PÓST- OG FJARSKIPTASTOFNUN

Ákvörðun nr. 24/2016

Öryggisatvik á vefsvæði Fjarskipta hf. í nóvember 2013.

I.
Forsaga málsins

1.1 Almennt

Í lok nóvember 2013 kom upp öryggisatvik á vefsvæði Fjarskipta hf. þegar brotist var inn á vefkerfi þess sem innihélt vefsvæðið vodafone.is og „Mínar síður“ félagsins, þar stolið gögnum sem vistuð voru á gagnagrunnum félagsins á vefsvæðinu og þau birt opinberlega á internetinu. Um var að ræða innihald smáskilaboðasendinga (SMS), umferðarskráningar þeirra, notendanöfn viðskiptavina þeirra o.fl.

1.2 Ákvörðun nr. 1/2014

Stofnunin hóf formlega skoðun á atvikinu með bréfi sínu, dags. 23. desember 2013, þar sem var óskað upplýsinga um þau gögn sem voru andlag innbrotsins og birt voru á internetinu. Þá var óskað eftir nákvæmri lýsingu á viðmóti vefkerfisins, með hvaða hætti og á hvaða tímabili mögulegt var að senda smáskilaboð úr vefkerfi félagsins. Þá hafði stofnuninni borist erindi frá einstaklingum er vörðuðu umrætt öryggisatvik og óskaði stofnunin eftir athugasemdum félagsins við þeim erindum.

Póst- og fjarskiptastofnun bárust gögn frá félaginu þann 23. janúar 2014 varðandi spurningar stofnunarinnar. Aftur á móti var óskað eftir frekari fresti til að taka af stöðu til þeirra kvartana sem borist höfðu. Í svarbréfi félagsins frá 23. janúar 2014 var gerður sérstakur fyrirvari þess efnis að veiting upplýsinga af hálfu félagsins fæli ekki í sér viðurkenningu á því að

fjarskiptalög og eftirlitsvald Póst- og fjarskiptastofnunar næðu yfir umrætt atvik. Stofnunin tók þá sjálfstæða ákvörðun nr. 1/2014 þess efnis að vefsvæði Fjarskipta hf. væri hluti af almennu fjarskiptaneti þess þar sem almenn fjarskiptaþjónusta væri veitt. Í ákvörðunarorðum segir:

> „Það sendikerfi sem flytur merki af vefsvæði Fjarskipta hf., vodafone.is, yfir í SMS miðlara í farsímakerfi félagsins telst vera fjarskiptanet í skilningi 13. tl. 3. gr. laga, nr. 81/2003, um fjarskipti.
>
> Sú þjónusta sem veitt er á vefsvæði Fjarskipta hf., vodafone.is, sem felur í sér sendingu smáskilaboða af internetinu yfir í farsíma telst vera fjarskiptaþjónusta í skilningi 15. tl. 3. gr. laga, nr. 81/2001, um fjarskipti.
>
> Sá hluti fjarskiptanets sem miðlar merkjum af vefsvæði Fjarskipta hf., vodafone.is, yfir í SMS miðlara í farsímakerfi félagsins og veitir viðskiptavinum félagsins sem tengjast „Mínum síðum“ með símanúmeri sínu telst hluti af almennu fjarskiptaneti þess í skilningi 5. tl. 3. gr. laga, nr. 81/2003, um fjarskipti.“

Fjarskipti hf. kærðu ákvörðun stofnunarinnar til úrskurðarnefndar fjarskipta- og póstmála sem staðfesti ákvörðunina að öllu leyti og tiltók sérstaklega að umrædd þjónusta teljist vera fjarskiptaþjónusta í skilningi fjarskiptalaga og *„*[þ]*ví falli fjarskiptastarfsemi kæranda undir ákvæði 47. gr. fjarskiptalaga og reglna nr. 1221/2007 settra á grundvelli hennar.“,* sbr. úrskurð nefndarinnar í máli nr. 3/2014.

Þann 9. apríl 2015 lagði félagið fram stefnu í héraðsdómi Reykjavíkur þar sem farið er fram á að ógiltur verði framangreindur úrskurður úrskurðarnefndar fjarskipta- og póstmála. Málið er enn fyrir dómi og með úrskurði héraðsdóms, dags. 3. maí sl., óskaði dómstóllinn ráðgefandi álits EFTA-dómstólsins í málinu.

Póst- og fjarskiptastofnun hélt áfram rannsókn sinni á öryggisatvikinu eftir töku ákvörðunar nr. 1/2014 og óskað upplýsinga frá félaginu, sbr. bréf dags. 26. mars 2014. Svarbréf félagsins barst í lok apríl. Í millitíðinni hafði félagið kært ákvörðun stofnunarinnar, sbr. framangreint. Af þeim sökum frestaði stofnunin frekari rannsókn á málinu þar til endanleg niðurstaða á stjórnsýslustigi lægi fyrir. Það var svo með bréfi Póst- og fjarskiptastofnunar til félagsins, dags. 3. febrúar sl., að óskað var ítarlegri svara við einstaka spurningum frá fyrra bréfi. Stofnuninni bárust viðbótarsvör félagsins þann 16. mars sl. Eftir yfirferð á þeim gögnum telur stofnunin að nægjanlegar upplýsingar liggi fyrir til ákvörðunartöku í máli þessu, sbr. síðari umfjöllun.

1.3 Kvartanir einstaklinga

1.3.1 Ósk um athugasemdir Fjarskipta hf. við fyrstu kvörtunum

Póst- og fjarskiptastofnun bárust strax í kjölfar öryggisatviksins kvartanir frá lögmannsstofunni Rétti f.h. tveggja einstaklinga. Þá barst þriðja kvörtunin frá stofunni í janúar 2014. Töldu einstaklingarnir sig hafa orðið fyrir miklum skaða sökum birtingar á innihaldi skilaboða sem vörðuðu oft á tíðum mjög viðkvæm persónuleg málefni. Taldi Réttur að

varðveisla gagna um hlutaðeigandi umbjóðendur lögmannsstofunnar hafi verið með öllu óheimil. Eins væri Fjarskiptum hf. einungis heimilt að varðveita fjarskiptaumferðarupplýsingar í sex mánuði, skv. 42. gr. fjarskiptalaga. Að mati Réttar höfðu Fjarskipti hf. gerst brotleg við XI. kafla laga, nr. 81/2003, um fjarskipti, einkum 42. og 47. gr., sbr. 1. mgr., sbr. 3. mgr. 73. gr. sömu laga.

Þá taldi Réttur að opinberir eftirlitsaðilar hefðu brugðist skyldum sínum gagnvart umbjóðendum stofunnar sem neytendum fjarskiptaþjónustu Fjarskipta hf. Vísar lögmannsstofan til ákvæða 1., 4. og 5. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun máli sínu til stuðnings.

Þá bárust kvartanir frá þremur einstaklingum sem leituðu beint til Póst- og fjarskiptastofnunar í byrjun desember 2013.

Með bréfi sínu, dags. 23. desember 2013 óskaði Póst- og fjarskiptastofnun athugasemda Fjarskipta hf. við þeim fimm kvörtunum sem þá höfðu borist vegna öryggisatviksins, þ.e. tveimur frá Rétti og hinum þremur sem einstaklingar sendu sjálfir til stofnunarinnar. Með bréfum Fjarskipta hf., dags. 7. febrúar 2014, voru settar fram athugasemdir félagsins við kvörtununum.

Í bréfum Fjarskipta hf. er því hafnað að félagið hafi gerst brotlegt við fjarskiptalög. Afstaða félagsins var sett fram með sambærilegum hætti í öllum bréfum, þótt svarbréfum vegna kvartana sem bárust frá Rétti hafi fylgt afrit af sérstöku svari félagsins til lögmannsstofunnar. Sjónarmið félagsins er hin sama varðandi allar kvartanirnar en félagið telur að þau gögn sem stolið var á vefsíðunni falli ekki undir gildissvið fjarskiptalaga. Í einu bréfinu segir:

> „Vodafone bendir á að 42. gr. fjarskiptalaga er ætlað að ná til fjarskiptaumferðar, eða eins og hún er skilgreind skv. ákvörðun PFS nr. 29/2011: *„ ....tengiupplýsingar sem verða til í fjarskiptaneti og greiðslukerfum fjarskiptafyrirtækja vegna fjarskiptanotkunar viðskiptavina og liggja til grundvallar gjaldfærslu fyrir þjónustuna.“*
>
> Fjarskiptaumferð nær þarf af leiðandi ekki til aðgerða á þjónustusíðum viðskiptavina fjarskiptafélaga eða annarra fyrirtækja hér á landi heldur til þeirrar umferðar sem um fjarskiptakerfi félagsins fara og öryggi þeirra upplýsinga á þeim tíma sem þær fara um þau kerfi. Þjónustusíður fyrirtækja hafa þann tilgang að veita viðskiptavinum sínum yfirlit yfir viðskipti sín. Einnig er algengt að viðskiptavinum sé boðið upp á að breyta þjónustu sinni eða stillingum eftir þeirra eigin þörfum. Vodafone telur að um þjónustusíður félagsins gildi sömu reglur og gilda um þjónustusíður annarra fyrirtækja, t.d. tryggingafélaga, flugfélaga, orkufyrirtækja, opinberra aðila, verslana o.s.frv. Þjónustusíður Vodafone falli því ekki undir frekar en þjónustusíður annarra fyrirtækja.

> Ástæða geymslu þeirra gagna var sú að þjónustusíða félagsins og vefsíður almennt eru forritaðar með þeim hætti að þær breyta öllum þeim aðgerðum sem gerðar eru á þjónustusíðunni í vefkóða sem síðan geymist sjálfkrafa. Umræddar upplýsingar falla ekki undir fjarskiptaumferðargögn og hafði Vodafone þar af leiðandi ekki gripið til þeirra aðgerða við eyðingu gagna líkt og fjarskiptalög tilgreina að gera þurfi í kringum fjarskiptaumferðargögn. Þess ber að geta að allar vefsíður geyma upplýsingar með sama hætti og leiddu yfirlýsingar annarra fjarskiptafélaga sem og annarra félaga hér á landi eftir innbrotið slíkt í ljós.“

Staðfestir félagið í sumum svarbréfa sinna að *„ ... öll fjarskiptaumferðargögn um kvartanda hafi verið fjarlægð úr kerfum ... „* félagsins. Ekki er í svörum félagsins til stofnunarinnar að finna skýra afstöðu þess til varðveislu á efnisinnihaldi skilaboðanna sem send voru af vefsvæði félagsins heldur er fyrst og fremst vikið að fjarskiptaumferðargögnum.

1.3.2 Framsending erinda milli Póst- og fjarskiptastofnunar og Persónuverndar

Póst- og fjarskiptastofnun átti í samskiptum við Persónuvernd vegna umrædds öryggisatviks og þeirra kvartana sem borist höfðu, sbr. bréf Persónuverndar dags. 16. desember 2013 og bréf Póst- og fjarskiptastofnunar dags. 14. febrúar 2014. Var niðurstaðan í samskiptum stofnananna sú að Persónuvernd myndi fjalla um varðveislu skilaboða og meint samþykki fyrir þeim og Póst- og fjarskiptastofnun myndi fjalla um öryggi þeirra upplýsinga sem vistaðar voru á vefsvæði Fjarskipta hf. Aftur á móti áskildi Póst- og fjarskiptastofnun sér því rétt, þegar Persónuvernd hefur lokið málsmeðferð sinni, til að meta í frumkvæðisrannsókn sinni hvort tilefni sé til að fjalla um varðveislu persónuupplýsinganna á grundvelli ákvæða fjarskiptalaga nr. 81/2003, sér í lagi m.t.t. 42. og 4. mgr. 47. gr. laganna.

Póst- og fjarskiptastofnun framsendi því framangreindar kvartanir og þau svör sem borist höfðu frá Fjarskiptum hf. til Persónuverndar til þóknanlegrar málsmeðferðar, sbr. bréf stofnunarinnar dags. 14. febrúar 2014, og fékk að sama skapi framsend til sín erindi tveggja einstaklinga sem leitað höfðu til Persónuverndar vegna málsins, sbr. bréf stofnunarinnar dags. 31. janúar 2014.

1.3.3 Ósk um athugasemdir Fjarskipta hf. við framsendum kvörtunum

Með bréfum Póst- og fjarskiptastofnunar, dags. 31. mars 2014, óskaði stofnunin athugasemda Fjarskipta hf. við þeim kvörtunum sem framsendar höfðu verið frá Persónuvernd. Umrædd bréf voru send eftir töku ákvörðunar nr. 1/2014, þar sem kveðið var á um að vefsvæði Fjarskipta hf. og sú þjónusta sem þar var veitt félli undir gildissvið fjarskiptalaga.

Í svarbréfum Fjarskipta hf., dags. 15. apríl 2015, kom fram sú skoðun félagsins að það telji umrædda ákvörðun stofnunarinnar ranga og að það hafi ekki gerst brotlegt við fjarskiptalög hvað varðar vefsvæði félagsins. Þá hafi félagið farið eftir ákvæðum laganna í hvívetna þegar kemur að upplýsingum í fjarskiptakerfum félagsins.

1.3.4 Afstaða Póst- og fjarskiptastofnunar til einstakra kvartana

Að mati Póst- og fjarskiptastofnunar mun niðurstaða hinnar almennu rannsóknar stofnunarinnar á því öryggisatviki sem átti sér stað á vefsvæði Fjarskipta hf. jafnframt veita efnislega niðurstöðu í máli þeirra einstaklinga sem sendu inn kvörtun til stofnunarinnar. Stofnunin mun því ekki taka sérstakar ákvarðanir í málum einstakra kvartenda enda mun ákvörðun vegna öryggisatviksins og sú niðurstaða sem hér er boðuð ná til hagsmuna þeirra sem og annarra sem atvikið náði til.

II.
Lagaumhverfi

2.1 Vernd persónuupplýsinga og friðhelgi einkalífs

Ljóst er að þar til bær stjórnvöld á stjórnsýslustigi telja að sú þjónusta sem veitt var af hálfu Fjarskipta hf. á vefsvæði þess telst vera almenn fjarskiptaþjónusta veitta á almennu fjarskiptaneti þess. Þá er jafnljóst, að mati stjórnvalda, að umrætt öryggisatvik fellur undir eftirlitsvald stofnunarinnar.

Póst- og fjarskiptastofnun hefur eftirlit með framkvæmd fjarskiptalaga og skal stofnunin framfylgja þeim lögum og stuðla að því að markmið þeirra náist, sbr. 1. tl. 1. mgr. 3. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun. Eitt af lögbundnum hlutverkum stofnunarinnar er að stuðla að vernd neytenda í viðskiptum þeirra við fjarskiptafyrirtæki og vinna að ráðstöfunum til að vernda persónuupplýsingar og friðhelgi einkalífs, sbr. b og c liði 4. tl. 1. mgr. 3. gr. tilvitnaðra laga um stofnunina.

Innan Evrópusambandsins var talin þörf á að grípa til sérstakra verndarráðstafana fyrir persónuupplýsingar í fjarskiptum og með tilskipun Evrópuþingsins og Ráðsins, nr. 2002/58/EB, um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta (og forvera hennar) voru meginreglur, sem settar voru fram í tilskipun nr. 95/46/EB, um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga, yfirfærðar í sértækar reglur fyrir fjarskiptasviðið. Eru ákvæði tilskipunarinnar viðbót við og nánari umfjöllun um ákvæði síðarnefndu tilskipunarinnar, sbr. 2. mgr. 1. gr. og 4. lið inngangsorða tilskipunar nr. 2002/58/EB.

Þannig er tilskipuninni ætlað að vernda grundvallarréttindi einstaklinga og einkum rétt þeirra til friðhelgi einkalífsins sem og einnig réttmætra hagsmuna lögaðila. Leggur tilskipunin þá skyldu á aðila, sem býður fram rafræna fjarskiptaþjónustu, að gera viðeigandi ráðstafanir til að standa vörð um öryggi þeirrar þjónustu sem hann veitir, sbr. 1. mgr. 4. gr. tilskipunarinnar. Felur þetta í sér ráðstafanir til að koma í veg fyrir óheimilan aðgang að fjarskiptasendingum, til að standa vörð um leynd fjarskiptasendinga, þ.m.t. bæði efni og hvers kyns gögn sem tengjast slíkum fjarskiptasendingum, sbr. 21. lið inngangsorða hennar.

Þá fjallar tilskipunin um fjarskiptaleynd, sbr. 5. og 6. gr. tilskipunarinnar. Þar er lögð skylda á aðildarríki, með innlendri löggjöf, að fjarskiptaleynd og leynd tengdra umferðargagna við

notkun almennra fjarskiptaneta og rafrænnar fjarskiptaþjónustu, sem er öllum aðgengileg, sé tryggð. Með fjarskiptaleynd er hvort tveggja átt við efnisinnihald fjarskipta sem og umferðargögn þeirra.

Í IX. kafla fjarskiptalaga er fjallað um vernd persónuupplýsinga og friðhelgi einkalífs. Byggja ákvæði kaflans að mörgu leyti á framangreindri tilskipun um vinnslu persónuupplýsinga og vernd einkalífs á sviði rafrænna fjarskipta. Hluti kaflans kom nýr inn í fjarskiptalöggjöf hér á landi við gildistöku fjarskiptalaga árið 2003 en aftur á móti var ákvæðum kaflans, er varða öryggi fjarskipta, breytt umtalsvart árið 2007 þar sem auknar kröfur voru lagðar á fjarskiptafyrirtæki til að tryggja leynd og vernd upplýsinga á fjarskiptanetum.

2.2 Ákvæði 47. gr. fjarskiptalaga

Í 47. gr. fjarskiptalaga er fjallað um öryggi og þagnarskyldu í fjarskiptum. Ákvæði 47. gr. er ætlað að gegna lykilhlutverki þegar kemur að leynd fjarskipta til verndar friðhelgi einkalífs áskrifenda og er mikilvægur þáttur í öryggi fjarskiptaþjónustu. Sá hluti ákvæðisins er varðar kröfur um vernd upplýsinga er að finna í 1. og 2. mgr. ákvæðisins og kom að mestu leyti inn í fjarskiptalög með lögum, nr. 39/2007, um breytingu á lögum um fjarskipti nr. 81/2003. Voru með þeirri lagabreytingu lagðar skyldur á fjarskiptafyrirtæki um að verja upplýsingar sem fara um fjarskiptanet þeirra. Var hér lögfest inntak upplýsingaöryggis, þ.e. að tryggð skuli leynd upplýsinga, lögmætan aðgang að þeim, aðgengi þeirra og réttleika.

Málsgreinarnar eru svohljóðandi:

> *Fjarskiptafyrirtæki sem veita almenna fjarskiptaþjónustu skulu gera viðeigandi ráðstafanir til þess að tryggja öryggi þjónustunnar í samráði við rekstraraðila fjarskiptaneta ef við á. Verja skal upplýsingar sem fara um fjarskiptanet gegn því að þær glatist, skemmist eða breytist fyrir slysni eða að óviðkomandi fái aðgang að þeim. Ef sérstök hætta er á að leynd fjarskipta á tilteknu neti verði rofin skal þjónustuveitandinn upplýsa áskrifendur um hættuna.*
>
> *Fjarskiptafyrirtæki skulu skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, gera áhættumat og ákveða öryggisráðstafanir á grundvelli þess. Póst- og fjarskiptastofnun setur reglur um vernd upplýsinga í almennum fjarskiptanetum þar sem nánar er mælt fyrir um þær kröfur sem gerðar eru til skipulags upplýsingaöryggis. Skulu reglurnar m.a. kveða á um:*
>
> *a. hvernig skjalfesta skuli skipulag upplýsingaöryggis,*
> *b. hlítingu við tiltekna staðla,*
> *c. framkvæmd innra eftirlits,*
> *d. helstu öryggisráðstafanir sem viðhafa skal,*
> *e. tilkynningar vegna öryggisrofs,*
> *f. eftirlitsúrræði Póst- og fjarskiptastofnunar.*

Er í 1. mgr. 47. gr. kveðið á um þá skyldu fjarskiptafyrirtækja, sem veita almenna fjarskiptaþjónustu, að þau skuli gera viðeigandi ráðstafanir til þess að tryggja öryggi

þjónustunnar. Skulu þau verja upplýsingar sem fara um fjarskiptanet gegn því að þær glatist, skemmist eða breytist fyrir slysni eða að óviðkomandi fái aðgang að þeim. Eins er kveðið á um skyldu félaganna um að upplýsa áskrifendur ef sérstök hætta er á að leynd fjarskipta á tilteknu neti verði rofin.

Í athugasemdum með frumvarpi er varð að breytingarlögunum segir jafnframt að túlka skuli hugtakið *upplýsingar* með rúmum hætti og er því ekki eingöngu átt við persónuupplýsingar heldur einnig þau gögn sem teljast til fjarskipta, sbr. skilgreiningarákvæði laganna. Í 16. tölul. 3. gr. fjarskiptalaga kemur fram að til fjarskipta teljist *„*[h]*vers konar sending og móttaka tákna, merkja, skriftar, mynda og hljóða eða hvers konar boðmiðlun eftir leiðslum, þráðlausri útbreiðslu eða öðrum rafsegulkerfum.“*

Í 2. mgr. ákvæðisins er enn fremur sett sú skylda á fjarskiptafyrirtæki að skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, gera áhættumat og ákveða öryggisráðstafanir á grundvelli þess. Er gerð skriflegs fyrirkomulags um upplýsingaöryggi nauðsynlegur liður í því að meta gæði þess. Gerir ákvæðið þannig ráð fyrir því að stjórnendur fjarskiptafyrirtækja móti sér *öryggisstefnu* þar sem afstaða þeirra til upplýsingavinnslunnar ásamt helstu áherslum í tengslum við öryggi hennar kemur fram.

Þá skal í *áhættumati* skilgreina þær hættur sem steðja að öryggi fjarskipta, meta líkindi þess að slíkar hættur verði að veruleika og afmarka umfang hugsanlegs tjóns af völdum þeirra. Þá skulu fjarskiptafyrirtækin, til að draga úr og sporna við hættunum, skjalfesta til hvaða *öryggisráðstafana* skuli gripið, þ.e. hvaða tæknilegu og skipulagslegu ráðstafanir skuli viðhafa. Þannig skulu hinar völdu öryggisráðstafanir tryggja nægilegt öryggi miðað við áhættu af vinnslunni og eðli þeirra gagna sem verja á, að teknu tilliti til nýjustu tækni og kostnaðar við framkvæmd þeirra.

Ákvæðið gerir þá kröfu að Póst- og fjarskiptastofnun setji reglur um vernd upplýsinga í almennum fjarskiptanetum þar sem nánar er kveðið á um þær kröfur sem gerðar skulu til slíks skipulags upplýsingaöryggis. Hefur Póst- og fjarskiptastofnun sett reglur nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.

2.3 Reglur nr. 1221/2007

Framangreindar reglur ná til net- og upplýsingaöryggis í almennum fjarskiptanetum, þ.e. hinum eiginlegu fjarskiptanetum svo og upplýsingakerfum sem þau styðjast við og tengjast, á gildissviði laga nr. 81/2003 um fjarskipti, sbr. 1. mgr. 2. gr. þeirra. Markmið reglnanna er að *„ ... auka neytendavernd og treysta stoðir upplýsingasamfélagsins með því að gera auknar kröfur til öryggis fjarskiptakerfa sem almenningur og fyrirtæki nota.“*

Þannig kveða reglurnar á um þær ráðstafanir sem að Póst- og fjarskiptastofnun telur að nauðsynlegt sé fyrir fjarskiptafyrirtæki að grípa til, til að tryggja vernd umferðar og upplýsinga á almennum fjarskiptanetum. Þannig segir að leitast skuli við *„ ... að tryggja leynd upplýsinga, lögmætan aðgang að þeim, tiltækileika þeirra og réttleika.“*

Í reglunum er að finna almennar kröfur og leiðbeiningar þegar kemur að vernd almennrar fjarskiptaþjónustu og leynd þeirra upplýsinga sem finna má á almennum fjarskiptanetum. Með leynd er átt við vernd upplýsinga gegn óviðkomandi aðgangi, bæði á meðan þær eru sendar á milli staða og þar sem þær eru vistaðar, sbr. skilgreiningarákvæði 3. gr. reglnanna. En samkvæmt sama ákvæði teljast upplýsingar vera hvers konar tákn, merki, skrift, mynd og hljóð sem send eru eða móttekin eða hvers konar boðmiðlun eftir leiðslum, með þráðlausri útbreiðslu eða öðrum rafsegulmiðlum.

Net- og upplýsingaöryggi felur, skv. 3. gr., í sér hæfni fjarskiptaneta til að tryggja að ákveðin fyrirfram skilgreind öryggismörk standist þegar ógnir steðja að eða ef veilur myndast, t.d. vegna mannlegra mistaka eða skemmdarverka, sem stofna í hættu leynd, réttleika og tiltækileika upplýsinga í fjarskiptanetum. En það getur að auki falið í sér aðra eiginleika, svo sem ósvikni, ábyrgð, óhrekjanleika og áreiðanleika.

Líkt og áður segir ná reglurnar til net- og upplýsingaöryggis í fjarskiptanetum og leggja þær skyldur á fjarskiptafyrirtæki að gera *viðeigandi ráðstafanir* til að tryggja vernd upplýsinga sem um þau fara. Skulu þær ráðstafanir, að teknu tilliti til tæknistigs og kostnaðar við framkvæmdina, tryggja hæfilegt öryggisstig miðað við þá áhættu sem um er að ræða, sbr. 4. gr. reglnanna. Í ákvæðinu segir:

> *Fjarskiptafyrirtæki skulu gera viðeigandi ráðstafanir til þess að tryggja vernd almennrar fjarskiptaþjónustu og fjarskiptaneta sem þau reka, m.a. verja upplýsingar sem um þau fara gegn ólöglegri eyðileggingu, glötun eða breytingum fyrir slysni eða vegna óleyfilegs aðgangs. Þessar ráðstafanir skulu, að teknu tilliti til tæknistigs og kostnaðar við framkvæmdina, tryggja hæfilegt öryggisstig miðað við þá áhættu sem um er að ræða.*

Eins skulu fjarskiptafyrirtækin, skv. 5. gr., tryggja að viðskiptavinir þeirra njóti verndar gagnvart hlustun, hlerun, geymslu eða annars konar hindrun eða vöktun fjarskipta, þ.m.t. *skilaboða* og *auðkenna*, sem fara um fjarskiptanet þeirra, nema að slíkt fari fram með *samþykki* viðskiptavinanna eða samkvæmt heimild í lögum, sbr. einnig 4. mgr. 47. gr. laganna. Undanþegið þessu er þó tímabundin tæknileg geymsla upplýsinga meðan þær eru í flutningi á því tilskyldu að innihald þeirra sé ekki birt á neinn hátt. Í ákvæðinu segir:

> *Fjarskiptafyrirtæki skulu tryggja að viðskiptavinir þeirra njóti verndar gagnvart hlustun, hlerun, geymslu eða annars konar hindrun eða vöktun fjarskipta, þ.m.t. skilaboða og auðkenna, sem fara um fjarskiptanet þeirra, nema að slíkt fari fram með samþykki viðskiptavinanna eða samkvæmt heimild í lögum. Undanþegin er tímabundin tæknileg geymsla upplýsinga meðan þær eru í flutningi enda sé innihald þeirra ekki birt á neinn hátt.*
>
> *Enn fremur skal tryggja að geymsla eða aðgengi fjarskiptafyrirtækjanna að upplýsingum í endabúnaði viðskiptavina sé aðeins heimiluð ef notandanum eru gefnar greinargóðar upplýsingar um tilganginn og gert kleift að hafna því. Þetta skal*

þó heimilt í þeim tæknilega tilgangi að flytja rafræn boð yfir fjarskiptanet eða sem hluti af reglulegum uppfærslum.

Þá skulu félögin tryggja réttleika upplýsinga viðskiptavina sinna og vernda þær fyrir breytingum, sbr. 6. gr. reglnanna. Í ákvæðinu segir:

Fjarskiptafyrirtæki skulu tryggja réttleika upplýsinga viðskiptavina sinna á þann hátt að þær verði ekki fyrir breytingum, bæði þeirra upplýsinga sem eru í flutningi um almenn fjarskiptanet og aðrar fjarskiptaupplýsingar.

Til að tryggja vernd almennrar fjarskiptaþjónustu og þeirra upplýsinga sem um fjarskiptanet fara í samræmi við framangreind ákvæði er fjarskiptafélögum gert skylt í 7. gr. reglnanna að útbúa og viðhalda skjalfestri lýsingu á stjórnkerfi sem tryggir upplýsingaöryggi í fjarskiptaþjónustu og fjarskiptanetum og byggir að lágmarki á gerð *öryggisstefnu, áhættumati* og lýsingu á *öryggisráðstöfunum.* Ber fjarskiptafyrirtækjum að setja sér skriflega öryggisstefnu, sbr. 1. tl. greinarinnar en þar segir:

Fjarskiptafyrirtæki skal setja sér skriflega öryggisstefnu. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda fjarskiptafyrirtækis til öryggismála. Í stefnunni skulu koma fram markmið og meginreglur upplýsingaöryggis samkvæmt rekstrarstefnu og rekstrarmarkmiðum. Stefnan skal kynnt öllum starfsmönnum fjarskiptafyrirtækisins sem hafa með fjarskiptarekstur að gera. Við mótun öryggisstefnu skal taka mið af því hvaða upplýsingar skuli vernda, hvernig skuli vernda þær, þeirri aðferð sem viðhöfð verður við vinnslu þeirra og hver beri ábyrgð á öryggi þeirra. Skal öryggisstefnan birt starfsmönnum.

Þá er fjarskiptafyrirtækjum skylt að skilgreina aðferðarfæði áhættumats um upplýsingaöryggi, sbr. 2. tl. greinarinnar en þar segir:

Fjarskiptafyrirtæki skal skilgreina aðferðarfræði áhættumats um upplýsingaöryggi og henni fylgt eftir með skriflegu áhættumati um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu. Áhættumat skal bera kennsl á áhættuþætti, umfang þeirra og forgangsraða þeim miðað við ásættanlega áhættu og þau markmið sem skipta máli fyrir fyrirtækið. Áhættumat skal skilgreina eignir og gera á þeim einfalt mat og mat á þeim áhrifum sem myndast af völdum rofs á leynd, réttleika og tiltækileika. Miklir veikleikar og ógnir eru skilgreind fyrir eignirnar, ásamt mati á líkindum þeirra. Áhættan fyrir hvert atriði er reiknuð út og hún borin saman við fyrirframgerðan mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum og skal það endurskoðað reglulega.

Fjarskiptafyrirtækjum er enn fremur skylt að setja sér verklagsreglur um örugga meðferð upplýsinga og eyðingu þeirra, sbr. 3 tl. greinarinnar en þar segir:

Fjarskiptafyrirtæki skulu setja sér verklagsreglur um örugga meðferð upplýsinga og eyðingu þeirra. Gerðar skulu öryggisráðstafanir og settar fram skriflegar lýsingar á þeim. Tilgreina skal hvaða öryggisráðstöfunum verði beitt og hvernig þær verði útfærðar, þ.á.m. við hönnun, þróun, rekstur, prófun og viðhald hvers kerfis. Þá skal og tekið fram hvernig brugðist verði við áföllum í rekstri fjarskiptaneta og fjarskiptaþjónustu. Öryggisráðstafanir skal endurskoða reglulega. Skriflegar leiðbeiningar skulu vera til staðar fyrir einstaka ferla sem nauðsynlegir eru fyrir upplýsingaöryggi fjarskiptaneta og fjarskiptaþjónustu. Fjarskiptafyrirtækið skal sjá til þess að ákvæðum stefnunnar um upplýsingaöryggi sé framfylgt, líka þegar verktakar vinna fyrir fyrirtækið. Fjarskiptafyrirtækið skal sjá til þess að starfsmenn þess framfylgi stefnunni um upplýsingaöryggi.

Þá er sett sú skylda í 8. gr. reglnanna að viðhaft sé innra eftirlit til að tryggja að unnið sé í samræmi við öryggisstefnu og skjalfestar verklags- og öryggisreglur öryggisskipulags og að uppbygging þess sé í samræmi við lög og reglur. Framkvæma ber innra eftirlit með kerfisbundnum hætti samkvæmt fyrirfram skilgreindri aðferð og skal tíðni og umfang þess ákveðið með hliðsjón af skilgreindri áhættu, eðli þeirra upplýsinga sem um er að ræða, tækni sem notuð er til að tryggja öryggi þeirra og kostnaði af framkvæmd eftirlitsins. Ákvæðið setur þó þá lágmarkskröfu að það skuli framkvæmt eigi sjaldnar en árlega og skulu fjarskiptafyrirtækin gera skýrslu um niðurstöður þess. Í ákvæðinu segir:

Viðhafa skal innra eftirlit til að tryggja að unnið sé í samræmi við öryggisstefnu og skjalfestar verklags- og öryggisreglur öryggisskipulags og að uppbygging þess sé í samræmi við lög og reglur. Innra eftirlit skal framkvæma kerfisbundið samkvæmt fyrirfram skilgreindri aðferð. Tíðni og umfang eftirlitsins skal ákveðið með hliðsjón af skilgreindri áhættu, eðli þeirra upplýsinga sem um er að ræða, tækni sem notuð er til að tryggja öryggi þeirra og kostnaði af framkvæmd eftirlitsins. Það skal þó framkvæmt eigi sjaldnar en árlega. Fjarskiptafyrirtæki skulu gera skýrslu um niðurstöður innra eftirlits.

Í III. kafla reglnanna er svo fjallað um öryggisráðstafanir og eru í 12. gr. reglnanna settar skýrar kröfur um að fjarskiptafyrirtæki skuli viðhafa nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að verja almenn fjarskiptanet sín. Eru í ákvæðinu taldar upp, í tíu eftirfarandi töluliðum, ákveðnar ráðstafanir sem þau skulu, eftir því sem við á, viðhafa:

1. *Stýringar fjarskiptabúnaðar skulu vera varðar gegn óheimilum aðgangi að skilaboðum og auðkennum í flutningi, svo sem með dulkóðun eða lokuðum stýrinetum.*
2. *Nota aðgangsheimildir, aðgangsstýringu og óhrekjanleika.*
3. *Staðfesta skal að óskir um breytingu á fjarskiptaþjónustu komi frá áskrifanda hennar, eða séu með samþykki hans.*
4. *Tryggja óhrekjanleika aðgerða.*
5. *Tryggja rekjanleika uppflettinga og vinnsluaðgerða.*
6. *Takmarka aðgang starfsmanna að upplýsingum við þær sem eru þeim nauðsynlegar til að þeir geti sinnt starfi sínu, og við þann tíma sem nauðsynlegur er.*

7. *Upplýsingaöflun vegna afgreiðslu og reikningagerðar, skal aðskilja frá öflun upplýsinga um fjarskiptaumferð sem nýtast kann í þágu rannsókna opinberra mála og almannaöryggis, t.d. innihald fjarskipta.*
8. *Viðhalda órofinni slóð sönnunargagna sem nýst gætu vegna öryggisatburða. Skilgreina búnað og vinnslu fyrirfram á þann hátt að sem flest mikilvæg þess háttar tilvik komi með skýrum hætti fram í eftirlitskerfum.*
9. *Halda skrá um aðgangsheimildir og aðgangsréttindi og yfirfara reglulega. Skal fjarskiptabúnaður vera stilltur til samræmis við þá skráningu.*
10. *Viðhafa skal viðeigandi ráðstafanir til að tryggja öryggi upplýsinga í boðskiptum endanna á milli við eftirtaldar aðstæður:*
    a. *Starfsmenn vinna í fjarvinnslu við viðkvæm fjarskiptakerfi.*
    b. *Fjarskiptafyrirtæki veita viðskiptavinum sínum sérstakt fjarvinnsluaðgengi að kerfum viðskiptavinarins, með stýringu og viðkomu í kerfum fjarskipta-fyrirtækisins, svo sem aðgengi að pósthúsum eða gagnageymslum fyrir-tækja frá farsíma.*

2.4 Ákvæði 42. gr. fjarskiptalaga

Í 42. gr. fjarskiptalaga er fjallað um gögn um fjarskipti, meðferð þeirra og eyðingu. Ákvæðið byggir að mestu leyti á 6. gr. áðurnefndrar tilskipunar Evrópuþingsins og Ráðsins 2002/58/EB um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta. Við gildistöku fjarskiptalaga árið 2003 innihélt ákvæði 42. gr. fimm málsgreinar en árið 2005 tóku gildi lög um breytingu á lögum um fjarskipti, nr. 81/2003, sem breytti ákvæðinu með þeim hætti að við bættust tvær nýjar málsgreinar, þ.e. núgildandi 3. og 7. mgr.

Ákvæðið kveður á um þá meginreglu að gögnum um fjarskiptaumferð notenda, sem geymd eru og fjarskiptafyrirtæki vinnur úr, skal eyða eða gera nafnlaus þegar þeirra er ekki lengur þörf við afgreiðslu ákveðinnar fjarskiptasendingar, sbr. 1. mgr. Frá þessari meginreglu er þó að finna ákveðnar undanþágur.

Í fyrsta lagi er í 2. mgr. ákvæðisins kveðið á um heimild fjarskiptafélaga til að geyma gögn um fjarskiptanotkun sem nauðsynleg eru til reikningsgerðar fyrir áskrifendur og uppgjörs fyrir samtengingu þar til ekki er lengur hægt að vefengja reikning eða hann fyrnist. Í frumvarpi er varð að fjarskiptalögum árið 2003 kemur fram að 1. mgr. ákvæðisins geri þá kröfu að gögnum um fjarskiptaumferð áskrifenda sé eytt eftir að þeirra er ekki þörf við stýringu og afgreiðslu fjarskiptanna. Segir í athugasemdunum að við *„ ... sendingu hvers konar fjarskipta verða til í netum og stoðkerfum ýmsar upplýsingar, t.d. um leiðir sem valdar hafa verið fyrir sambandið hverju sinni, lengd þeirra, tímasetningu og magn ... “* en ekki sé nauðsynlegt að geyma öll þessi gögn eftir að samband hefur verið rofið.

Í ákvörðun Póst- og fjarskiptastofnunar nr. 29/2011 komst stofnunin að þeirri niðurstöðu að hámarksvarðveislutími fjarskiptaumferðarupplýsinga geti að hámarki verið sex mánuðir þegar reikningur hefur verið greiddur. Þessar upplýsingar, sem reikningar byggja á, séu gjaldfærsluupplýsingar sem í eðli sínu eru persónurekjanlegar. Í samandreginni niðurstöðu stofnunarinnar segir að varðveislutími fjarskiptaumferðarupplýsinga, skv. 2. mgr. ákvæðisins,

skuli afmarkaður á almennan, sjálfstæðan hátt og eingöngu á grundvelli brýnnar nauðsynjar, svo sem til þess að geta brugðist við vefengingu reiknings innan hæfilegs tíma frá því hann hefur verið greiddur. Sá tími, geti að mati stofnunarinnar, að hámarki verið sex mánuðir, enda gildi lengri varðveislutími fyrir reikninga sem eru í vanskilum. Þannig skuli eyða upplýsingum eða gera þær ópersónugreinanlegar við lok skilgreinds varðveislutíma hafi reikningur verið greiddur.

Í öðru lagi er um að ræða varðveislu á lágmarksskráningu gagna um fjarskiptaumferð í sex mánuði í þágu rannsókna sakamála og almannaöryggis, sbr. 3. mgr. ákvæðisins. Undanþáguákvæði 3. mgr. var sett árið 2005 að ósk ríkislögreglustjóra og miðar að því að tryggja lögreglu og ákæruvaldi nægjanlegt svigrúm til að upplýsa brot, að uppfylltum skilyrðum ákvæða sakamálalaga nr. 88/2008. Er fjarskiptafyrirtækjum jafnframt óheimilt að nota eða afhenda umræddar upplýsingar öðrum en lögreglu eða ákæruvaldi, sbr. núgildandi 7. mgr. 47. gr. fjarskiptalaga.[1] Í frumvarpinu var lagt til að geymslutími þessarar lágmarksskráningu gagna sem fjarskiptafyrirtækjum væri skylt að varðveita yrðu tólf mánuðir. Í þinglegri meðferð þáverandi samgöngunefndar var gerð sú breyting á frumvarpinu og varðveislutíminn var styttur úr tólf mánuðum niður í sex mánuði. Taldi meiri hluti nefndarinnar að í ákvæðinu vægust á almannahagsmunir og réttur einstaklinga til persónuverndar og á grundvelli meðalhófs og m.t.t. til umsagnar Persónuverndar við frumvarpið, sem taldi tólf mánaða varðveislutíma ekki samrýmast meðalhófssjónarmiðum sem viðra bæri við meðferð persónuupplýsinga, var gerð framangreind breytingartillaga á frumvarpinu, sem síðar var samþykkt af Alþingi.

Samkvæmt 7. mgr. 42. gr. skulu fjarskiptafyrirtæki einnig setja sér verklagsreglur um meðferð persónuupplýsinga og eyðingu gagna í samræmi við ákvæðið og skilyrði sem Persónuvernd kann að setja. Í athugasemdum við frumvarp það er varð að umræddum breytingarlögum segir að um nýmæli sé að ræða og það sé í samræmi við athugasemdir sem m.a. Persónuvernd hefur sett fram um meðferð og eyðingu gagna í vörslum fjarskiptafyrirtækjanna. Samkvæmt ákvæðinu skulu fjarskiptafyrirtækin setja sér verklagsreglur um hvernig sé staðið að þessum málum í starfsemi þeirra og um eyðingu gagna.

Þá er fjarskiptafyrirtækjunum heimilt að vinna úr gögnum vegna markaðssetningar að fengnu samþykki áskrifenda, sbr. 4.-6. mgr. greinarinnar. Þessi ákvæði koma ekki til sérstakrar skoðunar í máli þessu og verður því ekki fjallað sérstaklega um þau.

Líkt og áður segir byggir ákvæði 42. gr. á 6. gr. persónuverndartilskipunar Evrópusambandsins á sviði fjarskipta nr. 2002/58/EB. Í 6. gr. er fjallað um umferðargögn, þ.e. gögn sem unnin eru í þeim tilgangi að flytja fjarskiptasendingu á rafrænu fjarskiptaneti eða til að gefa út reikninga vegna þess, sbr. b lið 2. mgr. 2. gr. tilskipunarinnar. Er í 1. mgr. 6. gr. kveðið á um eyðingu umferðargagnanna eða aðskilnað þeirra frá nafni áskrifanda um leið og þeirra er ekki lengur þörf til að senda fjarskiptasendingu, sbr. þó undanþáguákvæði annarra

[1] Í ákvæði 3. mgr. 42. gr. fjarskiptalaga er vísað til 3. mgr. 47. gr. laganna. Breytingar hafa verið gerðar á síðarnefndu greininni, sbr. lög nr. 39/2007, um breytingu á lögum um fjarskipti nr. 81/2003, þar sem fjórum málsgreinum var bætt inn í 47. gr. fjarskiptalaga. Þessar breytingar leiða að tilvísun 3. mgr. 42. gr. ætti að vera í 7. mgr. 47. gr.

málsgreina ákvæðisins. Er í þeim málsgreinum að finna samhljóða undanþágu og í 2. mgr. 42. gr., þ.e. að heimilt er að vinna úr gögnum sem nauðsynleg eru til útgáfu reikninga en slík vinnsla er þó einungis heimil til loka þess tímabils þegar lögum samkvæmt er hægt að vefengja reikning eða krefjast greiðslu.

Í 26. gr. inngangsorða tilskipunarinnar kemur einnig fram að gögn um áskrifendur, sem notuð eru á rafrænum fjarskiptanetum til að koma á tengingum og til að senda upplýsingar, innihalda upplýsingar um einkalíf einstaklinga og snerta rétt þeirra til að samskiptin séu bundin trúnaði eða þau snerta réttmæta hagsmuni lögaðila. Kemur líka fram að slík gögn megi aðeins geyma að því marki sem nauðsynlegt er til að veita þjónustuna, gefa út reikninga og innheimta gjöld fyrir samtenginu og einungis í takmarkaðan tíma. Samkvæmt 29. lið inngangsorðanna er fjarskiptafyrirtækjum þó heimilt að vinna umferðargögn um áskrifendur í einstökum tilvikum og eins þau umferðargögn sem nauðsynleg eru vegna útgáfu reikninga til að koma upp um og stöðva svik sem felast í ógreiddri notkun rafrænu fjarskiptaþjónustunnar.

Þannig er markmið 42. gr. að tryggja einkalíf áskrifenda með sem bestum hætti og er, að mati Póst- og fjarskiptastofnunar, nauðsynlegt að samlesa ákvæðið með tilliti til 47. gr. fjarskiptalaga en saman er þessum ákvæðum ætlað að tryggja fjarskiptaleynd, sbr. 5. gr. framangreindrar tilskipunar. Þannig ber fjarskiptafyrirtækjum að eyða innihaldi fjarskiptasendingar án tafar eftir afgreiðslu hennar enda sé ekki um að ræða sérstaka lagaheimild fyrir varðveislunni eða samþykki áskrifanda. Eins skulu fjarskiptafyrirtækin uppfylla afdráttarlausa kröfu 42. gr. laganna, þ.e. að upplýsingum um fjarskiptaumferð sé eytt eða þau gerð nafnlaus þegar þeirra er ekki lengur þörf við afgreiðslu hennar nema þegar undanþáguákvæði 2. og 3. mgr. eiga við. Þannig ættu ekki að finnast neinar persónugreinanlegar upplýsingar um fjarskiptaumferð í kerfum fjarskiptafyrirtækja að sex mánuðum liðnum nema þegar reikningur hefur ekki verið greiddur.

2.5 Samþykki áskrifanda fyrir geymslu og vinnslu gagna

Í 4. mgr. 42. gr. er gert ráð fyrir því að áskrifandi geti samþykkt vinnslu úr gögnum um fjarskiptaumferð. Þá er í 4. mgr. 47. gr. lagt bann við hlustun, upptöku, geymslu eða hlerun fjarskipta nema með samþykki notenda eða á grundvelli lagaheimildar.

Hugtakið *samþykki* er ekki skilgreint í fjarskiptalögum en í f -lið 2. mgr. 3. gr. títtnefndrar tilskipunar nr. 2002/58/EB segir að samþykki notanda eða áskrifanda samsvari samþykki skráðs aðila í tilskipun nr. 95/46/EB, sbr. og 17. lið inngangsorða tilskipunar nr. 2002/58/EB.

Í 7. tl. 1. mgr. 2. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, sem byggir á h -lið 2. gr. tilvitnaðrar tilskipunar nr. 95/46/EB, er samþykki skilgreint með eftirfarandi hætti:

> „Sérstök, ótvíræð yfirlýsing sem einstaklingur gefur af fúsum og frjálsum vilja um að hann sé samþykkur vinnslu tiltekinna upplýsinga um sig og að honum sé kunnugt um tilgang hennar, hvernig hún fer fram, hvernig persónuvernd er tryggð, um að honum sé heimilt að afturkalla samþykki sitt o.s.frv.“

Hugtakið samþykki má jafnframt finna í 46. gr. fjarskiptalaga, sem fjallar um óumbeðin fjarskipti, og byggt er á 12. gr. sömu tilskipunar Evrópusambandsins nr. 2002/58/EB. Póst- og fjarskiptastofnun hefur í fjölmörgum ákvörðunum sínum, er varða túlkun á 46. gr. fjarskiptalaga, skilgreint hvað felst í hugtakinu samþykki í skilningi framangreindrar tilskipunar og 46. gr. laganna.

Í ákvörðunum Póst- og fjarskiptastofnunar er varðar óumbeðin fjarskipti og skilgreiningu á hugtakinu er litið til álita 29. gr. starfshóps, sem starfar á grundvelli persónuverndartilskipun Evrópusambandsins. Í áliti hans, nr. 5/2004, er lýtur að túlkun hugtaksins samþykki vegna óumbeðinna fjarskipta, kemur fram að samþykki sem veitt er sem hluti af almennu samþykki á skilmálum samnings, svo sem áskriftarsamnings þar sem samþykkis er óskað fyrir markaðspóst, verður jafnframt að uppfylla framangreind skilyrði tilskipunar 95/46/EB. Þannig getur samþykki aðila falist í því að haka í reiti á vefsíðu og lýsa þar með yfir vilja sínum um ákveðið efni.[2] Er það því álit hópsins að samþykkið verði að fela í sér ákveðna athöfn af hálfu hlutaðeigandi svo það teljist vera ótvírætt samþykki til að uppfylla kröfur tilskipunar 95/46/EB.[3] Athafnaleysi viðkomandi getur því ekki verið forsenda fyrir samþykki hans í skilningi tilskipunarinnar. Þannig geti fyrirfram útfylltir reitir, sem viðkomandi þarf að taka merkingu af, ekki talist uppfylla skilyrði þau sem gerð eru fyrir samþykki.[4] Að mati Póst- og fjarskiptastofnunar verður ekki lagður annar skilningur í hugtakið samkvæmt 42. og 47. gr. fjarskiptalaga enda byggja ákvæðin á sömu tilskipun.

Þessi túlkun Póst- og fjarskiptastofnunar er einnig í samræmi við túlkun Persónuverndar sem í nokkrum úrskurðum sínum komst að því að Fjarskipti hf. hafi ekki haft heimild til varðveislu þeirra fjarskiptaskilaboða sem varðveitt voru á vefsvæði félagsins þar sem skilyrði hugtaksins samþykkis voru ekki uppfyllt. Í úrskurði Persónuverndar í máli nr. 2013/1509 segir:

> „Eins og fyrr greinir verða fjarskiptafyrirtæki hins vegar almennt að gera ráð fyrir að í fjarskiptaskilaboðum geti verið viðkvæmar persónuupplýsingar, en af því leiðir meðal annars að um þarf að vera að ræða yfirlýsingu sem fjarskiptanotandi sjálfur *gefur,* sbr. orðalag fyrrnefnds ákvæðis. Það að ekki sé afhakað við reit, þar sem fram kemur að unnið verði með persónuupplýsingar, verður ekki talið fela í sér að slík yfirlýsing hafi verið *gefin.*
>
> Í ljósi framangreinds var kröfum til samþykkis samkvæmt 7. tölul. 2. gr. laga nr. 77/2000 ekki fullnægt gagnvart kvartanda, en auk þess verður ekki séð að aðrar vinnsluheimildir en samþykki geti hér átt við. Með vísan til þess er niðurstaða

[2] Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, adopted on 27 February 2004 (WP90). Bls. 5.
[3] Opinion 15/2011 on the definition of consent frá 13. júlí 2011.
[4] Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, adopted on 27 February 2004 (WP90). Bls 5. *(e. Implied consent to receive such mails is not compatible with the definition of consent of Directive 95/46/EC and in particular with the requirement of consent being the indication of someone's wishes, including where this would be done ´unless opposition is made' (opt-out). Similarly, pre-ticked boxes, e.g., on websites are not compatible with the definition of the Directive either.)*

Persónuverndar sú að heimild hafi brostið til varðveislu umræddra fjarskiptaskilaboða.“

III.
Vefkerfi Fjarskipta hf.

3.1 Almennt

Póst- og fjarskiptastofnun hóf, líkt og áður segir, rannsókn sína á öryggisatviki á vefsvæði Fjarskipta hf. með bréfi sínu, dags. 23. desember 2013, þar sem óskað var upplýsinga á grundvelli 5. gr. laga nr. 69/2003 um Póst- og fjarskiptastofnun. Rannsóknin hefur tekið töluverðan tíma og skýrist það fyrst og fremst af þeim ágreiningi sem ríkir á milli stofnunarinnar og Fjarskipta hf. um valdsvið stofnunarinnar í málinu, sbr. ákvörðun stofnunarinnar nr. 1/2014 og úrskurð úrskurðarnefndar fjarskipta- og póstmála í máli nr. 3/2014.

Póst- og fjarskiptastofnun ákvað að fresta rannsókn málsins á meðan kærumeðferð fyrir úrskurðarnefnd stóð en í kjölfar úrskurðar nefndarinnar var rannsókn haldið áfram. Þá er ljóst að dómsmál sem Fjarskipti hf. reka fyrir héraðsdómi Reykjavíkur hefur haft áhrif á rannsóknartíma málsins. Óskaði héraðsdómur eftir ráðgefandi áliti EFTA-dómstólsins í málinu. Það álit var birt þann 22. desember sl., sbr. álit dómstólsins í máli nr. E-6/16.

Póst- og fjarskiptastofnun taldi aftur á móti rétt að halda áfram skoðun og rannsókn á öryggisatvikinu sjálfu eftir töku ákvörðunar nr. 1/2014 um gildissvið fjarskiptalaga. Með bréfi stofnunarinnar til Fjarskipta hf., dags. 26. mars 2014, var félaginu kynnt þau ákvæði fjarskiptalaga og reglna 1221/2007, sem við eiga í málinu sem og að stofnunin óskaði eftir ítarlegum upplýsingum varðandi i) öryggisskipulag félagsins, ii) öryggisatvikið sjálft og iii) viðbrögð starfsmanna félagsins við öryggisatvikinu.

Póst- og fjarskiptastofnun bárust svör frá Fjarskiptum hf. þann 30. apríl 2014. Um var að ræða sérstakt svarbréf ásamt 11 fylgiskjölum. Í bréfinu er greint frá því að Fjarskipti hf. hafi kært ákvörðun stofnunarinnar nr. 1/2014 til úrskurðarnefndar fjarskipta- og póstmála en að félagið hyggist samt sem áður leitast við að svara öllum fyrirspurnum stofnunarinnar og afhenda öll þau gögn sem óskað hafi verið eftir. Áréttaði félagið þá skoðun sína um að ákvæði fjarskiptalaga og reglna nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum, næðu ekki yfir vefsíðu félagsins.

Í bréfi félagsins var farið í gegnum spurningar Póst- og fjarskiptastofnunar og þeim svarað. Við yfirferð Póst- og fjarskiptastofnunar á svarbréfi félagsins taldi stofnunin þó að svörum við ýmsum spurningum stofnunarinnar væri ábótavant og taldi nokkuð skorta á nákvæma og skýra upplýsingagjöf hjá félaginu. Stofnunin sendi því á ný bréf til Fjarskipta hf., dags. 3. febrúar 2015, en þá lá fyrir úrskurður úrskurðarnefndar fjarskipta- og póstmála nr. 3/2014 sem staðfesti ákvörðun stofnunarinnar, og óskaði frekari svara við ákveðnum spurningum. Var

frestur veittur til 23. febrúar 2015 til að skila inn ítarlegri svörum og frekari umbeðnum upplýsingum.

Póst- og fjarskiptastofnun barst á ný svarbréf frá félaginu, dags. 16. mars 2015, ásamt tólf fylgiskjölum. Í svarbréfinu fóru Fjarskipti hf. yfir hvern lið hverrar spurningar og settu fram svör félagsins.

Póst- og fjarskiptastofnun sendi Fjarskiptum hf. bréf, dags. 13. júlí sl. þar sem boðuð var fyrirhuguð niðurstaða stofnunarinnar vegna öryggisatviksins. Í bréfinu var óskað athugasemda félagsins við hina boðuðu afstöðu og skyldi afstaðan ná til umfjöllunar um lagaumhverfi, túlkun stofnunarinnar á svörum félagsins, lýsingar stofnunarinnar á öryggisatvikinu sjálfu og afstöðu hennar til skýrslna varðandi öryggisatvikið, heimfærslu öryggisráðstafana félagsins á hlutaðeigandi ákvæði fjarskiptalaga og afleiddra réttarheimilda sem og afstöðu stofnunarinnar til þeirra.

Í kjölfar boðunarbréfsins óskuðu Fjarskipti hf. eftir fundi með Póst- og fjarskiptastofnun og auknum fresti til að skila inn athugasemdum félagsins. Var fallist á að frestur yrði veittur þar til munnlegur málflutningur fyrir EFTA-dómstólnum hefði farið fram. Sá málflutningur fór fram þann 18. október sl. Á fundi 7. nóvember kynntu Fjarskipti hf. afstöðu sína til boðunarbréfsins og skiluðu inn viðbótargögnum.

Það er mat Póst- og fjarskiptastofnunar að málið sé nú nægjanlega upplýst svo að til efnislegrar ákvörðunartöku geti komið. Rannsókn stofnunarinnar hefur lotið að því hvort Fjarskipti hf. hafi farið að þeim ákvæðum fjarskiptalaga og reglna nr. 1221/2007, sem kveða á um öryggi og leynd fjarskipta og viðhaft viðeigandi ráðstafanir til verndar þeim upplýsingum sem geymdar voru innan almenns fjarskiptanets félagsins, eða upplýsingakerfum sem við þau styðjast, þegar innbrot átti sér stað í nóvember 2013.

Upplýsingabeiðnir Póst- og fjarskiptastofnunar og svör Fjarskipta hf., ásamt fylgigögnum, eru umfangsmikil. Þá hefur stór hluti gagnanna að geyma upplýsingar er varða upplýsingaöryggi félagsins. Að mati stofnunarinnar er eðlilegt að slíkar upplýsingar njóti trúnaðar og verður því í ákvörðun þessari fjallað um slíkar upplýsingar með almennum hætti en að öðrum kosti verður hluti textans felldur út.

Í kafla þessum verður reynt að varpa ljósi á uppbyggingu vefkerfisins og þeirrar þjónustu sem þar var veitt. Hluti þeirrar þjónustu var vistun gagna og verður sérstaklega fjallað um skilyrði fyrir slíkri vistun.

3.2 Þjónusta og uppbygging vefkerfisins og vistun gagna

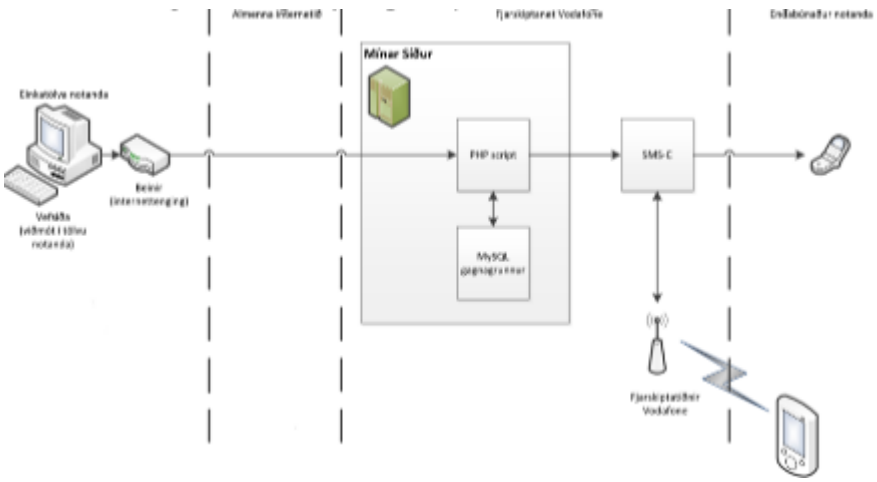
3.2.1 Þjónustutegundir vefkerfisins

Fjarskipti hf. hafa í yfir áratug boðið upp á skilaboðaþjónustu á vefkerfi sínu. Fyrst var boðið upp á svo kölluð FRÍ-SMS en sú þjónusta var uppbyggð með þeim hætti að allur almenningur gat farið inn á heimasíðu félagsins, valið móttakandi símanúmer (B-númer), skrifað skilaboð og sent. Ekki var krafist innskráningar til að nýta þessa þjónustu. Þessum skeytum var eytt og

vistuðust ekki í skeytasögu. Á síðasta ársfjórðungi árið 2012 hættu Fjarskipti hf. að veita þessa þjónustu.

Árið 2004 var kerfi félagsins hins vegar endurforritað og flutt úr .Net umhverfi í PHP. Þá settu Fjarskipti hf. upp „Mínar síður“, þar sem eingöngu áskrifendur félagsins gátu skráð sig inn á símanúmeri sínu ásamt lykilorði. Þar var í boði svokölluð „VEF-SMS“ þjónusta, þ.e. sending smáskilaboða frá hlutaðeigandi símanúmeri (A-númer) til móttakandi símanúmers (B-númer) sem valið var. Á „Mínum síðum“ var, frá 2008, hægt að senda skilaboð á einn eða fleiri viðtakanda, vista viðtakendur í nafnaskrá og tengja þá saman í hópa. Var sá möguleiki mikið notaður t.d. af félagasamtökum sem senda fjölda skilaboða á stóran hóp. Þá var kerfið einnig notað til að senda skilaboð er vörðuðu bókanir í læknaþjónustu og aðra sérfræðiþjónustu, sem og af öðrum þjónustufyrirtækjum.

Í kjölfar þessara breytinga óskaði félagið eftir ábendingum frá notendum um hvaða eiginleika þeir óskuðu eftir að kerfi félagsins hefði. Niðurstöður þess voru þær að vistun skilaboða í skeytasögu var bætt við þjónustu félagsins í desember 2010.



Var virkni kerfisins með þeim hætti að sendandi skilaboðanna skráði sig inn á „Mínar síður“ á endabúnaði sínum með símanúmeri sínu og lykilorði. Ritaði þar skilaboð sem sendust eftir almenna internetinu í gegnum hugbúnað á vefsvæði Fjarskipta, svo kallaðar PHP-scriptur, sem móttók, vann úr og áframsendi skilaboðin yfir í SMS-miðlara Fjarskipta hf. sem miðlaði skilaboðunum til móttakanda þeirra. Ef vistað var í skeytasögu vistuðust skeytin í MySQL gagnagrunnum sem staðsettir voru á vefsvæðinu, sbr. skýringarmynd hér að ofan.

3.2.2 Skilyrði fyrir vistun í skeytasögu

Virkni kerfis Fjarskipta hf. var með þeim hætti að skilaboðin vistuðust sjálfkrafa á MySQL gagnagrunni á vefsvæði félagsins. Til að koma í veg fyrir slíka sjálfkrafa vistun þurfti áskrifandi að taka hak úr „Vista í skeytasögu“ merkingu. Að öðrum kosti vistuðust skeytin og var saga áskrifandans honum alltaf sýnileg þegar ný skeyti voru send. Hugmyndin með skeytasögu var annars vegar að veita áskrifandanum yfirlit yfir hvað hann hafði sent og hins vegar að bjóða upp á endurnýtingu skilaboða, þegar skilaboð sem viðkomandi sendi voru eins eða lítið breytt á milli sendinga.

Að mati Fjarskipta hf. er framangreind aðferð við að afla samþykkis fyrir vistun gagna í samræmi við ákvæði og skilyrði laga. Máli sínu til stuðnings vísar félagið til h -liðar 1. mgr.

2. gr. persónuverndartilskipunar Evrópusambandsins þar sem fram kemur að upplýst samþykki teljist vera *„ ... óþvingað, sértækt og upplýst viljayfirlýsing skráðs aðila um að hann samþykki vinnslu persónuupplýsinga er varða hann sjálfan.“* Enda var viðskiptavinum í sjálfsvald sett hvort að skeyti voru geymd á gagnagrunni félagsins þar sem viðkomandi gat tekið hak úr þar til gerðum reit og þannig komið í veg fyrir að skeyti vistuðust.

Að mati Fjarskipta hf. liggur því fyrir samþykki af hálfu viðskiptavina félagsins, sbr. f -lið 2. mgr. 2. gr. tilskipunar nr. 2002/58/EB sem byggir á h -lið 1. mgr. 2. gr. tilskipunar nr. 95/46/EB (persónuverndartilskipun). Telur félagið að samþykki viðskiptavinar sé *„ ... ekki fengið fram með þvinguðum, sérstökum og óupplýstum hætti.“* Viðskiptavinir þess höfðu alltaf haft alla möguleika til að koma í veg fyrir vistun skilaboðanna eða eyða þeim gögnum á hvaða tímapunkti sem er ef þeir hafi ekki talið ástæðu til að eiga þau.

3.2.3 Gögn í vefkerfinu

Auk þeirra skeyta sem vistuð voru í skeytasögu viðskiptavina var einnig að finna töluvert magn annarra upplýsinga og ganga á vefsvæði Fjarskipta hf. en heildarmagn þeirra gagna sem komist var yfir í öryggisatvikinu nam [...][5]. Mikill hluti þeirra voru þó ýmist ópersónuleg eða órekjanleg, svo sem tilraunaupplýsingar, bilanatilkynningar fyrir heimasíðu, lýsing og flokkun á smáforritum (öppum), kvikmyndaflokkun o.s.frv. Aftur á móti var einnig umtalsvert magn af persónugreinanlegum upplýsingum.

Hvað varðar slíkar persónugreinanlegar upplýsingar var í fyrsta lagi um að ræða upplýsingar er varða fjarskiptin sjálf, svo sem upplýsingar um innihald skilaboðanna sjálfra sem send voru af „Mínum síðum“, dagsetningu þeirra sem og símanúmer sendanda og móttakanda. Þá var í öðru lagi um að ræða upplýsingar um netföng, ódulkóðuð lykilorð og kennitölur, tengingu símanúmera við IP tölur og netföng o.s.frv. Er hér í flestum tilfellum um að ræða upplýsingar sem almennt falla undir ákvæði fjarskiptalaga og Evróputilskipana um fjarskiptaleynd og fjarskiptafyrirtækjum ber alla jafna að eyða nema sérstakar undanþágur eða heimildir séu fyrir varðveislu þeirra.

Hvað varðar skilaboða-sendingarnar sérstaklega þá er ljóst að um umtalsvert magn sendinga er að ræða. En í töflunni hér að til hliðar má finna upplýsingar um fjölda skeyta og skeytasendinga sem fram komu í svari Fjarskipta hf. [...][6]

[...][7]

3.2.4 Uppbygging vefkerfisins

[...][8]

[5] Fellt út vegna trúnaðar.
[6] Tafla felld út vegna trúnaðar.
[7] Fellt út vegna trúnaðar.
[8] Fellt út vegna trúnaðar.

IV. kafli
Öryggi vefkerfis Fjarskipta hf.

4.1 Almennt

Við mat á öryggi vefkerfis Fjarskipta hf. var óskað eftir upplýsingum og ítarlegum útlistunum á almennu öryggi vefkerfisins og þeirra upplýsinga sem þar voru geymdar. Var t.a.m. óskað eftir öryggisstefnu félagsins, áhættumati sem nær yfir vefkerfið sem og skriflegar öryggisráðstafanir sem settar hafa verið á grundvelli þess áhættumats, svo sem aðgengi starfsmanna félagsins að vefkerfinu, atburðaskráningar, breytingastjórnun þess o.s.frv. Þá var einnig óskað upplýsinga varðandi öryggisatvikið sjálft.

Í þessum kafla verður fjallað um öryggi vefkerfisins, hvort tveggja út frá almennu öryggisskipulagi Fjarskipta hf., svo sem öryggisstefnu, áhættumati, skriflegum öryggisráðstöfunum og innra eftirliti, sem og út frá kerfislegu öryggi.

4.2 Öryggisskipulag vefkerfisins

4.2.1 Öryggisstefna Fjarskipta hf.

Líkt og áður greinir er fjarskiptafélögum skylt að setja sér skriflega öryggisstefnu, sbr. 1. tl. 7. gr. reglna nr. 1221/2007, sbr. 47. gr. fjarskiptalaga, þar sem fram á að koma almenn lýsing á afstöðu æðstu stjórnenda fyrirtækisins til öryggismála. Skal stefnan taka mið af því hvaða upplýsingar skuli vernda, hvernig skuli vernda þær, þeirri aðferð sem viðhöfð verður og hver ber ábyrgð á öryggi þeirra.

Öryggisstefna Fjarskipta hf. er í samræmi við kröfur framangreindra reglna en í henni kemur fram að hún nái til *„ ... allrar starfsemi Vodafone og þjónustu sem fyrirtækið veitir viðskiptavinum sínum.“* Þá er tilgreint að hlutverk stefnunnar sé að lýsa skuldbindingu félagsins um að vernda upplýsingaeignir sínar gegn ógnum, innan frá eða utan, vísvitandi eða óviljandi. Í stefnunni er greint frá því að markmið stjórnunar upplýsingaöryggis sé að tryggja öryggi upplýsingaeigna fyrirtækisins og áframhaldandi rekstur upplýsingakerfa og að félagið hafi af þeim sökum sett sér markmið er varðar leynd, réttleika gagna og tiltækileika þeirra.

Aftur á móti má gera athugasemdir við að ekki komi skýrt fram í stefnunni hvaða einn stjórnandi er ábyrgur fyrir henni þótt fram komi í öðrum gögnum málsins að ábyrgðarmenn hennar séu Gæða- og öryggisráð ásamt Gæða- og öryggisstjóra félagsins. Þá var stefnan ekki undirrituð af formanni stjórnar sem ætti samkvæmt stefnunni að staðfesta hana með undirritun sinni.

Eins mátti sjá að öryggisstefnan var, þegar öryggisatvikið átti sér stað í nóvember 2013, síðast formlega endurskoðuð og uppfærð þann 22. maí 2009, þótt fram komi í henni að hana beri að endurskoða árlega. En vefþjónusta fyrir smáskilaboð hafði verið í boði af hálfu Fjarskipta hf. allt frá aldamótum en þá án innskráningar, þ.e. A-númers. Líkt og áður segir hófst þó vistun skilaboða á vefkerfinu í desember 2010. Öryggisstefna félagsins var því síðast endurskoðuð um 18 mánuðum áður en að fyrst var boðið upp á að skeytasaga vistaðist á vefkerfi félagsins. Þá var þjónustan endurskoðuð árið 2012 en á síðasta ársfjórðungi 2012 var hætt að bjóða upp

á þjónustuna án sérstakrar innskráningar. Það liggur því fyrir að upplýsingaöryggisstefna Fjarskipta hf. var ekki endurskoðuð sérstaklega m.t.t. til breytinga á fjarskiptaþjónustu félagsins á vefkerfi þess þrátt fyrir að í árslok 2010 mátti vera ljóst að umtalsvert magn upplýsinga, þ.m.t. innihald smáskilaboða, voru vistuð á gagnagrunnum í vefkerfi félagsins. Hið rúma orðalag stefnunnar, um að hún muni taka til allrar þjónustu félagsins við viðskiptavini þess, gerir það þó að verkum að hún nái til þeirrar þjónustu sem félagið veitti á vefkerfi sínu.

Hins vegar kemur fram af hálfu Fjarskipta hf. að stefnan hafi verið uppfærð fljótlega eftir að innbrotið átti sér stað, samhliða vinnu félagsins við vottun félagsins á grundvelli ISO 27001 staðalsins.

4.2.2 Áhættumat

Auk þess að setja sér skriflega öryggisstefnu er fjarskiptafyrirtækjum skylt að skilgreina aðferðarfræði áhættumats um upplýsingaöryggi og fylgja henni eftir með skriflegu áhættumati um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu, sbr. 2. tl. 7. gr. reglna nr. 1221/2007, sbr. 47. gr. fjarskiptalaga.

Áhættumat Fjarskipta hf. náði ekki að öllu leyti yfir vefkerfi félagsins. Náði það einungis yfir „Mínar síður“ en ekki vefsvæðið vodafone.is, sbr. mynd í kafla 3.3.4. Þannig var einungis hluti netþjónsins [...][9] innan áhættumatsins, þ.e. sá hluti sem tengdist [...][10] og kjarnakerfi félagsins, en sá hluti netþjónsins sem tengdist við gagnagrunna vefkerfisins, [...][11], var utan þess. Það öryggisatvik sem til skoðunar er hér varðar vefsvæði félagsins, vodafone.is og voru þær upplýsingar og gögn sem voru andlag innbrotsins vistuð á gagnagrunnum á því vefsvæði. Smáskilaboðaþjónusta Fjarskipta hf. og vistun gagnanna voru því ekki innan áhættumats félagsins.

Af gögnum málsins má sjá að stuttu áður en innbrot átti sér stað, þ.e. í ágúst 2013, var tekin ákvörðun um afmörkun umfangs þeirra eigna sem skyldu vera hluti af vottunarferli félagsins samkvæmt ISO 27001 staðlinum. Það liggur því fyrir af gögnum málsins að umfang þess náði ekki til vefsvæðisins, vodafone.is, og þeirra gagna sem þar voru vistuð. Þannig voru þau gögn sem geymd voru á vefsvæðinu ekki innan áhættumats þess þegar innbrot átti sér stað í nóvember 2013.

Í þessu tilliti er vert að benda á að vefkerfi Fjarskipta hf. hafði áður orðið fyrir netárás. Í mars árið 2012 var vefsíðu félagsins var breytt (e. deface). Fjarskipti hf. brugðust við umræddu öryggisatviki með ákveðnum tímabundnum viðbrögðum, svo sem að loka á „providerinn“ sem innbrotsaðili kom frá. Þá er einni lokað á útlandasambönd á vefinn á meðan ákveðnar viðgerðir áttu sér stað.

[9] Fellt út vegna trúnaðar.
[10] Fellt út vegna trúnaðar.
[11] Fellt út vegna trúnaðar.

Í kjölfar þessa öryggisatviks var farið í vinnu við að bæta öryggi vefkerfisins. Þá voru gerðar þrjár úttektir á öryggi þess. Tvær voru framkvæmdar strax eftir umrætt atvik, önnur af Þekkingu en hin af GSOC (e. Global Security Operations Center). Var unnið að endurbótum á vefkerfi félagsins á grundvelli niðurstaðna þessara úttekta og var því starfi lokið í marslok 2012. Síðar framkvæmdi Capacent hf. IP-öryggisúttekt á kerfi félagsins þar sem kannað var hvort hægt væri að komast inn á kjarnaupplýsingakerfi þess frá vefkerfinu, þ.e. í gegnum [...][12]. Skilaði Capacent ehf. niðurstöðum sínum í janúar 2013. Sú skýrsla laut því ekki að vefsvæðinu sjálfu, þ.e. vodafone.is, heldur þeim hluta vefkerfisins sem hafði að geyma „Mínar síður“ og [...][13].

Það var svo í maí 2013 að ákvörðun var tekin af Fjarskiptum hf. að hefja ferli við vottun samkvæmt ISO 27001 staðli. Umfang þess var afmarkað í ágúst 2013 þar sem, líkt og áður segir, hluti vefkerfis félagsins, vefsvæðið vodafone.is, var undanskilinn áhættumati. Áhættumati vegna vottunarferlis lauk um miðjan nóvember 2013.

4.2.3 Öryggisráðstafanir

Eins og áður hefur komið fram ber fjarskiptafyrirtækjum að setja sér verklagsreglur um örugga meðferð upplýsinga og eyðingu þeirra. Skulu þau gera öryggisráðstafanir og setja fram skriflegar lýsingar á þeim, sbr. 3. tl. 7. gr. reglna nr. 1221/2007, sbr. 47. gr. fjarskiptalaga. Þessar öryggisráðstafanir skulu endurskoðaðar reglulega.

Fjarskipti hf. hafa, á grundvelli framangreinds ákvæðis, sett fram stefnur og verklagsreglur sem fjalla um öryggisráðstafanir í meðferð upplýsinga hjá félaginu. Aftur á móti hefur komið fram í gögnum málsins að einungis sjö öryggisráðstafanir hafi náð yfir vefkerfið í samræmi við ákvæði reglnanna. Skýrist það af þeirri afstöðu félagsins að ekki hafi verið um almennt fjarskiptanet félagsins að ræða eða að veitt hafi verið fjarskiptaþjónusta á vefsvæði þess.

Þær sjö ráðstafanir sem um er að ræða varða i) aðgangsstýringar inn á kerfi félagsins af hálfu starfsmanna, ii) trúnaðaryfirlýsingar starfsmanna, iii) skráningar á útföllum vefkerfisins og viðbrögð við þeim, iv) neyðaráætlun, þ.e.a.s. viðbrögð við innbrotum á vefkerfi, v) afritun kerfa, vi) eftirlit með uppitíma, http vöktun, þ.e. vöktun á „noci“, og vii) kerfisskráning (kerfisloggar), svo sem kerfisnotendur sem tengjast inn á kerfið.

Þegar þessar ráðstafanir eru skoðaðar og heimfærðar upp á ákvæði reglna nr. 1221/2007 má sjá að fyrsta tilgreinda öryggisráðstöfunin, þ.e. aðgangsstýringar starfsmanna inn á kerfi félagsins, fellur að kröfu í 1. tl. 11. gr. reglnanna, þ.e. að stýra skuli aðgangi að húsnæði og búnaði fjarskiptaneta með úthlutun aðgangskorta, lykilorða, eða með öðrum fullnægjandi hætti þar sem því verður við komið. Aftur á móti er óljóst með hvaða hætti þessar aðgangsstýringar náðu til þeirra upplýsinga sem finna mátti á vefsvæði félagsins eða með hvaða hætti haldið var utan um þessi aðgangsréttindi og hversu reglulega þau voru yfirfarin, sbr. 9. tl. 12. gr. reglnanna.

[12] Fellt út vegna trúnaðar.
[13] Fellt út vegna trúnaðar.

Önnur öryggisráðstöfun félagsins vísar til 2. tl. 10. gr. reglnanna, varðandi trúnaðaryfirlýsingar starfsmanna. Þá verður að telja að skráningar á útföllum vefkerfisins, gerð neyðaráætlunar um viðbrögð við innbrotum í vefkerfi og eftirliti með uppitíma sé ætlunin að uppfylla kröfu 9. gr. reglnanna sem kveður á um áætlun um samfelldan rekstur. Ákvæðið gerir þá kröfu um að sérstakar ráðstafanir séu gerðar til *„ ... að tryggja öryggi upplýsinga komi til þjónusturofs, s.s. vegna bilunar, óhappa eða annarra atvika sem ógnað geta öryggi fjarskiptaneta.“* Um frekari ráðstafanir í þessu tilliti er fjallað um í reglum 1222/2007 um virkni almennra fjarskiptaneta, sbr. 8. gr. þeirra. Ekki er þó ljóst hvað felst í þessari neyðaráætlun eða með hvaða hætti hún byggi á niðurstöðum áhættumats enda var slíkt ekki til staðar fyrir vefsvæðið vodafone.is.

Með fimmtu öryggisráðstöfun félagsins, þ.e. afritun kerfa, verður að telja að verið sé að koma til móts við 8. tl. 12. gr. reglna nr. 1221/2007 þar sem fram kemur að viðhalda skuli órofinni slóð sönnunargagna sem nýst gætu vegna öryggisatburða.

Að lokum verður að telja að öryggisráðstöfun félagsins er lýtur að kerfisskráningu (kerfisloggun), t.a.m. þegar notendur skrá sig inn á vefkerfið, falli að 2. tl. 12. gr. reglna nr. 1221/2007 þar sem kveðið er á um að nota skuli aðgangsheimildir, aðgangsstýringu og óhrekjanleika. Eins er ljóst að það að áskrifandi hafi þurft að skrá sig inn á vefkerfi félagsins með notendanafni og lykilorði, til að nýta sér þá fjarskiptaþjónustu sem þar var veitt, fellur að þessari öryggisráðstöfun reglnanna.

Ákvæði 3. tl. 7. gr. reglnanna gerir jafnframt kröfu um að gerðar séu skriflegar leiðbeiningar fyrir einstaka ferla sem nauðsynlegir eru fyrir upplýsingaöryggi fjarskiptaneta og fjarskiptaþjónustu. Fjarskipti hf. hafa, líkt og áður segir, sett fram ákveðnar stefnur varðandi upplýsingaöryggi, svo sem stefnur um breytingarstjórnun, aðgangsstýringu, rekstrarsamfellu og afritun en einnig verklagsreglur fyrir spillikóða og innra eftirlit. Aftur á móti hafa Fjarskipti hf. ekki getað sýnt fram á gerð ferlanna sjálfra sem þó má ætla að gerðir séu í framhaldi af setningu umræddra stefna. Þessir ferlar eru jafnframt nauðsynlegir fyrir starfsmenn félagsins að fara eftir en starfsmenn félagsins geta ekki, að mati Póst- og fjarskiptastofnunar farið beint eftir stefnunum.

Póst- og fjarskiptastofnun gerir ekki formlegar athugasemdir við framangreindar ráðstafanir. Stofnunin telur er ekki tilefni að setja fram afstöðu stofnunarinnar til framangreindra tilfallandi öryggisráðstafana í ljósi þess að umrætt vefsvæði var ekki innan áhættumats Fjarskipta hf. á þeim tíma og að ekki hafi verið settar skriflegar lýsingar á öryggisráðstöfunum á grundvelli niðurstaðna þess. Að mati stofnunarinnar þarf að horfa heildstætt á öryggi og öryggisráðstafanir vefsvæðisins og er það meginniðurstaða stofnunarinnar að skriflegar öryggisráðstafanir fyrir vefsvæðið hafi skort, sbr. 3. tl. 7. gr. reglna nr. 1221/2007.

4.2.4 Innra eftirlit

Líkt og fram hefur komið ber fjarskiptafyrirtækjum að viðhafa innra eftirlit til að tryggja að unnið sé í samræmi við öryggisstefnu og skjalfestar verklags- og öryggisreglur öryggisskipulags félagsins, sbr. 8. gr. reglna nr. 1221/2007.

Stjórnkerfi upplýsingaöryggis Fjarskipta hf. gerir ráð fyrir að framkvæmdar séu almennar innri úttektir í september til október ár hvert. Þá lýsi skjalfestar verklagsreglur framkvæmd þess og starfsáætlun gæða- og öryggisráðs tilgreinir eftirfylgni ráðsins við framkvæmd eftirlitsins. Aftur á móti höfðu ekki verið framkvæmdar formlegar innri úttektir á vodafone.is umhverfinu þar sem ekki var um fjarskiptakerfi að ræða að mati félagsins. Hins vegar má benda á þær úttektir sem gerðar voru, og vinnu sem unnin var, í kjölfar innbrots á vefkerfi félagsins í mars 2012. Voru þá gerðar úttektir á veikleikum síðunnar og þeir lagaðir, greiðslukortaupplýsingar voru fjarlægðar af vefsvæðinu, öryggi tenginga frá vefsvæði vodafone.is inn á innri kerfi félagsins var eflt sem og dulkóðun á lykilorðum á „Mínum síðum“ útbúin og hætt var að senda ódulkóðuð lykilorð með tölvupósti.

Þá var kerfishögun félagsins með þeim hætti að vefsvæði vodafone.is sé stillt utan við eldveggi innri viðskipta- og fjarskiptakerfa til þess að tryggja öryggi þeirra mikilvægu innviða. Var slíkt gert þar sem erfitt getur verið að útiloka að hægt sé að brjótast inn á vefi tengda við internet. Hins vegar jók félagið varnir síðunnar eftir 30. nóvember 2013 með uppsetningu eldveggja fyrir framan vodafone.is.

Það er því ljóst að ekki var, í aðdraganda öryggisatviksins, viðhaft formlegt innra eftirlit fyrir öryggi vefsvæðis félagsins þótt vissulega hafi verið farið í ákveðnar öryggisaðgerðir eftir fyrra öryggisatvik á vefsíðu þess. Í þeim aðgerðum var fyrst og fremst unnið að lagfæringu þeirra veikleika sem fundust en ekki framkvæmt heildarmat á vefsvæðinu, áhættum sem að því stafaði eða settar niður öryggisráðstafanir m.t.t. þeirra áhætta.

Póst- og fjarskiptastofnunar telur aftur á móti að Fjarskiptum hf. hafi mátt vera ljóst að vefkerfi þeirra gæti verið andlag árása tölvuþrjóta líkt og raunin varð í nóvember 2013. Þótt félagið hafi vissulega brugðist við fyrri öryggisatvikum er jafnframt ljóst að hluti vefkerfisins, vodafone.is, þar sem gögn voru vistuð, var ekki tekið með markvissum með undir áhættumat félagsins þegar það var afmarkað í ágúst 2013.

Hvað varðar tæknilega hlítingu upplýsingakerfa vefsvæðisins við staðla um innleiðingu öryggis og hvernig henni var háttað, sem hluta af innra eftirliti hjá félaginu, sýna gögn málsins að framkvæmd hennar var skipt í þrennt, þ.e. a) hlítingu við kröfur birgja, b) hlítingu við „best-practice“ öryggisráðstafanir og c) hlítingu við samþykkt verklag samkvæmt stjórnkerfi upplýsingaöryggis.

Farið var eftir kröfum ISO 27001:2013 staðli þegar kemur að könnunum á tæknilegum hlítingum, sér í lagi kröfu A.18.2.3 og þær framkvæmdar eftir þörfum en úttektaráætlun Fjarskipta hf. gerir þó ráð fyrir árlegum innri úttektum. Hins vegar gefa gögn málsins ekki skýra mynd af því hvernig hinar tæknilegu kannanir voru framkvæmdar að öðru leyti.

4.3 Kerfislægar öryggisráðstafanir vefkerfisins

4.3.1 Kerfislægar varnir við innbroti

Ytri varnir fyrir vefkerfi Fjarskipta hf. samanstóðu af tveimur eldveggjum [...][14] ásamt einni pakkasíu [...][15], en slíkar síur gegna svipuðu hlutverki og eldveggur.

Ekki voru að finna sérstakar kerfislegar varnir gegn innbrotum á vefkerfi Fjarskipta hf. að öðru leyti en að aðgangi að vélum og gagnagrunnum hafi verð aðgangsstýrt með hefðbundnum aðferðum sem og að ráðstafanir í formi aðgangsstýringa hafi verið notaðar til að verjast innbrotum. Þannig voru allar vélar og gagnagrunnar varðar með slíkum aðgangsstýringum, þ.e. notendanafni og lykilorði.

Þótt framangreindar ráðstafanir teljist til eðlilegra ráðstafana til að verjast innbrotum er ljóst að kerfislegar ráðstafanir til varnar innbrotum voru almennt ekki til staðar eða þá af mjög skornum skammti á vefsvæði Fjarskipta hf. , enda taldi félagið svæðið ekki hluta af fjarskiptaneti sínu.

Eftirlitskerfi Vodafone hafði eftirlit með vélbúnaði félagsins og fylgdist með öllum helstu mælikvörðum og frávikum hans. Hafi komið til fráviks frá hefðbundnu ástandi búnaðarins myndi berast tilkynning á stjórnborð félagsins, þ.e. rautt ljós í eftirlitskerfinu. Eftirlitskerfið nam því ekki innbrotið eða aðgang að gagnagrunnunum heldur einungis breytingu á forsíðu á vefsíðu félagsins eftir að innbroti lauk.

4.3.2 Kerfislægar viðvaranir við innbrot

Við skoðun á öryggisatvikinu kom í ljós að engar kerfislegar viðvaranir bárust við innbrot eða á meðan að innbrot átti sér stað. Þá voru ekki til staðar kerfislegar ráðstafanir sem sýndu að gagnaflutningur innan kerfis eða út úr kerfinu ætti sér stað eða hefði átt sér stað. Eftirlitskerfi félagsins sendi einungis tilkynningu um villu í vef félagsins, vodafone.is, eftir að innbrot lauk og gögn höfðu verið fjarlægð af vefsvæðinu, þegar skipt var um forsíðu vefsins (e. deface). Þá barst einnig tilkynning frá GSOC við innbrotið. Þannig bárust umræddar tilkynningar einungis þegar að skipt var um forsíðu vefsíðunnar (e. deface), en hvorki við innbrotið né á meðan því stóð. Það var því í raun eingöngu breyting á forsíðu vefsíðunnar sem varð til þess að upp komst um innbrot og gagnastuld. Ef tölvuþrjótur hefði ekki sjálfur látið vita um innbrotið og gagnastuldinn með þessum hætti er óvíst hvort eða hvenær upp hefði komist um innbrotið og gagnastuldinn enda var ekkert í kerfum Fjarskipta hf. sem hefði tilkynnt öryggisatvikið.

4.3.3 Verndun upplýsinga

Ljóst er að verndun upplýsinga á vefsvæði Fjarskipta hf., vodafone.is var töluvert ábótavant. Gagnagrunnarnir sem hýstu hin stolnu gögn voru settir upp á sér vélum með tenginu við netþjóninn, þ.e. vélina [...][16] sem hýsti vefsíðuna. Gagnagrunnarnir sjálfir voru verndaðir með notandanafni og lykilorði og var það gert til að færa upplýsingarnar sem á þeim voru

[14] Fellt út vegna trúnaðar.
[15] Fellt út vegna trúnaðar.
[16] Fellt út vegna trúnaðar.

lengra frá mögulegu innbroti. Aftur á móti voru þessar aðgangsstýringar ekki varðar með sérstökum hætti. Þannig voru lykilorð gagnagrunnanna auðlesanleg í mörgum mismunandi skrám á netþjóninum og engar sérstakar ráðstafanir gerðar til verndar þeim. Veitti slíkt óhindraðan aðgang að gagnagrunnum vefsvæðisins án þess að brjótast þyrfti inn á þá.

Hvað varðar þau gögn sem vistuð voru á gagnagrunnunum þá höfðu Fjarskipti hf. brugðið á það ráð að dulkóða hluta þeirra, þ.e. lykilorð og notendanöfn áskrifenda Fjarskipta hf. Aftur á móti láðist að eyða skrá sem innihélt hin sömu lykilorð ódulkóðuð. Því voru bæði dulkóðuð og ódulkóðuð gögn inn á gagnagrunnsvélinni, [...][17].

Þá er ljóst að ekki voru gerðar sérstakar ráðstafanir til að verja önnur gögn á gagnarunnum vefsvæðisins, þ.á.m. fjarskiptagögn. Ekki voru gerðar ráðstafanir til að vernda innihald þeirra skilaboða sem voru vistuð í skeytasögu áskrifenda og geymd á [...][18] eða upplýsingar um símanúmer sendanda og móttakenda eða tímasetningu sendinganna.

4.4 Viðbrögð Fjarskipta hf. við öryggisatviki

Eftir að upp komst um innbrot og gagnastuld á vefsvæði Fjarskipta hófst umfangsmikil vinna hjá starfsmönnum félagsins sem miðaði að því að lágmarka þann skaða sem hlaust af innbrotinu fyrir viðskiptavini þess. Ekki er þörf á að fjalla um viðbrögð félagsins með ítarlegum hætti í ákvörðun þessari en vert er að nefna að um er að ræða viðbrögð er lutu að tafarlausum tæknilegum viðbrögðum og virkjun neyðaráætlunar, samskiptum við fjölmiðla, greiningu innbrots, öryggisráðstöfunum, miðlun upplýsinga til viðskiptavina og innri úttekt á hlítingu við lög og reglur. Þá fólust viðbrögðin m.a. í samskiptum við GSOC, lögreglu, Póst- og fjarskiptastofnun, netöryggissveitina CERT-IS og fjölmiðla. Þá margfaldaðist umfang málsins þegar í ljós kom að gögnin höfðu verið birt á netinu.

Póst- og fjarskiptastofnun telur að viðbrögð starfsmanna Fjarskipta hf. strax eftir að innbrot, eins og þeim er ítarlega lýst í gögnum málsins, hafi verið góð og ekki hægt að ætlast til annarra eða frekari viðbragða af þeirra hálfu. Gert hafi verið eins mikið og hægt var til þess að koma í veg fyrir að frekara tjón hlytist af öryggisatvikinu. Aftur á móti hafði gögnum þegar verið stolið þegar starfsmenn félagsins fengu tilkynningar og því ekki mögulegt á þeim tímapunkti að koma í veg fyrir gagnastuldinn eða birtingu gagnanna á netinu.

4.5 Aðgerðir Fjarskipta hf. eftir öryggisatvik

Eftir öryggisatvikið hófu Fjarskipti hf. umfangsmikla vinnu við að tryggja öryggi kerfa félagsins og gagna þess. Meðal þess sem gert var, var að tryggja öryggi nýs vefs félagsins, vodafone.is, með innlendum og erlendum sérfræðingum. Var virkni hans takmörkuð í upphafi en síðan aukin í áföngum. Þá var gerð nákvæm greining á tæknilegri hlið innbrotsins af erlendu sérfræðingateymi í tölvurannsóknum. Eins hefur félagið sett upp öflugri eldvegg, uppfært neyðaráætlun sína og endurbætt kafla um utanaðkomandi árásir, misnotkun eða skemmdarverk á fjarskiptakerfum og/eða þjónustuvefjum sínum sem og farið í heildarendurskoðun á neyðaráætlun sinni.

[17] Fellt út vegna trúnaðar.
[18] Fellt út vegna trúnaðar.

Fjarskipti hf. hafa einnig framkvæmt innri úttekt á hlítingu við fjarskiptalög og afleiddar réttarheimildir. Þá hefur félagið samið við utanaðkomandi öryggissérfræðinga varðandi veikleikaprófanir á áhættusömustu nettengdum þjónum þess. Þá var gert mat á öllum vélum Fjarskipta hf. sem tengdar voru ytri netum og reglulegum veikleikaskönnunum komið í ferli. Félagið hefur jafnframt endursett lykilorð aðgangs að innri kerfum sem og lykilorð starfsmanna sem og skipt um VPN profile. Þá voru allir víðtækir aðgangar (e. admin) að innri upplýsingakerfum yfirfarnir. Þá hefur öryggi greiðslumiðlunar verið aukið og var greiðsluupplýsingum skipt yfir í sýndarnúmar sem gerir það að verkum að upplýsingarnar nýtast engum sem yfir þær kunna að komast.

Það var svo í maí 2014 sem Fjarskipti hf. fengu vottað stjórnkerfi upplýsingaöryggis samkvæmt alþjóðlega staðlinum ISO 27001:2005, en félagið uppfærði stjórnkerfið árið 2015 í nýjustu útgáfu staðalsins, ISO 27001:2013. Félagið hefur því hlotið eina umfangsmestu vottun upplýsingaöryggis fjarskiptafélaga hér á landi í kjölfar innbrotsins. Stjórnkerfið er tekið út árlega af erlendum og óháðum úttektarmanni. Þá hefur netöryggisteymi félagsins verið eflt, bæði í mannauð, tækjum og tækni, auk þess sem samstarfið við netöryggisteymi Vodafone Global hefur aukist. Þá hefur fræðsla um upplýsingaöryggi verið efld, áhugi starfsmanna félagsins verið vakinn og endurmenntun aukin.

Fjarskipti hf. hafa einnig miðlað reynslu sinni af innbrotinu á fjölmörgum kynningum og ráðstefnum.

V.
Öryggisatvik

5.1 Almennt

Líkt og fram hefur komið sendu Fjarskipti hf. Póst- og fjarskiptastofnun skýrslur þriðju aðila sem innihéldu greiningu á umræddu öryggisatviki. Um er að ræða skýrslu Syndis slf., þar sem finna má niðurstöður frumskoðunar á atvikinu, og skýrslu AccessData Professional Service, þar sem finna má ítarlegri greiningu á öryggisatvikinu.

Eftir rýni Póst- og fjarskiptastofnunar á þessum tveimur skýrslum, sér í lagi skýrslu AccessData má draga eftirfarandi ályktanir á málsatvikum.

Skýrslunum ber saman um að aðgerðarskrár sýni að upphaf innbrotsins hafi verið þann 27. nóvember 2013 og hafi staðið yfir fram til snemma morguns þann 30. s.m. þegar uppsetningu á vefsíðu Fjarskipta hf. var breytt (e. defaced). Þá er ljóst að afrit var tekið af gögnum frá a.m.k. tveimur MySQL gagnagrunnum félagsins, þau flutt út af vefsvæði þess og síðar birt á netinu. Í skýrslu Syndis slf. kemur einnig fram að engin af þeim aðgerðarskrám eða gögnum sem félagið fékk til skoðunar gefi til kynna að brotið hafi náð til annarra kerfa að undanskyldum gagnagrunnstengingum sem notaðar voru til að flytja efni út af svæði félagsins. Er það einnig staðfest í skýrslu AccessData, þ.e. að engar vísbendingar séu um að árásin hafi náð til annarra svæða eða kjarnafjarskiptakerfis Fjarskipta hf.

Í báðum skýrslum kemur fram að um sé að ræða frekar almenna og einfalda árás þar sem þekktar aðferðir hafi verið notaðar. Þá benda gögn málsins til þess að innbrotsaðili hafi verið hluti af stærri hópi sem, eftir að bakdyr voru settar upp, hafi jafnframt getað komist inn á svæði félagsins. Þá virðast gögn af svæðinu hafa verið sótt gegnum þekktar bakdyr sem jafnframt sýni hið almenna eðli þessarar árásar.

[...][19]

5.2 Innbrot á vefsvæði

5.2.1 Aðgangur inn í kerfið [...][20]

[...][21]

Líkt og að framan greinir var sá veikleiki sem árásaraðili nýtti sér að koma fyrir bakdyrum á þjóninum [...][22], ásamt þeim galla að skrár sem hlaðið var upp voru keyranlegar fyrir alla, nægjanlegur fyrir árásaraðila til að komast inn á gagnagrunnana og þær upplýsingar sem þar voru vistaðar. Að mati Póst- og fjarskiptastofnunar verður slíkt að teljast til ófullnægjandi verklags.

5.2.2 MySQL gagnagrunnsþjónn [...][23]

[...][24]

5.2.3 MySQL gagnagrunnsþjónn [...][25]

[...][26]

5.2.4 MySQL gagnagrunnur [...][27]

[...][28]

5.2.5 Samtekt á öryggisatviki

Póst- og fjarskiptastofnun hefur farið ítarlega yfir framangreindar skýrslur. Af þeim upplýsingum sem þar koma fram má sjá að skannið, sem talið er vera undirbúningur árásarinnar, hafi hafist þann 27. nóvember 2013. [...][29] Ástæða veikleikans eru mistök í forritun. [...][30] Að mati Póst- og fjarskiptastofnunar er hér ákveðna yfirsjón að ræða af hálfu

[19] Fellt út vegna trúnaðar.
[20] Fellt út vegna trúnaðar.
[21] Fellt út vegna trúnaðar.
[22] Fellt út vegna trúnaðar.
[23] Fellt út vegna trúnaðar.
[24] Fellt út vegna trúnaðar.
[25] Fellt út vegna trúnaðar.
[26] Fellt út vegna trúnaðar.
[27] Fellt út vegna trúnaðar.
[28] Fellt út vegna trúnaðar.
[29] Fellt út vegna trúnaðar.
[30] Fellt út vegna trúnaðar.

Fjarskipta hf. sem gerði kleyft [...][31], sem leiddi til þess að notendaupplýsingar að gagnagrunnsþjónunum urðu aðgengilegar.

[...][32]

VI.
Skortur öryggisráðstafana og fjarskiptaleyndar á vefsvæði Fjarskipta hf.

6.1 Almennt

Áður en fjallað verður um skort á öryggisráðstöfunum og fjarskiptaleynd á vefsvæði Fjarskipta hf. telur Póst- og fjarskiptastofnun rétt að setja fram það álit sitt að eðlilegast hefði verið fyrir Fjarskipti hf. að geyma ekki þau gögn, sem voru andlag öryggisatviksins, á stað sem tengdur er internetinu. Slíkt er, að mati stofnunarinnar, ávallt varasamara og eykur til muna hættu á að þau geti komist í hendur óviðkomandi aðila. Í ljósi þess að um viðkvæm persónuleg gögn var að ræða í þessu tilviki, sem rík lagaskylda er til að vernda, verður ekki annað sagt en að óvarlega hafi verið staðið að geymslu gagnanna af hálfu Fjarskipta hf.

6.2 Skortur á áhættumati og gerð skriflegra öryggisráðstafana

Ljóst er af gögnum málsins að galli var til staðar í forritun á vefsvæði Fjarskipta hf. þegar öryggisatvikið átti sér stað. Verður slíkt ekki talið annað en að um yfirsjón hafi verið að ræða sem leiddi til þess að mögulegt varð að hlaða upp skrám, þ.e. bakdyrum, án takmarkana.

Fyrir liggur í gögnum málsins, og er ekki um það deilt í málinu, að öryggisskipulag Fjarskipta hf. náði á þeim tíma ekki með fullnægjandi hætti yfir vefsvæði félagsins. Þótt rúmt orðalag öryggisstefnu félagsins leiði til þess að vefkerfi félagsins falli undir hana er ljóst að vefsvæði félagsins, vodafone.is, var undanskilið áhættumati þess. Þá höfðu ekki verið gerðar skriflegar öryggisráðstafanir m.t.t. slíks áhættumats í samræmi við ákvæði 7. gr. reglna nr. 1221/2007, um vernd upplýsinga á almennum fjarskiptanetum, sbr. 2. og 3. tl. ákvæðisins, og 1. og 2. mgr. 47. gr. fjarskiptalaga nr. 81/2003.

Hefðu Fjarskipti hf. fylgt framangreindum ákvæðum laga og afleiddra réttarheimilda hefðu verið mun meiri líkur á að til staðar hefðu verið viðhlítandi öryggisráðstafanir til að vernda vefsvæði félagsins og þær upplýsingar sem þar voru geymdar. Hefðu, líkt að framan hefur verið lýst, tiltölulega einfaldar kerfislægar öryggisráðstafanir jafnframt mögulega getað komið í veg fyrir innbrot, eða í það minnsta, minnkað til muna líkur á því og dregið umtalsvert úr alvarleika þess, þrátt fyrir hina umræddu yfirsjón. Það er mat Póst- og fjarskiptastofnunar að þær ráðstafanir sem Fjarskipti hf. þó viðhafði hafi alls ekki verið nægjanlegar til þess að tryggja vernd fjarskiptanets félagsins eða þeirra upplýsinga sem um það fóru og þar voru vistaðar.

[31] Fellt út vegna trúnaðar.
[32] Fellt út vegna trúnaðar.

Í öðru lagi má ætla að yfirsjón í forritun á vefsvæðinu hefði síður átt sér stað ef skipuleg öryggisstjórnun hefði verið til staðar. Að mati Póst- og fjarskiptistofnunar ætti gerð áhættumats, árleg endurskoðun þess og val öryggisráðstafana, á vefsvæðum sem þessum, t.a.m. að fela í sér rýni á forritskóðum þess og útgáfustjórnun á þeim. Þannig ætti sú útskráning á kóða, sem rýndi tegund skráa á vefþjóninum, að hafa verið rýnd, hún metin og við henni brugðist með viðeigandi hætti. Útgáfustjórnun á forritun vefsvæðisins hefði enn fremur getað sýnt hvenær slík útskráning kóða hafi átt sér stað og hver hafi framkvæmt hana. Virkt öryggisskipulag, líkt og kveðið er á um í lögum og reglum, með gerð áhættumats og skriflegra öryggisráðstafana sem þessara, eru til þess gert að minnka til muna líkur á öryggisgöllum sem hægt er að misnota, líkt og raunin varð á í þessu tilviki.

6.3 Skortur öryggisráðstafana að vefsvæði Fjarskipta hf.

Nauðsynlegt er að hafa í huga, við skoðun á vefsvæðinu og mati á öryggi þess, að það er í eðli sínu opið að ákveðnu marki, þ.e. áskrifendur Fjarskipta hf., þurfa að hafa aðgang að því til að geta nýtt sér þjónustuna. Það er því ekki hægt að setja upp þannig varnir að reynt sé að koma í veg fyrir alla umferð heldur verður að mati Póst- og fjarskiptastofnunar að koma í veg fyrir og varna óeðlilegri og vafasamri umferð inn á svæðið, að fylgst sé með athöfnum inn á vefsvæðinu og takmarka heimildir innan þess.

Ytri varnir vefsvæðis Fjarskipta hf. samanstóðu í aðdraganda öryggisatviksins af tveimur eldveggjum sem og einni pakkasíu. Þá var um að ræða ákveðna takmarkaða umferðarskráningu sem hægt var að fylgjast með en algjör skortur var á slíku eftirliti og eftirfylgni. Svör Fjarskipta hf. sýna ekki fram á annað. Þá er ekki að sjá af gögnum málsins að frekari varnir hafi verið til staðar til að verjast og/eða fylgjast með óvanalegri umferð eða IP-tölum að vefkerfi félagsins.

Að mati Póst- og fjarskiptastofnunar hefði í fyrsta lagi verið viðeigandi að fylgjast betur með slíkri umferð að vefkerfinu. Er hægt að gera slíkt með virku eftirliti með umferð inn á vefþjóninn [...][33]. Slíkt eftirlit getur ýmist verið handvirkt eða sjálfvirkt t.a.m. með því því að setja upp IDS-búnað sem greinir umferð að vefsvæðinu. Slíkur sjálfvirkur búnaður getur sjálfkrafa tilkynnt ákveðin frávik, svo sem að fylgst sé með hlutfalli af þjónustuvillum á vefnum, s.s. þegar ekki er notuð rétt auðkenning, samanborið við eðlilega umferð, þ.e. þegar aðgangur er veittur á grundvelli gilds notendanafns og lykilorðs. Slíkur búnaður gæti þannig greint þær IP-tölur sem sýna óeðlilegar þjónustuvillur (rangar aðgangsbeiðnir) og jafnframt lokað á fyrirspurnir frá slíkum IP-tölum.

Í öðru lagi telur Póst- og fjarskiptastofnun að eðlilegt hefði verið að Fjarskipti hf. hefðu keyrt lista yfir þekktar varasamar IP-tölur við þær IP-tölur sem sendu inn beiðnir að vefkerfi þess. Þannig hefði verið hægt með tiltölulega einföldum hætti að fylgjast með mögulegum ógnum sem steðjað gætu að öryggi fjarskiptanets félagsins og þeim upplýsingum sem þar voru vistaðar. Yrði búnaður félagsins var við að þjónustubeiðnir (og þjónustuvillur) væru að berast

[33] Fellt út vegna trúnaðar.

frá IP-tölum af listanum myndi kerfið annað hvort gera stjórnstöð félagsins viðvart eða loka á fyrirspurnir frá hinum þekktu varasömu IP-tölum.

Framangreindar öryggisráðstafanir eru í eðli sínu fyrirbyggjandi og veita ákveðið öryggi gegn þeim ógnum sem innbrot af þessu tagi eru. Þær eru ekki of tæknilega flóknar og er kostnaður þeirra ekki óhóflegur miðað við eðli þeirra upplýsinga sem ráðstöfunum er ætlað að vernda.

Þá telur stofnunin í þriðja lagi að viðeigandi hefði verið að fylgst væri með umferð út af vefsvæðinu (e. exfiltration), svo sem stærð þeirra gagnapakka sem sóttir eru. Þannig myndi það teljast til eðlilegrar umferðar að litlir gagnapakkar væru sóttir, þ.e. þegar áskrifendur félagsins eru að nýta sér þá fjarskiptaþjónustu sem þarna var veitt. Aftur á móti, ef umferðarskráning sýnir að stórir gagnapakkar eru fluttir af vefsvæðinu, skrár sem fluttar eru séu óvenjulegar skrár, t.a.m. tar-skrár, eða erlendar IP- tölur eru að flytja út gögn, er eðlilegt að til staðar sé búnaður sem tilkynnir slíkt til stjórnstöðvar Fjarskipta hf. sem gæti þá viðhaft viðeigandi skoðun á umferðinni og gripið til aðgerða ef með þyrfti. [...][34] Ekkert í kerfi Fjarskipta hf. gerði félaginu viðvart um þessa mjög svo óeðlilegu gagnaflutninga af almennu fjarskiptaneti þess.

Þótt þessi ráðstöfun sé ekki til þess fallin að fyrirbyggja innbrot líkt og átti sér stað er þetta eðlileg og vel framkvæmanleg ráðstöfun til að takmarka mögulegt tjón sem hlotist getur af innbrotum sem þessum, sem og að hún gerir félaginu kunnugt um umfangsmikinn gagnaflutning af vefsvæði þess. Mögulegt hefði verið að grípa til lokana á kerfinu ef vitneskja hefði verið um þessa óeðlilegu umferð. Félaginu var hvorki kunnugt um innbrot fyrr en skipt var um forsíðu vefsíðu þess (e. deface) né að gögnum hafi verið stolið fyrr en þau voru birt á netinu.

Hér eru einungis tilgreindar ákveðnar öryggisráðstafanir sem hefði verið hægt að viðhafa án umtalsverðs tilkostnaðar. Ekki er um tæmandi talningu að ræða eða upptalningu á öryggisráðstöfunum sem Fjarskipti hf. hefði verið skylt að hafa samkvæmt öryggisskipulagi sínu. Aftur á móti er það mat Póst- og fjarskiptastofnunar að ráðstafanir sem þessar teljist til eðlilegra varna sem viðhafðar eru á opnum vefsvæðum sem þessum og séu í samræmi við „best-practice“, a.m.k. þegar vefsvæði hýsir og miðlar fjarskiptaupplýsingum sem njóta skulu leyndar. Aftur á móti áréttar Póst- og fjarskiptastofnun að öryggisráðstafanir fjarskiptafélaga eiga að byggja á mati félagsins á þeirri hættu sem að geta ógnað eignum þess. Slíkt skorti í tilviki vefsvæðis Fjarskipta hf. og voru því engar öryggisráðstafanir til staðar í aðdraganda öryggisatviksins til að varna ytra aðgengi að vefsvæði félagsins að undanskyldum eldveggjunum tveim, pakkasíu og svo auðkenningu áskrifenda.

6.4 Skortur öryggisráðstafana á vefsvæði Fjarskipta hf.

Auk þeirra varna sem fjallað er um hér að framan, hefði verið nauðsynlegt að viðhafa ákveðið innra eftirlit á vefsvæðinu sjálfu. Svör Fjarskipta hf. sýna að einu öryggisráðstafanirnar sem finna mátti inn á vefsvæðinu sjálfu voru aðgangsorð inn á MySQL gagnagrunna svæðisins

[34] Fellt út vegna trúnaðar.

sem og dulritun á auðkennum áskrifenda. [...][35] Þá er jafnframt ljóst að þótt auðkenni áskrifenda hafi verið dulrituð voru þau einnig að finna ódulrituð á gagnagrunnum félagsins. Þær ráðstafanir sem Fjarskipti hf. reyndi að viðhafa skiluðu ekki árangri sökum þessa.

Að mati Póst- og fjarskiptastofnunar getur innra eftirlit vefsvæðisins í fyrsta lagi falist í tengingum milli vefþjónsins við MySQL gagnagrunnana, svo sem eftirliti með gagnagrunnsfyrirspurnum innan kerfis, þ.e. frá [...][36]. Þannig væri hvort tveggja ákveðið eftirlit með fyrirspurnum einstakra áskrifenda inn í MySQL gagnagrunnana sem og mögulegar takmarkanir á hversu mikið af upplýsingum viðkomandi áskrifandi getur nálgast og kallað eftir frá gagnagrunnunum. Slíkar öryggisráðstafanir, ásamt traustri dulritun á aðgangsorðum gagnagrunna hefðu getað komið í veg fyrir að innbrotsaðili hefði getað nálgast hinar umfangsmiklu upplýsingar. Hefði innbrotsaðili getað fundið leið fram hjá þessum vörnum hefði traustri dulritun á auðkennum notenda þó getað dregið úr því umfangsmikla tjóni sem af innbrotinu hlaust.

Í öðru lagi hefði verið eðlileg ráðstöfun að viðhafa eftirlit með breytingum sem gerðar eru inn á vefsvæðinu og á gagnagrunnunum, svo sem gerð nýrra skráa, eyðingu skráa, breytinga á skrám sem og breytingar á réttindum á skrám. Ef fylgst hefði verið með slíkum aðgerðum hefði gerð afritunarskráar og skjalasafns, sem og eyðing upplýsinga af gagnagrunnum, ekki átt sér stað án vitundar félagsins líkt og gerðist í umræddu öryggisatviki. Að mati Póst- og fjarskiptastofnunar hefðu tilkynningar um slíkar aðgerðir á vefsvæðinu getað komið í veg fyrir hið mikla tjón sem varð. Ef kerfi félagsins hefði gert starfsmönnum þess viðvart um þær aðgerðir sem fram fóru á vefsvæðinu hefðu þeir getað skoðað þær og brugðist við með viðhlítandi hætti.

Í þriðja lagi hefði þurft að viðhafa ákveðnar öryggisráðstafanir er varða dulritun og aðgang að réttindum. Líkt og áður segir þá er ekki um að ræða algjörlega lokað vefsvæði heldur verða áskrifendur Fjarskipta hf. að hafa aðgang að því til að geta nýtt sér þá fjarskiptaþjónustu sem félagið bauð upp á. Þannig getur dulritun á lykilorðum inn á gagnagrunna orðið tæknilega flóknari. Kerfið allt þarf að vera sjálfvirkt og geta lesið auðkenni og lykilorð hvers áskrifenda fyrir sig og meta aðgang hans að hinu dulritaða lykilorði. Að mati Póst- og fjarskiptastofnunar hefði takmörkun á lesréttindum á skrám sem innihéldu lykilorð að gagnagrunnunum þó verið nauðsynleg í þessu tilviki. Aðgangur að skrám í netþjóninum [...][37] var heimilaður til allra skráa á honum. Takmörkun hér á hefði gert innbrotsaðila mun erfiðara fyrir að komast yfir aðgangsorð fyrir gagnagrunna svæðisins, [...][38], og þær upplýsingar sem þar var að finna.

Þá er ljóst að eðlilegt og viðeigandi er að viðhafa ákveðnar innri varnir fyrir MySQL gagnagrunna. Slíkar öryggisráðstafanir geta falið í sér takmörkun aðgangs að MySQL gagnagrunnum við þekktar IP-tölur, umferðarskráningar og virku eftirliti með óeðlilegum fyrirspurnum um upplýsingar, s.s. ef um stórar, margar og tíðar fyrirspurnir er að ræða. Þá

[35] Fellt út vegna trúnaðar.
[36] Fellt út vegna trúnaðar.
[37] Fellt út vegna trúnaðar.
[38] Fellt út vegna trúnaðar.

væri eðlilegt að fylgjast með flutningi gagna af slíkum gagnagrunnum. Fjarskipti hf. hafa ekki sýnt að nokkrar slíkar ráðstafanir hafi verið til staðar á MySQL gagnagrunnum félagsins. Hefði verið til staðar sjálfvirkur búnaður sem næmi og tilkynnti um slíkar óeðlilegar fyrirspurnir og flutning gagna hefði verið mögulegt fyrir félagið að bregðast við og koma í veg fyrir að gögn væru flutt til á vefsvæði þess eða út af því.

Í fjórða lagi verður enn fremur að telja, í ljósi eðlis þeirra gagna sem vistuð voru á gagnagrunnum félagsins, að dulritun gagnanna sjálfra, þ.e. innihald skilaboðanna, hefði verið nauðsynleg ráðstöfun til að tryggja fjarskiptaleynd og vernd einkalífs. Þannig ætti öll skeytasaga hlutaðeigandi áskrifanda einungis að vera lesanleg honum. Sú staðreynd að skeytasaga hvers áskrifanda var ekki vistuð á grundvelli réttmæts samþykkis hans eykur enn á alvarleika þessa brests í öryggisráðstöfunum Fjarskipta hf. og þeirra fjarskiptaleyndar sem hverju fjarskiptafyrirtæki ber að tryggja. Nær þetta hvort tveggja til innihalds skilaboðanna sem og fjarskiptaumferðarupplýsinga í formi umferðarskráa (e. log). Er ljóst að ef gögn og upplýsingar sem vistuð voru á gagnagrunnum vefsvæðisins hefðu verið dulrituð hefði það dregið verulega úr þeirri áhættu að fjarskiptaleynd yrði rofin.

Fyrir liggur í málinu að vefsvæði félagsins, vodafone.is, var ekki innan áhættumats þess. Því höfðu ekki verið gerðar skriflegar öryggisráðstafanir fyrir vefsvæði félagsins í samræmi við niðurstöður slíks áhættumats.

Með töku ákvörðunar Póst- og fjarskiptastofnunar nr. 1/2014, sbr. úrskurð úrskurðarnefndar fjarskipta- og póstmála í máli nr. 3/2014, fellur vefsvæði Fjarskipta hf. undir ákvæði fjarskiptalaga og afleiddra réttarheimilda, enda telst vefkerfið vera almennt fjarskiptanet í skilningi 5. tl. 3. gr. fjarskiptalaga nr. 81/2003. Á Fjarskiptum hf. hvíldi því skýr skylda að fella vefsvæði sitt undir öryggisskipulag þess með virkum hætti og framkvæma framangreint áhættumat og setja skriflegar öryggisráðstafanir á grundvelli þess, sbr. 2. mgr. 47. gr. fjarskiptalaga og ákvæði reglna nr. 1221/2007, um vernd upplýsinga á almennum fjarskiptanetum, sbr. 7. gr. þeirra. Kröfur þessara ákvæða voru á þessum tíma ekki uppfylltar af hálfu Fjarskipta hf.

Þá er það mat Póst- og fjarskiptastofnunar að ekki hafi verið til staðar, þegar öryggisatvikið átti sér stað árið 2013, viðeigandi eða nauðsynlegar ráðstafanir, í samræmi við ákvæði 4., 5. og 12. gr. framangreindra reglna og 1. mgr. 47. gr. fjarskiptalaga, til að tryggja vernd fjarskiptaþjónustu félagsins eða fjarskiptanet þess, þ.m.t. ráðstafanir til að verja þær upplýsingar sem þar voru vistaðar fyrir eyðileggingu, glötun eða óleyfilegum aðgangi. Ekkert í kerfi félagsins greindi óeðlilega umferð inn eða út af vefsvæði þess eða gerði því viðvart um að eitthvað óeðlilegt væri um að vera á vefsvæði þess. Það var eingöngu fyrir tilstuðlan innbrotsaðila sjálfs, þ.e. breyting á forsíðu vefsvæðisins og birtingu upplýsinga á internetinu, sem gerði Fjarskiptum hf. ljóst að innbrot og gagnastuldur hafði átt sér stað. Slíkt verður að telja sérstaklegan alvarlegan öryggisbrest. Þá eykst alvarleikinn til muna í ljósi þess að á vefsvæðinu voru geymd fjarskiptagögn, hvort tveggja innihald skilaboða sem og umferðarupplýsingar. Kröfur þessara ákvæða voru ekki uppfylltar af hálfu Fjarskipta hf.

Að mati Póst- og fjarskiptastofnunar hefðu tiltölulega einfaldar öryggisráðstafanir varðandi umferðarskráningar og eftirlit með þeim getað komið í veg fyrir innbrot eða a.m.k. dregið verulega úr líkum á því. Hefði vefsvæðið haft sjálfvirka vöktun og gert starfsmönnum viðvart um óeðlilegar þjónustuvillur og umferð eru líkur á að hægt hefði verið að grípa til aðgerða til að koma t.a.m. í veg fyrir innbrot sem og hinn gríðarlega gagnaflutning af vefsvæði þess. Einu varnirnar inn á vefsvæðið fólust í auðkenningu áskrifenda með notendanafni og lykilorði sem og umferðarskráning sem ekkert eftirlit var með. Að mati stofnunarinnar getur slíkt ekki talist viðeigandi eða nægjanlegt miðað við það mikla magn af fjarskiptaupplýsingum og persónuupplýsingum sem vistaðar voru á vefkerfi félagsins.

Þá verður ekki komist að annarri niðurstöðu en að fyrri árásir á vefsvæðið hefðu átt að hvetja félagið til að fella það með virkum hætti undir öryggisskipulag þess með því að fella það undir áhættumat félagsins og setningu skriflegra öryggisráðstafana í samræmi við áðurnefnd ákvæði fjarskiptalaga og reglna nr. 1221/2007. Slíkt gerði félagið þó ekki fyrr en í kjölfar innbrotsins.

Af svörum félagsins má sjá að formleg endurskoðun öryggisstefnu þess hafði ekki, þegar öryggisatvikið átti sér stað, verið framkvæmd síðan árið 2009, þ.e. áður en til innskráninga var þörf á „Mínar síður“ og boðið var upp á geymslu smáskilaboða. Þá er ljóst að ekki var á þessum tíma til staðar formlegt innra eftirlit var með vefsvæði félagsins og öryggisráðstafana þess og verður að telja það alvarlegan brest hjá félaginu við að uppfylla skyldur sem á það eru lagðar í 8. gr. reglna nr. 1221/2007, að viðhafa ekki slíka endurskoðun eða innra eftirlit.

6.5 Skortur á fjarskiptaleynd

Ekki er um það deilt í málinu að á gagnagrunnum á vefsvæði Fjarskipta hf. var hvort tveggja að finna gögn, í formi aðgerðarskráa, sem sýndu hvort tveggja ákveðnar tengiupplýsingar, þ.e. A- og B-númer, dagsetningu sendingar og verð hennar, sem og upplýsingar um innihald fjarskiptasendinga sem ekki hafði verið sérstaklega óskað eftir að yrðu ekki vistuð. Að mati Póst- og fjarskiptastofnunar höfðu Fjarskipti hf. ekki heimildir til geymslu umræddra gagna sbr. ákvæði 42. gr. og 4. mgr. 47. gr. fjarskiptalaga. Ákvæði þessi eiga m.a. að tryggja fjarskiptaleynd áskrifenda og fela í sér að ekki er heimilt að geyma gögn um fjarskiptaumferð nema í sex mánuði og að innihald þeirra skuli ekki geymt nema á grundvelli lagaheimildar eða samþykkis áskrifenda.

Hvað varðar gögn um fjarskiptaumferð er ljóst af gögnum málsins að upplýsingar í aðgerðarskrám sem geymdar voru á gagnagrunnum félagsins sýna símanúmer sendanda og móttakanda, þ.e. A- og B-númer, dagsetningu sendingar sem og verð umræddrar sendingar. Að mati stofnunarinnar er alveg ljóst að hér er um að ræða gögn um fjarskiptaumferð í samræmi við skilgreiningu stofnunarinnar á þeim, enda er um að ræða upplýsingar sem eru hluti af stýringu og afgreiðslu fjarskiptakerfanna. Þá verða upplýsingarnar til í fjarskiptakerfi Fjarskipta hf. vegna notkunar viðkomandi á fjarskiptaþjónustu félagsins sem félagið innheimtir fyrir. Fyrir liggur í málinu að um er að ræða mun eldri upplýsingar en sex mánaða og því verður ekki komist að annarri niðurstöðu en að Fjarskipti hf. hafi ekki uppfyllt kröfu 42. gr. um að eyða gögnum um fjarskiptaumferð að sex mánuðum liðnum. Helgast sú

niðurstaða einnig af því að ekki var til staðar upplýst samþykki áskrifenda fyrir geymslu slíkra gagna til lengri tíma.

Hvað varðar innihald skilaboða er ljóst að geymsla fjarskipta er óheimil nema hún fari fram með samþykki notanda eða samkvæmt heimild í lögum, sbr. 4. mgr. 47. gr. fjarskiptalaga. Fyrir liggur í málinu að upplýsingar um innihald skilaboða sem send voru af „Mínum síðum“ voru vistuð sjálfkrafa á gagnagrunnum á vefsvæði Fjarskipta hf. Þá er enn fremur ljóst að sá háttur sem hafður var á varðandi ætlað samþykki notenda uppfyllti ekki skilyrði ákvæðisins um upplýst samþykki líkt og það hefur verið skilgreint af hálfu stofnunarinnar, sbr. einnig úrskurði Persónuverndar varðandi skilyrði upplýsts samþykkis á grundvelli laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga. Það er því niðurstaða stofnunarinnar að Fjarskipti hf. hafi ekki uppfyllt ákvæði 4. mgr. 47. gr. fjarskiptalaga og viðhaft óheimila geymslu á fjarskiptum, þ.e. innihaldi smáskilaboða.

VII.
Niðurstaða Póst- og fjarskiptastofnunar

Líkt og fjallað er um í köflum 4.4 og 4.5 í ákvörðun þessari hafa Fjarskipti hf. í kjölfar öryggisatviksins brugðist við með margvíslegum hætti og eflt varnir sínar. Félagið hefur hlotið eina umfangsmestu vottun upplýsingaöryggis fjarskiptafélaga hér á landi í kjölfar innbrotsins og hefur nú vottað stjórnkerfi upplýsingaöryggis samkvæmt alþjóðlega staðlinum ISO 27001:2005, en félagið uppfærði stjórnkerfið árið 2015 í nýjustu útgáfu staðalsins, ISO 27001:2013. Þá stóðst félagið nýverið úttekt Póst- og fjarskiptastofnunar á öryggi og meðferð fjarskiptaupplýsinga en niðurstaða úttektarinnar er á þann veg að Fjarskipti hf. uppfylla nú kröfur um öryggi og meðferð umræddra persónuupplýsinga.

Hins vegar náði öryggisskipulag Fjarskipta hf., þegar öryggisatvik átti sér stað í nóvember 2013, ekki með virkum hætti yfir vefsvæði félagsins, vodafone.is. Vefsvæði sem telst vera hluti af almennu fjarskiptaneti þess og þar sem veitt er almenn fjarskiptaþjónusta. Var það hvorki innan áhættumats félagsins né höfðu verið valdar viðeigandi öryggisráðstafanir m.t.t. niðurstöðu slíks áhættumats fyrir þann hluta fjarskiptanets félagsins eða þær upplýsingar sem á því voru vistaðar. Varðar það við ákvæði 1. og 2. mgr. 47. gr. fjarskiptalaga og 2. og 3. tl. 7. gr. reglna nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.

Þá er það jafnframt mat Póst- og fjarskiptastofnunar að þær öryggisráðstafanir sem viðhafðar voru á þessum tíma til að vernda vefsvæði félagsins sem og þær upplýsingar sem þar voru vistaðar hafi ekki verið viðeigandi til að vernda öryggi þjónustunnar eða þeirra gagna sem þar voru. Varðar það við ákvæði 1. mgr. 47. gr. fjarskiptalaga og 4. og 5. gr. reglna nr. 1221/2007 um vernd upplýsinga á almennum fjarskiptanetum, sbr. einnig 12. gr. reglnanna.

Það er enn fremur niðurstaða Póst- og fjarskiptastofnunar að fyrir innbrot uppfylltu Fjarskipti hf. ekki kröfur um upplýst samþykki fyrir vistun gagna á vefsvæði sínu. Geymsla þeirra varðar því við 4. mgr. 47. gr. fjarskiptalaga.

Póst- og fjarskiptastofnun telur enn fremur að Fjarskiptum hf. hafi borið að eyða eða gera nafnlausar upplýsingar um fjarskiptaumferð áskrifenda félagsins. Almennar umferðarskráningar sem fela í sér slík fjarskiptaumferðargögn ber að eyða eftir sex mánuði eða gera ópersónugreinanlegar, nema ef viðkomandi áskrifandi sé í vanskilum við félagið vegna þjónustunnar. Varðar þetta við 42. gr. fjarskiptalaga nr. 81/2003, enda var, þegar öryggisatvikið átti sér stað, ekki til staðar samþykki áskrifanda fyrir frekari varðveislu gagnanna.

Með þessu athafnaleysi félagsins fyrir öryggisatvikið braut það með alvarlegum hætti gegn meginákvæðum fjarskiptalaga um vernd persónuupplýsinga og friðhelgi einkalífs, sbr. IX. kafla fjarskiptalaga.

Á k v ö r ð u n a r o r ð

Fjarskipti hf. brutu, þegar öryggisatvik átti sér stað í nóvember 2013, gegn ákvæðum 4., 5., 2. og 3. tl. 7., 8. og 12. gr. reglna nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum, sbr. 1. og 2. mgr. 47. gr. fjarskiptalaga nr. 81/2003, sem og 1. mgr. 42. gr., sbr. 2. og 3. mgr. ákvæðisins, og 4. mgr. 47. gr. fjarskiptalaga nr. 81/2003, með því að:

a) **Viðhafa ekki virkt öryggisskipulag fyrir vefsvæði félagsins, vodafone.is, sem hluta af almennu fjarskiptakerfi þess, með því að undanskilja það áhættumati félagsins og gera ekki skriflegar lýsingar á öryggisráðstöfunum á grundvelli þess í samræmi við 2. og 3. tl. 7. gr. reglna nr. 1221/2007, sbr. einnig 12. gr. reglnanna, og 2. mgr. 47. gr. laga um fjarskipti nr. 81/2003.**

b) **Viðhafa ekki viðeigandi ráðstafanir til að tryggja vernd vefsvæðis félagsins, sem hluta af almennu fjarskiptaneti þess, og þeirra upplýsinga sem þar voru vistaðar gegn óleyfilegum aðgangi, breytingum eða eyðileggingu í samræmi við 4. gr. reglna nr. 1221/2007, sbr. einnig 12. gr. reglnanna, og 1. mgr. 47. gr. fjarskiptalaga nr. 81/2003.**

c) **Viðhafa ekki a.m.k. árlegt innra eftirlit fyrir vefsvæði félagsins til að tryggja að unnið sé í samræmi við öryggisstefnu og skjalfestar verklags- og öryggisreglur öryggisskipulags og að uppbygging þess sé í samræmi við lög og reglur í samræmi við 8. gr. reglna nr. 1221/2007.**

d) **Tryggja ekki að áskrifandi að almennri fjarskiptaþjónustu félagsins hafi notið verndar gegn geymslu skilaboða og auðkenna sem fór um og voru geymd á**

vefsvæði félagsins, án samþykkis áskrifanda, í samræmi við 5. gr. reglna nr. 1221/2007 og 4. mgr. 47. gr. fjarskiptalaga nr. 81/2003.

e) Hafa ekki eytt eða gert nafnlaus gögn um fjarskiptaumferð áskrifenda, sem nýttu sér almenna fjarskiptaþjónustu félagsins á vefsvæði þess, og sem þar voru vistuð, eftir sex mánuði í samræmi við 1. mgr. 42. gr. fjarskiptalaga nr. 81/2003.

Ákvörðun þessi er kæranleg til úrskurðarnefndar fjarskipta- og póstmála og skal kæran berast úrskurðarnefnd innan fjögurra vikna frá því viðkomandi varð kunnugt um ákvörðun Póst- og fjarskiptastofnunar sbr. 13. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun og 5. gr. reglugerðar nr. 39/2009 um úrskurðarnefnd fjarskipta- og póstmála. Um kostnað vegna málskots fer samkvæmt 5. mgr. 13. gr. sömu laga, auk þess sem greiða ber sérstakt málskotsgjald að upphæð 150.000, skv. 6. gr. reglugerðar um úrskurðarnefnd fjarskipta- og póstmála. Sem neytanda ber kvartanda þó ekki að greiða umrætt málskotsgjald.

Reykjavík, 29. desember 2016

Hrafnkell V. Gíslason, forstjóri	Unnur Kristín Sveinbjarnard.