FORSVARSMINISTERIET

KOMMENTERET HØRINGSOVERSIGT
vedrørende
forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Dato: Marts 2021

Enhed: JSN
Sagsnr.: 2020/008732
Dok.nr.: 212633
Bilag: Ingen

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Et udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur har i perioden fra den 7. december 2020 til den 4. januar 2021 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Amnesty International, Bauer Media, Borch Teknik, Cibicom, Danmarks Radio, Dansk Beredskabskommunikation, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Dansk Kabel TV, Danske Advokater, Danske Regioner, Datatilsynet, Den Danske Dommerforening, DI Digital, Domstolsstyrelsen, Fibia, Forenede Danske Antenneanlæg, Globalconnect, Hi3G Denmark, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KL, Norlys, præsidenten for Vestre Landsret, præsidenten for Østre Landsret, Retspolitisk Forening, Rigsombudsmanden i Grønland, Rigsombudsmanden på Færøerne, Rigsrevisionen, Rådet for Digital Sikkerhed, samtlige byretspræsidenter, TDC, TeleDCIS, Teleindustrien (TI), Telenor, Telia Company Danmark, Tilsynet med Efterretningstjenesterne, TT-Netværket, TV 2 DTT og Waoo.

Forsvarsministeriet har modtaget høringssvar fra:

Advokatsamfundet, Chinese Chamber of Commerce in Denmark (CCCD), Danmarks Radio (DR), Dansk Energi, Dansk Erhverv og IT-Branchen, Danske Regioner, Datatilsynet, DI, Domstolsstyrelsen, Forenede Danske Antenneanlæg, Huawei, Institut for Menneskerettigheder, KL, præsidenten for Københavns Byret på vegne af byretspræsidenterne, præsidenterne for henholdsvis Vestre og Østre Landsret, Retspolitisk Forening, Rigsrevisionen, Rådet for Digital Sikkerhed, Teleindustrien og Tilsynet med Efterretningstjenesterne.

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Forsvarsministeriets kommentarer til høringssvarene er angivet i kursiv.

1. Generelle bemærkninger

Datatilsynet, Domstolsstyrelsen, Forenede Danske Antenneanlæg, KL og Tilsynet med Efterretningstjenesterne har ikke bemærkninger til lovforslaget. Præsidenten for Københavns Byret på vegne af byretspræsidenterne, præsidenterne for henholdsvis Vestre og Østre Landsret samt Rigsrevisionen har ikke ønsket at udtale sig om lovforslaget. Advokatrådet har oplyst, at rådet har besluttet ikke at afgive høringssvar.

Det bemærkes for god ordens skyld, at myndighederne på Færøerne og i Grønland indgår i en arbejdsgruppe med danske myndigheder. Arbejdsgruppens arbejde er ikke afsluttet.

DR anerkender, at der er en høj trussel fra cyberspionage mod telesektoren i Danmark. De er derfor også enige i behovet for at styrke telemyndighederne for at kunne forbyde konkrete leverandøraftaler vedrørende den kritiske teleinfrastruktur, hvis aftalerne vurderes at udgøre en trussel mod statens sikkerhed.

Dansk Energi bakker grundlæggende op om lovforslagets hovedformål om at sikre en robust teleinfrastruktur og derigennem beskytte Danmark mod bl.a. spionage, sabotage og nedbrud af samfundskritiske funktioner.

Dansk Erhverv og IT-Branchen samt Forenede Danske Antenneanlæg støtter regeringens overordnede hensigt om at øge sikkerheden i teleinfrastrukturen. Dansk Erhverv og IT-Branchen støtter private udbyderes og offentlige myndigheders fortsatte systematiske og vedholdende arbejde for at sikre teleinfrastrukturen og øvrig digital infrastruktur.

Danske Regioner finder det som udgangspunkt positivt, at Center for Cybersikkerhed med lovforslaget får bedre muligheder for at kunne varetage sikkerheden i den teleinfrastruktur, som regionerne benytter til kritisk kommunikation i forbindelse med patientbehandling og levering af sundhedsydelser. Danske Regioner finder således, at lovforslaget understøtter en styrket sikkerhed i den samfundskritiske sundhedssektor og regionernes arbejde med cyber- og informationssikkerhed.

DI støtter behovet for en lovgivning, der øger sikkerheden i den danske teleinfrastruktur. Organisationen anfører, at teleinfrastrukturen er kritisk samfundsinfrastruktur, og at det er væsentligt at beskytte den mod eventuelle sikkerhedsrisici.

Huawei anfører, at virksomheden støtter en klar og streng regulering af krav til netværkssikkerhed i den kritiske teleinfrastruktur.

Retspolitisk Forening anfører, at de er enige i, at der hersker et presserende behov for at øge leverandørsikkerheden i den kritiske teleinfrastruktur, og organisationen kan derfor støtte, at der som foreslået vedtages en lov, som bl.a. vil give Center for Cybersikkerhed beføjelser til at forbyde visse aftaler om leverancer af kritisk teleinfrastruktur.

Rådet for Digital Sikkerhed finder det positivt, at cybersikkerhed gøres til en parameter i forbindelse med indkøb af komponenter til den kritiske infrastruktur.

Teleindustrien finder det positivt, at regeringen sætter fokus på den digitale infrastrukturs samfundskritiske funktion, og organisationen anfører, at lovforslaget tager udgangspunkt i, at velfærd og velstand i det danske samfund i høj grad afhænger af en velfungerende og sikker teleinfrastruktur. Det er en vurdering, som telebranchen i allerhøjeste grad deler.

2. Anvendelsesområdet

Dansk Erhverv og IT-Branchen anfører, at organisationerne anser definitionen af "kritisk infrastruktur" for at være uklar, og at den efter organisationernes opfattelse skal præciseres væsentligt.

DI vurderer, at det vil være mere oplagt at harmonisere definitionen af kritisk teleinfrastruktur i forhold til EU's 5G-toolbox, som graduerer kritisk teleinfrastruktur, i stedet for at anvende et skarpt skel mellem kritisk og ikke-kritisk teleinfrastruktur.

Huawei anfører, at definitionen af kritiske netkomponenter, systemer og værktøjer ikke følger tilgangen til definition af kritisk infrastruktur i EU's NIS Toolbox. Huawei anbefaler, at definitionerne i lovforslaget tilpasses til definitionerne i den internationale vejledning, der findes i f.eks. internationale sikkerhedscertificeringsordninger som NESAS/SCAS og Common Criteria, og opfordrer til, at der hentes inspiration fra definitionerne i NIS Tool Box vedrørende eksempler på mindre indgribende foranstaltninger. Huawei finder, at en sådan harmoniserende tilgang bør fastlægges direkte i lovforslaget for at sikre transparente og klare kriterier samt for i højere grad at sikre, at reguleringen proaktivt kan fungere markedskorrigerende i sig selv, uden at Center for Cybersikkerhed reaktivt skal håndhæve reguleringen.

Rådet for Digital Sikkerhed finder, at der er foretaget en dansk forsimpling af kritisk eller ikke kritisk infrastruktur, hvilket efter rådets opfattelse ikke er meningsfuldt, når EU arbejder med flere nuancer.

Teleindustrien konstaterer, at den nuværende definition i lovforslagets § 1, nr. 1, svarer til samme definition i net- og informationssikkerhedsloven. Organisationen finder, at definitionen er meget bred. Organisationen anfører endvidere, at stort set alle it-systemer, der anvendes i en teleudbyders forretning – herunder tjenesteudbydere, der ikke har eget netværk, men anvender egne support-systemer – vil blive omfattet af loven. Organisationen finder det også uklart, hvad der forstås ved "centrale routere og servere i backbonenettet", og giver udtryk for, at der ingen afgrænsning er af, hvad der er "centrale" og "ikke-centrale" routere. Organisationen finder det tilsvarende uklart, hvad der menes med "hardware […], der anvendes i corenet". Det er organisationens opfattelse, at udbyderne er overladt til Center for Cybersikkerheds uforudsigelige vurdering af, om et netværkselement er omfattet. Teleindustrien opfordrer til, at de dele af udbydernes infrastruktur, der omfattes af loven, entydigt angives, samt at dette afgrænses til kun at gælde det absolut mest nødvendige.

Lovforslagets § 1, nr. 1, definerer kritiske netkomponenter, systemer og værktøjer, og den anvendte definition svarer til definitionen i § 1, nr. 1, i bekendtgørelse nr. 258 af 22. februar 2021 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester, som er udstedt i medfør af lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021.

Definitionen var genstand for nøje overvejelser i forbindelse med udstedelsen af den første bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed i 2016. Definitionen indeholder således en detaljeret opregning af de dele af telenettet, der vurderes at være kritiske. I lovforslaget bliver disse dele beskrevet nærmere og eksemplificeret i bemærkningerne til bestemmelsen.

Det vurderes ikke hensigtsmæssigt at udarbejde en mere udtømmende liste over alle kritiske dele af teleudbydernes systemer og komponenter. En sådan liste ville blive meget omfattende og ville i praksis kræve hyppige ændringer af loven, da den teknologiske udvikling på teleområdet gør, at der løbende anskaffes nye typer af kritiske systemer og kritiske komponenter.

Definitionen af kritiske netkomponenter, systemer og værktøjer har været anvendt i net- og informationssikkerhedsreguleringen siden 2016. Det er dermed en definition, der er velkendt af telebranchen. Forsvarsministeriet har ikke kendskab til, at anvendelsen af definitionen i praksis skulle have givet anledning til grundlæggende udfordringer.

For regeringen er det vigtigt, at reguleringen sikrer en robust teleinfrastruktur og derigennem beskytter Danmark mod bl.a. spionage, sabotage og nedbrud af samfundskritiske funktioner. Reguleringen bør derfor omfatte alle de dele af teleinfrastrukturen, der er kritiske for telenettets funktion. Forsvarsministeriet finder på den baggrund ikke grundlag for at ændre – og herunder graduere – definitionen af kritiske netkomponenter, systemer og værktøjer.

3. Kriterier for forbud

Teleindustrien anfører, at organisationen anser kriterierne for, om der foreligger en "trussel mod statens sikkerhed", for at være uklare og uforudsigelige, hvilket efter organisationens opfattelse medfører en meget stor regulatorisk usikkerhed for såvel teleselskaber som udstyrsleverandører. Organisationen giver således udtryk for, at det er vanskeligt at se, at der er tale om objektive og klare kriterier. CCCD og Huawei anfører tilsvarende, at de anser kriterierne for at være uklare, og at det efter deres opfattelse kan føre til uforudsigelige afgørelser.

Lovforslaget indebærer, at Center for Cybersikkerhed i særlige tilfælde vil kunne forbyde teleudbydere at indgå en leverandøraftale, der vedrører kritiske dele af teleinfrastrukturen, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed.

Ved vurderingen af, om en aftale udgør en trussel mod statens sikkerhed, vil Center for Cybersikkerhed kunne lægge vægt på forhold vedrørende den leverandør, som teleudbyderen ønsker at anvende. I vurderingen vil kunne indgå forhold vedrørende både leverandøren, leverandørens væsentligste underleverandører samt andre aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren, f.eks. leverandørens ejere eller bestyrelsesmedlemmer.

Der vil være tale om en samlet vurdering, hvori der vil indgå en række objektive kriterier. Eksempelvis vil Center for Cybersikkerhed kunne lægge vægt på, om en leverandør m.v. er hjemmehørende i eller varetager produktionen eller driften fra et land, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med. Der vil også kunne lægges vægt på, om leverandøren m.v. er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter det pågældende lands lovgivning er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage.

Herudover vil Center for Cybersikkerhed kunne lægge vægt på, om leverandøren m.v. direkte eller indirekte kontrolleres af et andet lands

statslige organer, herunder militære myndigheder, samt om leverandøren m.v. er eller har været involveret i aktiviteter i Danmark eller andre lande, som har medført en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden.

Forsvarsministeriet anser denne model, hvor der med udgangspunkt i en række objektive kriterier foretages en samlet vurdering, der er baseret på Center for Cybersikkerheds telefaglige og sikkerhedsmæssige ekspertise, for at være hensigtsmæssig. Modellen sikrer, at Center for Cybersikkerhed kan inddrage en række forskellige – og ofte modsatrettede – aspekter i den samlede vurdering, herunder at Center for Cybersikkerhed får mulighed for at lægge vægt på de aspekter, som teleudbyderne måtte fremføre i dialogen med centeret.

Vurderingen af, om aftalen vil udgøre en trussel mod statens sikkerhed, vil typisk ske som sidste trin i forbindelse med den underretningsordning, der i forvejen er etableret i medfør af lov om sikkerhed i net og tjenester. Allerede på det tidspunkt, hvor en teleudbyder påbegynder overvejelserne om at indgå en ny leverandøraftale, vil teleudbyderen derfor være i kontakt med Center for Cybersikkerhed, og centeret vil i den efterfølgende proces kunne give teleudbyderen omfattende rådgivning og vejledning om de sikkerhedsmæssige aspekter af aftalen, herunder aspekter, som efter centerets vurdering vil kunne udgøre en trussel mod statens sikkerhed. Det sikrer en høj grad af forudsigelighed i det senere forhandlingsforløb, hvor teleudbyderen på et tidligt tidspunkt vil være bekendt med Center for Cybersikkerheds vurdering af den konkrete aftale.

I forhold til allerede indgåede aftaler vil lovforslaget i første omgang ikke omfatte aftaler, der er indgået forud for høringstidspunktet (den 7. december 2020). Det foreslås dog, at ældre aftaler, der stadig måtte være i kraft, omfattes fra den 1. januar 2026. Det er Forsvarsministeriets vurdering, at meget få aftaler på teleområdet har så lang varighed, men også i forhold til eksisterende aftaler vil Center for Cybersikkerhed indgå i et rådgivnings- og dialogforløb med teleudbyderen, bl.a. med henblik på at afklare, om mindre indgribende foranstaltninger end et forbud vil være tilstrækkelige.

Teleudbyderen vil således altid kunne få rådgivning og vejledning hos Center for Cybersikkerhed vedrørende de sikkerhedsmæssige aspekter af konkrete aftaler.

Teleindustrien anser lovforslagets kriterium om leverandører m.v., der har været involveret i aktiviteter, som har medført "en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden", for at være cirkulært formuleret, idet det kan være en trussel

mod statens sikkerhed, hvis aktøren har haft en negativ påvirkning af statens sikkerhed. Organisationen anfører videre, at selv en undskyldelig fejl i et stykke software kan udgøre en "negativ påvirkning af informationssikkerheden", og dermed være en trussel mod statens sikkerhed.

Forsvarsministeriet kan bekræfte, at det ved vurderingen af, om en leverandøraftale kan udgøre en trussel mod statens sikkerhed, vil kunne indgå, om leverandøren har været involveret i aktiviteter i Danmark eller udlandet, der har medført en negativ påvirkning af statens sikkerhed. Har leverandøren udført sådanne aktiviteter i andre sammenhænge, vil det selvsagt tale for, at der er risiko for en gentagelse – og at den nye aftale dermed kan udgøre en trussel mod statens sikkerhed.

For så vidt angår undskyldelige fejl hos en leverandør, som har medført en negativ påvirkning af informationssikkerheden, vil dette normalt ikke medføre, at en aftale anses for at udgøre en trussel mod statens sikkerhed.

Teleindustrien henstiller til, at der undgås tvivl om, hvad der forstås ved hhv. "statens sikkerhed" og "national sikkerhed".

Som anført i bemærkningerne til lovforslagets § 2 anvendes udtrykket statens sikkerhed i forvejen i lov om sikkerhed i net og tjenester, og udtrykket skal forstås i overensstemmelse med det EU-retlige udtryk den nationale sikkerhed.

Teleindustrien anfører, at det er uklart, hvad der forstås ved "kontrol" og "betydelig indflydelse" i lovforslagets § 2, stk. 1, (§ 2, stk. 2, i det fremsatte lovforslag).

Som anført i bemærkningerne til lovforslagets § 2 vil aktører, der udøver kontrol over eller betydelig indflydelse på leverandøren, være aktører, der direkte eller indirekte er i besiddelse af eller har kontrol over ejerandele eller stemmerettigheder i en virksomhed, eller har tilsvarende kontrol ved andre midler, herunder langfristede lån, som giver betydelig indflydelse på ledelsesmæssige, finansielle eller udviklings- eller driftsmæssige forhold.

Teleindustrien anfører, at det ikke er klart for organisationen, hvilke lande Danmark har indgået sikkerhedsaftaler med, og som dermed i tilstrækkeligt omfang opfylder kriteriet i lovforslagets § 2, stk. 1, nr. 1, (§ 2, stk. 2, nr. 1, i det fremsatte lovforslag). Organisationen anfører videre, at det ikke synes nærmere defineret, hvad der forstås ved begrebet "tilsvarende sikkerhedssamarbejder". Tilsvarende anfører organisationen, at teleudbyderne ikke har indsigt i, hvilke lande det efter

lovgivningen er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage. Organisationen foreslår derfor, at Center for Cybersikkerhed forpligtes til løbende at udarbejde og offentliggøre en oversigt over lande og producenter, som potentielt udgør en trussel mod statens sikkerhed. Teleindustrien anfører desuden, at der fremgår af kriterierne i lovforslagets § 2, stk. 1, nr. 2 og 3, (§ 2, stk. 2, nr. 2 og 3, i det fremsatte lovforslag), at der udover lande, hvor leverandøren er hjemmehørende, også kan lægges vægt på lande, hvor produktionen eller driften varetages fra. Det er ifølge organisationen uklart, om teleudbyderne uden risiko vil kunne indgå aftaler med leverandører fra lande, som Danmark har en aftale om sikkerhedssamarbejde med, men som har henlagt hele eller dele af deres produktion til ikke-vestlige lande, som Danmark formentlig ikke har en sikkerhedsaftale med.

Dansk Energi anfører, at den udløsende faktor for nedlæggelse af forbud efter lovforslagets kapitel 2 vil være forhold vedrørende leverandøren og/eller underleverandører til leverandøren, men at det for Dansk Energi ikke fremstår klart, hvordan teleudbyderne fremover skal kunne identificere og udvælge leverandører, idet teleudbyderne ikke vil have viden om hvilke leverandører, som Center for Cybersikkerhed måtte anse for at udgøre en trussel mod statens sikkerhed.

Lovforslaget indebærer ikke, at der vil blive foretaget en vurdering af, om konkrete leverandører vil udgøre en trussel mod statens sikkerhed eller ej. Derimod vil der blive foretaget en vurdering af, om de enkelte leverandøraftaler samlet set vil udgøre en trussel mod statens sikkerhed. Der vil således ikke være tale om, at teleudbyderne udelukkes fra at anvende bestemte leverandører.

Spørgsmålet om, hvorvidt leverandøren m.v. er hjemmehørende i eller varetager produktionen eller driften fra et land, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med, eller om leverandøren m.v. er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter det pågældende lands lovgivning er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage, vil indgå i den samlede vurdering, men sammen med en række andre aspekter.

I forbindelse med den dialog, der er mellem teleudbyderen og Center for Cybersikkerhed forud for indgåelsen af leverandøraftaler vedrørende den kritiske teleinfrastruktur, vil Center for Cybersikkerhed nærmere kunne rådgive teleudbyderen om, hvorvidt der i forbindelse med den konkrete aftale er forhold, som gør, at centeret vurderer, at aftalen vil udgøre en trussel mod statens sikkerhed.

Teleindustrien har noteret sig, at det er en forudsætning for anvendelsen af lovforslagets § 3, at der ikke blot kan konstateres en trussel mod statens sikkerhed, som er tilfældet med forbud efter lovforslagets § 2, men at truslen skal være "væsentlig". Organisationen giver dog udtryk for den opfattelse, at der ikke er nogen kvalificering af væsentlighedsbegrebet i lovens bemærkninger.

Som anført i bemærkningerne til lovforslagets § 3 vil det, for at der foreligger en væsentlig trussel mod statens sikkerhed, være et krav, at truslen er mere konkretiseret end en trussel efter lovforslagets § 2.

Teleindustrien finder, at der bør tages særlige hensyn forud for anvendelse af forbud mod indgåelse af aftaler, der vedrører en forlængelse eller genforhandling af eksisterende aftaler. Organisationen finder således, at et sådant forbud mod f.eks. en aftale om support eller reservedele de facto kan medføre, at allerede leveret og lovligt udstyr bliver ubrugeligt. Organisationen opfordrer derfor til, at det direkte kommer til at fremgå af lovteksten, at forbud efter lovens § 2, for så vidt angår forlængelse eller genforhandling af eksisterende aftaler, og forbud efter § 3 ikke kan bringes i anvendelse, med mindre der er sket en konkret og væsentlig ændring af den sikkerhedsmæssige vurdering i forhold til den konkrete aftales parter og indhold, og før mindre indgribende foranstaltninger, som Center for Cybersikkerhed har taget i anvendelse, jf. lov om net- og informationssikkerhed, har vist sig utilstrækkelige.

Det følger udtrykkeligt af lovforslagets § 2, stk. 3, og § 3, stk. 4, at Center for Cybersikkerhed kun kan nedlægge forbud mod en aftale m.v., hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Som det fremgår af bemærkningerne til lovforslagets § 3 vil bestemmelsen først og fremmest finde anvendelse, hvis det ved den oprindelige aftaleindgåelse er blevet vurderet, at der ikke har været grundlag for at nedlægge forbud mod aftalen efter den foreslåede § 2, men der efterfølgende er sket en ændring, som gør, at der ville være blevet nedlagt forbud, hvis de ændrede forhold havde været en realitet ved aftaleindgåelsen. Disse forhold skal dog udgøre en væsentlig trussel mod statens sikkerhed.

Forsvarsministeriet finder ikke, at der ved forlængelse af aftaler, som er omfattet af lovforslagets § 2, er grundlag for at fastsætte en anden ordning end ved indgåelse af nye aftaler, idet de samme hensyn vil gøre sig gældende i de to situationer.

Institut for Menneskerettigheder anfører, at det efter instituttets opfattelse vil være problematisk, hvis en så indgribende foranstaltning som at nedlægge et forbud mod en teleudbyders aftaleindgåelse med en konkret leverandør alene baseres på medieomtale. I sager, som Center for Cybersikkerhed bliver gjort opmærksom på via medierne, må centeret efter Institut for Menneskerettigheders opfattelse i det mindste være forpligtet til at indgå i en dialog med den virksomhed, som kan risikere at blive mødt af et forbud, hvilket gælder så meget desto mere, når centeret har mulighed for at offentliggøre et forbud i ikke-anonymiseret form. Institut for Menneskerettigheder anbefaler, at Forsvarsministeriet i lovudkastets bemærkninger forudsætter, at Center for Cybersikkerhed ikke alene kan basere en afgørelse om at nedlægge et forbud på medieomtale.

En forudsætning om, at Center for Cybersikkerhed som udgangspunkt ikke alene kan basere en afgørelse om at nedlægge et forbud på medieomtale, fremgår allerede af bemærkningerne til lovforslagets § 2 om forbud mod indgåelse af aftaler. Her er det anført, at det vil påhvile Center for Cybersikkerhed at sikre, at sagen er tilstrækkeligt oplyst til, at der kan træffes afgørelse om et forbud, og det anføres videre, at et forbud dermed normalt ikke alene vil kunne baseres på f.eks. medieomtale.

CCCD giver udtryk for, at organisationen anser kriteriet i lovforslagets § 2, stk. 1, nr. 1, (§ 2, stk. 2, nr. 1, i det fremsatte lovforslag), for at udgøre diskrimination af virksomheder hjemmehørende i lande, som Danmark ikke har en forsvarsalliance med, eller som Danmark ikke har et sikkerhedsmæssigt samarbejde med. Huawei anfører ligeledes, at der efter virksomhedens mening med lovforslaget sker forskelsbehandling baseret på nationalitet. Huawei finder ikke, at der er et retligt grundlag for undtagelse fra de juridiske garantier for ikke-diskrimination i international ret.

Hovedformålet med lovforslaget er at skabe hjemmel til, at Center for Cybersikkerhed kan forbyde konkrete leverandøraftaler vedrørende den kritiske teleinfrastruktur, hvis aftalerne vurderes at udgøre en trussel mod statens sikkerhed. Vurderingen vil ske med udgangspunkt i objektive kriterier, og der er således ikke tale om, at lovforslaget er rettet mod bestemte leverandører eller bestemte lande.

CCCD og Huawei bemærker, at alle leverandører deler den samme globale forsyningskæde. De giver på den baggrund udtryk for, at et forbud mod en leverandør baseret på nationalitet derfor ikke vil forbedre sikkerheden, men alene hindre fri samhandel.

Forsvarsministeriet skal understrege, at der ikke med lovforslaget skabes hjemmel til at forbyde leverandører, men alene hjemmel til, at konkrete leverandøraftaler m.v. vil kunne forbydes efter en individuel vurdering.

4. Proportionalitet

Dansk Erhverv og IT-Branchen finder, at afgørelser om forbud kun bør kunne træffes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige.

DI bemærker, at det i bestemmelserne om proportionalitet kan være relevant at uddybe, hvilke konkrete foranstaltninger Center for Cybersikkerhed skal forsøge, inden der nedlægges et forbud efter kapitel 2. Desuden finder organisationen, at det bør overvejes, om leverandøren og teleudbyderen kan inddrages i processen, således at den mindst indgribende foranstaltning kan anvendes.

Huawei støtter det generelle princip i lovforslaget om, at et forbud alene kan anvendes, såfremt mindre indgribende foranstaltninger ikke effektivt kan afværge risikoen, og at de mindre indgribende foranstaltninger altid skal anvendes som den foretrukne løsning. Huawei anbefaler, at Forsvarsministeriet lader sig inspirere af definitionerne i NIS Tool Box vedrørende eksempler på mindre indgribende foranstaltninger.

Rådet for Digital Sikkerhed og Teleindustrien anfører, at indgrebsmuligheden kun bør anvendes helt undtagelsesvis og efter en nøje afvejning af truslen mod statens sikkerhed på den ene side og de operationelle sikkerhedsaspekter samt markedsmæssige konsekvenser på den anden side. Organisationerne finder, at afgørelser om forbud kun bør udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige. Organisationerne anfører endvidere, at det altid bør vurderes, om leverandørsikkerhed kan opnås på en mindre indgribende måde.

Kravet om proportionalitet fremgår udtrykkeligt af lovforslagets § 2, stk. 3, og § 3, stk. 4. Det følger af disse bestemmelser, at Center for Cybersikkerhed kun kan nedlægge forbud mod bl.a. indgåelse og opretholdelse af aftaler, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

Indholdet af bestemmelserne er uddybet i bemærkningerne, hvoraf det fremgår, at Center for Cybersikkerhed forud for nedlæggelse af et forbud skal have søgt at opnå det ønskede resultat gennem mindre indgribende midler. Det vil således være en forudsætning, at centeret har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen eller de

sikkerhedsmæssige ændringer af kritiske komponenter, systemer m.v., som vil være nødvendige for, at der ikke længere vurderes at være en trussel mod statens sikkerhed. Center for Cybersikkerhed vil også skulle have vurderet de relevante muligheder i lov om sikkerhed i net og tjenester, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

Gennem det rådgivnings- og dialogforløb, der således forudsættes at være mellem teleudbyderne og Center for Cybersikkerhed, vil teleudbyderne løbende have mulighed for at fremføre deres synspunkter over for centeret. Teleudbyderne vil i den forbindelse også have mulighed for at byde ind med forslag til konkrete mitigerende sikkerhedsforanstaltninger med inspiration fra f.eks. internationale standarder eller EU's 5G Toolbox.

5. Erstatning i forbindelse med afgørelser om forbud

Dansk Energi er af den opfattelse, at forbud, der retter sig mod netkomponenter, systemer og værktøjer, som er indkøbt og taget i brug før den 7. december 2020, og som Center for Cybersikkerhed ikke tidligere har vurderet skulle udgøre en trussel mod statens sikkerhed, bør anses for ekspropriative indgreb, og derfor bør udløse fuldstændig erstatning. Organisationen foreslår derfor, at det præciseres i lovforslaget, at indgreb, der retter sig mod anvendelsen af netkomponenter, systemer og værktøjer, som er leveret eller taget i anvendelse inden den 7. december 2020, udgør ekspropriative indgreb, således at teleudbydernes usikkerhed, for så vidt angår både direkte og indirekte omkostningsdækning, fjernes. Alternativt ønsker organisationen, at der indføres en kompensationsordning, som sikrer teleudbyderne dækning for de tab, som et indgreb medfører.

Dansk Erhverv og IT-Branchen anfører, at teleudbyderne bør have ret til fuld erstatning ved afgørelser om forbud, der får betydning for anvendelsen af lovligt leveret udstyr, uanset om afgørelsen kan anses for at udgøre ekspropriation. Ligeledes anfører DI, at afgørelser efter lovforslagets kapitel 2 kan lede til omfattende tab for udbyderne, og at lovforslaget derfor bør suppleres med en ordning, hvorefter der skal ydes fuld erstatning efter de almindelige regler om erstatning, også for afgørelser, der ikke har karakter af ekspropriation.

Huawei anfører, at det er uklart, i hvilket omfang kravene til ekspropriation kan være opfyldte, hvis Center for Cybersikkerhed udsteder et forbud, der påvirker brugen af lovligt udstyr. Det bør efter Huaweis opfattelse fastlægges, at en part i en sådan situation som minimum kan forvente kompensation, ikke bare for installationsomkostninger, men også for den service og support, der ville være leveret i produk-

tets levetid, og ikke kun frem til det tidspunkt, som forbuddet specifikt omfatter. Derudover anbefaler Huawei, at det fremgår, at et forbud mod at deltage i udbudsprocesser (eller politisk eller administrativ indblanding heri) udgør ekspropriation og et tab, der fuldt ud vil blive kompenseret.

Rådet for Digital Sikkerhed og Teleindustrien giver udtryk for, at leverandørerne skal have ret til fuld erstatning ved forbud, der får betydning for anvendelse af lovligt leveret udstyr, uanset om det kan anses for at udgøre ekspropriation.

Teleindustrien anfører endvidere, at det ved en nærmere gennemgang af lovbemærkningerne er uklart for organisationen, hvornår der er tale om ekspropriation, og hvordan grundlovens begreb "fuldstændig erstatning" skal forstås i forbindelse med ekspropriation efter lovforslaget. Teleindustrien bemærker endvidere, at lovforslaget, så vidt det ses, ikke tager stilling til, at krav efter lovforslaget kan medføre betydelige direkte og indirekte negative økonomiske følgevirkninger i form af øgede udgifter til nyanskaffelser, forringede netværksoplevelser for kunderne og med evt. tabte markedsandele til følge m.m. Teleindustrien giver udtryk for den opfattelse, at et forbud mod direkte eller indirekte anvendelse af allerede leveret og lovligt udstyr vil udgøre et ekspropriativt indgreb. Teleindustrien henstiller derfor til, at det eksplicit præciseres i lovbemærkningerne, at et forbud mod allerede indgåede aftaler, herunder forbud der direkte eller indirekte får betydning for anvendelse af lovligt leveret udstyr, vil give udbyderen ret til fuld erstatning. Det gælder særligt aftaler, der er indgået før 7. december 2020.

Det følger af grundlovens § 73, stk. 1, at ejendomsretten er ukrænkelig, og at ingen kan tilpligtes at afstå sin ejendom, uden hvor almenvellet kræver det. Det kan kun ske ifølge lov og mod fuldstændig erstatning.

Lovforslaget fastsætter – i overensstemmelse med grundlovens § 73 – en ordning, hvorefter afgørelser om forbud mod en aftale m.v., der udgør ekspropriation, vil skulle ske mod fuldstændig erstatning.

Det er forventningen, at der sjældent vil være behov for at træffe afgørelser om forbud mod aftaler m.v. efter lovens kapitel 2. Men i de tilfælde, hvor Center for Cybersikkerhed vurderer, at der er behov for at nedlægge et forbud, vil centeret skulle foretage en vurdering af, om forbuddet vurderes at udgøre ekspropriation (og dermed skal ske mod fuld erstatning). Vurderingen vil skulle foretages på baggrund af en vurdering af indgrebets beskaffenhed, herunder indgrebets formål, i hvilken grad indgrebet er generelt eller konkret, indgrebets intensitet

samt indgrebets begrundelse (causa). Ved vurderingen af, om et forbud udgør ekspropriation, vil det indgå, om forbuddet vedrører indgåelse af en ny aftale eller forbud mod anvendelse af allerede leveret udstyr.

I det omfang en afgørelse om forbud måtte blive gennemført ved ekspropriation, vil der være adgang til domstolsprøvelse efter de særlige regler herom i grundlovens § 73, stk. 3.

Lovforslaget vil i øvrige situationer have karakter af erstatningsfri regulering.

Det er Forsvarsministeriets opfattelse, at der ikke er grundlag for at indføre yderligere kompensationsordninger i forbindelse med den foreslåede ordning. Det skal også ses i lyset af, at det i vidt omfang er en fælles interesse for myndigheder og teleudbydere at sikre, at der ikke indgås eller opretholdes aftaler, der kan udgøre en trussel mod statens sikkerhed, således at Danmark også fremadrettet vil råde over en robust og sikker teleinfrastruktur.

Det skal for god ordens skyld bemærkes, at de almindelige erstatningsretlige regler på sædvanlig vis vil finde anvendelse, hvis Center for Cybersikkerhed handler ansvarspådragende i forbindelse med behandlingen af sager i medfør af lovforslaget.

6. Forholdet til offentlighedsloven og forvaltningsloven

Dansk Energi giver udtryk for, at idet der er tale om ganske vidtgående indgreb efter lovforslagets §§ 2 og 3, findes det væsentligt for retssikkerheden, at det gældende princip i lov om Center for Cybersikkerhed, hvorefter centeret i videst muligt omfang forudsættes at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, fortsat bør gælde. Endvidere anfører organisationen, at Forsvarsministeriet som minimum i højere grad bør kvalificere og underbygge behovet for helt at fjerne muligheden for at efterleve principperne i offentlighedsloven og forvaltningsloven, når centeret skal træffe afgørelser.

Dansk Erhverv og IT-Branchen bemærker, at teleudbyderne skal sikres mulighed for partshøring og begrundelse i forbindelse med afgørelser efter lovforslaget.

DI finder, at det er vigtigt, at der findes en balance mellem at sikre klassificeret viden samtidig med, at sagen oplyses grundigt. DI anfører, at det bør overvejes, om der kan indføres metoder til at høre leverandøren og øvrige relevante parter på en måde, så de får mulighed for at foretage relevante ændringer og imødegå den kritik, der måtte være

bevæggrund for et forbud. Konkret foreslår DI eksempelvis at udvide partsbegrebet eller præcisere, hvad der forstås ved relevante parter i disse afgørelser.

Huawei anbefaler, at beslutningsprocessen skal understøttes af grundlæggende principper om god offentlig forvaltning, såsom partshøring, for bedst muligt at oplyse sagen og identificere potentielle mindre indgribende foranstaltninger og sikre korrekte afgørelser, krav om altid – i videst muligt omfang, af hensyn til statens sikkerhed – at oplyse om de elementer og det faktum, som afgørelsen er baseret på, samt at efterleve princippet om aktindsigt, herunder især i forhold til princippet om egenacces.

Rådet for Digital Sikkerhed ønsker, at der skal være retssikkerhedsmæssige garantier for leverandørerne, herunder mulighed for partshøring og begrundelse for afgørelserne.

Institut for Menneskerettigheder anfører, at forslagets undtagelse fra offentlighedsloven og forvaltningslovens kapitel 4-6 kan medføre en risiko for, at oplysninger, som en part kunne blive gjort bekendt med uden at kompromittere hensynet til statens sikkerhed, ikke vil komme til partens kendskab, fordi centeret undlader at foretage en nærmere vurdering heraf. Endvidere anser instituttet det for uklart, hvorvidt og i så fald hvilke oplysninger centeret forventer at gøre en part bekendt med, hvilket både gælder forinden der træffes en afgørelse om forbud m.v. og selve begrundelsen for en afgørelse. Instituttet bemærker, at det særligt vil være problematisk i en sag, hvor der ikke forinden har været dialog mellem virksomheden og Center for Cybersikkerhed, og hvor parten således ikke nødvendigvis er bekendt med grundlaget for afgørelsen om forbud. Her kan virksomheden være henvist til at anlægge en sag ved domstolene for at blive bekendt med de dele af begrundelsen, som indgår i sagens åbne del. Instituttet anbefaler, at der i bemærkningerne til lovforslaget tilføjes en forudsætning om, at centeret så vidt muligt overholder principperne i offentlighedsloven og forvaltningslovens kapitel 4-6.

Teleindustrien giver udtryk for, at organisationen finder det stærkt kritisabelt, at teleudbyderne afskæres fra helt grundlæggende retssikkerhedsgarantier. Teleindustrien anfører, at man har forståelse for, at der kan være oplysninger, der af hensyn til nationale eller internationale sikkerhedsinteresser ikke kan videregives til parten, men det begrunder dog efter organisationens opfattelse ikke, at partshøring og begrundelse for afgørelsen helt undtages. Teleindustrien henviser til Erhvervsministeriets udkast til lovforslag om investeringsscreening, herunder at danske teleudbydere opnår en ringere retsbeskyttelse end udenlandske parter, der ønsker at investere i et selskab, der råder over

kritisk infrastruktur. Endeligt anfører Teleindustrien, at for at Center for Cybersikkerhed kan foretage vurderingen af mindre indgribende foranstaltninger, er det nødvendigt, at centeret er forpligtet til at partshøre teleudbyderen, da centeret sjældent vil have tilstrækkeligt viden om teleudbyderens infrastruktur og sikkerhedssystemer til at foretage en tilstrækkelig afdækning af de faktiske forhold og dermed undersøge alternative forholdsregler. Teleindustrien henstiller til, at lovforslagets § 5 udgår og erstattes med tilsvarende regler, som fremgår af § 38 i udkastet til investeringsscreeningslov.

I de tilfælde, hvor Center for Cybersikkerhed træffer afgørelse om et forbud, vil der forud for, at afgørelsen træffes, typisk gennem længere tid have været et forløb, hvor teleudbyderen og centeret har været i dialog.

Lovforslaget bygger således ovenpå de gældende regler i lov om sikkerhed i net og tjenester, hvor Center for Cybersikkerhed underrettes forud for, at en teleudbyder indleder forhandlinger med en leverandør. Dermed får centeret mulighed for at rådgive og vejlede. Desuden ligger det i proportionalitetsafvejningen, jf. afsnit 4 ovenfor, at det er en forudsætning, at centeret først har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen eller de sikkerhedsmæssige ændringer af kritiske komponenter, systemer m.v., som vil være nødvendige for, at der ikke længere vurderes at være en trussel mod statens sikkerhed.

Gennem det rådgivnings- og dialogforløb, der således forudsættes at være mellem teleudbyderne og Center for Cybersikkerhed, vil teleudbyderne løbende have haft mulighed for at fremføre deres synspunkter over for centeret. Centeret vil således gennem rådgivnings- og dialogforløbet sikre, at sagen er tilstrækkeligt oplyst ved bl.a. at få viden om teleudbydernes virksomhed, herunder muligheden for at træffe mindre indgribende sikkerhedsforanstaltninger.

Det forudsættes imidlertid også, at Center for Cybersikkerhed i forbindelse med afgørelser om forbud i størst muligt omfang gennemfører egentlige partshøringer samt begrunder afgørelsen, så længe det ikke kompromitterer hensynene bag lovforslaget. Forsvarsministeriet vil justere bemærkningerne til lovforslaget, således at dette udtrykkeligt fremgår.

7. Afgørelseskompetence

Dansk Erhverv og IT-Branchen samt Rådet for Digital Sikkerhed anbefaler, at afgørelseskompetencen tillægges Forsvarsministeriet, og at afgørelsen træffes efter indstilling fra Center for Cybersikkerhed og efter høring af andre relevante myndigheder.

Teleindustrien giver udtryk for, at det er organisationens principielle synspunkt, at Center for Cybersikkerheds opgaver på dette område, som tilfældet er i hovedparten af de øvrige EU-lande, bør flyttes til den civile del af forvaltningen. Teleindustrien bemærker dog også, at en sådan ressortændring næppe er mulig inden for den tidsramme, der er sat for det fremlagte lovudkast. Teleindustrien ønsker, at en beslutning om forbud forberedes grundigt og træffes på højeste niveau i ministeriet. Organisationen giver udtryk for, at siden opsplitningen af den tidligere IT- og Telestyrelse er kompetencer og viden om telebranchen i dag spredt på en række myndigheder. Organisationen bemærker, at Energistyrelsen, Erhvervsstyrelsen og Konkurrence- og Forbrugerstyrelsen alle har indgående kendskab til tekniske og markedsmæssige forhold på teleområdet og bør derfor høres, inden der træffes afgørelse. Teleindustrien opfordrer derfor til, at en afgørelse om forbud træffes af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og efter høring af andre relevante ministerier og myndigheder.

Lovforslaget indebærer bl.a., at Center for Cybersikkerhed kan træffe afgørelser om forbud mod aftaler, der vurderes at udgøre en trussel mod statens sikkerhed. Det vurderes naturligt, at afgørelseskompetencen placeres hos Center for Cybersikkerhed, som er myndighed for informationssikkerhed og beredskab på teleområdet. Afgørelserne forudsætter således den særlige faglige viden om henholdsvis sikkerhedsmæssige og teletekniske forhold, som Center for Cybersikkerhed besidder. Derudover har centeret gennem de forudgående rådgivnings- og dialogforløb med teleudbyderne fået den nødvendige viden om bl.a. teleudbydernes forhold, der vil gøre det muligt at træffe den mindst indgribende afgørelse samt afveje hensynet til statens sikkerhed overfor hensynet til teleudbyderens forhold.

Det er væsentligt at understrege, at indgrebsmuligheden alene vil blive anvendt i de forventeligt ganske få tilfælde, hvor en aftale vurderes at udgøre en trussel mod statens sikkerhed, og hvor der ikke er andre og mindre indgribende muligheder for at imødegå truslen.

Center for Cybersikkerhed vil som led i den almindelige sagsoplysning inddrage fagmyndigheder, såsom Erhvervsstyrelsen og Energistyrelsen, i relevant omfang. Dette vil blive præciseret i bemærkningerne til lovforslaget.

8. Administrativ rekurs og tilsyn med Center for Cybersikkerhed

Dansk Erhverv og IT-Branchen ønsker, at der skal indføres regler om effektiv prøvelse af afgørelser og om tilsyn med Center for Cybersikkerhed.

DI anfører, at afskæring af klageadgangen udgør et problem for markedet, idet en domstolsbehandling, der er alternativet, vil være for langsommelig, når en teleudbyder står midt i en konkret forhandling vedrørende kritisk teleinfrastruktur. Det vil betyde, at teleudbyderen således typisk vil være nødsaget til at vælge en anden leverandør. Desuden anfører DI, at de ikke finder argumentet om, at Center for Cybersikkerhed besidder et særligt fagligt indblik i henholdsvis efterretningsmæssige og teletekniske forhold, for overbevisende i forhold til at afskære klageadgangen. DI foreslår konkret, at Forsvarsministeriet kan beskikke særlige eksperter eller nedsætte et egentligt nævn.

Huawei finder, at de væsentligt indgribende konsekvenser, som en afgørelse truffet af Center for Cybersikkerhed i henhold til §§ 2 og 3 vil have, kræver mulighed for en fremskyndet prøvelse, som en civil retssag under de sædvanlige domstole ikke kan erstatte. Det bør efter Huaweis opfattelse være en hurtig prøvelse i et separat, uafhængigt klagenævn, enten et nyoprettet nævn eller eventuelt det nuværende tilsyn med efterretningstjenesterne (TET).

Rådet for Digital Sikkerhed ønsker, at der skal være mulighed for, at leverandører kan klage over afgørelser, og rådet anfører, at klageretten ikke bør kunne tilsidesættes politisk. Rådet finder desuden, at der bør indføres regler om tilsyn med Center for Cybersikkerhed.

Teleindustrien anbefaler, at der indsættes en bestemmelse i loven, der giver Tilsynet med Efterretningstjenesterne hjemmel til at føre et effektivt tilsyn med Center for Cybersikkerheds forvaltning af såvel lov om leverandørsikkerhed og lov om net- og informationssikkerhed.

Lovforslaget indebærer, at den administrative rekurs afskæres i relation til de afgørelser, som Center for Cybersikkerhed træffer om bl.a. forbud mod indgåelse og opretholdelse af aftaler, der vurderes at være en trussel mod statens sikkerhed.

Afskæringen af rekurs skal ses i lyset af, at afgørelserne forudsætter et særligt fagligt indblik i efterretningsmæssige og teletekniske forhold. Som det altovervejende udgangspunkt ville Forsvarsministeriet ikke ved prøvelse af en afgørelse som led i administrativ rekurs have den fornødne tekniske viden til at kunne efterprøve centerets faglige skøn.

Forsvarsministeriet vil imidlertid som led i det almindelige over-/underordnelsesforhold fortsat føre tilsyn med Center for Cybersikkerhed, herunder med centerets varetagelse af opgaven som myndighed for informationssikkerhed og beredskab på teleområdet.

Derudover er Center for Cybersikkerheds behandling af personoplysninger under løbende kontrol af Tilsynet med Efterretningstjenesterne, der hvert år udgiver en redegørelse om det tilsyn, der udøves med Center for Cybersikkerhed. Dette tilsyn vil ligeledes omfatte centerets behandling af personoplysninger i forbindelse med sager omfattet af lovforslaget.

Det har desuden været overvejet, om der var grundlag for at nedsætte et særligt sagkyndigt klagenævn. Det forventes imidlertid, at afgørelser om forbud mod indgåelse eller opretholdelse af bestemte aftaler kun vil blive truffet i ganske få tilfælde, hvor en aftale vurderes at udgøre en trussel mod statens sikkerhed, og hvor der ikke er andre og mindre indgribende muligheder for at imødegå truslen. Det vurderes på den baggrund, at antallet af klagesager ikke meningsfuldt vil kunne retfærdiggøre, at der anvende store ressourcer på at nedsætte og drive et særligt klagenævn, som typisk vil bestå af et antal dommere og sagkyndige personer. Der lægges i den forbindelse også vægt på, at afgørelserne under alle omstændigheder vil kunne indbringes for domstolene.

9. Domstolsprøvelse

Dansk Energi bemærker, at der i lovforslaget gøres ganske meget ud af at sikre virksomheders retssikkerhedsgarantier ved den efterfølgende mulighed for domstolsprøvelse af den afgørelse Center for Cybersikkerhed træffer i medfør af §§ 2 og 3.

DI finder, at lovforslagets bestemmelser om det, som organisationen betegner som en indskrænket domstolsproces, gør det svært for en leverandør at kunne imødegå den kritik, der måtte være, idet leverandøren i processen ikke kan få at vide, hvilken kritik der måtte eksistere, og at et egentligt forsvar og relevante modforanstaltninger derfor bliver svækket i praksis. DI giver udtryk for forståelse for, at man ikke ønsker at dele klassificeret viden, og organisationen foreslår derfor, at lovforslaget udbygges med en metode til at dele så meget, man kan, af det klassificerede materiale.

Huawei giver udtryk for, at virksomheden er imod enhver begrænsning af retten til at vælge sin egen advokat. Hvis lovforslagets ordning alligevel fastholdes, mener Huawei, at der bør være klarhed omkring, hvordan man kan sikre, at den særligt beskikkede advokat ikke har nogen interessekonflikt, og at advokaten besidder en kombination af tilstrækkelig proceserfaring og domæneviden. Huawei bemærker, at netværkssikkerhedsregulering og teleregulering er et meget specialiseret område, som kun et meget begrænset antal advokater i Danmark beskæftiger sig med, hvilket der bør tages højde for.

Retspolitisk Forening bemærker, at der i lovforslagets afsnit 6 opereres med det, som foreningen betegner som en helt speciel form for hemmelig retspleje, som er kendt fra et par andre sagsområder. Foreningen giver udtryk for, at der herved sker endnu en fravigelse fra det fundamentale princip om offentlighed i retsplejen og om retfærdig rettergang, herunder kontradiktion og lige muligheder for parterne (equality in arms), og foreningen finder, at der ved hver nye og yderligere fravigelse sker endnu en markant svækkelse af retsstaten. Foreningen anfører, at de finder det paradoksalt, at lovforslagets åbenlyse overordnede mål er at beskytte netop denne selvsamme demokratiske retsstat mod angreb.

Rådet for Digital Sikkerhed finder, at der bør indføres regler om effektiv prøvelse af afgørelser.

Teleindustrien mener, at lovudkastet skal tilrettes, således at der gives teleudbyderen mulighed for fuld partsrepræsentation ved egen advokat, idet organisationen anfører, at med den foreslåede § 9 afskæres udbyderne fra en sådan adgang. Det forhold, at udbyderne ikke selv må lade sig repræsentere, men skal anvende en særlig udpeget sikkerhedsadvokat, der ikke må dele fortroligt materiale med udbyderen, vil efter Teleindustriens mening gøre det nærmest umuligt for udbyderne at bidrage til sagens oplysning. Teleindustrien mener, at det er afgørende, at udbyderens advokat i det mindste har fuld indsigt i grundlaget for afgørelsen, og at sagen kan drøftes med udbyderen – også når advokaten har fået indsigt i fortroligt materiale. Organisationen mener derfor, at det kun bør være indholdet af de fortrolige oplysninger om statens sikkerhed, der ikke må drøftes med udbyderen. I det omfang, udbyderen har sikkerhedsgodkendt personale, bør det efter organisationens mening desuden være muligt at drøfte sådanne oplysninger med udbyderen.

Center for Cybersikkerheds afgørelser efter lovforslagets kapitel 2 og 3 vil ofte være baseret på fortroligt materiale, herunder højt klassificerede oplysninger, der, hvis de bliver offentligt tilgængelige, vil kunne skade Danmarks sikkerhed.

Forsvarsministeriet har derfor overvejet, hvordan teleudbyderens og leverandørens ret til domstolsprøvelse kan forenes med de særlige sikkerhedsmæssige fortrolighedshensyn. Forsvarsministeriet finder, at disse hensyn kan varetages ved, at der med inspiration fra udlændingeretten etableres særlige procedureregler, hvorefter domstolsprøvelsen opdeles i en åben og en lukket del.

Der vil under sagens lukkede del kunne ske fremlæggelse af fortroligt materiale, som af sikkerhedsmæssige grunde ikke kan videregives til parterne i sagen. Til varetagelse af partens interesser under den lukkede del af sagen vil der kunne beskikkes en særlig advokat, som på partens vegne får kendskab til og kan udtale sig om det fortrolige materiale, der fremlægges for retten. Den særlige advokat vil kunne udøve partsbeføjelser under den lukkede del af sagen, dog således at den særlige advokat ikke må drøfte sagen med parten og partens advokat. Parten vil derimod godt kunne instruere den særlige advokat, således at den særlige advokat kan varetage partens interesser i den lukkede del af retssagen.

Den særlige advokat, der udøver partsbeføjelser på vegne af parten med hensyn til de fortrolige oplysninger, beskikkes af retten på baggrund af en liste over advokater, som Justitsministeriet har antaget. Ordningen forudsætter, at retten i almindelighed beskikker den advokat, der »står for tur«. Retten kan dog beskikke en anden advokat, hvis parten har begrundede indsigelser mod beskikkelsen af den pågældende, eksempelvis hvis den beskikkede advokat er inhabil i sagen.

De nærmere regler vedrørende de pågældende advokater, herunder regler for antagelse og sikkerhedsgodkendelse af de særlige advokater, vil af justitsministeren blive fastsat i en bekendtgørelse efter den foreslåede § 12, 2. pkt. I forbindelse med udstedelsen af de nærmere regler vil der blive set på, hvorledes det sikres, at de antagne advokater har de fornødne forudsætninger, herunder den tilstrækkelige erhvervsretlige erfaring, til at varetage opgaven. Det forventes desuden, at Justitsministeriets antagelse af de særlige advokater, som det er tilfælde for antagelse af særlige advokater efter udlændingeloven, vil ske efter inddragelse af både Østre Landsret, Københavns Byret og Advokatrådet.

Huawei anfører, at principperne for offentlig og åben retspleje, baseret på parts- og kontradiktionsprincippet og behørig sagsoplysning, retten til at vælge din egen advokat og i øvrigt generelle principper for retfærdig rettergang, er forfatningsmæssigt funderet og internationalt anerkendt som grundlæggende menneskerettigheder, og at det efter Huaweis opfattelse ikke er noget, der kan afskæres med henvisning til statens sikkerhed.

Forsvarsministeriet finder ikke, at lovforslagets ordning vedrørende domstolsprøvelse rejser spørgsmål i forhold til Den Europæiske Menneskerettighedskonvention. For en nærmere redegørelse heraf henvises til lovforslagets afsnit 4.1 om forholdet til Den Europæiske Menneskerettighedskonvention.

Teleindustrien giver udtryk for, at hvis der er oplysninger, der har ligget til grund for Center for Cybersikkerheds oprindelige afgørelse, og en dommer mener, at der er oplysninger, som udbyderen bør se, vil det være helt urimeligt, at forsvarsministeren kan beslutte, at oplysningerne ikke længere skal indgå i sagen. Hvis denne mulighed opretholdes i lovforslaget, bør konsekvensen efter Teleindustriens opfattelse være, at oplysningerne ikke kan indgå i prøvelsen, og dermed ikke vil kunne tillægges vægt ved domstolens vurdering af, om forbuddet er lovligt.

Det følger af den foreslåede § 9, stk. 2-4, at retten af egen drift eller efter begæring fra den særlige advokat ved en kendelse kan bestemme, at fortrolige oplysninger, der er indgået i vurderingen i afgørelser omfattet af kapitel 2 og 3, videregives til parten og dennes advokat, hvis sikkerhedsmæssige forhold ikke kan begrunde, at oplysningerne ikke videregives. Hvis retten har truffet afgørelse om, at fortrolige oplysninger videregives til parten og dennes advokat, skal forsvarsministeren eller den, ministeren bemyndiger hertil, have mulighed for at bestemme, at de pågældende oplysninger ikke indgår i sagen for retten.

En sådan beslutning vil have som konsekvens, at retten ikke kan lægge vægt på oplysningerne, og den dommer, som har deltaget i afgørelsen om, at de pågældende oplysninger videregives til parten og dennes advokat, vil ikke længere kunne deltage som dommer i sagen. Dermed sikres det, at retten ikke har kendskab til de pågældende oplysninger under bedømmelsen af sagen, og oplysningerne vil således ikke indgå i prøvelsen af sagen.

Huawei finder, at en prøvelse af Center for Cybersikkerheds afgørelser bør indebære opsættende virkning. Virksomheden finder, at den opsættende virkning bør forlænges i tilfælde af, at sagen efterfølgende anlægges som en retssag i henhold til lovforslagets § 7. Huawei anfører dog, at det kunne overvejes, om visse trusler kunne være af en sådan alvorlig karakter og indebære en så overhængende risiko for fare, at den opsættende virkning skal begrænses eller helt kunne fraviges. I så fald bør der efter Huaweis opfattelse være tale om fastsatte processer og kontroller, og Huawei henviser til tilgangen i Tyskland.

Teleindustrien mener, at en indbringelse af en forbudsafgørelse for domstolene automatisk bør få opsættende virkning. Organisationen anfører, at en domstolsprøvelse uden opsættende virkning kan have den konsekvens, at teleoperatøren, uanset udfaldet af retssagen, vil være nødt til enten at slukke for eller nedtage og udskifte den del af netværket, som er omfattet af tvisten. Organisationen anfører endvidere, at dette kan medføre uoprettelig skade for den udbyder, det går ud

over, men også for konkurrencen på markedet, hvilket vil være direkte til skade for slutbrugerne. Organisationen anfører desuden, at sådanne skadegørende virkninger af en ulovlig afgørelse ikke fuldt ud vil kunne kompenseres ved, at der ydes en økonomisk erstatning til den pågældende udbyder.

Forsvarsministeriet finder, at en retsstilling, hvorefter indbringelse af Center for Cybersikkerheds afgørelser for retten som altovervejende hovedregel får opsættende virkning, vil have uacceptable konsekvenser. Forbud vil kun blive nedlagt, hvis en aftale m.v. vurderes at udgøre en trussel mod statens sikkerhed. Opsættende virkning vil således indebære, at en leverandøraftale vil skulle fortsætte, uanset at aftalen f.eks. vurderes at indebære, at en fremmed magt vil få mulighed for at udøve sabotage eller spionage, der er rettet mod den kritiske teleinfrastruktur.

Forsvarsministeriet finder således ikke grundlag for at fravige den almindelige ordning, som kommer til udtryk i grundlovens § 63, stk. 1, 2. pkt., hvorefter der ikke pr. automatik tillægges opsættende virkning ved indbringelse af sager vedrørende forvaltningsretlige afgørelser, men hvor domstolene konkret vil kunne beslutte at tillægge indbringelsen af sagen opsættende virkning. Dermed vil domstolene konkret kunne afveje hensynet til statens sikkerhed overfor eksempelvis økonomiske hensyn.

10. Offentliggørelse af afgørelser m.v.

Huawei anbefaler, at der ikke sker offentliggørelse af afgørelser, der er påklaget. Virksomheden anfører endvidere, at når afgørelser er endelige, bør der forud for offentliggørelse foretages en proportionel afvejning af, om afgørelsen bør være anonym. Endvidere anfører Huawei, at endelige afgørelser alene bør offentliggøres i ikke-anonymiseret form, når parten har haft fuld adgang til den dokumentation, som afgørelsen er baseret på.

Teleindustrien giver udtryk for, at henset til, at kriterierne for, hvornår loven kan finde anvendelse, efter Teleindustriens opfattelse er uklare og uigennemskuelige, er det helt urimeligt, at Center for Cybersikkerhed kan anvende offentliggørelse af en afgørelse som pression. Dette gælder efter Teleindustriens opfattelse særligt i tilfælde, hvor centeret har meddelt forbud i medfør af lovforslagets § 3. Teleindustrien opfordrer på den baggrund til, at lovforslagets § 14 udgår.

Institut for Menneskerettigheder anfører, at det efter instituttets opfattelse må forventes, at en teleudbyder ikke ønsker offentlighed omkring forbud eller retssager, der vedrører teleudbyderens manglende hensyn-

tagen til statens sikkerhed, med de mulige negative konsekvenser det kan have over for navnlig selskabets kunder. Instituttet finder, at det i det lys er problematisk, at Center for Cybersikkerhed kan offentliggøre forbud i ikke-anonymiseret form, uden at centeret forinden har kontaktet den pågældende virksomhed, idet problemet kan skyldes omstændigheder hos en underleverandør eller fremmede stater, som virksomheden ikke behøver at være bevidst om.

Derudover anfører Institut for Menneskerettigheder, at det er principielt problematisk, at det er op til centeret at vurdere, om retssager vedrørende ekspropriation skal offentliggøres, idet det kan risikere at afholde en virksomhed fra at anlægge et sådant søgsmål, hvis det kan have negative konsekvenser for virksomhedens omdømme. Hensynet til at få teleudbyderne til at overholde reglerne og til at give kunderne kendskab hertil og hensynet til statens sikkerhed gør sig, efter instituttets opfattelse, ikke gældende, når der er tale om retssager om prøvelse af spørgsmål vedrørende ekspropriation, idet denne vurdering først foretages, når det er fastlagt, om et forbud m.v. kan nedlægges. Instituttet anbefaler, at det af hensyn til forudsigeligheden for de berørte virksomheder beskrives nærmere i lovforslagets bemærkninger, hvornår centeret kan forventes at ville henholdsvis ikke ville benytte muligheden for at offentliggøre i ikke-anonymiseret form.

Lovforslagets § 14 giver Center for Cybersikkerhed mulighed for at offentliggøre afgørelser m.v.

Centeret vil forventeligt kun i ganske få tilfælde træffe afgørelse om forbud, idet sikkerhedsmæssige aspekter først og fremmest forudsættes håndteret gennem dialog med og rådgivning af teleudbyderne. At centeret træffer afgørelse om forbud vil således først blive en realitet i de situationer, hvor telebyderen ikke har ønsket at følge eller ikke har opsøgt rådgivning fra Center for Cybersikkerhed om de tilpasninger af aftalen eller de sikkerhedsmæssige ændringer af kritiske komponenter, systemer m.v., som vil være nødvendige for, at der ikke længere vurderes at være en trussel mod statens sikkerhed.

Offentliggørelsesordningen har til formål at give teleudbyderne øget incitament til at overholde reglerne i lovens kapitel 2, ligesom bestemmelsen giver telekunder og offentligheden i øvrigt mulighed for at få kendskab til, hvorvidt en teleudbyder f.eks. har indgået eller opretholder en aftale, der vurderes at udgøre en trussel mod statens sikkerhed. Særligt for så vidt angår afgørelser efter lovforslagets § 3 bemærkes, at det vurderes vigtigt, at telekunder kan gøres bekendt med, om en teleudbyder aktuelt anvender kritiske netkomponenter, systemer og værktøjer, hvis anvendelse vurderes at udgøre en væsentlig trussel mod statens sikkerhed.

Offentliggørelsesordningen vurderes at udgøre et effektivt redskab, der kan medvirke til at sikre et højt sikkerhedsniveau i den kritiske teleinfrastruktur.

Det forudsættes imidlertid, at offentliggørelse kun sker, hvis det er i offentlighedens interesse. Forud for offentliggørelse forudsættes Center for Cybersikkerhed at foretage en afvejning af offentlighedens interesser over for en eventuel skadevirkning for den pågældende teleudbyders virksomhed. Forsvarsministeriet vil præcisere dette i lovforslagets bemærkninger. Det bemærkes desuden, at det er anført i bemærkningerne til bestemmelsen, at offentliggørelse ikke må indeholde oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el.lign., for så vidt det er af væsentlig økonomisk betydning for den teleudbyder, som oplysningerne angår.

Der lægges også op til, at afgørelser om ekspropriation skal kunne offentliggøres, idet det vil give mulighed for at præsentere et samlet og nuanceret billede af indgrebet for offentligheden. Det bemærkes, at der naturligvis heller ikke i den forbindelse vil ske offentliggørelse af følsomme oplysninger om drifts- eller forretningsforhold, jf. ovenfor.

Derudover bemærkes det, at lovforslagets § 14, stk. 2, vil indebære, at forsvarsministeren kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse. Bemærkningerne til bestemmelsen nævner specifikt, at der vil kunne fastsættes regler om forudgående høring eller orientering af en udbyder i forbindelse med centerets overvejelser om offentliggørelse.

11. Virkning

Teleindustrien anfører, at en udfasning og udskiftning af allerede leveret infrastruktur forudsætter, at der først igangsættes analyse af behov, herefter en udbudsfase og kontraktindgåelse og dernæst en implementering af den nye leverandørs udstyr samt udfasning af tidligere leverandører. En sådan proces vil ifølge organisationen være forceret frem mod 2026 og kan ikke gennemføres uden betydelige omkostninger for de berørte udbydere, hvilket kan stille dem væsentlig ringere i konkurrencen overfor andre udbydere på telemarkedet.

Dansk Erhverv og IT-Branchen finder, at loven enten ikke bør have virkning for aftaler indgået før 7. december 2020, eller at loven først fra 1. januar 2030 bør få tilbagevirkende kraft for aftaler indgået før 7. december 2020.

DI finder ikke, at behovet for, at lovforslaget skal have tilbagevirkende kraft, er velbegrundet, idet lovforslaget indeholder mulighed for at forbyde allerede indgåede aftaler.

Huawei anbefaler, at lovforslaget ikke tillægges tilbagevirkende kraft.

Teleindustrien opfordrer til, at lovens tilbagevirkende kraft helt opgives eller alternativt tidligst får virkning fra 1. januar 2030. Tilsvarende bør lovens ikrafttrædelse efter organisationens opfattelse udskydes for aftaler om forlængelse eller genforhandling af eksisterende aftaler indgået før 7. december 2020, idet et forbud mod indgåelse af sådanne aftaler ifølge Teleindustrien de facto vil medføre, at allerede lovligt leveret udstyr vil være ubrugeligt.

Lovforslaget indebærer, at loven får virkning for aftaler, der er indgået den 7. december 2020, hvor lovforslaget blev sendt i høring, eller senere, samt at loven fra den 1. januar 2026 også får virkning for aftaler, der er indgået før den 7. december 2020.

Ordningen indebærer, at Center for Cybersikkerhed fra lovens ikrafttræden alene vil kunne træffe afgørelse om forbud mod opretholdelse af aftaler, jf. § 3, stk. 1, og forbud mod anvendelse af kritiske komponenter, systemer m.v., jf. § 3, stk. 2, når disse aftaler er indgået den 7. december 2020 eller senere.

Bestemmelsen sikrer, at teleudbyderne ved lovens ikrafttræden ikke kan mødes med et forbud mod allerede indgåede aftaler, der er indgået før lovforslagets ordning blev offentligt kendt. Samtidig sikres det, at der ikke opstår et incitament for teleudbyderne til at omgå lovens ordning ved at indgå aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som udgør en væsentlig trussel mod statens sikkerhed, i perioden fra lovforslaget blev sendt i offentlig høring og frem til, at loven træder i kraft.

For at sikre, at ordningen i fremtiden, hvor Danmarks afhængighed af teleinfrastrukturen vil blive yderligere forøget, omfatter alle aftaler, indebærer lovforslaget, at loven fra den 1. januar 2026 også får virkning for aftaler, der er indgået før den 7. december 2020. Denne udskudte tilbagevirkende kraft indebærer, at teleudbyderne fra lovens ikrafttræden vil få en længere periode til selv at afvikle eventuelle aftaler, der er indgået før den 7. december 2020, som udgør en væsentlig trussel mod statens sikkerhed.

Det er dog forventningen, at langt de fleste omfattede aftaler, der er indgået før den 7. december 2020, på dette tidspunkt vil være udløbet.

12. Forudgående screening og standstill-periode

Dansk Energi finder det nødvendigt, at der enten tilvejebringes screeningsværktøjer eller anden information, som teleudbyderne kan anvende i forbindelse med afsøgning af markedet for relevante leverandører. Dansk Energi mener endvidere, at i det omfang Center for Cybersikkerhed har ny viden om eller måtte få ny viden om, at en fortsat anvendelse af tidligere leverede kritiske netkomponenter, systemer og værktøjer kan være forbundet med en væsentlig trussel for statens sikkerhed, bør centeret rette henvendelse til den pågældende teleudbyder, når denne viden foreligger. Dansk Energi anfører, at det er vigtigt for teleudbydere, at de så tidligt som muligt får et varsel, så teleudbyderne får de bedst mulige betingelser for at kunne planlægge og disponere i forhold til en eventuel udfasning og udskiftning af udstyr. Denne viden bør efter Dansk Energis mening overføres til teleudbyderen hurtigst muligt og ikke først umiddelbart før eller efter 1. januar 2026. Dansk Energi foreslår derfor, at Center for Cybersikkerhed forpligtes til at dele relevant viden med teleudbydere, så snart denne viden foreligger.

Dansk Energi foreslår desuden, at der gives teleudbyderne mulighed for en dialog med Center for Cybersikkerhed om en screeningsproces, for så vidt angår kritiske netkomponenter, systemer eller værktøjer, som teleudbyderen har taget i brug før 1. juli 2016, og som måtte forventes stadig at være i brug i 2026. Dette vil give teleudbyderen mulighed for så tidligt som muligt at kunne planlægge og disponere i forhold til en eventuel udfasning og udskiftning af udstyr. Dansk Energi foreslår desuden, at Center for Cybersikkerhed tilbyder at gennemføre en audit hos interesserede teleudbydere.

Teleindustrien mener ikke, at det er korrekt, at teleudbyderne allerede ved lovens fremsættelse kan begynde at indrette sig, da det efter organisationens mening er fuldstændig uklart, hvilke lande og hvilke specifikke leverandører Center for Cybersikkerhed anser for at udgøre en trussel mod statens sikkerhed. Teleindustrien anfører, at først når den viden er konkretiseret og kommunikeret til udbyderne, kan de begynde at lægge planer for udskiftning af allerede leveret infrastruktur. Teleindustrien anfører endvidere, at Center for Cybersikkerhed har et indgående kendskab til de leverandøraftaler, der anvendes på det danske marked, samt hvilke aftaler der fra den 7. december 2020 er på vej til at blive indgået. Det bør derfor efter Teleindustriens opfattelse allerede ved lovforslagets fremsættelse gøres entydigt klart, om der er leverandører, som Center for Cybersikkerhed anser som en trussel mod statens sikkerhed. I det omfang dette ikke fremgår, må det efter Teleindustriens opfattelse kunne lægges til grund, at Center for Cybersikkerhed på nuværende tidspunkt ikke finder, at der er leverandører på det

danske marked, der på nuværende tidspunkt udgør en risiko for statens sikkerhed.

Lovforslagets ordning er ikke rettet mod konkrete leverandører eller produkter, og der vil derfor ikke blive foretaget en vurdering af, om konkrete leverandører eller produkter vil udgøre en trussel mod statens sikkerhed eller ej. Derimod vil der blive foretaget en konkret vurdering af, om de enkelte leverandøraftaler samlet set vil udgøre en trussel mod statens sikkerhed.

Center for Cybersikkerhed har allerede i dag en tæt dialog med de teleudbydere, som er omfattet af informationssikkerhedsbestemmelserne i lov om sikkerhed i net og tjenester. Som led i den løbende dialog vil Center for Cybersikkerhed overordnet kunne tilkendegive, om en aftale vurderes at kunne blive omfattet af et forbud.

Det kan imidlertid ikke udelukkes, at en aftale, der i dag vurderes at være uproblematisk, vil kunne vurderes at udgøre en væsentlig trussel mod statens sikkerhed på et senere tidspunkt, hvis leverandørens forhold ændrer sig. Det kan f.eks. være tilfældet, hvis der sker et ejerskifte, eller ved at den pågældende leverandør deltager i aktiviteter i andre lande, der negativt påvirker den offentlige orden, informationssikkerhed eller statens sikkerhed i det pågældende land. Lovforslaget indebærer dog, at der alene vil kunne nedlægges forbud mod opretholdelse af eksisterende aftaler, såfremt aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Der stilles dermed et skærpet krav om, at der skal være en mere konkretiseret trussel mod statens sikkerhed.

Dansk Energi giver udtryk for, at organisationen er uforstående over for behovet for at udvide standstill-perioden i lov om net- og informationssikkerhed fra 10 til 25 arbejdsdage, og Dansk Energi finder ikke, at udvidelsen af perioden er tilstrækkeligt begrundet i lovforslaget.

Teleindustrien foreslår, at der i stedet for en forlængelse af standstill-perioden indsættes en bestemmelse om, at Center for Cybersikkerhed senest 20 arbejdsdage efter, at teleudbyderen har foretaget en underretning, skal træffe afgørelse om, at et færdigt udkast til aftale skal indsendes til centeret, hvilke påtænkte påbud centeret agter at udstede, hvis aftale med leverandøren indgås, eller at centeret vil indstille til Forsvarsministeriet, at der skal nedlægges forbud efter leverandørsikkerhedslovens § 2. Såfremt konkrete forhold ikke gør det umuligt for centeret at træffe en afgørelse inden for fristen, kan der gives centeret mulighed for at forlænge fristen med f.eks. 2 gange 10 arbejdsdage.

Lovforslaget indebærer, at Center for Cybersikkerhed i særlige tilfælde vil kunne forbyde teleudbydere at indgå en leverandøraftale, der vedrører kritiske dele af teleinfrastrukturen, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed.

Vurderingen af, om en aftale udgør en trussel mod statens sikkerhed, vil typisk blive foretaget, efter at Center for Cybersikkerhed har modtaget det endelige aftaleudkast fra teleudbyderen i medfør af den eksisterende underretningsordning efter lov om sikkerhed i net og tjenester med tilhørende bekendtgørelser.

Det følger af denne ordning, at Center for Cybersikkerhed kan udstede påbud om, at en teleudbyder skal indsende det endelige udkast til aftale forud for indgåelsen af den endelige aftale. Herefter vil der indtræde en standstill-periode på maksimalt 10 arbejdsdage. Det bemærkes i den forbindelse, at Center for Cybersikkerhed kun i helt særlige tilfælde udsteder påbud om indsendelse af det endelige aftaleudkast, og at standstill-mekanismen alene har været bragt i anvendelse få gange siden juli 2016, hvor net- og informationssikkerhedsloven (den nuværende lov om sikkerhed i net og tjenester) trådte i kraft.

Den nuværende standstill-periode på 10 arbejdsdage er fastsat ud fra et hensyn til, at Center for Cybersikkerhed skal have mulighed for at gennemgå aftalen og rådgive teleudbyderen.

Som led i den foreslåede ordning vil standstill-perioden blive udvidet til 25 arbejdsdage. Det skal ses i lyset af, at centeret – udover som hidtil at gennemgå aftalen og indgå i et rådgivningsforløb med teleudbyderen – også vil skulle vurdere et eventuelt forbud mod den endelige aftale, herunder om mindre indgribende tiltag kan anvendes, inddrage andre relevante myndigheder, udarbejde en afgørelse om forbud, overveje om afgørelsen vil have ekspropriativ karakter, og i så fald fastsætte størrelsen på erstatningen. Dette vurderes ikke at være muligt indenfor den nuværende frist på 10 arbejdsdage, og det foreslås derfor, at fristen forøges til 25 arbejdsdage.

13. Lovforslagets betydning for konkurrence og innovation på teleområdet

Dansk Energi anfører, at hvis der ikke tilvejebringes et tilstrækkeligt informationsgrundlag til brug for teleudbydernes udvælgelse af leverandører, risikeres planlagt infrastrukturudbygning at blive forsinket, ligesom der kan skabes tvivl om selve investeringsgrundlaget for infrastrukturudbygningen. Hertil kommer, at Center for Cybersikkerheds nye beføjelser til at nedlægge forbud ifølge Dansk Energi kan føre til, at konkurrencen mellem leverandører i markedet bliver mindre, og det vil

alt andet lige lede til højere priser på det efterspurgte udstyr samt også lavere innovationskraft.

Danske Regioner finder, at forbud mod indgåelse af kontrakter kan betyde, at udbyderen vil kunne vælge mellem færre leverandører, hvilket vil kunne medføre stigende priser. Danske Regioner bemærker, at lovforslaget ikke redegør for, hvordan lovforslaget i den forbindelse økonomisk kan påvirke offentlige myndigheder.

Rådet for Digital Sikkerhed bemærker, at hvis der med lovforslaget helt kan udelukkes givne leverandører, vil det have betydning for udbydernes mulighed for at vælge leverandører, og det vil dermed mindske udbydernes muligheder for at vælge leverandør, og dermed kan det i sidste ende have negative konsekvenser for konkurrencen. Rådet finder, at hvis der gennemtvinges en forceret omlægning, kan det påvirke den sikkerhedsmæssige stabilitet i infrastrukturen og medføre store omkostninger for udbyderne. Rådet finder, at dette kan have alvorlige økonomiske konsekvenser og også påvirke incitament for leverandørerne til at udvikle innovative løsninger. Det er endvidere ifølge rådet væsentligt, at disse omkostninger holdes nede, også af hensyn til brugerne af disse tjenester, da omkostningerne i sidste ende risikerer at bliver væltet over på brugerne af tjenesterne.

Teleindustrien anfører, at såfremt det med lovforslaget er tanken helt at udelukke bestemte leverandører, vil det for eksempelvis betyde, at udbyderens muligheder for valg af leverandør af radionetværk til mobilnettene vil blive meget begrænset. Lovforslaget vil dermed medføre en betydelig svækkelse af konkurrencen. Organisationen forventer, at reguleringen vil medføre højere priser og mindre innovative produkter til de danske forbrugere.

Forsvarsministeriet skal understrege, at der ikke med lovforslaget skabes hjemmel til at forbyde leverandører, men alene hjemmel til, at konkrete leverandøraftaler m.v. vil kunne forbydes efter en individuel vurdering.

Som anført i lovforslagets afsnit 6 anerkender Forsvarsministeriet, at lovforslaget vil kunne medføre en reduceret konkurrence, fordi teleudbyderne i forbindelse med konkrete aftaler om leverancer potentielt vil kunne vælge mellem færre tilbud fra leverandører, hvilket vil kunne medføre stigende priser for teleudbyderne og eventuelt have negativ effekt på innovationen på teleområdet. Dette vil potentielt kunne få betydning for alle, der anvender telenettet, herunder offentlige myndigheder, men det er ikke givet, at det også vil lede til stigende priser for dem. Det vil afhænge af forhold såsom teleudbydernes markedsstrategi, prisstrategi og generelle tilgang til ordningen, som ikke vil

kunne fastlægges på nuværende tidspunkt. En sådan eventuel afledt økonomisk konsekvens er på den baggrund ikke beskrevet nærmere i lovforslaget.

Teleindustrien bemærker, at lovforslaget alene finder anvendelse på "væsentlige erhvervsmæssige udbydere". Dermed falder f.eks. ejere af private netværk udenfor for lovens anvendelsesområde. Hvis kun mobiludbyderne forbydes at anvende udstyr fra visse leverandører, kan der efter Teleindustriens opfattelse opstå en konkurrenceforvridende situation ved, at private virksomheder kan indgå aftaler med de selvsamme leverandører, som udbyderne er afskåret fra at anvende.

Lovforslaget finder anvendelse på væsentlige erhvervsmæssige udbydere af elektroniske kommunikationsnet og -tjenester. Udbyderbegrebet benyttes i dag i de bekendtgørelser, der udmønter lov om sikkerhed i net og tjenester, hvorved det sikres, at de særlige underretningspligter og de mest restriktive sikkerhedskrav alene stilles til de teleudbydere på markedet, der har størst betydning for den kritiske teleinfrastruktur.

Det er Forsvarsministeriets opfattelse, at det med det foreslåede udbyderbegreb sikres, at de nye regler er målrettet de væsentligste udbydere af den danske teleinfrastruktur.

14. Øvrige bemærkninger

DR anfører, at institutionen har en public service-forpligtelse, som betyder, at hvis Center for Cybersikkerhed træffer afgørelse, som medfører, at DR ikke kan udkomme, vil det udgøre et indgreb i DR's uafhængighed og dermed efter DR's opfattelse også et potentielt indgreb i ytrings- og informationsfriheden efter menneskerettighedskonventionen (EMRK) artikel 10.

Teleindustrien anfører, at en forceret udfasning kan få vital betydning for driftsstabiliteten af netværkene og kan i værste fald betyde, at udbyderne ikke kan benytte en kritisk leverandør til at forhindre et nedbrud, hvilket i sig selv vil være samfundskritisk og udgøre en alvorlig sikkerhedsmæssig trussel.

Det er ikke Forsvarsministeriets forventning, at der i medfør af lovforslaget vil blive nedlagt forbud, som forhindrer DR i at udkomme, eller at der i øvrigt vil ske en forceret udfasning, som vil få negativ indvirkning på driftsstabiliteten.

Det fremgår af bemærkninger til lovforslagets § 3, at nedlæggelse af forbud ikke bør føre til, at der sker afbrydelser på telenettet, fordi tele-

udbyderen ikke har haft mulighed for at indgå eller implementere en ny aftale. På den baggrund anføres det, at Center for Cybersikkerhed som udgangspunkt bør fastsætte en nærmere frist, som er baseret på, hvornår en loyalt agerende teleudbyder kan have taget de nødvendige forholdsregler.

Forsvarsministeriet vil i lovforslagets bemærkninger præcisere, at samme hensyn skal iagttages i forhold til varetagelsen af public service-relaterede forpligtelser.

Danske Regioner mener, at det er uklart, hvordan lovforslaget står i forhold til konkurrencelovgivningen, og de anfører, at det kan medføre tidsmæssige og økonomiske konsekvenser i forbindelse med forlængede processer. De finder desuden, at det er uklart, om det vil være lovligt at indhente forhåndstilsagn forud for indgåelse af leverandøraftaler. Danske Regioner finder det endvidere uklart, hvad tilgangen er til prækvalificerede leverandører i forbindelse med udbud.

Vurderingen af, om en omfattet aftale vil udgøre en trussel mod statens sikkerhed, vil typisk ske som sidste trin i forbindelse med den underretningsordning, der i forvejen er etableret i medfør af lov om sikkerhed i net og tjenester. Allerede på det tidspunkt, hvor en teleudbyder begynder overvejelserne om at indgå en ny leverandøraftale, vil teleudbyderen derfor være i kontakt med Center for Cybersikkerhed, og centeret vil i den efterfølgende proces kunne give teleudbyderen omfattende rådgivning og vejledning om de sikkerhedsmæssige aspekter af aftalen, herunder aspekter, som efter centerets vurdering vil kunne udgøre en trussel mod statens sikkerhed. Det sikrer en høj grad af forudsigelighed i det senere forhandlingsforløb, hvor teleudbyderen på et tidligt tidspunkt vil være bekendt med Center for Cybersikkerheds vurdering af aftalen. Lovforslagets ordning indebærer således ikke, at teleudbyderen får krav på et egentligt forhåndstilsagn, før den endelige aftale er forelagt Center for Cybersikkerhed, men centeret vil i den indledende fase kunne træffe afgørelse om, hvorvidt aftalen vurderes at være omfattet af ordningen.

Desuden skal det bemærkes, at et forbud efter lovforslaget alene kan nedlægges overfor væsentlige erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, dvs. udbydere af net, hvor disse net anvendes af mere end 50.000 slutbrugere eller udbydere, der gennem aftaler med statslige myndigheder og institutioner betjener mere end 500 slutbrugere.