Tak for henvendelsen.

Advokatrådet har besluttet ikke at afgive høringssvar.

Med venlig hilsen

ADVOKATSAMFUNDET
RETSSIKKERHED · UAFHÆNGIGHED · INTEGRITET

Henriette Fagerberg Erichsen
Sekretær

Advokatsamfundet, Kronprinsessegade 28, 1306 København K
D +45 33 96 97 28
hfe@advokatsamfundet.dk - www.advokatsamfundet.dk

From
Chinese Chamber of Commerce in Denmark(CCCD)
Ole Maaløes Vej 3, 2200 København N

To whom it may concern,

The Chinese Chamber of Commerce in Denmark is a non-profit, non-governmental organization representing Chinese enterprises which are operating business in Denmark.

Contact: John Liu, john.liu@cccdk.dk

Subject: make reference to "sagsnummer 2020/008732"

CCCD would like to send the comments to draft Bill on supplier security in the critical telecommunications infrastructure ("Forslag til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur")

The draft describes a situation in which a vendor can be banned from having access to supplying telecommunications equipment to Danish operators.

In the draft, a delivery agreement can be forbidden in case it poses a threat to Danish national security.

In assessing this, the draft law a.o. says:

(Page2,§2)
The assessment will include, among other things, whether the supplier, the supplier's most important subcontractors, and actors who exercise control over or have a significant influence on the supplier:
1) Is domiciled in or handles the production or operation from a country with which Denmark has not entered into a security agreement, or with which Denmark does not have corresponding cooperation on security matters.

*("*I vurderingen vil blandt andet kunne indgå, om leverandøren, leverandørens væsentligste underleverandører samt aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren: 1) 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.

In our view, such a criterion clearly constitutes discrimination against companies domiciled in countries that are not in a defence alliance or has security cooperation with Denmark.

The criterion is furthermore very vague and therefore appears unpredictable and could lead to random decisions.

It makes little sense to attribute a certain nationality to a supplier as all suppliers share the same global supply chain. All equipment uses a multitude of components that are designed and manufactured in not one, but in many countries. Forbidding one supplier based on nationality will not improve security, but will only hinder free trade.

In the remarks to the draft, it is stated that issues in relation to nationality discrimination under WTO/GATT and bilateral trade agreements are exempted with reference to national security.

With our knowledge of Danish law, we question if there is legal basis for exemptions from the legal guarantees of non-discrimination in international law. We therefore strongly encourage the Ministry to eliminate the discriminatory parts of the draft law.

Best regards.

John Liu

Secretary in General

Chinese Chamber of Commerce in Denmark (CCCD)
03.01.2021

Til: fmn@fmn.dk
Kopi: nbb@fmn.dk og nls@fmn.dk

Sagsnummer 2020/008732

DR | ØKONOMI, TEKNOLOGI OG MEDIEPRODUKTION

www.dr.dk

Teknologi Ledelsesstab
Kenneth Bülow

KEBL@dr.dk

21. december 2020

Høringssvar vedrørende udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

DR har modtaget ovennævnte udkast til lovforslag i høring og ønsker hermed at fremkomme med bemærkninger hertil, jævnfør forsvarsministeriets anmodning af 7. december 2020.

DR anerkender at der er en høj trussel fra cyberspionage mod telesektoren i Danmark. DR er derfor også enig 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.

Det fremgår af lovforslagets § 3, at Center for Cybersikkerhed (CFCS) i særlige tilfælde kan forbyde DR at opretholde indgåede aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf, hvis opretholdelsen af aftalen vurderes at udgøre en væsentlig trussel mod statens sikkerhed.

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

Lovforslaget indeholder en gennemgang af forslagets overensstemmelse med gældende ret. Fsva. EMRK forholder forslaget sig alene til artikel 6 om retten til en retfærdig rettergang. Det er DR's opfattelse, at der i lovforslagets bemærkninger også bør redegøres for lovforslagets forhold til ytrings- og informationsfriheden i EMRK artikel 10, herunder kravet om nødvendighed og proportionalitet.

DR står naturligvis til rådighed, hvis ovenstående giver anledning til spørgsmål eller der er behov for uddybning. I så fald kan der rettes henvendelse til Teamleder for DR Distribution Jesper Kjeldsen på telefon 28703410 eller e-mail JEKJ@dr.dk.

Med venlig hilsen

Kenneth Bülow
Stabschef

Forsvarsministeriet

Høringssvar sendes til fmn@fmn.dk
med kopi til nbb@fmn.dk og nls@fmn.dk

Vedr. sagsnummer 2020/008732.

Dok. ansvarlig: MOB
Sekretær:
Sagsnr: s2020-1212
Doknr: d2020-33926-13.0
4. januar 2021

Høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Dansk Energi afgiver hermed sine bemærkninger til det udkast til forslag til ny lov om leverandørsikkerhed i den kritiske teleinfrastruktur, som Forsvarsministeriet den 7. december 2020 har sendt i høring.

Generelle bemærkninger

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 Energi er således enig i, at der er tale om et så beskyttelsesværdigt formål, at det kan begrunde, at drastiske midler må tages i anvendelse – også midler, der naturligt sætter spørgsmålstegn ved både proportionaliteten i det enkelte indgreb samt retssikkerhedsgarantier.

Dansk Energi bemærker således også, at lovforslaget i flere bestemmelser eksplicit nævner proportionalitet, som et element, der skal indgå, når der træffes afgørelse – det vil sige, at et indgreb alene kan finde sted, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

At proportionalitetsprincippet nævnes eksplicit i selve lovteksten og at ministeriet på den måde ser behov for at understrege dette princip, ser Dansk Energi som et udtryk for, at Center for Cybersikkerhed (CFCS) med lovforslaget netop får et ganske indgribende værktøj. Det nævnes alene eksplicit, hvor der er tale om ganske vidtgående myndighedsindgreb – som fx i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter.

Dansk Energi bemærker videre, at der i lovforslaget gøres ganske meget ud af at sikre virksomheders retssikkerhedsgarantier ved den efterfølgende mulighed for domstolsprøvelse af den afgørelse CFCS træffer i medfør af §§ 2 og 3. Her har Forsvarsministeriet overvejet, hvordan teleudbyderens eller leverandørens ret til domstolsprøvelse kan forenes med de særlige sikkerhedsmæssige fortrolighedshensyn. Forsvarsministeriet finder, at disse hensyn kan varetages ved, at der etableres særlige procedureregler, der på den ene side sikrer hensynet til fortrolighed, men på den anden side samtidig sikrer hensynet til partsbeføjelser.

Samme analyse og afvejning finder Dansk Energi mangler i lovforslaget for den del, der handler om, at CFCS ikke i sin myndighedsudøvelse efter §§ 2 og 3 skal anvende principperne i offentlighedsloven og forvaltningsloven. Her har man – uden videre – blot fjernet det ellers gældende princip efter § 8 i lov om Center for Cybersikkerhed (med tilhørende bemærkninger), hvorefter CFCS forudsættes i videst muligt omfang at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, herunder § 19 om partshøring.
Der henvises endog i bemærkningerne til, at den gældende undtagelse fra offentlighedsloven og forvaltningsloven indebærer, at CFCS ikke vil være forpligtet til at gengive efterretningsmæssige oplysninger i forbindelse med en begrundelse for en afgørelse truffet i medfør af lovforslagets kapitel 2 og 3. Desuden vil CFCS ikke være forpligtet til at lade de tilsvarende oplysninger indgå i behandlingen af en aktindsigtssag. Dansk Energi stiller sig undrende over for hvorfor denne gældende regulering ikke er nok. Ministeriet finder imidlertid, at denne gældende mulighed for undtagelse ikke vil være tilstrækkelig i de konkrete sager.

Da der er tale om ganske vidtgående myndighedsindgreb efter lovforslagets §§ 2 og 3 finder Dansk Energi det væsentligt for retssikkerheden, at det gældende princip i lov om Center for Cybersikkerhed, hvorefter CFCS forudsættes i videst muligt omfang at efterleve principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, herunder § 19 om partshøring 4-6, fortsat bør gælde.

Som minimum bør Forsvarsministeriet i højere grad kvalificere og underbygge behovet for helt at fjerne muligheden for efterlevelse af principperne i offentlighedsloven og forvaltningsloven, når CFCS skal træffe afgørelser efter lovforslagets kapitel 2 og 3.

<u>Bemærkninger til lovforslagets kapitel 2</u>

Det fremgår at lovforslaget, at det udgør en overbygning på den underretningsordning, som i dag er udmøntet i bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Som noget nyt giver lovforslaget efter §§2 og 3 CFCS beføjelser til at nedlægge et decideret forbud vedrørende væsentlige erhvervsmæssige udbyderes indgåelse af bestemte typer aftaler, såfremt aftalerne vurderes at udgøre en trussel mod statens sikkerhed, ligesom der også fra 1. januar 2026 vil gives beføjelser til med tilbagevirkende kraft at nedlægge forbud mod opretholdelse af aftaler, der er indgået før 7. december 2020, idet omfang de vurderes at udgøre en væsentlig trussel mod statens sikkerhed. Desuden får CFCS fra 1. januar 2026 beføjelser til at forbyde en væsentlig erhvervsmæssig udbyder fortsat at anvende kritiske netkomponenter, systemer og værktøjer der tidligere er leveret og fortsat anvendes, uanset tidspunktet for ibrugtagning af disse komponenter og systemer, idet omfang de vurderes at udgøre en væsentlig trussel mod statens sikkerhed.

Disse nye beføjelser er ganske vidtrækkende, griber ind i aftalefriheden og kan potentielt indebære særdeles store omkostninger for de berørte udbydere.

Den udløsende faktor for nedlæggelse af forbud beror på forhold vedrørende leverandøren og/eller underleverandører til leverandøren.

For Dansk Energi fremstår det ikke klart, hvordan teleudbyderne fremover skal kunne identificere og udvælge leverandører, idet teleudbyderne ikke vil have viden om hvilke leverandører, som CFCS måtte anse for at udgøre en trussel mod statens virksomhed.

Teleudbydernes usikkerhed ved udvælgelse af leverandører bliver ikke mindre af, at det ikke af lovgivningen fremgår klart om leverandører hjemmehørende i fx vestlige lande, som Danmark må formodes at have en sikkerhedsaftale med, ikke skulle kunne udgøre en trussel mod statens sikkerhed. Det fremgår således af lovforslaget, at ikke kun landet, hvor leverandøren er hjemmehørende, lægges til grund for CFCS´ vurdering, men at der også kan lægges vægt på hvor produktionen eller driften varetages fra. Det kendetegner således mange leverandører, hjemmehørende i vestlige lande, at de har produktionsfaciliteter mange forskellige steder i verden, herunder også i lande som eventuelt kan være betænkelige set i et nationalt sikkerhedsperspektiv.

Dansk Energi ser desværre ikke umiddelbart, at lovforslaget leverer klare svar på hvordan denne situation kan afhjælpes. Dansk Energi finder det derfor nødvendigt, at der enten tilvejebringes screening-værktøjer eller anden information, som teleudbyderne kan anvende i forbindelse med afsøgning af markedet for relevante leverandører.

Hvis der ikke fra CFCS tilvejebringes et tilstrækkeligt informationsgrundlag til brug for teleudbydernes udvælgelse af leverandører, risikeres planlagt infrastrukturudbygning således at blive forsinket, ligesom der kan skabes tvivl om selve investeringsgrundlaget for infrastrukturudbygningen. Hertil kommer, at CFCS nye beføjelser til at nedlægge forbud mod at aftaler indgås med bestemte leverandører, kan føre til at konkurrencen mellem leverandører i markedet bliver mindre. Det vil alt andet lige lede til højere priser på det efterspurgte udstyr samt også lavere innovationskraft.

I forhold til et forbud mod anvendelse af de kritiske netkomponenter, systemer og værktøjer der tidligere er leveret og fortsat anvendes af teleudbyderen, må CFCS grundlæggende forventes at være bekendt med eksistensen heraf i det omfang, at de er indkøbt og taget i anvendelse efter 1. juli 2016, hvor en underretningspligt for teleudbyderne første gang trådte i kraft.

I det omfang CFCS har ny viden om eller måtte få ny viden om, at en fortsat anvendelse heraf kan være forbundet med en væsentlig trussel for statens sikkerhed, bør CFCS rette henvendelse til den pågældende teleudbyder, når denne viden foreligger. 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 overføres til teleudbyderen hurtigst muligt og ikke først umiddelbart før eller efter 1. januar 2026. Det foreslås derfor, at CFCS forpligtes til, efter de

konkrete omstændigheder, at dele relevant viden med teleudbydere, så snart denne viden foreligger.

Ligeledes bør teleudbydere, 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, kunne indlede en dialog med CFCS med sigte på at iværksætte en screening-proces, for så vidt angår disse netkomponenter, systemer eller værktøjer. Dette vil på tilsvarende vis give teleudbyderen mulighed for så tidligt som muligt at kunne planlægge og disponere i forhold til en eventuel udfasning og udskiftning af udstyr. En mulighed kunne være, at CFCS tilbyder at gennemføre et audit hos interesserede teleudbydere, hvor udstyrs- og leverandørlister gennemgås og vurderes med udgangspunkt i om visser typer udstyr kan udgøre en trussel mod statens sikkerhed. På tilsvarende vis bør der foreligge en mulighed for at teleudbydere på eget initiativ kan rådføre sig med CFCS, for så vidt angår udstyr, der er taget i anvendelse før 1. juli 2016.

Bemærkninger til lovforslagets kapitel 3

Efter en første læsning af lovforslagets § 4 vedrørende ekspropriation fik Dansk Energi det indtryk, at forbud, der vedrører teleudbyderes aktuelle og lovlige anvendelse af kritiske netkomponenter, systemer og værktøjer m.v., vil være at betragte som ekspropriative indgreb, og at gennemførelsen af sådanne indgreb derfor som hovedregel vil udløse fuldstændig erstatning.

Lovbemærkningerne til § 4 efterlader dog Dansk Energi med et helt andet indtryk. Her fremgår det at navnlig det forhold, at forbud mod indgåelse af en aftale, opretholdelse af en indgået aftale eller fortsat anvendelse af kritiske komponenter, systemer m.v., som vil være begrundet i hensyn til statens sikkerhed, må antages at tale med vis vægt imod, at der vil være tale om ekspropriation. Heroverfor taler det alene det forhold at et indgreb mod konkrete aftaler efter omstændighederne vil kunne have betydelig intensitet over for den pågældende aftalepart, at det på den baggrund ikke kan *udelukkes,* at et forbud efter omstændighederne vil kunne anses for ekspropriativt.

Dansk Energi er af den opfattelse, at forbud som retter sig mod netkomponenter, systemer og værktøjer, som er indkøbt og taget i brug forud for offentliggørelse af lovforslaget den 7. december 2020, og som CFCS ikke tidligere har udtrykt betænkeligheder over at skulle udgøre en trussel mod statens sikkerhed, bør anses for ekspropriative indgreb, og derfor bør udløse fuldstændig erstatning. Det foreslås 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 7. december 2020, udgør ekspropriative indgreb således, at teleudbydernes usikkerhed, for så vidt angår både direkte og indirekte omkostningsdækning, fjernes. Alternativt bør der indføres en kompensationsordning, som sikrer teleudbyderne dækning for de tab, som et indgreb medfører.

Bemærkninger til lovforslagets kapitel 11

Efter de gældende regler i § 4, nr. 2, i lov om net- og informationssikkerhed, som er udmøntet i §§ 3-5, i bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed, kan CFCS udstede påbud om, at et endeligt udkast til en aftale mellem teleudbyderne og dennes aftalepart skal fremsendes til CFCS forud for indgåelse af den en-

delige aftale. Den endelige aftale vil herefter først kunne indgås, når udbyderen har modtaget en tilbagemelding fra CFCS senest 10 arbejdsdage efter modtagelse.

Med lovforslaget foreslås denne stand-still periode fra 10 til 25 dage. Dansk Energi stiller sig umiddelbart uforstående heroverfor. Forud for at der indledes forhandlinger med leverandører skal der således allerede efter bekendtgørelsen ske underretning om:
1) Hvilke kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som aftalen påtænkes at omfatte.
2) Aftalens påtænkte omfang.
3) Eventuel placering af opgaver uden for Danmark.
4) Eventuelle leverandører, der påtænkes inddraget i aftaleforhandlingerne.
5) Overordnet tidsplan for aftaleforhandlingerne.
6) Aftalens påtænkte varighed.

Der burde således allerede være etableret grundlag for CFCS til inden for de gældende 10 dage at kunne vurdere aftaleudkastet. Dansk Energi savner en nærmere begrundelse for forslaget om en udvidelse af stand-still perioden, eftersom en sådan udvidelse vil udgøre et forholdsvis vidtgående indgreb i forhold til aftaleparterne.

Med venlig hilsen

Dansk Energi

DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Forsvarsministeriet
Holmens Kanal 9
1060 København K
Sagsnr. 2020/008732

Den 4. januar 2021

Høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Dansk Erhverv og IT-Branchen takker for invitationen til at deltage i høringen over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Samtidig bemærker vi dog, at høringsfristen er meget kort henset til forslagets vidtgående karakter, og at høringen foregår hen over jul og nytår.

Generelle bemærkninger

Dansk Erhverv og IT-Branchen støtter regeringens overordnede hensigt om at øge sikkerheden i teleinfrastrukturen. Det danske samfund er i de seneste årtier blevet et af de mest digitaliserede lande i verden, hvilket giver en række markante fordele for borgere, virksomheder og myndigheder. Forsat udvikling af nye digitale forretningsmodeller og automatisering af erhvervslivet er afgørende for Danmarks konkurrenceevne og mulighed for at opretholde et højt niveau af velstand og velfærd.

Den øgede digitalisering betyder samtidig, at samfundet i meget høj grad er afhængigt af en velfungerende og sikker teleinfrastruktur, og at potentielle sårbarheder skal adresseres. Dansk Erhverv og IT-Branchen støtter derfor private udbyderes og offentlige myndigheders fortsatte systematiske og vedholdende arbejde for at sikre teleinfrastrukturen og øvrig digital infrastruktur.

Dette arbejde er således allerede højt prioriteret i det danske erhvervsliv, herunder særligt i telebranchen, og udviklingen i 2020 har yderligere åbnet øjnene for betydningen af en velfungerende og sikker digital infrastruktur. Intensiv anvendelse af fx hjemmearbejde, nethandel og elektronisk kommunikation er kun mulig pga. en veludbygget og robust teleinfrastruktur. Fx blev 3 ud af 10 lønkroner tjent ved hjemmearbejde fra medio marts og de følgende måneder, da mange danskere måtte forlade deres fysiske arbejdsplads og fortsætte arbejdet derhjemme.

Set i lyset af, at den danske telebranche allerede på nuværende tidspunkt i tæt koordination med Center for Cybersikkerhed arbejder intenst med at skabe sikkerhed og netintegritet, finder Dansk Erhverv og IT-Branchen, at forslaget om leverandørsikkerhed indeholder en række vidtgående tiltag med indbyggede problemer, der risikerer at skabe usikkerhed om rammerne for de investeringer, der hidtil har sikret, at Danmark har opnået EU's aktuelt bedste teleinfrastruktur. Forud-

sætningen for at bevare et højst investeringsniveau, der alene i 2019 udgjorde 8,6 mia. kr., er forudsigelige og gunstige rammevilkår, der også betrygger selskaberne i deres fremtidige investeringsstrategier.

Specifikke bemærkninger
Med hensyn til specifikke bemærkninger til loven henvises til Teleindustriens høringssvar. Dansk Erhverv og IT-Branchen anbefaler således særligt, at lovforslaget ændres på følgende centrale punkter:

1. Forbudsbeslutninger skal foretages af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og høring af andre relevante myndigheder.
2. Teleudbyderne skal sikres mulighed for partshøring og begrundelse for afgørelserne.
3. Afgørelser om forbud kan kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige.
4. Lovens tilbagevirkende kraft for aftaler indgået før 7. december 2020 udgår eller udskydes til tidligst 1. januar 2030.
5. Teleudbyderen 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.
6. Der skal indføres regler om effektiv prøvelse af afgørelser og tilsyn med Center for Cybersikkerhed.
7. Definitionen af ”kritisk infrastruktur” er uklar og skal præciseres væsentligt.

Vi står naturligvis til rådighed, hvis svaret ønskes uddybet.

Med venlig hilsen,

Poul Noer
Chefkonsulent
Dansk Erhverv

Mette Lundberg
Direktør for kommunikation og politik
IT-Branchen

Høringssvar fra Danske Regioner

19-01-2021
EMN-2021-00033
1404867

Høringssvar vedrørende lovforslag om leverandørsikkerhed i den kritiske teleinfrastruktur

Forsvarsministeriet har anmodet Danske Regioner om bemærkninger til lovforslag om leverandørsikkerhed i den kritiske teleinfrastruktur. Danske Regioner fremsender et samlet høringssvar på vegne af de fem regioner. Høringssvaret sendes med forbehold for godkendelse i Danske Regioners Udvalg for Sundhedsinnovation og Erhvervssamarbejde den 11. februar 2021.

Danske Regioner noterer sig, at lovforslaget indebærer, at Center for Cybersikkerhed kan forbyde en erhvervsmæssig udbyder af offentligt tilgængelige kommunikationsnet og -tjenester at indgå en aftale, der vurderes at udgøre en trussel mod statens sikkerhed. I lovforslaget defineres en udbyder som en, der skal have et kommercielt formål. Danske Regioner vurderer derfor ikke, at regionerne er direkte målgruppe for lovforslaget, hvilket Forsvarsministeret har bekræftet telefonisk.

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. Hermed understøtter lovforslaget også en styrket sikkerhed i den samfundskritiske sundhedssektor og regionernes eget arbejde med cyber- og informationssikkerhed.

Det bør dog bemærkes, at der i lovforslaget ikke redegøres for, hvordan lovforslaget økonomisk kan påvirke offentlige myndigheder, når de er kunder hos de kommercielle udbydere, der potentielt er genstand for indgriben fra Center for Cybersikkerhed. Forbud mod indgåelse af kontrakter kan betyde, at udbyderen vil kunne vælge mellem færre leverandører, hvilket vil kunne medføre stigende priser.

Endvidere er det uklart, hvordan lovforslaget står i forhold til konkurrencelovgivning, hvilket kan medføre tidsmæssige (og økonomiske) konsekvenser i forbindelse med forlængede processer. Det er uklart, om det vil være lovligt at indhente forhåndstilsagn forud for indgåelse af leverandøraftaler. Det er endvidere uklart, hvad tilgangen er til prækvalificerede leverandører i forbindelse med udbud, samt om usikkerheden består også efter indgåelse af aftaler. Dette kan med fordel præciseres i det videre arbejde med lovforslaget.

Med venlig hilsen

Stephanie Lose

Ulla Astman

Til Forsvarsministeriet

Forsvarsministeriet har den 7. december 2020 anmodet om Datatilsynets bemærkninger til udkast til forslag til lov om leverandørsikkerhed i den kritiske infrastruktur.

Udkastet giver ikke Datatilsynet anledning til bemærkninger.

Med venlig hilsen

Sara Hansen
Fuldmægtig, cand.jur.

DATATILSYNET

Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
www.datatilsynet.dk

Til Forsvarsministeriet
fmn@fmn.dk med kopi til
nbb@fmn.dk og nls@fmn.dk

Der henvises til
sagsnummer 2020/008732

Den 04. januar 2021
MOKR

Høringssvar vedr. lov om leverandørsikkerhed

1. Generelle bemærkninger

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

Overordnet er DI skeptiske over for lovforslag, der indeholder vide beføjelser, der ikke er indhegnet af gennemsigtige og forudsigelige rammer eller kriterier. I den konkrete sag kan det være vanskeligt at gøre kriterierne bag vurderingen af en eventuel sikkerhedsrisiko helt objektive. Der kan derfor være behov for en undtagelse, der dog forpligter myndighederne til en åben dialog med virksomhederne frem mod vurderingen.

DI skal tage et generelt forbehold for, at ikke alle aspekter er blevet behandlet behørigt under hensyn til at høringen løber hen over julen. Lovforslaget indebærer omvæltninger af retssikkerhedsmæssig karakter, som gennemføres i en forkortet høringsproces. Der er bl.a. tale om fravigelse af principper i den offentlige retspleje vedr. domstolsbehandlingen, som bør drøftes mere grundigt med det brede civilsamfund end en høringsfrist hen over jul giver mulighed for.

En anden grundlæggende udfordring er, at der i medfør af lovudkastet ikke synes at være mulighed for, at leverandøren kan imødegå den kritik, der måtte være bevæggrunden for et forbud. Det gælder både ved en afgørelse om forbud og en efterfølgende domstolsbehandling. Det rejser spørgsmål om, hvorvidt sagen er oplyst godt nok og efterfølgende om der gives

mulighed for at fejlrette og afhjælpe hvad der måtte betragtes som en trussel. Der vendes tilbage til det konkret nedenfor.

2. Konkrete bemærkninger

DI foreslår en EU harmoniseret definition på kritisk infrastruktur

§ 2: Definitionen af kritisk infrastruktur er ikke gradueret. Der er således enten tale om kritisk eller ikke kritisk infrastruktur. I modsætning hertil opererer EU-reglerne, fx EU's 5G toolbox med flere grader af kritisk infrastruktur. DI vurderer, at det synes mere oplagt at harmonisere de danske regler i forhold til EU-reglerne snarere end at have særlige nationale definitioner. En graduering er relevant idet gruppen af kritisk infrastruktur ellers kan blive uforholdsmæssig stor.

§§ 2 og 3: Lovforslagets §§ 2 og 3 indeholder vidtgående hjemler for CFCS til at foretage en afgørelse om forbud mod at indgå eller mod allerede indgåede aftaler om kritisk infrastruktur.
Ved sådanne vidtgående hjemler er det vigtigt, at der gives vid mulighed for at teste og vurdere om afgørelsen er rigtig.

Dette gælder navnlig hvor, der indgår klassificeret viden i afgørelsen.

DI efterlyser bedre muligheder for at inddrage leverandøren både ved afgørelsen om et forbud samt ved domstolsbehandlingen

DI vurderer, at det er vigtigt at finde en balance mellem at sikre klassificeret viden samtidig med at oplyse sagen grundigt. Det bør derfor 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 betrygge CFCS i forhold til, hvad de måtte betragte som en trussel. Hermed kan der muligvis også findes mulighed for at identificere fejlretninger eller andre tekniske måder at imødegå identificerede trusler på. Konkret kan man fx udvide partsbegrebet eller præcisere, hvad man forstår ved relevante parter i disse afgørelser.

§ 2 stk. 2 og § 3 Stk. 4: Lovforslaget henviser til en proportionalitetsvurdering, hvor der kan træffes afgørelser om forbud. Jf. ovenfor kan det være relevant at uddybe denne proportionalitetsvurdering med konkrete foranstaltninger, som CFCS skal forsøge, inden der gribes til egentlige forbud. Det bør overvejes om leverandøren og teleoperatøren kan inddrages i denne proces. Jf. ovenfor kan en inddragelse af leverandøren give anledning til at mindre indgribende foranstaltninger.

§ 4: Lovforslaget henviser til reglerne om ekspropriation. Der er tale om potentielt indgribende forbud mod virksomheder med risiko for store tab til følge. Navnlig muligheden for at

forbyde allerede indgåede aftaler hvor teleselskaberne ikke har chance for indtænke risikoen på forhånd kan resultere i omfattende tab.

DI foreslår på den baggrund, at henvisningen til ekspropriationsbestemmelserne suppleres med en henvisning til, at der skal ydes fuld erstatning efter de almindelige regler for erstatning som følge af et påbud i de tilfælde, hvor der ikke er tale om ekspropriation i henhold til Grundlovens bestemmelser herom.

DI finder det relevant at der etableres en rekursmulighed i loven

§ 6: Ifølge lovforslaget afskæres rekursadgangen. Afskærelse af klageadgang er et problem for markedet, idet en domstolsbehandling, som således bliver eneste rekursmulighed, er for langsom, når en teleudbyder står midt i en konkret forhandling. En teleudbyder vil typisk være nødt til at vælge en anden leverandør alene ud fra en tidsmæssig betragtning.

Argumentet for at afskære rekursadgangen forekommer heller ikke overbevisende. Ifølge lovbemærkningerne, besidder Forsvarsministeriet ikke "fagligt indblik i henholdsvis efterretningsmæssige og teletekniske forhold, som Center for Cybersikkerhed besidder".

Set i lyset af de vidtgående hjemler og en domstolsbehandling, der er indskrænket i forhold til almindelige retsprincipper, så bør en ankeinstans være en mulighed. Såfremt man i Forsvarsministeriet ikke mener, at man besidder de relevante kompetencer hertil, så kan man evt. beskikke særlige eksperter eller nedsætte et egentligt nævn til at hjælpe hermed. Det har man gjort andre steder på teleområdet.

DI anbefaler, at man genovervejer den indskrænkede domstolsbehandling, som forslaget lægger op til.

Kapitel 6: Lovforslaget indeholder særlige regler for domstolsbehandlingen af en evt. klagesag. Der er tale om en indskrænket proces i forhold til de almindelige regler for retsplejen. Lovgivningen er kendt fra udlændingeområdet i forhold til de såkaldte fremmedkrigere, men anvendes nu også på erhvervsområdet i forhold til teleselskaber.

Konkret betyder indskrænkningen, at den leverandør hvis udstyr, der betragtes som en trussel ikke får mulighed for at se al den information, der udgør bevæggrunden for forbuddet, såfremt denne information er klassificeret.

Som nævnt i indledningen betyder en indskrænket domstolsproces, at det er 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. Et egentligt forsvar og relevante modforanstaltninger bliver derfor i praksis svækket.

Samtidig er DI forstående over for, at man ikke ønsker at dele klassificeret viden, og henviser derfor til, at lovforslaget bør udbygges med en metode, til at dele så meget man kan af den klassificerede materiale, eller at der indrettes en egentlig rekursmulighed jf. ovenfor og at der gives bedre tid og mulighed for at drøfte udformningen af domstolsbehandlingen med det brede civilsamfund.

§ 17: Lovforslagets ikraftrædelsesbestemmelser er udformet med tilbagevirkende kraft. DI vurderer, at det ikke synes velbegrundet i lovforslaget, hvorfor de er sat med tilbagevirkende kraft. Der henvises i forslaget til, at teleselskaberne således ikke får mulighed for, at indgå aftaler nu inden loven træder i kraft, hvilket de ellers havde et incitament til. Her skal blot bemærkes, at hvis der er mulighed for at forbyde allerede indgåede aftaler er der næppe incitament for teleselskaber til at gøre netop dette.

Med venlig hilsen

Morten Kristiansen
Chefkonsulent

Forsvarsministeriet har den 7. december 2020 (j.nr. 2020/008732) sendt udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur i høring med anmodning om eventuelle bemærkninger.

Forsvarsministeriet forventer, at der kun i sjældne tilfælde vil være behov for at anvende de foreslåede indgrebsmuligheder, hvorfor Domstolsstyrelsen på det foreliggende grundlag vurderer, at eventuelle merudgifter vil kunne holdes inden for den nuværende bevillingsmæssige ramme. Styrelsen vil følge sagsudviklingen nøje.

Med venlig hilsen

Helle Hübertz Krogsøe
forretningsejer
HHK@domstolsstyrelsen.dk

Domstolsstyrelsen
Jura og Forretning
St. Kongensgade 1-3
1264 København K.
Tlf.(hovednr.): + 45 70 10 33 22
www.domstol.dk

FDA FORENEDE DANSKE ANTENNEANLÆG
Danish Cable Television Association
www.fda.dk

Til FORSVARSMINISTERIET

Holmens Kanal 9
1060 København K

Sendes til fmn@fmn.dk samt nbb@fmn.dk & nls@fmn.dk

Højby den 21. december 2020.

”Høring over Udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur”

FDA, Forenede Danske Antenneanlæg takker for det tilsendte materiale og for muligheden for at tilkendegive vores bemærkninger til det fremsendte udkast.

FDA har ikke nogen bemærkninger til det fremsendte udkast, men vil gerne tilkendegive sin støtte til ønsket om at beskytte den kritiske teleinfrastruktur.

FDA står naturligvis til rådighed for Forsvarsministeriet i det omfang ministeriet har yderligere spørgsmål eller andet, som ønskes drøftet med os, ligesom vi fortsat gerne modtager høringer mv.

Med venlig hilsen
FDA, Forenede Danske Antenneanlæg

[afsendt elektronisk uden signatur]
Søren Birksø Sørensen
Sekretariatschef

Huawei Technologies (Denmark) ApS
Støberigade 14, 2450 København, Denmark
Tel.: +45 32873100
Website: www.huawei.com

FORSVARSMINISTERIET
Att.: Specialkonsulent Nicklas B. Baumgarten
Vores ref.: 0001/Matters/57307677.1

4. januar 2021

Sendt pr. e-mail til nbb@fmn.dk

HUAWEI'S HØRINGSSVAR TIL LOVUDKAST OM LEVERANDØRSIKKERHED I DEN KRITISKE TELEINFRASTRUKTUR AF 7. DECEMBER 2020

Den 7. december 2020 inviterede Forsvarsministeriet til høring om udkast til lov om leverandørsikkerhed i den kritiske teleinfrastruktur, ("Lovudkastet").

Huawei vil gerne benytte lejligheden til at kommentere på Lovudkastet.

Vores input fokuserer på følgende hovedtemaer, som vi nedenfor kommenterer på og kommer med vores anbefalinger til:

1. Huawei støtter en klar og streng regulering af krav til netværkssikkerhed i den kritiske teleinfrastruktur;

2. Diskriminerende regulering baseret på leverandørens nationalitet er et ulovligt og irrelevant kriterium til vurdering af risiko for netværkssikkerhed og skal i øvrigt kvalificeres yderligere for overhovedet at have den nødvendige klarhed;

3. Grundlæggende retssikkerheds garantier kan ikke afskæres eller begrænses alene med henvisning til statens sikkerhed.

1. HUAWEI STØTTER EN KLAR OG STRENG REGULERING AF KRAV TIL NETVÆRKSSIKKERHED I DEN KRITISKE TELEINFRASTRUKTUR

Huawei støtter strenge krav til netværkssikkerhed, som bør være baseret på objektive tekniske, transparente og klare kriterier og internationale standarder.

Definitionen af "*Kritiske netkomponenter, systemer og værktøjer*" i den nuværende § 1, stk. 1, svarer imidlertid ikke til EU's NIS Toolbox' forståelse af en tre-tier tilgang til definitionen af kritiske infrastruktur.

Det samme er tilfældet for de afgørende "*mindre indgribende foranstaltninger*" i §§ 2, stk. 2 og 3, stk. 4.

Huawei støtter det generelle princip i Lovudkastet 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 Forsvarsministeriet at tilpasse definitionerne til den internationale vejledning, der findes i f.eks. internationale sikkerhedscertificeringsordninger som NESAS/SCAS, Common Criteria og lade sig inspirere af definitionerne i NIS Tool Box vedrørende eksempler på mindre indgribende foranstaltninger. Sådan harmoniserende tilgang bør fastlægges direkte i Lovudkastet eller indirekte via lovbemærkningerne for at sikre transparente og klare kriterier. Dette også for i højere grad at sikre, at reguleringen proaktivt kan fungere markedskorrigerende i sig selv, uden at CFCS reaktivt skal håndhæve reguleringen.

Industrien må kunne stole på, at netværkskomponenter, der er certificeret i henhold til internationale sikkerhedscertificeringsordninger, kan betragtes som tilstrækkelig sikre og fri for risiko for at skulle underlægges særskilt prøvelse af CFCS.

Den samme tilgang er taget i Tyskland.

2. DISKRIMINERENDE REGULERING BASERET PÅ LEVERANDØRENS NATIONALITET ER ET ULOVLIGT OG IRRELEVANT KRITERIUM TIL VURDERING AF RISIKO FOR NETVÆRKSSIKKERHED OG SKAL I ØVRIGT KVALIFICERES YDERLIGERE FOR OVERHOVEDET AT HAVE DEN NØDVENDIGE KLARHED

Huawei støtter, som angivet, streng regulering af netværkssikkerhed baseret på objektive, tekniske, transparente, klare kriterier og internationale standarder, som ikke er diskriminerende.

Lovudkastet inkluderer og er baseret på diskrimination i forhold til leverandørens tilhørsforhold som "hjemmehørende" i lande, som Danmark ikke har indgået en sikkerhedsaftale med, eller som Danmark ikke har et tilsvarende sikkerhedsmæssigt samarbejde med.

De nuværende kriterier i §§ 2, stk. 1 og 3 stk. 1 og 2 er vage og uden nogen mulighed for, at industrien kan vurdere, hvornår en sådan nationalitetsrisiko kan komme i spil.

I Lovudkastet indgår en leverandørs nationalitet som en af nøglekriterierne i vurderingen af trusler mod statens sikkerhed. Dette er i praksis ikke et kriterium, som branchen selv arbejder med som en relevant risiko faktor for netværkssikkerhed, og som sådan stiller Huawei spørgsmålstegn ved, om dette overhovedet er et relevant kriterium for netværkssikkerhed.

Dette er desuden tilfældet, da den generelle antagelse om, hvor en leverandør er hjemmehørende, udfordres af det faktum, at alle leverandører/underleverandører/ operatører deler den samme globale distributionskæde. Lovudkastet forsøger at imødekomme dette ved at henvise til nationalitet som relateret til produktionssted, drift, placering af personale, m.v. Dette er alle elementer, som leverandørerne ikke arbejder med i en silotilgang, hverken i forhold til deres organisation som sådan, i forbindelse med bundling af deres netværkskomponenter og -tjenester eller underleverandørstyring.

Selv hvis "nationalitet" opretholdes som en nøglefaktor i sikkerhedsvurderingen, skal reguleringen og de deraf relaterede afgørelser stadig leve op til de internationalt funderede juridiske forbud mod diskrimination på baggrund af nationalitet.

Forsvarsministeriet anfører i bemærkningerne til Lovudkastet, at restriktionerne omkring nationalitetsdiskrimination under WTO/GATT, EU's grundlæggende principper om fri bevægelighed og eventuelle bilaterale handelsaftaler er undtaget med henvisning til national sikkerhed.

Det er en cyklisk argumentation, at anføre forskelsbehandling på grundlag af nationalitet som lovlig forskelsbehandling med henvisning til national sikkerhed, hvor spørgsmålet om nationalitet som grundlag for national sikkerhed er det omtvistede kriterium.

Huawei bestrider, at der er tale om et retligt grundlag for undtagelse fra de juridiske garantier for ikke-diskrimination i international ret.

Dilemmaet omkring forskelsbehandling på baggrund af nationalitet, den globale distributionskæde, uklare kriterier for national sikkerhed i en dynamisk udenrigspolitik, bevidst overtrædelse af international lov om ulovlig forskelsbehandling og behovet at sikre statens sikkerhed baseret på nationalitetskriterierne er noget, som ikke kun Danmark er udfordret af.

Huawei anbefaler, at Forsvarsministeriet ser mod nogle af de andre medlemslande for inspiration til, hvordan man håndterer dette dilemma. Huawei anbefaler at se mod Tyskland, som baserer sin lignende lovgivning på følgende:

a) Alle leverandører anses for lige;

b) Leverandøren udarbejder sammen med operatøren en "troværdighedsaftale", der ved kontraktindgåelse fremsendes til BSI, (Tysklands CFCS);

c) En leverandør anses for troværdig så længe alle elementer i aftalen overholdes. Ved manglende overholdelse af aftalen risikerer leverandøren at blive anset af BSI som "utroværdig"

d) Kritisk infrastruktur er klart defineret;

e) Ved leverancer af kritisk infrastruktur skal der leveres sikkerhedscertifikater for udstyret;

f) Der er krav om et multileverandør set-up ved aftaler om kritisk infrastruktur;

g) Regeringen har (alene som en politisk nødbremse) og alene ved særdeles tungtvejende grunde mulighed for at forbyde aftaler. Det kan imidlertid alene ske, såfremt tre ministerier (indenrigs, økonomi og udenrigs) er enige om det. Det er ikke et led i den sædvanlige tilsyns eller afgørelses proces, men alene et ekstraordinært instrument.

Alternativt anbefaler Huawei, at et forbud alene kan iværksættes i forbindelse med den indledende notifikationsproces og ikke først i forbindelse med fremsendelse af det endelige kontraktudkast eller senere.

3. GRUNDLÆGGENDE RETSSIKKERHEDS GARANTIER KAN IKKE AFSKÆRES ELLER BEGRÆNSES ALENE MED HENVISNING TIL STATENS SIKKERHED

Lovudkastet afskærer eller begrænser flere grundlæggende retssikkerhedsmæssige garantier med henvisning til statens sikkerhed.

Huawei finder en sådan undtagelse fra grundlæggende juridiske retssikkerhedsmæssige garantier for særdeles problematisk og uproportional.

Dette er tilfældet for hver af de enkelte særundtagelser. Dette er ydermere tilfældet, idet de hver især, men særligt samlet set udgør en risiko for vilkårlige eller utilstrækkeligt oplyste beslutninger truffet af CFCS, hvor der endvidere alene er begrænset mulighed for efterfølgende prøvelse. Derudover vil den efterfølgende manglende offentlighed om afgørelserne medføre en risiko for, at den pågældende part ikke kan blive bekendt med de elementer, som domstolen har baseret sin afgørelse på, ligesom afgørelse alene kan have en begrænset værdi som retspraksis.

De mest kritiske elementer er:

a) Regulering med tilbagevirkende kraft, idet Lovudkastet træder i kraft med virkning fra den 7. december 2020 og inden 1. januar 2026 med virkning på aftaler indgået inden den 7. december 2020, jf. § 17, stk. 2 og 3;

b) Undtagelse af principperne om god offentlig forvaltningsskik i forhold til f.eks. afskæring af partshøring, aktindsigt og forpligtelsen til at oplyse de faktiske omstændigheder og juridiske elementer, som en afgørelse er baseret på, jf. § 5;

c) Afskæring af retten til administrativ rekurs, jf. § 6;

d) Begrænsning af den grundlovssikrede ret og de generelle principper i retsplejeloven om, at en retssag skal være offentligt, åben, baseret på parts -og kontradiktionsprincippet og behørig sagsoplysning, jf. kapitel 6;

e) Undtagelse fra den grundlæggende og forfatningsmæssige ret til at vælge sin egen advokat, jf. § 8

f) Begrænsning af erstatning for CFCS' indgriben i en eksisterende kontrakt og forbud mod mulig kontrakt, jf. § 4

g) Anvendelse af en for lav eller uklar tærskel for udstedelse af et forbud begrænser muligheden for at afværge et forbud ved at implementere mindre indgribende foranstaltninger, jf. §§ 2 og 3.

<u>Huawei anbefaler i den forbindelse generelt</u>:

a) at eliminere enhver tilbagevirkende kraft, både således at loven først træder i kraft senest på vedtagelsestidspunktet, samt at loven ikke skal kunne gribe ind i tidligere gyldigt indgåede aftaler, jf. § 17, stk. 2 og 3.

b) Beslutningsprocessen skal understøttes af grundlæggende principper om god offentlig forvaltning, såsom i) partshøring for bedst muligt at oplyse sagen og identificere potentielle mindre indgribende foranstaltninger og sikre korrekte beslutninger, ii) 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, iii) herunder at efterleve princippet for aktindsigt, især i forhold til princippet om egen access, iv) ikke offentliggøre beslutninger, der er påklaget, og når afgørelser er endelige, da alene efter proportional overvejelse af, om afgørelsen bør være anonym, eks. henset til at afgørelsen i øvrigt alene er summarisk, v) endelige afgørelser bør alene offentliggøres i ikke-anonymiseret form, når den involverede part har haft fuld adgang til den dokumentation, som afgørelsen er baseret på.

c) De væsentligt indgribende konsekvenser, som en afgørelse truffet af CFCS 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 være en hurtig prøvelse af et separat uafhængigt klagenævn. Det kan være et nydannet nævn eller eventuelt det nuværende tilsyn med efterretningstjenesterne (TET). Prøvelsen bør indebære opsættende virkning. Den opsættende virkning bør forlænges, i tilfælde af at sagen efterfølges anlægges som en retssag i henhold til § 7. Det kunne dog overvejes, om visse trusler kunne være af en sådan alvorlig karakter og overhængende risiko for fare, at den opsættende virkning skal begrænses eller helt kunne fraviges, i så fald skal der være tale om fastsatte processer og kontroller, jf. eksempelvis tilgangen i Tyskland.

d) 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, der er beskrevet i EMRK, det europæiske charter og den danske grundlov. Dette er ikke noget, som Forsvarsministeriet eller CFCS bare kan afskære med en generel henvisning til statens sikkerhed. Forsvarsministeriet henviser til inspiration fra ordningen fra Retsplejelovens § 784, stk. 2, i sager om efterforskning af en overtrædelse af straffelovens regler om forbrydelser mod statens sikkerhed. Dette er ikke en situation, der kan sammenlignes med kriminelle terrorhandlinger. Retssagen beskrevet i kapitel 6 er en civil sag om en aftale om netværkskomponenter, -systemer og -værktøjer. Der er ikke begået nogen kriminelle handlinger, og de relaterede parter kan være private operatører eller leverandører uden relation til kriminelle handlinger eller udenlandske myndigheder.

    a. Hvis loven skulle indeholde et grundlag for begrænsning af sådanne grundlæggende juridiske rettigheder, bør der være tale om klar regulering, der giver domstolene de rette instrumenter til at manøvrere en balance i forholdet mellem statens sikkerhed og partens retssikkerhed. Der bør være tale om en mere specifik regulering, der klart anfører, at udgangspunktet er de sædvanlige grundlæggende rettigheder til en retfærdig rettergang m.v., og at enhver begrænsning heraf, herunder i omfanget af anvendelsen af den særligt beskikkede advokat, bør være begrænset til i) meget ekstraordinære tilfælde, ii) kun det absolut mest nødvendige omfang, iii) altid med pligt til i videst muligt omfang at sammenfatte nøgleelementerne af det afskårne for parten, iv) for at parten til enhver tid er i stand til at imødegå anbringenderne fra CFCS.

e) Huawei er imod enhver begrænsning af den grundlæggende ret for en part i en retssag til at vælge sin egen advokat. Såfremt Forsvarsministeriet alligevel går ned af den vej, skal der være klarhed omkring, hvordan man kan sikre, at den særligt beskikkede advokat i) ikke har nogen interessekonflikt, og kombinationen af tilstrækkelig ii) proceserfaring og

iii) domæneviden. De særligt beskikkede advokater får en betroet opgave af væsentlig karakter henset til begrænsningerne i udvekslingen af dokumentation og information med sin klient. Dette kræver nogle formalitetskrav i forhold til i) deres udnævnelse og ii) deres proceduremæssige rolle. Dette er et meget specialiseret område (netværkssikkerhedsregulering eller endda den bredere teleregulering), som kun et meget begrænset antal advokater i Danmark arbejder med. For at sikre tilstrækkelige kompetencer bør der være krav til, at gruppen af udnævnte advokater har sådanne kvalifikationer. Et forslag kunne være at få Danske Advokater til at varetage en liste over telekommunikations advokater med indstilling fra enten danske it-advokater (DITA) eller anden brancheorganisation. Udpegning kunne ske fra sag til sag via et forud fastsat panel. Der bør også være det sædvanlige krav til, at den pågældende advokat ikke er underlagt nogen interessekonflikt i medfør af de advokatetiske regler. Parten (og Forsvarsministeriet) skal også have ret til at gøre indsigelse mod udnævnelsen af den beskikkede advokat, f.eks. med henvisning til interessekonflikt, manglende sikkerhedsgodkendelse eller manglende kompetencer.

f) Der er usikkerhed omkring, i hvilket omfang kravene til ekspropriation kan være opfyldte, hvis CFCS udsteder et forbud, der påvirker brugen af lovligt udstyr. Det bør fastlægges, at en part i sådan situation som et minimum kan forvente kompensation ikke bare for installationsomkostninger, men også for den service og support, der ville være leveret i produktets levetid og ikke kun frem til det tidspunkt, som forbuddet specifikt omfattet. Derudover bør det fremgå, at et forbud mod at deltage i udbudsprocesser (eller politisk eller administrativ indblanding heri) udgør ekspropriation og et tab af, der fuld ud vil blive kompenseret.

g) Tærskelværdierne for "trussel" i §§ 2 og 3 bør øges til "væsentlig trussel" og "særligt væsentligt trussel" for at imødekomme de indgribende konsekvenser, som en forbudsafgørelse medfører og give plads til mindre indgribende foranstaltninger. Derudover bør tærsklen "negativ påvirkning" i § 2 øges til "væsentlig, signifikant og dokumenteret negativ påvirkning".

Huawei imødekommer en dialog med Forsvarsministeriet om ovenstående.

Med venlig hilsen

Mads Arnbjørn Rasmussen
CTO/CSO

Tlf. 61 63 06 46

INSTITUT FOR
MENNESKE
RETTIGHEDER

Forsvarsministeriet
Holmens Kanal 42
1060 København K
E-mail: fmn@fmn.dk
Kopi til: nbb@fmn.dk og nls@fmn.dk

WILDERS PLADS 8K
1403 KØBENHAVN K
TELEFON 3269 8888
MOBIL 91325719
MIKL@HUMANRIGHTS.DK
MENNESKERET.DK

DOK. NR. 20/03336-2

5. JANUAR 2021

HØRINGSSVAR OVER UDKAST TIL FORSLAG TIL LOV OM LEVERANDØRSIKKERHED I DEN KRITISKE TELEINFRASTRUKTUR

Forsvarsministeriet har ved e-mail af 7. december 2020 anmodet om Institut for Menneskerettigheders eventuelle bemærkninger til udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

Instituttet har følgende bemærkninger:

SAMMENFATNING

Med lovudkastet foreslås det, at Center for Cybersikkerhed skal gives mulighed for at kunne forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet- og tjenester at indgå en aftale, at opretholde en indgået aftale eller fortsat at anvende kritiske netkomponenter m.v.

Fravigelse af forvaltningsloven og offentlighedsloven

Det foreslås med lovudkastet, at forudsætningen om, at Center for Cybersikkerhed i videst muligt omfang efterlever principperne i offentlighedsloven og forvaltningslovens kapitel 4-6 ikke skal gælde for sager, hvor centeret nedlægger forbud.

Dette kan efter instituttets opfattelse 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 Center for Cybersikkerhed undlader at foretage en nærmere vurdering heraf.

- Institut for Menneskerettigheder anbefaler, at Forsvarsministeriet i lovudkastets bemærkninger tilføjer en forudsætning om, at Center for Cybersikkerhed så vidt muligt overholder principperne i offentlighedsloven og forvaltningslovens kapitel 4-6.

Offentliggørelse i ikke-anonymiseret form

Det fremgår af lovudkastet, at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre afgørelser, resuméer af domme eller bødevedtagelser om forbud m.v. og om prøvelse af spørgsmål om ekspropriation.

Det bør af hensyn til forudsigeligheden for de berørte virksomheder beskrives nærmere i bemærkningerne, hvornår Center for Cybersikkerhed kan forventes at ville henholdsvis ikke at ville benytte muligheden for at offentliggøre et forbud m.v. i ikke-anonymiseret form.

- Institut for Menneskerettigheder anbefaler, at Forsvarsministeriet i lovudkastets bemærkninger beskriver, hvornår Center for Cybersikkerhed kan forventes at ville henholdsvis ikke at ville offentliggøre forbud m.v. i ikke-anonymiseret form, herunder ved at give eksempler.

KORT OM LOVUDKASTETS INDHOLD

Det foreslås med lovudkastet, at Center for Cybersikkerhed skal gives mulighed for at kunne forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet- og tjenester at indgå en aftale, at opretholde en indgået aftale eller fortsat at anvende kritiske netkomponenter m.v. Aftaler indgået i strid med et forbud vil være ugyldige.

Derudover gives Center for Cybersikkerhed mulighed for at ekspropriere privat ejendom, hvis det er nødvendigt for at gennemføre et forbud.

Offentlighedslovens bestemmelser (bortset fra § 13 om notatpligt) og forvaltningslovens kapitel 4-6 finder ikke anvendelse ved sager om forbud. Ligesom der ikke er klageadgang over afgørelser om forbud.

Processen ved domstolene vil foregå på en særlig måde med en åben og lukket del, som det kendes fra visse sager om udvisning af udlændinge, som er til fare for statens sikkerhed, og sager om prøvelse af afgørelser om administrativ fratagelse af statsborgerskab, hvis følsomheden af de oplysninger, som ligger til grund for frakendelsen, kræver det.

Overtrædelse af forbud straffes med bøde, og Center for Cybersikkerhed vil i ikke-anonymiseret form kunne offentliggøre afgørelser og resuméer af domme og bødevedtagelser.

Endelig har loven virkning allerede fra den 7. december 2020, da lovudkastet blev sendt i høring, ligesom loven fra den 1. januar 2026 har virkning for aftaler, der er indgået før 7. december 2020.

FRAVIGELSE AF FORVALTNINGSLOVEN OG OFFENTLIGHEDSLOVEN

Det fremgår af lovudkastet, at offentlighedsloven (bortset fra § 13 om notatpligt) og forvaltningslovens kapitler 4-6 (om partens aktindsigt, partshøring og begrundelse) ikke finder anvendelse på de foreslåede regler (lovudkastets § 5).

Det fremgår videre af lovudkastet, at det i dag er en forudsætning, at Center for Cybersikkerhed (i dets øvrige virksomhed) i videst muligt omfang efterlever principperne i offentlighedsloven og forvaltningslovens kapitel 4-6, selvom centret er undtaget for offentlighedsloven og dele af forvaltningsloven (lovudkastets almindelige bemærkninger, afsnit 3.2.2).

Det foreslås med lovudkastet, at denne forudsætning om videst mulig efterlevelse ikke skal gælde for sager, hvor Center for Cybersikkerhed nedlægger forbud mod at indgå en aftale, at opretholde en allerede indgået aftale eller fortsat at anvende visse komponenter. Og det fremgår af lovudkastet, at Center for Cybersikkerhed således ikke vil være forpligtet til at gengive følsomme oplysninger i forbindelse med en begrundelse for sådanne afgørelser (lovudkastets bemærkninger til § 5).

Center for Cybersikkerhed vil således ikke nærmere skulle forholde sig til, om det i en konkret sag er muligt at anvende forvaltningslovens principper om partens aktindsigt, partshøring og begrundelse m.v., som det er tilfældet for Center for Cybersikkerheds øvrige virksomhed.

Dette kan efter instituttets opfattelse 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 Center for Cybersikkerhed undlader at foretage en nærmere vurdering heraf.

Det er på baggrund af beskrivelsen i lovudkastet uklart for instituttet, hvorvidt og i så fald hvilke oplysninger Center for Cybersikkerhed forventer at gøre en part bekendt med. Dette gælder både forinden centeret træffer afgørelse om forbud m.v. og selve begrundelse for en afgørelse.

Det vil særligt 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.

- Institut for Menneskerettigheder anbefaler, at Forsvarsministeriet i lovudkastets bemærkninger tilføjer en forudsætning om, at Center for Cybersikkerhed så vidt muligt overholder principperne i offentlighedsloven og forvaltningslovens kapitel 4-6.

FORBUD PÅ BAGGRUND AF MEDIEOMTALE

Det fremgår af lovudkastet, at Center for Cybersikkerhed skal sikre sig, at sagen er tilstrækkelig oplyst til, at der kan træffes afgørelse om at nedlægge et forbud, og at et forbud normalt ikke alene vil kunne baseres på for eksempel medieomtale af en aftaleindgåelse mellem en teleudbyder og en leverandør (lovudkastets bemærkninger til § 2).

I lovudkastet er det dog fortsat muligt for Center for Cybersikkerhed at træffe afgørelse om at nedlægge et forbud alene på baggrund af medieomtale.

Det vil efter instituttets opfattelse 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 i det mindste være forpligtet til at indgå i en dialog med den virksomhed, som kan risikere at blive mødt at et forbud. Dette gælder så meget desto mere, når centeret har mulighed for at offentliggøre et forbud i ikke-anonymiseret form (lovudkastets § 14, stk. 1).

- 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.

OFFENTLIGGØRELSE I IKKE-ANONYMISERET FORM

Det fremgår af lovudkastet, at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre afgørelser, resuméer af domme eller bødevedtagelser om forbud m.v. og om prøvelse af spørgsmål om ekspropriation (lovudkastets § 14).

Det fremgår videre af lovudkastet, at bestemmelsen har til formål at give teleudbyderne et øget incitament til at overholde reglerne og til at give telekunderne mulighed for at få kendskab hertil. Der er efter Forsvarsministeriets opfattelse tale om et samlet hensyn til statens sikkerhed, som vurderes at udgøre et effektivt redskab, der kan medvirke til at sikre et højt sikkerhedsniveau i den kritiske teleinfrastruktur (lovudkastets bemærkninger til § 14).

Det må efter instituttets opfattelse forventes, at en teleudbyder ikke ønsker offentlighed omkring forbud eller retssager, der vedrører teleudbyderens manglende hensyntagen til statens sikkerhed, med de mulige negative konsekvenser det kan have over for navnlig selskabets kunder.

Det er i det lys problematisk, at Center for Cybersikkerhed kan nedlægge og offentliggøre et 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 er det principielt problematisk, at det er op til Center for Cybersikkerhed at vurdere, om retssager vedrørende ekspropriation skal offentliggøres, da 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. kunne nedlægges.

Det bør af hensyn til forudsigeligheden for de berørte virksomheder beskrives nærmere i bemærkningerne, hvornår Center for Cybersikkerhed kan forventes at ville henholdsvis ikke at ville benytte muligheden for at offentliggøre et forbud m.v. i ikke-anonymiseret form.

Hvis reglerne skal virke præventivt bør det efter instituttets opfattelse være muligt for virksomhederne at indrette sig efter dem.

- Institut for Menneskerettigheder anbefaler, at Forsvarsministeriet i lovudkastets bemærkninger beskriver, hvornår Center for Cybersikkerhed kan forventes at ville henholdsvis ikke at ville offentliggøre forbud m.v. i ikke-anonymiseret form, herunder ved at give eksempler.

Der henvises til ministeriets sagsnummer 2020/008711.

Med venlig hilsen

Mikkel Lindberg Laursen
SPECIALKONSULENT

Til forsvarsministeriet

KL har ingen bemærkninger til den udsendte høring. Men såfremt Center for Cybersikkerhed forbyder visse leverandører og dette får økonomiske konsekvenser for kommunerne, forventer vi disse kompenseret.

Med venlig hilsen
Anne Kathrine Fjord-Marschall

Chefkonsulent
Digitalisering og Teknologi

Weidekampsgade 10
Postboks 3370
2300 København

D +45 3370
E 3797
AKF@kl.dk

T +45 3370 3370
W kl.dk

Københavns Byret

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Præsidenten
Domhuset, Nytorv 25
1450 København K.
Tlf. 99 68 70 15
CVR 21 65 95 09
administration.kbh@domstol.dk
J.nr. 9099.2020.71

Den 4. januar 2021

Ved en mail af 7. december 2020 har Forsvarsministeriet anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

Jeg skal i den anledning på vegne af byretspræsidenterne oplyse, at byretterne ikke ønsker at udtale sig om udkastet.

Det bemærkes dog, at det af udkastets § 7 fremgår, at Center for Cybersikkerheds afgørelser alene kan indbringes for Københavns Byret, samt at der ved afgørelserne skal deltage 3 dommere. Det må forudsættes, at disse sager, der formodes også at kunne vedrøre større multinationale selskabers retligheder, vil blive særdeles ressourcekrævende. Byretten må derfor tage forbehold for, at der tilføres de nødvendige ressourcer.

Der henvises til J.nr. 2020/008711.

Med venlig hilsen

Søren Axelsen

R E T S P O L I T I S K F O R E N I N G

HØRINGSSVAR

Til Forsvarsministeriet

Høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Høringsbrev af 7. december 2020 - med svarfrist 4. januar 2021.

Svar fremsendt pr. mail til fmn@fmn.dk med kopi til nbb@fmn.dk og nls@fmn.dk - att sagsnummer 2020/008732

RPF er ganske enig i, at der hersker et presserende behov for at øge leverandørsikkerheden i den kritiske teleinfrastruktur, og 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.

I offentligheden har især forløbet omkring den kinesiske 5G-udbyder vakt opmærksomhed og for mange understreget behovet for en klar og skærpet lovgivning. Hvor kompliceret og svært gennemskueligt hele dette område er, viser de beretninger, som også har været i medierne - men aldrig er officielt bekræftet - om sikkerhedsudstyr, herunder software, indkøbt af offentlige danske myndigheder hos et schweizisk firma, hvor det så angiveligt viste sig, at firmaet var delvist ejet og styret af amerikanske efterretningsinstanser. I forbindelse med den offentlige omtale af rapporten her i efteråret 2020 fra Tilsynet med Efterretningstjenesterne (TET) kom det endvidere frem, at der fra statslig amerikansk side var drevet spionage rettet mod danske ministerier og industrivirksomheder.

Med den hemmelighedsfuldhed, som udfoldes på dette område, kan det være svært at fastslå, hvad der er sandt eller falsk. Men det kan under alle omstændigheder konkluderes, at der skal udfoldes så stor forsigtighed og så sund skepsis, at man ikke bare henholder sig til, hvem man formelt set er allieret med, og hvem ikke, og det bør den foreslåede lovgivning og lovbemærkningerne tage højde for.

I lovforslaget her opereres der i afsnit 6 med den helt specielle form for hemmelig retspleje, som er kendt fra et par andre sagsområder. Der sker herved 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 ved hver eneste nye og yderligere fravigelse sker der endnu en markant svækkelse af retsstaten. Det paradoksale ved dette lovforslag er, at dets åbenlyse overordnede mål er at beskytte netop denne selvsamme demokratiske retsstat mod angreb.

RPF skal på den baggrund opfordre Folketinget til i forbindelse med behandlingen af lovforslaget at foretage en nøje og grundig gennemgang af alle de områder, hvor denne form for hemmelig retspleje er gældende i Danmark, med henblik på at sammenholde (interrelatere) og genoverveje nødvendigheden af hver enkelt af dem.

København, den 4. januar 2021

Bjørn Elmquist	Celina Justiva	Esben Obel
Formand	Bestyrelsesmedlem	Bestyrelsesmedlem

Forsvarsministeriet har den 7. december 2020 sendt udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur i høring.

Ministeriernes forpligtelse til at høre Rigsrevisionen er fastlagt af rigsrevisorloven, §§ 7 og 10 (Lovbekendtgørelse nr. 101 af 19/01/2012) og angår revisions- og/eller regnskabsforhold, der kan have betydning for Rigsrevisionens opgaver.

Vi har gennemgået lovforslaget og kan konstatere, at det ikke omhandler revisions- eller regnskabsforhold i staten eller andre offentlige virksomheder, der revideres af Rigsrevisionen.

Vi har derfor ikke behandlet henvendelsen yderligere.

Med venlig hilsen

Mette E. Matthiasen
Ledelsessekretariat

Landgreven 4
DK-1301 København K

Tlf. +45 33 92 84 00
Dir. +45 33 92 85 73
mem@rigsrevisionen.dk

www.rigsrevisionen.dk

Forsvarsministeriet
Holmens Kanal 9
1060 København KØ

Rådet for Digital Sikkerheds høring over Udkast til Forslag til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Forsvarsministeriet har sendt udkast til forslag til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur i høring.

Rådet for Digital Sikkerhed finder det positivt, at cybersikkerhed gøres til en parameter i forbindelse med indkøb af komponenter til den kritiske infrastruktur. Det er dog væsentligt, at evt. indgreb overfor væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester sker proportionalt og med retssikkerhed/klagemuligheder.

Rådet for Digital Sikkerhed takker for muligheden for at afgive høringssvar til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur. Det bemærkes dog, at der er tale om en forkortet høringsperiode hen over en juleferie, det er ikke optimalt, specielt ikke når der er tale om indskrænkninger i den almindelige retssikkerhed

Det er vigtigt, at udbydere af *elektroniske kommunikationsnet og -tjenester* infrastruktur har forudsigelige rammer, og at der en markedsbaseret udvikling for at sikre fortsatte investeringer i en robust og sikker dansk teleinfrastruktur uden for indgribende regulering fra myndighedsside. Forslag til lov om leverandørsikkerhed indeholder dog en række indgribende beføjelser, der begrænser aftalefriheden for udbyderne. Aftaler der er indgået på lovlig vis kan blive ændret og udbyderen kan tvinges til at omlægge sin infrastruktur.

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.

<u>Rådets holdning:</u>

- *Proportionalitet*: Der er behov for proportionalitets overvejelser når myndighederne på denne måde griber ind i og endda forhindrer markedet i at fungere. Indgrebsmuligheden 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
- *Retssikkerhed:* Der skal være retssikkerhedsmæssige garantier for leverandørerne.

    - Der skal være mulighed for at leverandører kan klage over afgørelser, og klageretten bør ikke kunne tilsidesættes politisk ligesom der skal være mulighed for partshøring og begrundelse for afgørelserne.
    - Afgørelser om forbud bør kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige. Der bør indføres regler om effektiv prøvelse af afgørelser og tilsyn med Center for Cybersikkerhed.
    - Endvidere skal forbudsbeslutninger foretages af Forsvarsministeren efter indstilling fra CFCS og høring af andre relevante myndigheder.
- *Erstatning:* 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. Derudover kan det kun være for 'allerede indgåede aftaler' og fordi man har besluttet at gennemføre loven med tilbagevirkende kraft
- *Regulatorisk forudsigelighed:* Gennemtvinges en forceret omlægning, kan det påvirke den sikkerhedsmæssige stabilitet i infrastrukturen og medføre store omkostninger for udbyderne. Dette kan have alvorlige økonomiske konsekvenser og også påvirke incitament for leverandørerne til at udvikle innovative løsninger. Det er væsentligt at disse omkostninger holdes nede også af hensyn til brugerne af disse tjenester, da disse i sidste ende risikeres at bliver væltet over på bruger af tjenesterne.
- Det bør altid vurderes, om *leverandørsikkerhed kan opnås på en mindre indgribende måde.*
- *EU harmonisering:* det giver ikke mening med den danske forsimpling af kritisk eller ikke kritisk infrastruktur, når EU arbejder med flere nuancer.

Om loven:

Det fremgår af lovforslaget, at CfCS kan forbyde udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at anvende givne leverandører:

- § 2. Center for Cybersikkerhed kan i særlige tilfælde forbyde en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at indgå en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, såfremt aftalen vurderes at udgøre en trussel mod statens sikkerhed.
- Ligesom CfCS jf § 3 kan forbyde teleudbydere, at opretholde en indgået aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf,
- Forsvarsministeren kan bestemme, at der af sikkerhedsmæssige grunde ikke udleveres kopi til den særlige advokat (der varetager interesser for parten/teleudbyderen) – jf §8 stk. 3.

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed

Forsvarsministeriet
Att.: Specialkonsulent Nicklas B. Baumgarten
Sendt pr. e-mail til nbb@fmn.dk

4. januar 2021

Høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Teleindustrien (TI) har noteret sig, at Forsvarsministeriet den 7. december 2020 har sendt udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur i høring med frist kl. 12, den 4. januar 2021.

TI finder det positivt, at regeringen sætter fokus på den digitale infrastrukturs samfundskritiske funktion. Forslaget 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.

En velfungerende og sikker teleinfrastruktur er afgørende for det danske samfund, teleselskabernes kunder og naturligvis også branchen selv. Med det afsæt har branchen over de seneste 10 år investeret 70 mia. kr. i at udbygge den digitale infrastruktur i Danmark med fokus på både kapacitet og sikkerhed. Udbygningen er sket i tæt dialog med danske myndigheder, herunder særligt Center for Cybersikkerhed. Det er med dette udgangspunkt, at nedenstående høringssvar skal læses.

Generelt
Forudsigelige rammer og en markedsbaseret udvikling har siden telemarkedets liberalisering været grundlæggende politiske og regulatoriske principper, der har ført til massive investeringer i en robust og sikker dansk teleinfrastruktur.

Lovudkastet indeholder imidlertid en række vidtrækkende beføjelser, som er yderst indgribende i aftalefriheden for TI's medlemmer, og som potentielt kan medføre, at en teleudbyder, der har støttet ret på en lovlig indgået aftale, kan blive tvunget til at omlægge sin infrastruktur. En forceret omlægning kan indvirke negativt på den operati-

onelle og sikkerhedsmæssige stabilitet af telenettet og kan medføre omkostninger i milliardklassen.

Dertil kommer, at konkurrencen blandt leverandører af teleinfrastruktur er afgørende for, at der fortsat er incitament for leverandørerne til at udvikle innovative løsninger og sikre, at omkostningerne holdes nede, hvilket i sidste ende er til gavn for brugerne af tjenesterne på markedet og samfundet som helhed.

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.

Tilmed lægges der op til, at Danmark indfører et af de mest restriktive og uforudsigelige forbudsregimer i EU, hvilket i sig selv vil betyde, at nogle af de mest innovative netværksleverandører vil fravælge Danmark. Det vil andet lige betyde højere priser og mindre innovative produkter til de danske forbrugere.

Det er derfor helt afgørende for TI, at det endelige lovforslag tilrettes således, at der skabes en langt højere grad af regulatorisk forudsigelighed, tilstrækkelige retssikkerhedsmæssige garantier for teleudbyderne, og at indgrebsmuligheden alene anvendes helt undtagelsesvis og efter en nøje vurdering af truslen mod statens sikkerhed på den ene side og de operationelle sikkerhedsaspekter samt markedsmæssige konsekvenser på den anden side.

Efter TI's opfattelse bør lovforslaget som minimum tilrettes på følgende centrale punkter:

1) Forbudsbeslutninger skal foretages af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og høring af andre relevante myndigheder.
2) Teleudbyderne skal sikres mulighed for partshøring og begrundelse for afgørelserne.
3) Afgørelser om forbud kan kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige.
4) Lovens tilbagevirkende kraft for aftaler indgået før 7. december 2020 udgår eller udskydes til tidligst 1. januar 2030.
5) Teleudbyderen 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.
6) Der skal indføres regler om effektiv prøvelse af afgørelser og tilsyn med Center for Cybersikkerhed.
7) Definitionen af "kritisk infrastruktur" er uklar og skal præciseres væsentligt.

TI har i det følende nærmere redegjort for disse overordnede punkter. Derudover følger en række yderligere forslag til præcisering af lovud-

kastet for at sikre en nødvendig og højere grad af forudsigelighed for teleudbyderne.

Ad 1) Forbudsbeslutninger skal foretages af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og høring af andre relevante myndigheder

TI har i forbindelse med vedtagelsen af CFCS-loven og lov om net- og informationssikkerhed kritiseret, at tilsynet med telesektoren er lagt i en forvaltningsmyndighed under Forsvarets Efterretningstjeneste og ikke som al anden erhvervsrettet lovgivning i den civile del af forvaltningen. Det medfører, at reguleringen af telesektoren på dette område ikke ses i sammenhæng med den øvrige regulering, og at selskaberne ikke har den nødvendige sikkerhed for inddragelse af andre samfundshensyn end snævre militære strategiske overvejelser.

Det er fortsat TI's 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. TI er dog opmærksom på, at en sådan ressortændring næppe er mulig inden for den tidsramme, der er sat for det fremlagte lovudkast.

Der er imidlertid med lovudkastet tale om meget indgribende foranstaltninger, der kan have vitale markedsmæssige konsekvenser, og som foretages på grundlag, som udbyderne ikke har indsigt i, hvilket stiller udbyderne i en svag retssikkerhedsmæssig position.

Det er derfor nødvendigt, at indgrebsmuligheden alene anvendes helt undtagelsesvis og efter en nøje vurdering af truslen mod statens sikkerhed på den ene side og de markedsmæssige konsekvenser på den anden side. Det bør derfor sikres, at en beslutning om forbud forberedes grundigt og træffes på højeste niveau i ministeriet. Efter opsplitningen af den tidligere IT- og Telestyrelse er kompetencer og viden om telebranchen i dag spredt på en række myndigheder. Energistyrelse, Erhvervsstyrelsen og Konkurrence- og Forbrugerstyrelsen har alle indgående kendskab til tekniske og markedsmæssige forhold på teleområdet og bør derfor høres, inden der træffes afgørelse. TI skal derfor opfodre til, at en afgørelse om forbud træffes af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og efter høring af andre relevante ministerier og myndigheder.

Der henvises i øvrigt til det lovforslag, der er sendt i høring af Erhvervsstyrelsen den 9. december 2020 om lov om screening af visse udenlandske direkte investeringer m.v. i Danmark (Investeringsscreeningsloven)[1], hvor afgørelser om forbud mod investeringer træffes af Erhvervsministeriet efter indstilling fra Erhvervsstyrelsen og høring af andre relevante myndigheder.

Det fremgår af rapporten fra den tværministerielle arbejdsgruppe[2] (s. 153 ff), der er udarbejdet forud for udkastet til Investeringsscree-

[1] https://hoeringsportalen.dk/Hearing/Details/64672

[2] Rapprt om en kommende generel ordning for screening af udenlandske investeringer mv. (windows.net)

ningsloven, at det er arbejdsgruppens anbefaling, at forbudsbeslutninger træffes af ministeriet og efter høring af andre relevante myndighederne. Det begrundes bl.a. i, at et forbud er vidtgående og andre lande, som Finland, Frankrig og Tyskland, Norge og USA, der har indført regler om forbud mod investeringer ikke har delegeret kompetencen for at træffe afgørelser om forbud væk fra ministeriet.

Der er vanskeligt at se, hvorfor samme hensyn ikke skal tages i forhold til indgreb overfor leverandører af kritisk teleinfrastruktur, henset til at indgrebet for den enkelte virksomhed kan have mindst lige så indgribende karakter som et indgreb mod udenlandske investeringer.

TI skal derfor henstille til, at lovforslaget ændres, så kompetencen til at træffe afgørelser om forbud mod visse leverandører ligger hos ministeriet.

Ad 2) Teleudbyderne skal sikres mulighed for partshøring og begrundelse for afgørelserne

Det fremgår af lovudkastet § 5, at offentlighedsloven (bortset fra lovens § 13), og forvaltningslovens kapitel 4-6 ikke finder anvendelse.

Efter lovbemærkningerne til lovforslaget (s. 16-17) må det forstås, at undtagelsen fra offentlighedsloven og forvaltningslovens principper om partshøring og begrundelse af afgørelser er mere vidtgående end den undtagelse, der er gælder i forhold til Center for Cybersikkerheds øvrige virksomhed, hvor det er forudsat, at centeret trods den generelle undtagelse til forvaltningsloven og offentlighedsloven i det væsentlige skal efterleve de forvaltningsretlige retssikkerhedsprincipper om partshøring og begrundelse. Der er således tale om en meget vidtgående indskrænkning i teleudbydernes retstilling og mulighed for at varetage deres interesser.

Det er efter TI's opfattelse stærkt kritisabelt, at teleudbyderne dermed afskæres fra helt grundlæggende retssikkerhedsgarantier. Dette skal særligt ses i forhold til, at et forbud efter lovudkastet vil være langt mere indgribende end de foranstaltninger, Center for Cybersikkerhed kan påbyde efter lov om net- og informationssikkerhed. Der er derfor i højere grad behov for, at teleudbydernes retssikkerhed styrkes og ikke indskrænkes.

TI har selvsagt forståelse for, at der kan være oplysninger, der indgår i vurderingen af, om en leverandør udgør en trussel mod statens sikkerhed, som af hensyn til nationale og internationale sikkerhedsinteresser ikke kan videregives til den teleudbyder, der er part i sagen. Det begrunder dog ikke, at partshøring og begrundelse for afgørelsen helt undtages.

I udkastet til Investeringsscreeningsloven, hvor Erhvervsstyrelsen og Erhvervsministeriet skal foretage sagsbehandling af tilsvarende for-

hold, er der ikke lagt op til en generel undtagelse for forvaltningslovens kap 4-6.

Det fremgår bl.a. således af lovbemærkningerne til § 38 i udkastet til Investeringsscreeningsloven (s. 92):

> *"Samtidig er det også væsentligt i videst muligt omfang at beskytte rettighederne for parterne i sagen, og ikke fravige mere fra reglerne i offentlighedsloven og forvaltningsloven end nødvendigt. Parterne i sager efter loven bør derfor som udgangspunkt have mulighed for at blive gjort bekendt med oplysninger i sagen, herunder navnlig oplysninger om deres personlige forhold. Der bør derfor kun være mulighed for at afskære fra partsaktindsigt i det omfang hensyn til national sikkerhed og offentlig orden efter en konkret vurdering gør det nødvendigt. Endvidere bør øvrige regler om sagsbehandling i offentlighedsloven og forvaltningsloven, der ikke vedrører aktindsigt, gælde også for sager efter denne lov."*

Sammenholdes de to lovudkast, vil den foreslåede retstilstand betyde, at danske teleudbydere opnår en ringere retsbeskyttelse end udenlandske parter, der ønsker at investere i et selskab, der råder over kritisk infrastruktur.

Det bemærkes endvidere, at det fremgår af udkastet til lovforslag om leverandørsikkerhed § 2, stk. 2, og § 3, stk. 4, at Center for Cybersikkerhed kun kan nedlægge forbud, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

For at Center for Cybersikkerhed kan foretage den vurdering, 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.

Det fremgår af bemærkningerne (s. 33), at

> "*Bestemmelsen [§ 2] typisk vil finde anvendelse, efter at der gennem længere tid har været dialog mellem teleudbyderen og Center for Cybersikkerhed om den pågældende aftale*."

Dette finder TI positivt, men forudsætningen om forudgående partshøring af teleudbyderen bør indføres direkte i loven.

På den baggrund skal TI henstille til, at lovudkastets § 5 udgår og erstattes med tilsvarende regler, som fremgår af § 38 i udkastet til Investeringsscreeningsloven.

Ad 3) Afgørelser om forbud skal kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige.

Det fremgår af § 2, stk. 2, og § 3, stk. 4, at det er en forudsætning for et forbud, at Center for Cybersikkerhed konkret har vurderet, at hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger end et forbud. Det fremgår i tilknytning hertil af lovbemærkningerne (s. 14f), at det således vil være en forudsætning, at Center for Cybersikkerhed har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen, som vil være nødvendige, for at den ikke længere vurderes at udgøre en trussel mod statens sikkerhed. Center for Cybersikkerhed vil også skulle have vurderet relevante muligheder i net- og informationssikkerhedsloven, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

TI er enig i, at et forbud ikke bør udstedes, før andre mindre indgribende foranstaltninger har været bragt i anvendelse.

Det gælder særligt i en situation, hvor teleudbyderen har indgået en aftale, efter aftalen har været anmeldt iht. lov om net- og informationssikkerhed, og Center for Cybersikkerhed ikke har fundet anledning til at udstede påbud efter lov om net- og informationssikkerhed. I en sådan situation (uanset om aftalen er indgået før eller efter lovudkastet er bragt i høring) har teleudbyderen indrettet sig i tillid til, at aftalen og de eventuelle iværksatte sikkerhedsforanstaltninger, som teleudbyderen har foretaget, ikke udgør nogen trussel mod statens sikkerhed.

Der bør derfor stilles skærpede krav til, hvornår et forbud efter § 3, stk. 1 og 2, kan bringes i anvendelse overfor allerede indgåede aftaler. TI har noteret sig, at det er en forudsætning for anvendelsen af § 3, at der ikke blot kan konstateres en trussel mod statens sikkerhed, som er tilfældet med forbud efter § 2, men at truslen skal være ”væsentlig”. Der er dog ikke nogen kvalificering af væsentlighedsbegrebet i lovens bemærkninger, idet de eksempler, der henvises til i lovbemærkningerne (s. 37), ikke adskiller sig fra de forhold, som kan begrunde et indgreb efter § 2. Kriteriet om, at der skal foreligge en ”væsentlig” trussel mod statens sikkerhed, udgør således ikke nogen reel beskyttelse af teleudbyderne.

Tilsvarende bør der tages særlige hensyn forud for anvendelse af forbud efter § 2 overfor aftaler, der vedrører en forlængelse eller genforhandling af eksisterende aftaler.

Et forbud mod indgåelse af en forlængelse af en aftale om fx support eller reservedele til udstyr, der er leveret iht. en allerede indgået aftale, kan være nødvendig for, at det allerede leverede udstyr fortsat kan anvendes. Det er helt sædvanligt, at sådanne supportaftaler ikke indgås med en varighed, der svarer til udstyrets levetid, og det derfor er nødvendigt med en løbende tilpasning af disse aftaler. Et forbud mod indgåelse af en sådan aftale om forlængelse eller genforhandling

kan derfor de facto medføre, at det allerede leverede og lovlige udstyr er ubrugeligt, og dermed tvinges udbyderen til at udskifte fuldt lovligt udstyr. Udbyderen kan også stå i en situation, hvor den operationelle stabilitet og sikkerhed påvirkes negativt, hvis eksisterende udstyr ikke længere må bruges, men ikke kan udskiftes, fordi der ikke umiddelbart er en anden mulig leverandør.

Tilsvarende gør sig gældende i forhold til softwareopdateringer, for eksempel sikkerhedsopdateringer, platformsudvidelser eller andre nødvendige funktionelle opdateringer til systemet til sikring af dets fortsatte drift og support af markedsinitiativer. Sådanne naturlige forlængelser og udbygninger af eksisterende aftaler, som er indgået i god tro før 7. december 2020 og under Center for Cybersikkerheds tilsyn i medfør af lov om net- og informationssikkerhed, bør som udgangspunkt ikke betragtes som værende omfattet af forbud efter § 2. Denne problemstilling forværres desuden af lovforslagets meget uklare definition af begrebet "kritisk infrastruktur", der potentielt kan omfatte stort set alle IT-systemer, der anvendes i en teleudbyders forretning, jf. nedenfor.

TI skal opfordre til, at det direkte fremgår 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.

Ad 4) Lovens tilbagevirkende kraft for aftaler indgået før 7. december 2020 udgår eller udskydes til tidligst 1. januar 2030.
Det fremgår af udkastet til lovforslag § 17, stk. 3, at loven får tilbagevirkende kraft på aftaler indgået før 7. december 2020. Som begrundelse herfor anføres det i lovbemærkningerne (s. 14):

> *Endvidere finder Forsvarsministeriet, at også aftaler, der er indgået før høringstidspunktet, bør omfattes af reguleringen fra den 1. januar 2026. Det er ministeriets vurdering, at meget få aftaler vil have så lang løbetid, men ordningen vil sikre, at der bliver mulighed for at tage stilling til, om sådanne aftaler skal forbydes, dog således, at teleudbyderne har haft næsten fem år til at indrette sig på, at aftalerne bliver omfattet af den skærpede regulering.*

TI skal gøre opmærksom på, at det ikke er korrekt, at teleudbyderne allerede ved lovens fremsættelse kan begynde at indrette sig, da det er fuldstændig uklart, hvilke lande og hvilke specifikke leverandører Center for Cybersikkerhed anser for at udgøre en trussel mod statens sikkerhed. Først når den viden er konkretiseret og kommunikeret til udbyderne, kan de begynde at lægge planer for udskiftning af allerede leveret infrastruktur.

Det er i øvrigt underordnet, at der er tale om få aftaler, der vil have så lang løbetid. Det er de enkelte aftalers omfang og det leverede udstyrs levetid, der er relevant, og selv om der vil være tale om få aftaler samlet set, så er de grundlaget for betydelige dele af infrastrukturen i på det danske marked.

Det bemærkes i den forbindelse, at Center for Cybersikkerhed har et indgående kendskab til de leverandøraftaler, der anvendes på det danske marked, samt hvilke aftaler der fra 7. december 2020 er på vej til at blive indgået. Det bør derfor 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 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.

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 og udfasning af tidligere leverandører. En sådan proces vil 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.

En forceret udfasning kan også 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 bemærkes i øvrigt, at den britiske regering med en beslutning fra november 2020[3] har meddelt operatørerne på det britiske marked, at RAN-udstyr fra en navngiven leverandør skal være ude af mobilnettene pr. 1. januar 2028. Det er værd at bemærke, at forbuddet alene omfatter en specifik leverandørs leverancer af RAN-udstyr i mobilnetværkene, og at perioden er mere end 2 år længere end den, der lægges op til i det danske lovforslag.

TI skal på den baggrund opfordre til, at lovens tilbagevirkende kraft helt opgives eller alternativt tidligst får virkning fra 1. januar 2030.

Tilsvarende bør lovens ikrafttrædelse udskydes for aftaler om forlængelse eller genforhandling af eksisterende aftaler indgået før 7. december 2020, idet et forbud mod indgåelse af sådanne aftaler de facto vil medføre, at allerede lovligt leveret udstyr vil være ubrugeligt, jf. bemærkningerne ovenfor.

---

[3] https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

Ad 5) Teleudbyderen 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

Det er positivt, at der i lovudkastet § 4 er taget stilling til, at der skal ydes fuld erstatning i tilfælde af afgørelser, der efter loven udgør et ekspropriativt indgreb.

Ved en nærmere gennemgang af lovbemærkningerne er det dog uklart, hvornår der er tale om ekspropriation, og hvordan grundlovens begreb "fuldstændig erstatning" skal forstås i forbindelse med ekspropriation efter lovforslaget.

Det fremgår også af bemærkningerne, at det er Forsvarsministeriets vurdering, at det er et begrænset antal afgørelser, hvor der vil være tale om ekspropriation.

Det fremgår således af bemærkningerne (bl.a. s. 21):

> *Navnlig det forhold, at forbud mod indgåelse af en aftale efter § 2, stk. 1, opretholdelse af en indgået aftale efter § 3, stk. 1, eller anvendelse af kritiske komponenter, systemer m.v. efter § 3, stk. 2, er begrundet i hensyn til statens sikkerhed, må antages at tale med en vis vægt imod, at der vil være tale om ekspropriation.*
> *(TI's understregning)*

Dette synes ikke at give nogen stor sikkerhed for, at indgreb med afståelse af ejendomsret til følge formelt vil blive betragtet som et ekspropriativt indgreb. De anførte bemærkninger giver dermed ikke noget reelt incitament for Center for Cybersikkerhed til at træffe forbudsafgørelser, hvor der er sikret den rette proportionale balance mellem statens sikkerhed og hensynet til teleudbydernes ejendomsret og investeringer.

Dertil kommer, 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.

Der er TI's klare opfattelse, at et forbud mod direkte eller indirekte anvendelse af allerede leveret og lovligt udstyr vil udgøre et ekspropriativt indgreb.

TI 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.

Ad 6) Der skal indføres regler om effektiv domstolsprøvelse af afgørelser og tilsyn med Center for Cybersikkerhed

Det fremgår af lovudkastet §§ 6 og 7, at Center for Cybersikkerheds afgørelser ikke kan påklages til anden administrativ myndighed, og at eneste prøvelse af afgørelserne kan foretages af domstolene. Med de begrænsninger, der fremgår af §§ 8-13, er der tilmed tale om en begrænset prøvelse af grundlaget for afgørelserne.

TI mener, at en indbringelse af en forbudsafgørelse for domstolene automatisk bør få opsættende virkning. En domstolsprøvelse uden opsættende virkning kan have den konsekvens, at teleoperatøren, uanset udfaldet af retssagen, vil være nødt til at enten slukke eller nedtage og udskifte den del af netværket, som er omfattet af tvisten. 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. Sådanne skadegørende virkninger af en ulovlig afgørelse vil ikke fuldt ud kunne kompenseres ved, at der ydes en økonomisk erstatning til den udbyder, det går ud over.

TI mener i øvrigt, at lovudkastet skal tilrettes således, at der gives teleudbyderen mulighed for fuld partsrepræsentation ved egen advokat. Med den foreslåede § 9 afskæres udbyderne imidlertid for 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 gøre det nærmest umuligt for udbyderne at bidrage til sagens oplysning. Selv når en dommer har besluttet, at relevante oplysninger skal forelægges for udbyderen, kan Forsvarsministeren afskære adgangen til de pågældende oplysninger, selvom de har været afgørende for forbudsafgørelsen, jf. § 9, stk. 3.

I forbindelse med prøvelse af en afgørelse er det 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. Det bør derfor kun være indholdet af de fortrolige oplysninger om statens sikkerhed, der ikke må drøftes med udbyderen. I det omfang, udbyderen har sikkerhedsgodkendt personale, bør det desuden være muligt at drøfte sådanne oplysninger med udbyderen.

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 være, at oplysningerne ikke kan indgå i prøvelsen, og dermed ikke vil kunne tillægges vægt ved domstolens vurdering af, om forbuddet er lovligt.

Center for Cybersikkerheds administration af loven bør også underlægges et effektivt tilsyn. Henvisningen i lovbemærkningerne (s. 11) til Tilsynet med Efterretningstjenesterne kan give det misvisende ind-

tryk, at Tilsynet med Efterretningstjenesterne også fører tilsyn med Center for Cybersikkerheds aktiviteter efter lov om leverandørsikkerhed. Det er imidlertid ikke tilfældet. Henset til, at der i forbudsafgørelser efter lovforslaget vil være oplysninger, som ikke kan deles med udbyderen, ligesom Center for Cybersikkerhed i dialogen med udbyderne forud for en eventuel forbudsafgørelse uretmæssigt kan få udbyderen til at give tilsagn om at implementere byrdefulde sikkerhedsmæssige foranstaltninger, bør der føres et effektiv tilsyn med, at Center for Cybersikkerhed forvalter sine beføjelser i overensstemmelse med lovens hensigt.

TI skal derfor anbefale, 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.

Ad 7) Definitionen af "Kritisk infrastruktur" er uklar og skal præciseres væsentligt

Det er afgørende, at der er en klar og entydig definition af begrebet kritisk infrastruktur og kritiske netkomponenter.

Den nuværende definition i lovudkastet § 1, nr. 1, svarer til samme definition i lov om net- og informationssikkerhed. Definitionen er meget bred, og de anvendte begreber som fx "operations support systemer" og "business support systemer" udgør ikke nogen entydig branchemæssig forståelse, hvorved stort set alle IT-systemer, der anvendes i en teleudbyders forretning, herunder tjenesteudbydere, der ikke har eget netværk, men anvender egne support-systemer, bliver omfattet af loven.

Det er også uklart, hvad der forstås ved "centrale routere og servere i backbonenettet". Der er ingen afgrænsning af, hvad der er "centrale" og "ikke-centrale" routere. Udbyderne er således overladt til Center for Cybersikkerheds uforudsigelige vurdering af, om et netværkselement er omfattet.

Det er tilsvarende uklart, hvad der menes med "hardware […], der anvendes i core-net". Det er uklart, om det også betyder, at fx passive dele som fiberkablerne i et core-net omfattes, selvom et fiberkabel vanskeligt kan indeholde aflytningsudstyr eller kan kompromitteres af leverandøren.

TI skal opfodre 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.

Yderligere bemærkninger

Ud over ovennævnte bemærkninger har TI i det følgende oplistet en række yderligere forslag til præcisering af lovudkastet for at sikre en højere grad af forudsigelighed for teleudbyderne.

Pligtsubjekter - konkurrenceforvridning
TI har noteret, at loven alene finder anvendelse på "væsentlige erhvervsmæssige udbydere", jf. § 1, nr. 3. Dermed falder fx ejere af private netværk udenfor for lovens anvendelsesområde. Dette skal sammenholdes med, at mobiludbyderne står overfor en kommende auktion af nye frekvenser, hvorefter en udbyder sandsynligvis vil blive forpligtet til at stille frekvensressourcer til rådighed for private netværk gennem erhvervelse af en frekvensmængde afsat til dette formål. En sådan udnyttelse til private formål vil i praksis blive relevant, hvis mobiludbyderne ikke tilbyder de specialtjenester, som de private virksomheder efterspørger. Hvis kun mobiludbyderne forbydes at anvende udstyr fra visse leverandører, kan der opstå en konkurrenceforvridende situation ved, at de private virksomheder kan indgå aftaler med de selvsamme leverandører, som udbyderne er afskåret fra at anvende.

Såfremt udkastet til lovforslag fastholdes, bør det sikres, at et forbud mod anvendelse af en bestemt leverandør også gælder for ejere af private net, der anvender frekvenser, der er tildelt en udbyder ved udbud eller auktion.

Trussel mod statens sikkerhed – uklare og uforudsigelige kriterier
Kriterierne i § 2 for vurdering af, om der foreligger en "trussel mod statens sikkerhed", er uklare og uforudsigelige. Der mangler indsigt i, hvordan de fire kriterier skal fortolkes. Der henvises i lovbemærkningerne til, at kriterierne er objektive, men reelt er de meget brede og uigennemskuelige. Dette medfører en meget stor regulatorisk usikkerhed for såvel teleselskaber som udstyrsleverandører.

Det ser imidlertid ud til, at der skal meget lidt til at bringe forbud i anvendelse. Det fremgår fx af § 2, stk. 1, nr. 4, at en aktør kan anses for at udgøre en trussel mod statens sikkerhed, hvis aktøren har været involveret i aktiviteter, der har medført "en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden." Kriteriet er cirkulært formuleret, idet det åbenbart kan være en trussel mod statens sikkerhed, hvis aktøren har haft en negativ påvirkning af statens sikkerhed. Derudover kan selv en undskyldelig fejl i et stykke software udgøre en "negativ påvirkning af informationssikkerheden", og dermed være en trussel mod statens sikkerhed. Det er vanskeligt at se, at der heri er tale om objektive og klare kriterier.

Sammenholdes dette med udkastet til Investeringsscreeningsloven, synes der at være noget højere krav til, at et forbud efter Investeringsscreeningsloven kan tages i anvendelse. Det fremgår således heraf, at et forbud forudsætter, at den "Nationale sikkerhed" eller den "Offentlige orden" er truet, og begge begreber er udførligt afgrænset i loven og dens bemærkninger. Eksempelvis er den "Nationale sikkerhed" eksplicit defineret i lovudkastets § 4, stk. 1, nr. 1 med følgende afgrænsning:

> *Forhold der vedrører Danmarks territorielle integritet og befolkningens overlevelse, risikoen for forstyrrelse af internationale relationer eller nationernes fredelige sameksistens samt trusler mod militære interesser, samt handlinger, der har til hensigt at forvolde Danmark skade, som er i strid med hensynet til national sikkerhed, herunder forbrydelser mod statens selvstændighed eller forbrydelser mod statsforfatningen og de øverste statsmyndigheder*

TI skal derfor henstille til, at der bringes overensstemmelse mellem begreberne i hhv. Leverandørsikkerhedsloven og Investeringsscreeningsloven for at undgå tvivl om, hvad der forstås ved hhv. "Statens sikkerhed" og "National Sikkerhed".

Det fremgår derudover af lovudkastet § 2, stk. 1, at Center for Cybersikkerhed i sin vurdering af en leverandør kan lægge vægt på "*aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren*". Det er dog uklart, hvad der forstås ved "kontrol" og "betydelig indflydelse". Det er nærliggende at antage, at begrebet må forstås i overensstemmelse med selskabslovens § 7 om "bestemmende indflydelse", men da det ikke er nærmere forklaret i lovbemærkningerne, skal TI henstille til, at dette præciseres.

Det er heller ikke klart for TI, hvilke lande Danmark har indgået sikkerhedsaftaler med, og som dermed i tilstrækkeligt omfang opfylder kriteriet. Dermed er det ikke muligt at vurdere, om en leverandør opfylder kriteriet i § 2, stk. 1, nr. 1. Og eftersom dette kan ændre sig, og Center for Cybersikkerhed får hjemmel til at forbyde opretholdelsen af allerede eksisterende aftaler, er der brug for adgang til en liste, der kontinuerligt opdateres.

Det synes derudover ikke nærmere defineret, hvad der forstås ved begrebet "tilsvarende sikkerhedssamarbejder". Af bemærkningerne til bestemmelsen fremgår således kun:

> *"Bestemmelsen omfatter også tilsvarende sikkerhedssamarbejder, hvor der ikke nødvendigvis er indgået en formel sikkerhedsaftale. Mere indirekte sikkerhedssamarbejder, der f.eks. indgås via internationale organisationer, vil ikke være omfattet af begrebet tilsvarende sikkerhedssamarbejder.*
>
> *En eventuel fastlæggelse, af hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, foretages af Center for Cybersikkerhed efter en konkret vurdering."*

Fraværet af en konkret og brugbar definition sammenholdt med, at kredsen af potentielt omfattede lande fastlægges af Center for Cybersikkerhed fra sag til sag, gør i store træk bestemmelsen uanvendelig som vejledning for såvel teleudbydere som udstyrsleverandører.

Tilsvarende har udbyderne heller ikke indsigt i, hvilke lande det efter lovgivningen er muligt at pålægge leverandører eller deres underleve-

randører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage. Det er fx uklart, om amerikanske selskaber og underleverandører har forpligtelser i forhold til NSA, og om NSA har aktiviteter i Danmark, som kan karakteriseres som spionage[4].

Der fremgår også af kriterierne i § 2, stk. 1, nr. 2 og 3, at der udover lande, hvor leverandøren er hjemmehørende, også kan lægges vægt på lande, hvor produktionen eller driften varetages fra. Det er uklart, hvad denne sondring indebærer, idet næsten alle leverandører fra vestlige lande, som Danmark formentlig har en aftale om sikkerhedssamarbejde med, har henlagt hele eller dele af deres produktion til ikke-vestlige lande, som Danmark formentlig ikke har en sikkerhedsaftale med. Det er uklart, om teleudbyderne kan indgå aftaler med sådanne leverandører uden risiko.

TI foreslår derfor, at Center for Cybersikkerhed med loven forpligtes til løbende at udarbejde og offentliggøre en oversigt over lande og producenter, som potentielt udgør en trussel mod statens sikkerhed.

Ikke-anonyme afgørelser
Center for Cybersikkerhed kan efter lovudkastet § 14, stk. 1, beslutte at offentliggøre ikke-anonyme afgørelser.

Det fremgår af lovbemærkningerne, at formålet hermed er at udstille de udbydere, der vælger at indgå aftaler med leverandører, der udgør en trussel mod statens sikkerhed.

Henset til, at kriterierne for, hvornår loven kan finde anvendelse, er uklare og uigennemskuelige, er det helt urimeligt, at Center for Cybersikkerhed kan anvende offentliggørelse af en afgørelse som pression. Det gælder særligt i tilfælde, når et forbud er nedlagt efter lovudkastets § 3, hvor udbyderen har indgået en aftale uden, at Center for Cybersikkerhed på forhånd har nedlagt forbud, og hvor der på tidspunktet for aftaleindgåelse ikke forelå omstændigheder, der udgjorde en trussel mod statens sikkerhed.

TI skal derfor opfodre til, at lovudkastets § 14 udgår.

Stand-still periode udvides
Af § 18 i lovudkastet fremgår det, at "Stand still-perioden" i net og informationssikkerhedsloven § 4 udvides fra 10 til 25 arbejdsdage. Isoleret set kan det umiddelbart anses som rimeligt, da en saglig vurdering af et muligt forbud vanskeligt kan gennemføres på 10 arbejdsdage.

Denne forlængelse skal dog ses i lyset af, at teleudbyderne efter net- og informationssikkerhedslovens § 4, nr. 2, 1. punkt, og § 3 i bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed skal underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger med en leverandør, og Center

[4] Se fx https://www.dr.dk/nyheder/indland/hemmelige-rapporter-usa-spionerede-mod-danske-ministerier-og-forsvarsindustri

for Cybersikkerhed på den baggrund kan påbyde udbyderen at indsende et færdigt udkast til aftale til centeret. Centeret kender således til aftaleforhandlingerne lang tid før, et færdig udkast til aftale indsendes til centeret.

Der dog ikke i lovgivningen fastsat nogen frist for, hvornår Center for Cybersikkerhed skal give et påbud om at få det færdigt udkast til aftale indsendt.

Teleudbyderen kan således stå i en situation, hvor centeret ikke har reageret på en underretning om opstart af forhandlinger med en leverandør, og udbyderen kan dermed have indrette sine forhandlinger på, at aftalen kan indgås uden anmærkninger fra Center for Cybersikkerhed.

Det vil i en sådan situation være helt urimeligt, hvis centeret har forholdt sig passivt og umiddelbart før aftaleforhandlingernes afslutning kan udstede et påbud om indsendelse af aftalen og tilmed anvende 25 arbejdsdage (5 uger) på at behandle forhold, som med rimelighed kunne være afdækket tidligere i forløbet.

TI skal derfor foreslå, at der i stedet for en forlængelse af fristen i lovens § 4 indsættes en bestemmelse om, at Center for Cybersikkerhed senest 20 arbejdsdage efter, underretning er foretaget, skal træffe afgørelse om i) et færdigt udkast til aftale skal indsendes til Center for Cybersikkerhed, ii) hvilke påtænkte påbud CFCS agter udstede, hvis aftale med leverandøren indgås eller iii) at Center for Cybersikkerhed vil indstille til Forsvarsministeriet, at der skal nedlægges forbud efter leverandørsikkerhedslovens § 2. Såfremt konkrete forhold ikke gør det umuligt for Center for Cybersikkerhed at træffe en afgørelse inden for fristen, kan der gives Center for Cybersikkerhed mulighed for at forlænge fristen med fx 2 gang 10 arbejdsdage.

Med en sådan ordning, vil udbyderen kunne få en vis sikkerhed for, om det kan betale sig at indlede forhandlinger med en leverandør, og såfremt forhandlingerne indledes, kan det endeligt afklares inden for 50 arbejdsdage (20+10+10+10) eller ca. 2 ½ måned, om der udstedes et forbud mod leverandøren.

Der mangler kompenserende initiativer og fælles europæiske koordinering

Som det er anført ovenfor, vil en begrænsning af leverandører på markedet medføre betydelig risiko for, at konkurrencen mindskes på udstyr, hvilket vil medføre øgede omkostninger, mindre innovation og højere priser til kunderne.

Hvis Folketinget vælger at vedtage lovforslaget, må der politisk tages initiativer til at adressere den manglende konkurrence, som dette utvivlsomt vil medføre, og som kan have langtrækkende betydning for både det danske og det europæiske telemarked. Der kan fx henvises til den Britiske regering, der har været meget bevidst om denne problemstilling og blandt andet har nedsat et udvalg med deltagelse

fra branchen til at vurdere, hvordan man kan få flere leverandører ind på markedet for teleudstyr[5]. Dette kunne fx ske gennem fælles europæisk målrettet stimulering og finansiering af øget forskning på området.

For at sikre gode investeringsvilkår og gode vilkår for konkurrencen, er det også vigtigt, at Danmark ikke går enegang i EU, og at der stiles mod ensartede regler i EU. Med det foreliggende udkast til lov lægges der op til, at Danmark indfører et af de mest restriktive forbudsregimer i EU. TI ser derfor helst, at den danske regering arbejder for en koordineret implementering af de sikkerhedskrav, der indføres i de forskellige EU-lande, jf. EU Kommissionen 5G tool box[6], inden der indføres danske særregler. TI kan dog forstå, at en fælles koordinering ikke kan nås, inden lovens fremsættelse. TI skal derfor opfodre til, at loven ikke bliver mere indgribende, end hvad der er absolut nødvendigt, og at loven tages op til revision om senest 2 år med henblik på en tilpasning i forhold til reglerne i de øvrige EU-lande.

Teleindustrien står naturligvis til rådighed for en eventuel uddybelse af ovenstående høringssvar.

Med venlig hilsen

Jakob Willer
Direktør

[5] https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

[6] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

Tilsynet med Efterretningstjenesterne

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Dato: 4. Januar 2021

Vedrørende Høring over udkast til forslag til lov om leverandørsikkerhed iden kritiske teleinfrastruktur

Ved brev af 7. december 2020 har Forsvarsministeriet anmodet Tilsynet med Efterretningstjenesterne om bemærkninger til udkast til Lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

I den forbindelse kan tilsynet oplyse, at udkastet ikke giver anledning til bemærkninger.

Der henvises til Forsvarsministeriets sagsnummer 2020/008732.

Med venlig hilsen
Tilsynet med Efterretningstjenesterne

v/Emil Bock Greve
Sekretariatschef

Borgergade 28, 1.
DK-1300 København K
t 25 50 10 34
www.tet.dk

Vestre Landsret
Præsidenten

Forsvarsministeriet
Holmens Kanal 9
1060 København K

17. december 2020

Sendt pr. mail til fmn@fmn.dk, nbb@fmn.dk og nis@fmn.dk

J.nr.: 20/02589-2
Sagsbehandler: Lars B Olesen

Forsvarsministeriet har ved brev af 7. december 2020 (sagsnr. 2020/008711) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Helle Bertung

Østre Landsret
Præsidenten

Forsvarsministeriet
Sendt pr. mail til fmn@fmn.dk og nls@fmn.dk

10. december 2020

J.nr.: 20/02507-2
Sagsbehandler: Christian Reinhold Jensen
Dir. tlf.:
Mail: ChristianReinholdJensen@OestreLandsret.dk

Forsvarsministeriet har ved brev af 7. december 2020 (Sagsnr. 2020/008711) anmodet om eventuelle bemærkninger til høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

I den anledning skal jeg meddele, at landsretten ikke ønsker at udtale sig om udkastet.

Med venlig hilsen

Carsten Kristian Vollmer

Ellen Busck Forsbo