med indgreb efter § 791 a, stk. 3, og ikke var mere indgribende end sådanne foranstaltninger. Landsretten tillod derfor indgrebet efter retsplejelovens § 791 a, stk. 3, eller denne bestemmelses analogi.

Højesteret udtalte, at foranstaltningen mest nærliggende må sidestilles med gentagen hemmelig ransagning, og tiltrådte på den baggrund og af de grunde, der var anført af byretten og af én dommer i landsretten, byrettens kendelse om ikke at tillade indgrebet.

Det bemærkes i den forbindelse, at Højesteret tidligere i en kendelse, der er gengivet i *Ugeskrift for Retsvæsen 1999, side 985,* og som er omtalt nærmere under pkt. 3.4.2.2. ovenfor, har udtalt, at en kendelse om hemmelig ransagning efter § 799 kun kan omfatte en enkelt ransagning inden for den periode, der er fastsat for foretagelse af indgrebet. Det var på denne baggrund ikke muligt at tillade indgrebet efter reglerne om hemmelig ransagning.

Som nævnt ovenfor har politiet ved hemmelig ransagning mulighed for – hvis det i øvrigt er praktisk muligt – at skaffe sig adgang til alle de elektroniske dokumenter, som opbevares i computeren, herunder også modtagne e-breve og kopier af afsendte e-breve.

Den nævnte højesteretskendelse indebærer imidlertid, at det efter de nugældende regler ikke er muligt at skaffe de samme oplysninger, hvis undersøgelsen af materialet i computeren sker ved en løbende aflæsning, der foretages af politiet fra et andet sted.

3.4.2. Justitsministeriets overvejelser

Som det fremgår ovenfor, består der allerede efter de gældende regler mulighed for, at politiet kan gøre sig bekendt med kommunikation mellem computere mv., og at politiet ved ransagning – evt. hemmelig ransagning – kan gøre sig bekendt med alle registreringer i en computer, herunder modtagne elektroniske meddelelser og kopier af sådanne meddelelser, der er afsendt.

På grund af tekniske forhold og som følge af risikoen for afsløring af indgrebene, er det imidlertid ikke i alle tilfælde muligt at udnytte denne eksisterende adgang for politiet til at gøre sig bekendt med elektroniske meddelelser og materiale i en computer.

Bl.a. i lyset af terrorangrebet mod USA den 11. september 2001, er det Justitsministeriets opfattelse, at politiet i forbindelse med efterforskningen af alvorlig kriminalitet – f.eks. gennem installering af særlige edb-programmer (»sniffer-programmer«) – kan have behov for løbende at kunne registrere indholdet og anvendelsen af bestemte computere mv.

Dette gælder efter Justitsministeriets opfattelse navnlig i forbindelse med efterforskningen i sager om overtrædelse af straffelovens kapitel 12 (forbrydelser mod statens selvstændighed og sikkerhed) og kapitel 13 (forbrydelser mod statsforfatningen og de øverste statsmyndigheder mv.) eller en overtrædelse af straffelovens § 180 om kvalificeret brandstiftelse, § 183, stk. 1 og 2, om forvoldelse af sprængning og spredning af skadevoldende luftarter, jernbaneulykke m.m., § 183 a om flykapring, § 186, stk. 1, forvoldelse af fare for menneskers liv eller helbred ved at tilsætte vandbeholdninger sundhedsfarlige stoffer mv., § 187, stk. 1, om at tilsætte gift eller andre lignende stoffer til ting, som er bestemt til forhandling eller udbredt benyttelse mv., § 191, om grove narkotikaforbrydelser, § 192 a om særligt grove våbenlovsovertrædelser samt § 237 om drab. En række af disse straffelovsovertrædelser kan efter deres karakter bl.a. tænkes at finde sted som led i eller i forbindelse med egentlige terrorhandlinger.

Det kan således f.eks. være nødvendigt for politiet at kunne foretage løbende aflæsning af ikke offentligt tilgængelige oplysninger i informationssystemer (f.eks. en personlig computer), som politiet er vidende om anvendes til udfærdigelse af en »drejebog« for kriminelle aktiviteter, herunder terroraktioner. På samme måde kan politiet have behov for løbende at kunne aflæse oplysninger i computere mv., der anvendes til fremstilling af falske pas, pengesedler eller andre falske dokumenter.

På denne baggrund foreslås der indsat en ny bestemmelse i retsplejelovens § 791 b, der giver politiet mulighed for, at anvende f.eks. de såkaldte »snifferprogrammer« eller andet udstyr med henblik på, at der løbende tilsendes politiet kopi af ikke offentligt tilgængelige oplysninger (herunder e-post og andre indtastninger mv.) i et informationssystem. Det foreslås, at indgrebet betegnes »dataaflæsning«. Dataaflæsning vil ligeledes omfatte elektroniske meddelelser, som er sendt til den mistænkte, og som opbevares i computerens hukommelse.

Det bemærkes i øvrigt, at en adgang for politiet til at anvende sådanne edb-programmer mv. i nogle tilfælde også vil give politiet mulighed for at læse elektroniske meddelelser, der sendes til eller fra en mistænkt via en computer mv., i tilfælde, hvor dette ellers ikke er muligt, fordi der benyttes kryptering, der medfører at meddelelsen ikke kan »aflyttes« under forsendelsen.

Den foreslåede bestemmelse i § 791 b giver politiet mulighed for at foretage dataaflæsning i informationssystemer af oplysninger, som ikke er offentligt tilgængelige. Aflæsning af oplysninger, som er offentligt tilgængelige, således at der også er fri adgang til oplys-