PÓST- OG FJARSKIPTASTOFNUN

Ákvörðun nr. 3/2021

Úttekt á öryggisskipulagi Tengis hf.

(mál nr. 2020010018)

I.
Upphaf máls

(1) Póst- og fjarskiptastofnun gegnir víðtæku eftirlitshlutverki á sviði fjarskipta hér á landi. Stofnunin fer með umsjón framkvæmdar fjarskiptalaga nr. 81/2003 og hefur eftirlit með starfsemi fjarskiptafyrirtækja. Eitt af því sem fellur undir eftirlitshlutverk stofnunarinnar er að tryggja að fjarskiptafyrirtæki viðhafi ráðstafanir til að tryggja heildstæði og öryggi almennra fjarskiptaneta. Getur stofnunin viðhaft frumkvæðisathuganir á starfsemi þeirra og krafið þau um upplýsingar sem nauðsynlegar þykja við athugun einstakra mála.

(2) Tengir hf. var stofnað árið 2002 og sinnir fjarskiptarekstri á Eyjafjarðarsvæðinu. Félagið sinnir fjölbreyttri fjarskiptaþjónustu, til bæði fyrirtækja og heimila, og gegnir því mikilvægu hlutverki í að tryggja traust fjarskipti á svæðinu.

(3) Á haustmánuðum 2020 framkvæmdi Póst- og fjarskiptastofnun úttekt á öryggisskipulagi Tengis hf. Í ákvörðun þessari er farið yfir aðferðarfræði úttektarinnar, lagaumhverfi og helstu niðurstöður.

II.
Lagaumhverfi

(4) Póst- og fjarskiptastofnun hefur það hlutverk að tryggja að heildstæði og öryggi almennra fjarskipta sé viðhaldið, sbr. f-lið 4. tl. 3. gr. laga nr. 69/2003, um Póst- og fjarskiptastofnun. Þá er mælt fyrir um það í 2. og 3. mgr. 47. gr. laga nr. 81/2003, um fjarskipti (hér eftir fjarskiptalög) að stofnunin setji sérstakar reglur um vernd upplýsinga og virkni almennra fjarskiptaneta. Í þessu skyni hefur Póst- og fjarskiptastofnun sett reglur nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum og reglur nr. 1222/2007, um virkni almennra fjarskiptaneta.

(5) Fjarskiptalög leggja skyldur á fjarskiptafyrirtæki um að viðhafa sérstakar ráðstafanir til að tryggja öryggi almennra fjarskiptaneta. Í 2. mgr. 47. gr. laganna kemur fram að

fjarskiptafyrirtæki skulu skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, framkvæma áhættumat og ákveða öryggisráðstafanir á grundvelli þess. Þá er í 3. mgr. sama ákvæðis kveðið á um að fjarskiptafyrirtæki skuli viðhafa sérstakar ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta.

(6) Framangreindar skyldur fjarskiptafyrirtækja eru nánar útfærðar í 7. gr. reglna Póst- og fjarskiptastofnunar nr. 1221/2007. Í 1. tölul. ákvæðisins er kveðið á um að fjarskiptafyrirtæki setji sér skriflega *öryggisstefnu*. Í 2. tölul. er fjallað um gerð skriflegs *áhættumats* með það að markmiði að skapa forsendur fyrir vali á *öryggisráðstöfunum* og skal það endurskoðað reglulega. Þá skal fjarskiptafyrirtæki samkvæmt 3. tölul. greinarinnar gera ákveðnar öryggisráðstafanir á grundvelli áhættumatsins og setja fram skriflegar lýsingar á þeim. Þannig skal fjarskiptafyrirtækið m.a. skilgreina hvaða öryggisráðstöfunum skuli beitt, hvernig þær verði útfærðar sem og taka fram hvernig brugðist verði við áföllum í rekstri fjarskiptaneta.

(7) Í reglum nr. 1222/2007 er svo nánar kveðið á um hvernig virkni almennra fjarskiptaneta skuli vera tryggð með sem bestum hætti. Þar er kveðið á um þær kröfur og lágmarksráðstafanir sem taldar eru nauðsynlegar, eftir því sem við á, að fjarskiptafyrirtækin viðhafi til að tryggja samfelldan rekstur almennra fjarskiptaneta sinna og raunlæga vernd þeirra. Þá er sérstaklega tilgreint að þær kröfur sem ekki koma beint fram í reglunum skulu fyrirtækin sjálf bera kennsl á með skipulegu áhættumati og viðhafa aðgerðir til að stýra og stjórna fjarskiptanetum með tilliti til áhættu, sbr. 4. gr. reglnanna. Er fjarskiptafyrirtækjum þannig gert að nýta sér áhrifagreiningu og áhættumat til að draga úr öllum stærri veikleikum og veilum í innviðum sínum, sbr. 7. gr. reglnanna.

(8) Þá skulu fjarskiptafyrirtæki gera neyðaráætlun sem byggir á niðurstöðu áhættumatsins, en í 8. gr. reglna nr. 1222/2007 eru talin upp þau atriði sem slík áætlun skal að lágmarki taka til. Regluverkið byggir á því að ábyrgðin á því að innleiða fullnægjandi öryggisskipulag og velja viðeigandi öryggisráðstafanir á grundvelli þess hvíli á fjarskiptafyrirtækjum. Fjarskiptafyrirtækjum ber þó ávallt að haga útfærslu öryggisskipulags í samræmi við viðurkennd viðmið t.d. í ISO 27001 (Stjórnkerfi upplýsingaöryggis), sbr. einnig 2. gr. reglna nr. 1221/2007 og 5. gr. reglna nr. 1222/2007.

(9) Framangreint felur það í sér að Tengir hf. hefur lögbundna skyldu til að tryggja öryggi og virkni fjarneta sinna m.a. með því að gera skriflega öryggisstefnu, framkvæma áhættumat á grundvelli fyrirliggjandi aðferðarfræði og viðhafa ákveðnar öryggisráðstafanir á grundvelli þess, sem og að setja sér neyðaráætlun, sbr. ákvæði framangreindra reglna.

(10) Eftirlitshlutverk Póst- og fjarskiptastofnunar felst fyrst og fremst í eftirfylgni á því að framangreint sé gert, t.a.m. með því að kalla eftir gögnum varðandi öryggisstefnuna og áhættumat sem og með því að gera úttektir á því hvort valdar öryggisráðstafanir séu til staðar og þær virkar þannig að tryggt sé með fullnægjandi hætti virkni og vernd fjarskiptaneta í samræmi við lög og reglur. Umfang úttektar þessarar takmarkast þó við að greina hvort að skjalfest skipulag öryggisskipulags Tengis hf. sé fullnægjandi.

III.
Aðferðarfræði

(11) Með þessari úttekt Póst- og fjarskiptastofnunar er ætlunin að staðreyna skjalfest skipulag upplýsingaöryggis Tengis hf.

(12) Úttektin er í formi skrifborðsúttektar. Fyrirkomulag skrifborðsúttektar er slíkt að Póst- og fjarskiptastofnun kallar eftir tilgreindum gögnum til að staðreyna hvort félagið hafi framfylgt þeim kröfum sem ákvæði fjarskiptalaga og afleiddra réttarheimilda gera til skjalfests skipulags upplýsingaöryggis. Er hér um að ræða tilvist öryggisstefnu, framkvæmd áhættumats, gerð skriflegra öryggisráðstafana og neyðaráætlunar sem og reglubundna endurskoðun þessara gagna. Séu umbeðin gögn ekki til staðar við úttekt telst slíkt varða við framangreind ákvæði, en skal þó tekið fram að metið er með almennum hætti hvort ígildi slíkra gagna séu til staðar hjá félaginu. Ef Póst- og fjarskiptastofnun telur að vöntun sé á einum eða fleiri þáttum öryggisskipulags telst almennt öryggisskipulag félagsins ábótavant. Mun stofnunin krefjast úrbóta á slíkum athugasemdum innan fjögurra mánaða.

IV.
Boðun úttektar og upplýsingaöflun

4.1. Kynning á fyrirhugaðri úttekt

(13) Póst- og fjarskiptastofnun boðaði fulltrúa Tengis hf. á fund þann 16. júní 2020 þar sem fyrirhuguð úttekt á öryggisskipulagi félagsins var kynnt. Einnig var farið yfir fyrirhugaða úttekt á raunlægu öryggi valinna tækjarýma Tengis hf., en þeim hluta úttektarinnar var frestað sökum aðstæðna í þjóðfélaginu af völdum Covid-19. Verður ekki fjallað frekar um það í ákvörðun þessari.

(14) Á fundinum var farið yfir það lagaumhverfi sem lýtur að öryggi fjarskiptaneta, sbr. ákvæði fjarskiptalaga og reglna nr. 1221/2007 og 1222/2007, sem og í hverju eftirlitshlutverk Póst- og fjarskiptastofnunar felst. Þá var einnig úttektarferli stofnunarinnar kynnt, bæði er varðar öryggisskipulag, sem þessi liður úttektarinnar lýtur að, og raunlægu öryggi tækjarýma. Fram kom að úttektarferli öryggisskipulags felst í kynningarsamtali og óformlegri upplýsingaöflun, kynningu á aðferðarfræði úttektarinnar, formlegri boðun á úttekt ásamt formlegri og ítarlegri upplýsingaöflun, heimfærslu niðurstöðu úttektar á lagaákvæði, andmælaréttur á boðaða niðurstöðu úttektar og að lokum er gefin út formleg stjórnsýsluákvörðun.

(15) Á framangreindum fundi með Tengi hf. var jafnframt farið yfir þau gögn sem Póst- og fjarskiptastofnun hugðist óska eftir, þ.e. öryggisstefnu félagsins, áhættumati þess, skriflegum öryggisráðstöfunum og neyðaráætlun. Í tölvupósti þann 25. júní 2020 var félaginu gefinn kostur á að senda stofnuninni hvaðeina upplýsingar sem félagið teldi gagnlegt að stofnunin fengi áður en úttekt yrði formlega boðuð. Tengir hf. svaraði Póst- og fjarskiptastofnun með tölvupósti þann 26. júní 2020 og bað um frestun á formlegri boðun úttektar, en um þetta leyti voru ófyrirséðar annir hjá félaginu sem og vegna aðstæðna í þjóðfélaginu. Pósti- og fjarskiptastofnun samþykkti að fresta boðun úttektar til lok sumars sama ár.

4.2. Boðun framkvæmd úttektar og öflun gagna

(16) Með tölvupósti 28. ágúst 2020 gaf Póst- og fjarskiptastofnun Tengi hf. að nýju tækifæri til að skila inn upplýsingum sem félagið teldi gagnlegt að stofnunin fengi áður en úttekt yrði formlega boðuð. Benti stofnunin á að slíkar upplýsingar myndu nýtast við að afmarka andlag úttektarinnar betur. Engin svör bárust stofnuninni.

(17) Póst- og fjarskiptastofnun boðaði því formlega úttekt á stjórnskipulagi með bréfi þann 4. september 2020. Í bréfinu kom fram að stofnunin myndi taka út skriflegt öryggisskipulag

Tengis hf. á Akureyri, sbr. 29. gr. reglna nr. 1222/2007, um virkni almennra fjarskiptaneta, sbr. einnig 3. mgr. 47. gr. laga nr. 81/2003, um fjarskipti. Með boðunarbréfinu var Tengir hf. upplýst um þær lagalegu kröfur sem gerðar eru um öryggisskipulag sem félaginu ber að uppfylla, og rakin hafa verið hér að framan. Þá var einnig fjallað um aðferðarfræði boðaðrar úttektar, þ.m.t. heimfærslu niðurstöðu úttektar yfir á lagaákvæði og kröfur sem hvíla á Tengi hf. Að lokum var félaginu boðið að gera athugasemdir við efni bréfsins. Engar athugasemdir bárust.

(18) Póst- og fjarskiptastofnun hóf formlega úttekt á öryggisskipulagi Tengis hf. með upplýsingabeiðni þann 21. október 2020. Í bréfi stofnunarinnar var óskað eftir eftirfarandi gögnum um öryggisskipulag Tengis hf. og tekið fram að viðkomandi gögn yrðu lögð til grundvallar við mat á því hvort að öryggisskipulag félagsins væri fullnægjandi skv. 2. mgr. 47. gr. laga nr. 81/2003, um fjarskipti, sbr. 7. gr. reglna Póst og fjarskiptastofnunar nr. 1221/2007 og 8. gr. reglna nr. 1222/2007. Þau gögn sem óskað var eftir voru:

1. Afriti af skriflegri öryggisstefnu.
2. Upplýsingar um aðferðarfræði áhættumats og afrit af skriflegu áhættumati.
3. Afriti af skriflegum öryggisráðstöfunum fyrir tækjarými félagsins á Akureyri.
4. Afrit af neyðaráætlun.

V.
Úttekt Póst- og fjarskiptastofnunar

5.1. Trúnaður niðurstöðuskýrslu

(19) Viðauki við ákvörðun þessa er ítarlegri útgáfa af ákvörðuninni þar sem farið er framkvæmd og niðurstöðu úttektarinnar, lið fyrir lið. Viðauki þessi er bundinn trúnaði.

(20) Í þessum kafla ákvörðunarinnar verður því einungis gerð grein fyrir helstu niðurstöðum stofnunarinnar á öryggisskipulagi félagsins. Ekki verður farið ítarlega í efni gagna félagsins, enda getur það varðar hagsmuni Tengis hf., öryggi starfsemi þeirra og öryggi og virkni fjarskiptaþjónustu viðskiptavina þeirra.

5.2. Úttekt Póst- og fjarskiptastofnunar

(21) Líkt og vikið hefur verið að þá óskaði Póst- og fjarskiptastofnun eftir gögnum frá Tengi hf. er varðar öryggisskipulag félagsins. Í samskiptum Póst- og fjarskiptastofnunar við Tengi hf. kom fram að félagið væri í vinnu við að uppfæra þau gögn sem óskað var eftir og í sumum tilvikum væri stuðst við ferla og vinnu annarra félaga þeim gögnum til fyllingar. Þá kom fram að Tengir hf. hygðist ráða til sín utanaðkomandi sérfræðing til að styðja við vinnu félagsins við að uppfæra öryggisskipulag og verkferla. Úttekt þessi tekur þó ekki mið af þeim fyrirætlunum heldur byggir aðeins á þeim gögnum sem voru í gildi á þeim tíma þegar úttektin var framkvæmd.

(22) Safn gagna bárust Póst- og fjarskiptastofnun með tölvupósti þann 10. og 11. nóvember 2020. Í samræmi við markmið úttektarinnar var það ekki ætlun Póst- og fjarskiptastofnunar að leggja efnislegt mat á öryggisskipulag Tengis hf. Markmiðið var fyrst og fremst að kanna hvort félagið uppfylli kröfur um gerð öryggisskipulags samkvæmt 2. mgr. 47. gr. fjarskiptalaga og ákvæði 7. gr. reglna nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum, sbr. einnig 4. gr. reglna nr. 1222/2007 um virkni almennra fjarskiptaneta. Að því sögðu var ekki hjá því komist að leggja mat á það hvort að innsend gögn uppfylltu þær lágmarkskröfur um form og inntak sem leiða af framangreindum ákvæðum.

(23) Úttekt Póst- og fjarskiptastofnunar á öryggisskipulagi Tengis hf. sýnir að hlítni félagsins við ákvæði 2. mgr. 47. gr. fjarskiptalaga og ákvæði 7. gr. reglna nr. 1221/2007, sbr. einnig 4. gr. reglna nr. 1222/2007 er ábótavant. Ekki eru til staðar öryggisstefna, áhættumat né neyðaráætlun sem uppfyllir lágmarkskröfur reglnanna. Þá hafa ekki verð skráðar öryggisráðstafanir valdra tækjarýma félagsins, líkt og áskilið er.

(24) Póst- og fjarskiptastofnun vill þó taka það fram að við framkvæmd úttektar þessar sýndi Tengir hf. mikinn vilja til samstarfs og til að bæta úr þeim vanköntum sem voru á öryggisskipulagi félagsins þegar úttektin fór fram. Ennfremur tjáði félagið stofnuninni að áætlað er að styrkja öryggisskipulag félagsins á næstu mánuðum.

VI.
Niðurstaða

(25) Að mati Póst- og fjarskiptastofnunar skortir heildstæði í uppbyggingu á öryggisskipulagi Tengis hf. sem fæst með fullri hlítni við þær kröfur sem gerðar eru í 2. mgr. 47. gr. fjarskiptalaga og ákvæði 7. gr. reglna nr. 1221/2007, sbr. einnig 4. gr. reglna nr. 1222/2007. Þær kröfur byggja á hugmyndafræði ISO 27001 staðalsins. Stofnunin hvetur félagið til að hefja þegar vinnu við framkvæmd fullnægjandi öryggisskipulags og bæta úr þeim vanköntum sem fram komu við úttekt þessa.

Ákvörðunarorð

1. **Öryggisskipulag Tengis uppfyllir ekki kröfur 2. mgr. 47. gr. laga um fjarskipti nr. 81/2003 og ákvæða II. og III. kafla reglna nr. 1222/2007, sbr. 7. gr. reglna nr. 1221/2007.**

2. **Tengir hf. skal setja sér öryggisstefnu, framkvæma heildstætt áhættumat, skilgreina skriflegar öryggisráðstafanir og setja sér skriflega neyðaráætlun, eigi síðar en fjórum mánuðum frá birtingu ákvörðunar þessarar, og skal upplýsa stofnunina um framvindu þeirrar vinnu að lágmarki á fjögurra vikna fresti fram að þeirri dagsetningu.**

3. **Ákvörðun þessi er kæranleg til úrskurðarnefndar fjarskipta- og póstmála, sbr. 1. mgr. 13. gr. laga nr. 69/2003, um Póst- og fjarskiptastofnun. Kæran skal berast úrskurðarnefnd innan fjögurra vikna frá því að viðkomandi var kunnugt um ákvörðun Póst- og fjarskiptastofnunar. Um kostnað vegna málskots fer samkvæmt 5. mgr. 13. gr sömu laga, auk þess sem greiða ber sérstakt málskotsgjald að upphæð kr. 150.000, skv. 6. gr. reglugerðar nr. 36/2009 um úrskurðarnefnd fjarskipta- og póstmála. Samkvæmt 4. mgr. 13. gr. sömu laga getur aðili einnig borið ákvörðun Póst- og fjarskiptastofnunar beint undir dómstóla án þess að mál sé fyrst borið undir úrskurðarnefnd. Slíkt mál skal höfðað innan þriggja mánaða frá því að viðkomandi fékk vitneskju um ákvörðun stofnunarinnar. Málskot frestar ekki réttaráhrifum ákvarðana stofnunarinnar. Málskot beint til dómstóla hindrar að úrskurðarnefnd sé heimilt að taka kæru til málsmeðferðar.**

Reykjavík, 20. apríl 2021

Hrafnkell V. Gíslason

Gabriella Unnur Kristjánsdóttir

Viðauki:
Niðurstöðuskýrsla Póst- og fjarskiptastofnunar, dags. 20. apríl 2021 – *Trúnaðarmál.*