TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Styrelsen for Samfundssikkerhed
e-mail: tele@cfcs.dk

Sagsnr.: 2025/003110

10.09.2025

**Høringsbidrag til erfaringer med lov om leverandørsikkerhed i den kritiske teleinfrastruktur**

Teleindustrien (TI) takker for muligheden for at afgive høringssvar vedrørende bemærkninger om erfaringer med lov om leverandørsikkerhed i den kritiske teleinfrastruktur (telesikkerhedsloven).

Styrelsen for Samfundssikkerhed har, jf. § 17, stk. 4, i Lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur (telesikkerhedsloven), på vegne af Ministeriet for Samfundssikkerhed og Beredskab iværksat udarbejdelsen af en rapport til Folketinget om erfaringerne med anvendelsen af loven.

Telebranchen fremkommer hermed med bemærkninger hertil. Først i mere overordnet form og herefter med specifikke bemærkninger til loven.

## Generelle bemærkninger

*Manglende retningslinjer for underretningspligten*
Branchen har fokus på og er i løbende dialog med Styrelsen for Samfundssikkerhed (SAMSIK) om aftaler, der vedrører leverede kritiske netkomponenter, systemer og værktøjer. Der sker løbende underretning forud for påbegyndte forhandlinger, og der følges løbende op på audit trail, herunder med fokus på sikkerhedsmæssige aspekter i aftalerne.

En generel udfordring, som telebranchen står overfor er, at det i nogle tilfælde ikke er tilstrækkeligt tydeligt, hvad der er omfattet af loven – det har historisk set været et punkt til løbende drøftelse. Der findes ikke vejledning i fortolkning af lovbestemmelserne, og dermed er der kun den endelige ordlyd i lovteksten at forholde sig til.

Branchens erfaring er, at der ofte opstår forskellig fortolkning af underretningspligter og variation i den praksisnære implementering af

lovgivningen på tværs af virksomheder i sektoren. Dette kan medføre usikkerhed om, hvilke leverancer der skal ske underretning om.

Branchens erfaring er, at denne usikkerhed om lovens rækkevidde i praksis har medført en forsigtig tilgang. Operatørerne har ofte valgt at underrette og handle bredere end, hvad der måske var strengt nødvendigt – en 'better safe than sorry'-tilgang – hvilket på den ene side har understøttet lovens sikkerhedsmæssige formål, men på den anden side kan have ført til, at relevante komponenter og systemer kan være blevet fravalgt uden saglig grund. Det samme gælder vurderingen af, hvilke leverandørlande der udgør en trussel og dermed hvilke landes virksomheder, der kan anvendes som leverandører, som har ført til meget forsigtige beslutninger.

Allerede i 2021 pegede TI på, at uklare definitioner af "kritiske netkomponenter" og uklare kriterier for, hvornår leverandører udgør en trussel, ville skabe usikkerhed. Resultatet er opfyldelse af lovens sikkerhedsmæssige formål – men med en bias mod overimplementering. Detaljerede retningslinjer vil kunne skabe større klarhed og ensartethed på tværs af sektoren og samtidig reducere behovet for gentagne forespørgsler om allerede tilgængelige oplysninger. Et godt eksempel herpå ses i forbindelse med implementeringen af NIS-direktivet, hvor tydeligere og mere ensartet vejledning omkring fx hændelser bidrager til at mindske forskelle i praksis og sikre en mere effektiv og harmoniseret efterlevelse af kravene.

*TI vil derfor foreslå, at SAMSIK udarbejder detaljerede retningslinjer for underretningspligten samt kritiske netkomponenter, systemer og værktøjer.*

*Erfaringer fra operatørerne*
Loven har samlet set været disciplinerende, men til den sikre side. Det kan ikke udelukkes, at operatørerne har truffet "for sikre" valg i forhold til leverandørvalg og teknologiske løsninger.

Det har været positivt for samfundets sikkerhed, men har også skabt risiko for unødig fordyrelse og fravalg af ellers relevante leverandører. Denne erfaring understøtter TI's tidligere vurdering af, at tydeligere kriterier, klare definitioner og øget transparens er nødvendige for at skabe en bedre balance mellem sikkerhed og effektiv markedsudvikling.

**Specifikke bemærkninger til loven**
*§ 1*
Definitionen af "Kritiske netkomponenter, systemer og værktøjer" er for bred og bør indsnævres for kun at omfatte de mest følsomme dele af infrastrukturen. Dette kan reducere antallet af komponenter, der er underlagt regulering.

SAMSIK kunne eventuel lade sig inspirere af vejledningen til bekendtgørelse nr. 963 – "Sikkerhedsgodkendelse af personer, som har funktioner inden for telesektoren", hvor det til §1, stk. 3 fremgår, at en

netkomponent, et system eller værktøj kun er kritisk, hvis en hændelse relateret til systemet kan *medføre større regionale eller nationale hændelser.*

*§§ 2-3*
Krav om proportionalitet. Det er væsentligt, at princippet om proportionalitet også fremover fastholdes som et krav, så det godtgøres, at mindre indgribende tiltag ikke er tilstrækkelige, inden SAMSIK udsteder et eventuelt forbud, jf. § 2, stk. 3 og § 3, stk. 4. TI mener dog, at proportionalitetsvurderingen i § 2 bør styrkes og præciseres, så det endnu mere klart fremgår, at forbud kun anvendes som en sidste udvej.

*§ 4*
Der bør opstilles objektive og strenge krav til dokumentation for nødvendigheden af ekspropriation.

Erstatningsreglerne bør præciseres og udvides for at sikre fuld kompensation for alle tab, herunder følgeskader og indirekte tab. Hurtig udbetaling til virksomhederne bør sikres, hvilket også er rimeligt pga. indgrebets ekstreme karakter. Dette kan med fordel også specificeres i de detaljerede retningslinjer, som branchen også beder SAMISIK om at udarbejde.

*§ 6*
Der bør være en administrativ klageadgang, og der bør sikres hurtig (og billig) prøvelse af afgørelser.

*§ 7*
Frist på 6 måneder for indbringelse af afgørelser for Københavns Byret, mener TI, er for kort, særligt når der er tale om så indgribende foranstaltninger, som det er tilfældet med aftaler omfattet af denne lov. TI mener, at fristen bør forlænges for at give virksomheder tilstrækkelig tid til at forberede deres sag.

*§§ 8-13*
Loven afholder i væsentligt omfang den specifikke teleudbyder fra at få viden om, hvilket grundlag et evt. forbud mod en aftale er baseret på. Det er i vid udstrækning kun en særligt udpeget forsvarer, som får denne viden. Dette bør ændres, så oplysninger kan deles med personer hos udbyderen, der er sikkerhedsgodkendt til det relevante niveau. Teleudbyderne skal i forvejen kunne håndtere dybt fortrolige og følsomme oplysninger, og de bør derfor også kunne informeres om grundlaget for forbudsafgørelser, som kan have afgørende betydning - både sikkerhedsmæssig og økonomisk - for udbyderen.

*TI vil derfor foreslå, at SAMSIK deler oplysninger om, hvilket grundlag et forbud mod en aftale baseres på.*

*§ 14*
Offentliggørelse bør være anonymiseret for at beskytte virksomhedens omdømme og forretningshemmeligheder.

*§ 15*
Muligheden for at afsætte medlemmer af en televirksomheds ledelse, mener TI, er for indgribende en foranstaltning.

Teleindustrien står naturligvis til rådighed for yderligere dialog og samarbejde om disse emner.

Med venlig hilsen

Jakob Willer
Direktør