pålæg om at indrette sit udstyr således, at det kan registrere afstanden til nærmeste mobilmast, selv om der ikke i dag findes tekniske standardløsninger herfor.

Enhedslistens medlem af udvalget bemærker, at lovforslaget som de øvrige dele af terrorpakken, er udtryk for regeringens manglende tillid til demokratiet. Der er i stedet tale om en ensidig fokusering på sikkerhed – og det på bekostning af retssikkerheden.

Det er især bekymrende, fordi regeringens embedsmandsgruppe, som lovforslagene i terrorpakken bygger på, slog fast i sin rapport fra november 2006, at det danske terrorberedskab ikke var utilstrækkeligt – eller sagt på almindeligt dansk: Det danske terrorberedskab er godt nok. Alligevel vælger regeringen at fremsætte lovforslag, som udvider efterretningstjenesternes operationsmuligheder, samtidig med at den uafhængige kontrol, eksempelvis domstolskontrollen, svækkes. Og med dette lovforslag lægger regeringen så at sige yderligere op til en »våbenoptrapning«. Det skal forstås på den måde, at de onde og de kløgtige vil gå over til kryptering af deres kommunikation og bruge trådløse såkaldte hotspots m.v., hvorefter regeringen vil være nødt til at stramme loven yderligere. Det bliver skruen uden ende, alt sammen til gene først og fremmest for den almindelige borger. Også på den baggrund mener Enhedslisten, at hverken dette lovforslag eller de øvrige lovforslag i terrorpakken er en retsstat værdigt.

Det er dybt bekymrende, at den teleudbyder, der har kundeforholdet, er forpligtet til at udlevere oplysninger om kundens adgang til elektroniske kommunikationsnet og -tjenester for alle elektroniske kommunikationsformer til politiet, herunder oplysninger om kundens adgang til internettet (IP-adresser og e-mail-adresser), uden at betingelserne for edition skal være opfyldt, og uden rettens godkendelse. I denne forbindelse er der hverken henvisning til straffelovens kapitel 12 og 13 om forbrydelser mod staten eller terror eller til nogen mindste strafferamme. Det indebærer en adgang for politiet til at få alle de grundlæggende oplysninger, politiet ønsker for at kunne gennemføre en aflytning eller overvågning af en hvilken som helst borger – eller alle borgere, om man vil – uden retskendelse. Påstanden er ikke, at det vil ske. Påstanden er, at det kan ske, fordi udbyderne er forpligtede til at udlevere oplysningerne – i princippet til enhver i politiet – uden at det skal godkendes af domstolene.

Frem for alt savner Enhedslisten en præcisering i lovforslaget af fundamentale principper for teleudbyderes pligt til at hjælpe politiet. Uden sådanne principper er der risiko for, at teleudbydere tvinges ud i en egentlig overvågning af borgerne, som aldrig har været politisk tilkendegivet. Særlig på baggrund af, at lovforslagene er enestående i international sammenligning, forekommer mangelen på et mere tilbundsgående forarbejde bekymrende.

Interesseorganisationen ITEK og Dansk Industri skriver bl.a. i deres høringssvar til lovforslaget: »Men den meget vidtgående åbning af adgangen til at kunne tilsidesætte almindelige retsprincipper taler for, at grænserne for, hvad man som virksomhed skal kunne tåle, underkastes en nøjere granskning – også i lyset af, at disse informationer kan risikere at komme i fremmede efterretningsmyndigheders eje.« Der er næppe tvivl om, at ITEK her tænker på øgede muligheder for industrispionage i almindelighed og på Echelon i særdeleshed.

Det er dybt bekymrende, at regeringen nu vil have private virksomheder til at udføre politiarbejde. Således er det eksempelvis ikke politiet, men kundens teleselskab, som skal sørge for enten provokerede opkald eller SMS'er i forbindelse med stedfæstelse af en mobiltelefon. Det fremgår af ministerens svar på spørgsmål 12.

Lovforslaget viser måske i højere grad end lovforslag nr. L 217 og L 218, som er terrorpakkens to øvrige lovforslag, at der er tale om, at regeringen ønsker at vise handlekraft frem for at se på årsagerne til terror. Således fremgår det af svar fra videnskabsministeren, at såkaldte VoIP-tjenester (voice over internet protocol) og chat er krypterede og ikke kan dekrypteres af teleudbyderne, hvorfor det vil være op til politiet, hvorvidt en konkret kryptering kan dekrypteres – eller sagt på almindeligt dansk: To af de hurtigst voksende teknologier inden for telekommunikation, nemlig VoIP og chat, kan ikke umiddelbart aflyttes, og det er tvivlsomt, om nogen kan bryde koden og på et senere tidspunkt »læse« indholdet af meddelelserne. Hertil kommer desuden, at politiet eller teleudbyderne ikke altid vil kunne se, hvem der kommunikeres med.