PÓST- OG FJARSKIPTASTOFNUN
SUÐURLANDSBRAUT 4
108 REYKJAVÍK

SÍMI 510 1500 PÓSTUR PFS@PFS.IS
FAX 510 1509 VEFUR WWW.PFS.IS

Alþingi – Umhverfis- og samgöngunefnd
b.t. Guðfríðar Lilju Grétarsdóttur, formanns
Austurstræti 8-10
150 REYKJAVÍK

Reykjavík, 1. febrúar 2012

Málsnúmer: 2011120052
Skjalalykill: 15.3.4

Alþingi
Erindi nr. Þ 140/954
komudagur 3.2.2012

Málefni: Umsögn um frumvarp til breytinga á fjarskiptalögum vorþing 2012

Póst- og fjarskiptastofnun (PFS) hefur gefist tækifæri á því að koma skriflegum athugasemdum á framfæri við umhverfis- og samgöngunefnd varðandi frumvarp um breytingu á lögum um fjarskipti nr. 81/2003, sbr. þingskjal 438 – 362 mál. Stofnunin hefur áður fengið tækifæri á því að kynna málið stuttlega fyrir nefndarmönnum og svara spurningum. Mun PFS í þessari umsögn árétta mikilvægustu atriði frumvarpsins og svara einstökum athugasemdum hagsmunaaðila við frumvarpið sem stofnunin telur að að séu byggðar á misskilningi.

1. CERT-starf brýtur ekki gegn persónuvernd og friðhelgi einkalífs
PFS telur nauðsynlegt að starfrækja viðbragðsteymi um netvarnir, s.k. CERT-ÍS hóps, til að efla varnir og viðbúnað landsins gegn netárásum. Árásir af því tagi og ýmiss skemmdarverk, sem hægt er að vinna með rafrænum hætti, er ein helsta ógn sem steðjar að nútíma upplýsingasamfélagi, þar sem helstu innviðir þess reiða sig á tölvustýrð upplýsingakerfi og jafnvel á samskipti við internetið. Um er að ræða s.k. ómissandi upplýsingainnviði á borð við raforkustýringu, greiðslumiðlunarkerfi og heildstæð sjúkraskárkerfi svo dæmi séu tekin. Eftirlit í tengslum við netvarnir af þessu tagi er alþjóðlegt og byggist á samstarfi slíkra hópa á milli landa. Samkvæmt tilmælum framkvæmdastjórnar ESB nr. COM(2011)163 skulu aðildarríki sambandsins skuldbinda sig til þess að koma á laggirnar CERT viðbragðsteymi fyrir árslok 2012. Þá á þetta verkefni sér líka grundvöll í samvinnu Norðurlandanna á vettvangi Norðurlandaráðsins, en í tillögu nr. 7 í skýrslu sem Jens Stoltenberg vann fyrir ráðið, er gert ráð fyrir að brugðist verði við netglæpum (e. Cyber Crime) með því að auka eftirlit og koma á fót viðbragðsteymum í löndum Norðurlanda.

Í dag sjá fjarskiptafyrirtæki og netþjónustuaðilar um mikilvægar varnir þegar kemur að því að tryggja örugga virkni almennra fjarskiptaneta, t.d. er reynt að stemma stigu við yfirflæði ruslpósts, auk þess sem fjarskiptaumferð er vöktuð með tilliti til þess hvort hún kunni að vera sviksamleg, þ.e. virkjuð vélrænt til að skapa ólögmætan ávinning, eða hún talin fela í sér ógn við heildstæði fjarskiptanetanna með einhverjum hætti. Þannig er reynt að einangra vírusa og annars konar spilliforrit sem dreift er um netið. Þessi vinna fjarskiptafyrirtækjanna fer fram án þess að um hana gildi sérstök lagaákvæði. Byggir þessi vinna fjarskiptafyrirtækja á almennum ákvæðum fjarskiptalaga sem leggja þær skyldur á herðar þeim um að tryggja örugga virkni almennra fjarskiptaneta, heildstæði þeirra og samfelldan rekstur, en það er grundvöllur allra fjarskipta í landinu. Þá hefur þessi framkvæmd fjarskiptafyrirtækja og netþjónustuaðila ekki verið talin fara í bága við ákvæði persónuverndarlaga, svo að PFS sé kunnugt. Í sumum

tilvikum er kveðið á um aðgerðir af þessu tagi í viðskiptaskilmálum við áskrifendur, t.d. hvað varðar síun ruslpósts, en með því er fengið samþykki hans fyrir aðgerðinni. Þá hefur fyrirtækjum um árabil staðið til boða að kaupa sérstaka þjónustu af upplýsingatæknifyrirtækjum um að skima þá netumferð sem berst til og frá upplýsingakerfum þeirra og netþjónum í þeim tilgangi að verja sig gegn ruslpósti, vírusum og ýmiss konar óværu á netinu.

Hvað er þá nýtt á ferðinni þegar um er að ræða eftirlit CERT-ÍS hópsins? Um er að ræða sams konar eftirlit sem tíðkast hefur um árabil af hálfu fjarskiptafyrirtækja, netþjónustuaðila og upplýsingatæknifyrirtækja. Tæknin við eftirlitið verður sú sama og ráðgert að nota búnað sem gegnir svipuðu hlutverki og sá búnaður sem þegar er í notkun af hálfu markaðsaðila. Ráðgert er að skima vélrænt netumferð til og frá tilteknum upplýsingainnviðum með sama hætti og á við um þá þjónustu sem fyrirtækjum stendur til boða að kaupa í dag. Engum dettur í hug að gera athugasemdir við það að fyrirtæki verji upplýsingakerfi sín með því að kaupa þjónustu sem felst í því að sía út ruslpóst, einangra og eyða vírusum eða öðrum spilliforritum, eða hvað þá að krefjast dómsúrskurðar til slíks. Að áliti PFS er ekki tilefni til að gera strangari kröfur til rekstraraðila þjóðfélagslegra mikilvægra upplýsingainnviða, sem varðar almannaheill að séu ávallt rekstrarhæf.

Ákvæði frumvarpsins um CERT-starfið felur í sér að eftirlitið verður samræmt og skipulagt af hálfu hlutlauss aðila á vegum hins opinbera og um það settar ákveðnar skorður og öryggiskröfur í lögum og í reglugerð, einmitt til að tryggja persónuvernd og friðhelgi einkalífs. T.d. er það sérstaklega áréttað í 3. mgr. 8. gr. frumvarpsins að það sé beinlínis *óheimilt að persónugreina þá umferð sem skimuð er* með vélrænum hætti. Hér felst því aukin vernd frá því sem gerist á almennum markaði á grundvelli einkaréttarlegs samningssambands milli tveggja fyrirtækja. Þá verður að hafa í huga að eftirlitið verður valkvætt, nema þegar um er að ræða hin almennu fjarskiptanet, þar sem eftirlit af þessu tagi krefst samvinnu við fjarskiptafyrirtækin. Þannig verður það ekki skylda, t.d. raforkufyrirtækja að gerast aðili að umsjónarneti CERT-ÍS, heldur geta þau fremur kosið, að óbreyttum lögum, að kaupa samskonar þjónustu af netþjónustuaðila eða upplýsingatæknifyrirtæki. Það er aftur á móti skoðun PFS að ef þetta eftirlit er miðlægt og samhæft á milli mismunandi þjóðfélagslegra mikilvægra upplýsingainnviða náist meira öryggi, betri yfirsýn yfir heildstæðar ógnir og hæfni til að bregðast við aðsteðjandi hættum, t.d. með samræmdum aðgerðum á landsvísu. Jafnframt verður verður að horfa til þess ávinnings að viðhafa eftirlit með netöryggi i formlegu samstarfi við önnur lönd, undir merkjum CERT, en í því felst samvinna t.d. um upplýsingaskipti um þekktar öryggisógnir og þátttaka í alþjóðlegum æfingum um samstilltar aðgerðir ríkja til fyrirbyggja eða bregðast við hættuástandi sem þegar hefur skollið á. Hér er um að ræða ávinning af alþjóðlegu samstarfi um eftirlit sem ekki er á færi einkaaðila, á borð við fjarskipta- og upplýsingatæknifyrirtækin, að tileinka sér og nýta. Telur PFS því að það komi vel til álita seinna meir að kveða á um skyldubundna aðild tiltekinna ómissandi upplýsingainnviða landsins að CERT-ÍS netumdæminu.

Hvað varðar fyrirhugaða heimild CERT-ÍS til þess að skoða efni fjarskiptasendinga, sbr. 4. mgr. 8. gr. frumvarpsins, þá er gert ráð fyrir því að *rökstuddur grunur* þurfi að vera fyrir hendi um að sending innihaldi spillikóta og að *samþykki* rekstraraðila viðkomandi upplýsingainnviða þurfi að koma til. Í þessu sambandi er byggt á þeim reglum sem gilt hafa um heimild fyrirtækja til þess að tryggja öryggi upplýsingakerfa sinna og það svigrúm sem þau hafa til þess að rannsaka slík atvik og bregðast við þeim. Endurspeglast þetta til að mynda í þeim reglum sem Persónuvernd hefur sett sér sjálf um skoðun tölvupóst starfsmanna sinna,

þ.m.t. einkatölvupóst, í tilefni af grunsemdum um öryggisatvik á borð tölvuveirur, en þar segir í reglunum:

> *„Þrátt fyrir ákvæði 1. mgr. er heimilt að skoða einkatölvupóst starfsmanna ef* brýna *nauðsyn ber til, s.s. vegna tölvuveiru eða sambærilegs tæknilegs atviks. Slíka skoðun má aðeins framkvæma að fyrirmælum forstjóra. Ávallt skal þó fyrst leita eftir samþykki starfsmanns ef þess er kostur. Enda þótt starfsmaður neiti að veita slíkt samþykki skal veita honum færi á að vera viðstaddur skoðunina."*

Ekki er gert ráð fyrir að afla þurfi dómsúrskurðar hér, né heldur þykir nauðsynlegt að styðjast við samþykki starfsmannsins eða mögulegan sendanda sendingarinnar. Leiðir það af umráðréttinum yfir viðkomandi upplýsingakerfi, en hann er hjá eiganda eða s.k. rekstraraðila netsins. Hins vegar ber að gæta upplýsinga- og tilkynningaskyldu gagnvart starfsfólki vegna netvöktunar af þessu tagi. Í athugasemdum við ákvæði frumvarpsins er einmitt gert ráð fyrir því að það sama gildi um vöktun CERT-ÍS, þ.e. rekstraraðila upplýsingainnviðanna ber að gera starfsfólki sínu grein fyrir henni.

Í umsögn sinni segir Persónuvernd hins vegar, án þess að það sé rökstutt nánar, að ekki sé hægt að bera saman tilvik um netvöktun vinnuveitanda við áformað eftirlit CERT-ÍS þar sem netvöktun vinnuveitanda takmarkast við upplýsingakerfi vinnuveitandans sjálfs. PFS er ekki ljóst hvað er átt við með þessari athugasemd eða hvaða önnur upplýsingakerfi Persónuvernd hefur hér í huga. Greiðslumiðlunarkerfi banka, sem telst til ómissandi upplýsingainnviða, og öll önnur upplýsingakerfi innan bankans sem við það tengjast, s.s. tölvupóst- og bókhalds-, og gjaldfærslukerfi, telst til upplýsingakerfa bankans sjálfs. Því er vandséð af hverju banki eða raforkufyrirtæki, þ.e. rekstaraðili ómissandi upplýsingainnviða, sem ætlar að fela sérfræðingum CERT-ÍS að skoða tölvupóst starfsmanns, þar sem vélræn skimun netumferðar hefur vakið upp grunsemdir um að hann innihaldi skaðlega tölvuveiru, þurfi að afla dómsúrskurðar fyrir því á meðan Persónuvernd telur sig ekki þurfa þess. PFS telur að athugasemdir Persónuverndar hljóti að byggjast á einhvers konar misskilningi um eðli eftirlitsins eða umfangi þess. Tekið er sérstaklega fram í frumvarpsákvæðinu, en það er mjög mikilvægt, að þessi heimild CERT-ÍS til þess að skoða efni sendingar með samþykki rekstraraðila ómissandi upplýsingainnviða *taki ekki* til efnis sendinga í hinum almennu fjarskiptanetum. Í þessu felst að fjarskiptafyrirtækjum eða rekstraraðilum ómissandi upplýsingainnviða er ekki heimilt að fela CERT-ÍS að skoða efni fjarskiptasendinga í hinum almennu fjarskiptanetum, en þetta á t.d. við um tölvupóstsamskipti milli einstaklinga sem fara um hin almennu fjarskiptanet. Allar upphrópanir um netlögreglu eða að eftirlitið standist ekki ákvæði stjórnarskrárinnar um friðhelgi einkalífs eiga því ekki við nokkur rök að styðjast.

Hvað varðar ábendingar Persónuverndar um að ekki komi fram í frumvarpinu hvaða leiðir aðrar þjóðir hafa farið þessum efnum þá verður að hafa í huga sérstöðu Íslands sem er herlaust land þar sem engin eiginleg leyniþjónusta starfar. Í öðrum ríkjum Evrópu er algengast að ríkisvaldið komi sér upp CERT-hópum í tengslum við starfsemi leyniþjónustu eða á vegum hersins og er þá byggt á víðtækum eftirlits- og inngripsheimildum slíkra þjóðfélagsstofnana ef hætta er talin á að upplýsingainnviðum stafi hætta af árásum, skemmdarverkum eða öðrum öryggisógnum sem geta rýrt rekstrarhæfni þeirra. Slíkar eftirlitsheimildir krefjast alla jafna ekki dómsúrskurðar en lúta annars konar eftirliti, t.d. innra eftirliti eða eftirliti sérstakra eftirlitsnefnda af hálfu löggjafarþingsins. Hvað varðar fyrirhugaða starfsemi CERT-ÍS er hins vegar, með undantekningu hvað varðar fjarskiptafyrirtækin, um að ræða valkvætt borgarlegt eftirlit af hálfu hins opinbera. Engu að síður þykir vera nauðsynlegt að skapa um þetta ramma með samþykki lagaákvæða sem taka til starfseminnar, sem m.a. er ætlað að tryggja gagnsæi

um eftirlitsheimildir hennar og kröfur til persónuupplýsingaöryggis. Í Danmörku hefur verið farin svipuð borgaraleg leið til þess að ná markmiðum um skilvirkt eftirlit með öryggi ómissandi upplýsingainnviða landsins, sbr. lög sem finna má á vefslóðinni sem gefin er upp í neðanmálsgrein hér að neðan[1]. Þar er að finna samskonar heimild DK-CERT til þess að skoða efni fjarskiptasendinga með samþykki rekstraraðila ómissandi upplýsingainnviða, án þess að afla þurfi undangengis dómsúrskurðar. Aftur á móti eru farnar aðrar leiðir í því að tryggja eftirlit með starfseminni, t.d. hefur sérstök nefnd eftirlit með starfseminni þar. Í íslenska frumvarpinu er fyrirhugaðri starfsemi CERT-IS aftur á móti settar nákvæmari og strangari skorður í sjálfum lagatextanum, auk þess sem gert er ráð fyrir því að hópurinn starfi í samræmi við ákvæði reglugerðar þar sem nánari kröfur verði útfærðar um verklag og öryggisráðstafanir í tengslum við eftirlitið, m.a. að Persónuvernd geti sett skilyrði um vinnsluna og komi að því að móta efnisleg ákvæði reglugerðarinnar.

Að öllu framangreindu virtu telur PFS að fyrirhuguð starfsemi CERT-ÍS sé nauðsynleg til þess að stuðla að frekara öryggi þjóðfélagslegra mikilvægra upplýsingainnviða. Telur stofnunin að fyrirhugað eftirlit byggi á málefnalegum sjónarmiðum og að það gangi ekki lengra en nauðsyn ber til. Að sama skapi er það álit PFS að þau skilyrði sem ákvæðið hefur að geyma til verndar persónuupplýsingum og friðhelgi einkalífs séu raunhæf og fullnægjandi án þess að skilvirku og árangursríku eftirlitskerfi sé varpað fyrir róða.

2. Sérstök kostnaðarskiptingarregla vegna fjárfestingar í fjarskiptainnviðum

Í 6. gr. frumvarpsins er að finna sérstaka kostnaðarskiptingarreglu þegar fjarskiptainnviðir eru lagðir samhliða vatns- og raflínulögnum af hálfu veitufyrirtækja. Gerir reglan ráð fyrir því að fjarskiptahlutinn, þ.e. ljósleiðarastrengurinn greiði einungis jaðarkostnað við framkvæmdina.

Gagnaflutningsþjónusta til næstu ára og áratuga krefst mikillar burðargetu í aðgangstengingum að stofnlínukerfum. Í því sambandi er einkum horft til ljósleiðartenginga sem leggja þarf út frá núverandi hringtengingu ljósleiðarans til dreifbýliskjarna á landsbyggðinni, alveg heim að húsum og einstökum bæjum. Að sama skapi er nauðsynlegt að tengja næstu kynslóðar farsímanet við ljósleiðara baknet til þess að ná þeim gagnaflutningshraða sem sú tækni býður upp á. Má ætla að markmið stjórnvalda um háhraða gagnaflutningsþjónustu fyrir alla landsmenn, sem birtast í fjarskiptaáætlun fyrir árin 2011-2022, sbr. mál 342 sem nú er til meðferðar á Alþingi, verði ekki náð nema að þessi uppbygging fari fram, þegar til lengri tíma er litið.

Hér er um að ræða mikla fjárfestingu í fjarskiptainnviðum og þegar horft er til fámennustu svæða landsbyggðarinnar er ljóst að hún mun í mörgum tilvikum ekki standa undir sér á markaðslegum forsendum. Því verður að telja mikilvægt að ýtrustu hagkvæmni sé gætt og að nýta verði samlegðaráhrif af fjárfestingum og framkvæmdum í vatns- og raforkukerfum eftir því sem kostur er. Í þessu sambandi er rétt að benda á hluti jarðvegsframkvæmda í lagningu raflína eða ljósleiðara í jörðu er um 75% af kostnaðinum. Viðbótarkostnaður við að leggja ljósleiðara samhliða raflínu er því tiltölulega lítill. Þá ber að geta þess að veitustarfsemi byggist oft á sérleyfum eða einokunarstöðu veitufyrirtækisins á viðkomandi markaði eða sínu starfssvæði eru burðir slíkra fyrirtækja til fjárfestingar í vatns- og raflínulögnum í jörðu oft meiri heldur en á við um fjárfestingar fjarskiptafyrirtækja í fjarskiptainnviðum. Horfa verður

[1] http://folketsting.dk/love/lov-om-behandling-af-personoplysninger-skal-muliggoere-driften-af-den-statslige/2051/lovtekst/vedtaget

til þess að í fjarskiptum er markaðsleg áhætta meiri, gerð er hærri arðsemiskrafa og fyrningartími búnaðar er skemmri, en þetta réttlætir lægri kostnaðarþátttöku fjarskiptahlutans.

PFS telur mikilvægt að hafa í huga að hér er um heimildarákvæði að ræða. Með örðum orðum er það á valdi veitufyrirtækis hvort að það sjálft samnýti jarðvegsframkvæmdir í þágu uppbyggingu á fjarskiptainnviðum eða heimili fjarskiptafyrirtæki að gera það. Eins og fram kemur í ákvæðinu eru sett ákveðin skilyrði varðandi þau fjarskiptavirki sem lögð eru á grundvelli þessa ákvæðis og eiga þau að tryggja að samkeppnisstöðu verði ekki raskað. Gilda skal opinn aðgangur að slíkum fjarskiptavirkjum, auk þess sem fjarskiptafyrirtækjum skal bjóðast að leggja sín eigin fjarskiptavirki við framkvæmdirnar á sömu kjörum, sé það tæknilega mögulegt. PFS telur að þessi skilyrði séu til þess fallin að tryggja að samkeppnisstöðu milli annars vegar veitufyrirtækja og mögulegra dótturfyrirtækja þeirra og hins vegar fjarskiptafyrirtækja á sviði netrekstrar verði ekki raskað. Þá fær PFS ekki séð að sértæk kostnaðarskiptingarregla, sem á sér hlutlæga stoð í mismunandi kostnaðarforsendum að baki fjárfestingum annars vegar á sviði veituframkvæmda og hins vegar í fjarskiptum, teljist vera ríkisstuðningur (e. state aid) eða vera niðurgreiðsla á samkeppnisrekstri.

3. Heimild til handa PFS að leggja á stjórnvaldssektir
Til þess að opinbert eftirlit geti talist skilvirkt og árangursríkt þarf viðkomandi eftirlitsstjórnvald að búa yfir stjórnsýslulegum úrræðum til þess að fylgja fyrirmælum sínum og ákvörðunum eftir. Beiting dagsekta er úrræði sem stjórnsýslustofnanir geta beitt til þess að knýja á um tiltekna breyttni markaðsaðila eða einstaklinga. Í flestum tilvikum getur sú leið reynst árangursrík, t.d. varðandi fyrirmæli um afhendingu á gögnum eða til fyrirtækis um að láta af tiltekinni ólögmætri háttsemi. Fyrirmælin horfa þannig til hegðunar fyrirtækis til framtíðar (*ex ante*) en tekur ekki til sektar (refsingar) fyrir háttsemi sem þegar hefur átt sér stað (*ex post*).

Í núgildandi fjarskiptalögum er það eingöngu á valdi saksóknara (lögreglustjóra) að ákæra fyrir hugsanleg brot á fjarskiptalögum og vísa til viðurlagaheimilda sem dómstólum einum er heimilt að beita. Þetta getur verið þunglamalegt ferli, auk þess sem ákæranda í þessu tilviki getur skort nægileg sérfræðiþekking á sviði fjarskipta til þess að útgáfa ákæru verði talin raunhæfur kostur. Því þarf ekki að koma á óvart að aldrei hafi komið til ákærumeðferðar af þessu tagi til þessa.

Að áliti PFS skapar beiting þvingunarúrræða á borð við dagsektir, sem eingöngu horfa til hegðunar til framtíðar, en ekki til brota sem þegar hafa átt sér stað, ekki nægt aðhald með því að fjarskiptafyrirtæki hlíti ákvæðum fjarskiptalaga og einstökum ákvörðunum PFS sem á þeim eru reistar. Verður að horfa til þess að hugsanlegt brot á fjarskiptalögum, sem mögulega kann að hafa verið viðvarandi og staðið um einhvern tíma, getur haft í för með sér verulegan fjárhagslegan ávinning fyrir fjarskiptafyrirtæki eða skapað því á óbeinan hátt ágóða með skekktri samkeppnisstöðu. Telur PFS að það sé raunhæf hætta á því að þessi staðreynd, lagaumhverfið eins og það er í dag, hafi neikvæð áhrif á hegðun fyrirtækja á fjarskiptamarkaði.

Vísar stofnunin til þess að nánast allar systurstofnanir hennar í Evrópu, með örfáum undantekningum sem að sumu leyti skýrast af annars konar fyrirkomulagi stjórnsýslunnar, t.d. um sérstaka stjórnsýsludómstóla, hafa yfir að ráð heimild til þess að leggja á stjórnvaldssektir. Yfirlit um stöðu þessara mála í ríkjum ESB er að finna í fylgiskjali með bréfi þessu, en því hefur einnig verið dreift til þingmanna umhverfis- og samgöngunefndar. Þar kemur m.a. fram að í fjórum ríkjum, þ.e. Bretlandi, Írlandi, Hollandi og Tékklandi, er farin nákvæmlega sú

sama leið við útfærslu sektarheimilda eftirlitsstjórnvaldsins, eins og gerð er tillaga um í frumvarpinu.

Að lokum bendir PFS á mikilvægi þess að stjórnsýslustofnunum verði búið það lagaumhverfi og aðbúnaður svo þær séu í stakk búnar til að uppfylla skyldur sínar þannig að markmið þeirra laga sem þær hafa eftirlit með nái fram að ganga. Vísar PFS m.a. til umfjöllunar í skýrslu rannsóknarnefndar Alþingis um bankahrunið, þar sem talið var almennt mikilvægt að styrkja stjórnsýslustofnanir og efla eftirlitsheimildir þeirra. Hvað Póst- og fjarskiptastofnun varðar sérstaklega þá hefur verið bent á það í skýrslu um stöðu íslenskrar stjórnsýslu, sem unnin var af alþjóðlega ráðgjafarfyrirtækinu Cullen í tenglum við aðildarviðræður Íslands að Evrópusambandinu, að nauðsynlegt væri að efla sjálfstæði hennar og eftirlitsúrræði (bls. 96).

Virðingarfyllst,

Björn Geirsson, forstöðumaður lögfræðideildar

Afrit sent til innanríkisráðuneytisins

Fylgiskjal með bréfi PFS, dags. 1. feb. 2012

Countries for which you (Veronica Bocarova) are author: DK, SE

Due Date: 18/11/2011

Instruction:

Table 1 - Financial penalties: minimum and maximum amount – November 2011

Last update: November 2011

Contact: martin.schraa@cullen-international.com

Article 10 of the Authorisation Directive as amended by the EU 2009 regulatory framework strengthens NRAs' enforcement powers so as to improve the effective implementation of the framework.

In particular it states that the NRAs should have the power to require the cessation of the breach of the conditions of the general authorisation or the imposed regulatory obligations, either immediately or within a reasonable time limit and shall take appropriate and proportionate measures aimed at ensuring compliance.

In this regard, the NRA shall have the power *"to impose **dissuasive** financial penalties where appropriate, which may include periodic penalties having retroactive effect".*

The table below shows whether:

- national legislation on electronic communications establishes the minimum and maximum amount of financial penalties that NRA may impose on electronic communications undertakings; and
- if yes, how applicable **minimum** and **maximum** amounts are defined: e.g. **nominal** amounts, percentage of turnover, etc.

The table distinguishes between lump sum penalties and running penalty fines, which continue until an infringement is stopped.

Country	Provisions on financial penalties in national legislation on electronic communications	Minimum and maximum amount – lump sum penalty	Minimum and maximum amount – Running penalty payment	Nov. 2011 OK?
AT	Administrative offences: § 109 TKG 2003 (to be imposed by the regional Telecommunication Offices, which are four public authorities under control of the Ministry) Skimming off of unlawful benefits: § 111 TKG 2003 (the NRA decides that it was an unlawful act and the Cartel Court afterwards decides on the amount)	Administrative offences: €0 to €4,000, €0 to €8,000, €0 to €37,000 or €0 to €58,000, depending on the severity of the offence. Skimming off of unlawful benefits: depending on the amount of the unlawful benefit, maximum 10% of the undertaking's turnover of the preceding year		
BE	BIPT has the power to imposed administrative fines in case of breach of the regulatory framework (Law of Jan. 17, 2003 setting the status of BIPT).	Minimum 0.5 – maximum 5% of the yearly turnover for the market concerned, with max. €12,5m		
DK	Under chapter 33, §79 and chapter 35, §81 of the Law No.169 of March 3, 2011 on electronic communications networks and services, running financial penalties and one-off fines can be imposed for non-compliance with the Law and specific obligations imposed under the Law. The NRA may issue orders but cannot impose fines directly.	No specific amount is defined in the Law on electronic communications. General provisions on financial penalties are set out in the Penal Code. From the preparatory notes to the Law on electronic communications (p. 109-110), it follows that similar principles should	No specific amount is defined in the Law on electronic communications. General provisions on financial penalties are set out in the Penal Code.	OK

	On the NRA request, the financial penalty can be imposed by the ordinary courts conditional upon the Director of Public Prosecutions raising charges.	apply as for sanctions foreseen under the Competition Law, as follows: The fine is calculated on the basis of three factors: • the seriousness, • the length of the infringement • the turnover of the undertaking. There are three stages of seriousness: minor infringements, serious infringements and very serious infringements. There are also three stages of length, i.e. infringements lasting less than one year, between one and five years and more than five years. The fine may be increased or modified on the basis of the two factors depending on the turnover of the undertaking. For minor infringements the amount of fine would be in the range of DKK 10,000-400,000 (€1,300-€54,000). Very serious infringements should normally result in a fine of more than DKK 15m (approx €2m).		
FI	Communications Market Act 393/2003 • §121 – A conditional fine under law 1113/1990 in order to bring an ongoing breach into an end with a threat of fine • §122 – A penalty payment for a breach of an individual SMP or non-SMP obligation (§18 – 20 of the Act)	Conditional fine • Min and max not defined.	Penalty payment • Min. €1,000 • Max. €1m. However, if the breach has especially significant effects on the market, this may be exceeded. In any case the penalty may not exceed 5% of the operator's turnover from electronic communications networks and services in the previous year.	
FR	The Code of Postal services and Electronic Communications (Law part and Decree part) provides for a number of different fines in relation with various breaches of the law.	Yes ARCEP may impose a fine of up to 5% of the turnover of the operator Legal basis Article L5-3		
DE	§ 149 TKG 2004 : The NRA can impose administrative penalties	€0 to €500,000, €0 to €300,000, €0 to €100,000, €0 to €50,000 or €0 to €10,000, depending on the severity of the offence. The penalty shall be higher than the unlawful benefit gained from the offence. If the above mentioned ranges are not sufficient, the NRA may impose higher penalties.		
GR				
IE	Section 46A(6) of Communications Regulation Act 2002, as amended by Communications Regulation (Amendment) Act	Maximum of €5m or 10% of turnover, whichever is the higher amount	n/a	OK

	2007.			
IT	Art. 98 of the Communications Code	• Breach of SMP obligation: min 2% and max. 5% of annual turnover from the market where the breach took place • Other breaches Many categories to which different fines apply (typically not above €250,000	•	•
LU				
NL	Law on telecommunication, art. 15§2	Maximum €450.000 or, if it's more, maximum 10% of the relevant turnover.		
NO	The Electronic Communications Act (in English) • §10-7 Running penalty payment in order to bring an ongoing breach into an end • §12-4 Penalty for a breach of the Act	Penalty • Min and max not defined ("fine or imprisonment up to six months")	Running penalty payment • Min and max. not defined	ok
PT	Law 51/2011, of Sep. 13, 2011 (in PT) amending the Electronic Communications Law. • art. 113 §6 (lump sums) • 116§3/4/5 (running penalties)	Light infringements: between €100 and €100K Serious infringements: between € 250 and €1mn Very serious infringements: between €750 and €5mn. The level of penalties within each category (light, serious and very serious) is based on the nature y of the infringer: an individual, a micro-enterprise, a small enterprise, a medium enterprise or a big enterprise.	Running penalties must be proportionate and reasonable by taking into account the annual turnover of the infringer in the year which precedes the negative impact on the market caused by the unlawful conduct. • Min: €2000 • Max: €100K The above payments can increase daily but must not exceed a total of €3mn over a max period of 30 days.	OK
ES	General Telecommunications Law differentiates between 'very serious', 'serious' and 'light' infringements. The penalties vary according to this distinction (Article 56 of Law 32/2003 of Nov. 2003).	Very serious infringements The amount of the penalty should not be below, the gross profit obtained with the infringement nor above the quintuple thereof. If this criteria cannot be applied, or if applying this criteria would lead to an amount which is lower than the highest amount indicated below, the higher amount should be the maximum limit of the penalty: *For infringements related to non-compliance with CMT decisions* NB 1% of the gross annual revenues in the last financial year (or in its absence, current year) in the "*affected activity*"; NB 5% of total funds used to commit the infringement; NB 20 million euro. *For other very serious infringements not related to non-compliance with CMT decisions:* NB 2 million euro.	In addition to lump sum penalties, daily penalty payments can be imposed to ensure compliance with CMT decisions or with decisions of the ministry of industry within their respective competences Min. amount: €100/day Max. amount:€10,000/day	OK

		Serious infringements Penalty not below the gross benefit obtained from the infringement and not higher than the double of the gross benefit or, if this criteria cannot be applied, 500,000 €. Light infringements The maximum penalty is of 30,000 €.		
SE	Under Chapter 7, 4§ of the Law on electronic communications (2003:389), if PTS finds a reason to suspect that any undertaking operating under the Law on eiectronic communications "*does not comply with the Law or the decisions on obligations or conditions or the regulations that have been issued under the Law, or is not operating a radio transmitter in accordance to the attached conditions*", it shall notify the undertaking concerned and give the undertaking an opportunity to state its views within a reasonable time limit. PTS has powers to request *immediate* compliance with the Law and combine its request with a financial penalty. PTS enforcement powers were strengthened in line with the new provisions of Article 10 of the Authorisation Directive, following adoption of the amendments to the Law on electronic communications (2003:389) transposing the EU 2009 framework in May 2011 (see also Chapter 11, Supervision of the government bill (Prop. 2010/11:115), with preparatory notes – p.139) In particular PTS was given powers to require *immediate* cessation of the breach of the law and to propose penalties to ensure compliance. Previously PTS could only propose penalties after providing a reasonable time to ensure compliance (not less than one month). PTS cannot impose the financial penalty directly but has to submit the argumented request on imposing the penalty to the administrative court.	No specific amount is defined in the Law on electronic communications. Financial penalties that are imposed by administrative authorities are regulated by Law on financial penalties (1985:206). Under Article 3 of the Act on financial penalties the amount of the fine is set taking into account the economic situation of the undertaking and conditions that presumably should make it follow the authority's order in connection with the penalty. The amount of the penalty cannot be so low that it would be more beneficial economically for the undertaking not to follow the request to comply. Setting the amount of the penalty such factors as turnover, profit or the number of affected customers could be taken into consideration (see PTS principles for supervision, section 4.3.6)	No specific amount is defined in the Law on electronic communications. Financial penalties that are imposed by administrative authorities are regulated by Law on financial penalties (1985:206). Running penalty payment can be combined with one-off penalty.	OK
CH	Art. 60 of the Law on telecommunications.	Maximum 10 % of the average turnover for the last 3 years.		
UK	Section 97 of Communications Act 2003	Maximum amount of 10% of turnover of the relevant business for the relevant period	n/a	OK