem.

### 3.1.3.2. Internettrafikdata

Internettets anvendelsesmuligheder er mangfoldige. Det udgør en væsentlig lettelse i den daglige kommunikation mellem mennesker og giver mulighed for at søge og udveksle oplysninger på en enkel, hurtig og billig måde. I kraft af Internettets komplicerede struktur giver det også gode muligheder for at være anonym i forbindelse med kommunikation og informationsudveksling. Disse muligheder udnyttes ikke mindst af de kriminelle.

Det ville være en illusion at tro, at det er muligt at overvåge hele Internettet. En sådant mål er heller ikke ønskeligt. Selv om det således ikke er muligt at bekæmpe al internetkriminalitet, bør man efter Justitsministeriets opfattelse ikke undlade at forbedre politiets efterforskningsmuligheder på de områder, hvor det kan lade sig gøre uden at tilsidesætte væsentlige hensyn til økonomi og privatlivets fred.

Justitsministeriet finder af de af Brydenscholt-udvalget anførte grunde, at der – af hensyn til mulighederne for en effektiv efterforskning og bekæmpelse af kriminalitet, der begås på eller ved hjælp af Internettet – bør tilvejebringes hjemmel til at kræve logning af internettrafik. Den seneste tids alvorlige terrorangreb på USA, herunder udbredelsen af militærbrandbakterier, forstærker denne opfattelse. Angrebene viser, hvor sårbare vore moderne samfærdsels- og kommunikationsmidler er over for de uspekulerede og – forud for angrebene – nærmest utænkelige handlinger, som terrorister foretager, og der er al mulig grund til at antage, at terrorister i forbindelse med planlægningen af terrorhandlinger kommunikerer med hinanden og tilvejebringer information ved hjælp af Internettet.

Det er hensigten at fastsætte de nærmere regler om logningspligtens indhold og omfang efter dialog med internetudbydere. Dette er ikke mindst afgørende for

at sikre en hensigtsmæssig teknologisk udformning af reglerne.

En ordning med pligtsmæssig logning af oplysninger om teletrafik til brug for efterforskning og retsforfølgning af strafbare forhold vil være en nyskabelse i forhold til den gældende retstilstand. Uanset, at forslaget om en nærmere regulering ved bekendtgørelse i vid udstrækning giver mulighed for løbende at tage højde for det praktiske behov for logning og den tekniske udvikling på området, finder Justitsministeriet det hensigtsmæssigt, at ordningen evalueres nogle år efter dens iværksættelse. Bestemmelsen i lovforslagets § 8 indebærer således, at ordningen i folketingsåret 2005-06 skal tages op til fornyet overvejelse.

Om baggrunden for forslaget om anvendelse af en bemyndigelsesbestemmelse henvises til pkt. 3.1.3.3. nedenfor.

Formålet med den foreslåede regulering er at sikre, at de elektroniske spor, der findes på Internettet i tilknytning til en kriminel aktivitet, ikke ender blindt hos internetudbyderen. Dette forudsætter, at udbyderen er i stand til at levere oplysninger om, hvem der har efterladt det pågældende spor. I praksis vil dette kun være muligt, hvis udbyderen er i besiddelse af præcise oplysninger om, hvilken kunde, der på det pågældende tidspunkt har anvendt en tildelt IP-adresse. Af hensyn til værdien af disse oplysninger er det vigtigt, at oplysningerne er nøjagtige, herunder ikke mindst for så vidt angår tidsangivelser. Ved anvendelsen af dynamiske IP-adresser vil det forekomme, at den IP-adresse, som den kriminelle har anvendt, kort tid før eller efter anvendes af en anden kunde hos den pågældende udbyder. Korrekt tidsangivelse er af afgørende betydning for, at det elektroniske spor kan føres tilbage til den person, der anvendte den pågældende IP-adresse på gerningstidspunktet.

Det har over for Justitsministeriet været fremført, at der i praksis vil kunne være tekniske hindringer for internetudbyderes registrering af det kaldende nummer (A-nummeret). Denne registrering, der kun vil være relevant, hvor forbindelsen til internetudbyderens server er etableret via telefonnettet, vil være af betydning ved undersøgelsen af, hvorfra opkaldet er etableret. Politiet vil dermed hurtigere kunne målrette efterforskningen mod den reelle gerningsmand. Dette medvirker til at styrke retssikkerheden for den kunde, hvis internetkonto måtte være blevet misbrugt til at skaffe kriminelle adgang til Internettet. Her vil det kunne være af væsentlig betydning for efterforskningen straks at kunne fastslå, at opkaldet til internetudbyderen er etableret fra en telefon, som kunden ikke kan have haft adgang til. Justitsministeriet finder, at