143. löggjafarþing 2013–2014.
Þingskjal 1314 — 423. mál.

Svar

innanríkisráðherra við fyrirspurn frá Birni Leví Gunnarssyni
um úttekt á netöryggi almennings.

1. *Hverjar voru helstu niðurstöður úttektar á netöryggi almennings sem boðuð var af hálfu ráðuneytisins í kjölfar tölvuinnbrots hjá fjarskiptafyrirtækinu Vodafone laugardaginn 30. nóvember 2013? Sundurliðað svar óskast um stöðu netöryggis, ábyrgð fjarskiptafyrirtækja, eftirlit opinberra stofnana, gæði lagarammans og réttarstöðu neytenda.*

a. Um stöðu netöryggis.

Í úttektinni, sem unnin var af Páli Ásgrímssyni hdl., kemur fram það mat að tvíþætt hlutverk Póst- og fjarskiptastofnunar (PFS) geti valdið hagsmunaárekstri. Þannig er stofnuninni annars vegar ætlað að hafa almennt eftirlit með fjarskiptafyrirtækjum, þ.m.t. meðferð þeirra á öryggisatvikum í tengslum við net- og upplýsingaöryggi, og hins vegar að sinna þjónustuhlutverki við sömu fjarskiptafyrirtæki og aðra rekstraraðila ómissandi upplýsingainnviða sem kjósa að gera þjónustusamninga við netöryggissveitina CERT-ÍS, sem nú er vistuð hjá PFS.

Í úttektinni er lagt til að stofnað verði sérstakt netöryggisteymi er sinni net- og upplýsingaöryggi stjórnvalda, svonefnd GOV-CERT-sveit. Þykir höfundi rétt að GOV-CERT-sveit á Íslandi verði vistuð hjá almannavarnadeild ríkislögreglustjóra.

Rétt er að geta þess að ráðherra hefur nú þegar lagt fyrir Alþingi frumvarp sem felur í sér flutning netöryggissveitarinnar frá PFS til almannavarnadeildar ríkislögreglustjóra. Til að sú sérþekking sem byggð hefur verið upp innan netöryggissveitar PFS glatist ekki er lagt til að starfsmenn sveitarinnar færist til almannavarnadeildar ríkislögreglustjóra. Hin nýja GOV-CERT-sveit færi þannig með öll sömu verkefni og CERT-ÍS gegnir nú, en að auki mundi sveitin sinna net- og upplýsingaöryggi stjórnvalda. Þar sem GOV-CERT fer öllu jöfnu ekki með hlutverk landstengiliðar væri að mati höfundar heppilegt að hin nýja sameinaða netöryggissveit mundi þó bera annað heiti en GOV-CERT.

Lagt er til í úttektinni að formbundið verði sérstakt netöryggisráð, sem leggur til á landsvísu stefnu og samræmingaráætlanir í net- og upplýsingaöryggismálum. Ráðið mundi samkvæmt tillögunum jafnframt hafa með höndum innleiðingu þeirrar stefnu og samræmingaráætlana. Slíkt ráð mundi heyra undir innanríkisráðherra og gæti verið samsett með svipuðum hætti og starfshópur sá sem nú vinnur að stefnumótun um net- og upplýsingaöryggi. Að mati höfundar kemur til álita að víkka út hópinn þannig að fulltrúar helstu ómissandi upplýsingainnviða eigi þar jafnframt sæti eða að um sé að ræða tvo aðskilda hópa.

b. Ábyrgð fjarskiptafyrirtækja.

Í úttektinni kemur fram að einkum sé mælt fyrir um skyldur fjarskiptafyrirtækja í 47. gr. fjarskiptalaga, um öryggi og þagnarskyldu. Er í framhaldinu tekið fram að ákvæði þetta hafi verið skýrt og túlkað í nýlegum héraðsdómi, sbr. dóm Héraðsdóms Reykjavíkur í máli nr. E-1774/2012, Síminn hf. gegn Póst- og fjarskiptastofnun og A. Þá sé að finna í 42. gr. fjarskiptalaga ákvæði um gögn um fjarskipti, þ.m.t. geymslutíma gagna. Bregðist fjarskiptafyrirtæki skyldum sínum samkvæmt fyrrgreindum lagaákvæðum, og reglum settum á grundvelli þeirra, eða öðrum ákvæðum fjarskiptalaga getur það varðað viðurlögum á grundvelli

viðurlagakafla fjarskiptalaga, sem og skaðabótaábyrgð, sbr. hér að aftan. Sama gildir um brot gegn ákvæðum 11.–13. gr. persónuverndarlaga. Þau varða viðurlögum samkvæmt ákvæðum þeirra laga og eftir atvikum bótaábyrgð.

Bregðist fjarskiptafyrirtæki í að sinna lögboðnum skyldum sínum á sviði net- og upplýsingaöryggis eða verði þau að öðru leyti uppvís að saknæmri háttsemi í andstöðu við sakarreglu bótaréttar geta þau að mati höfundar bakað sér skaðabótaskyldu samkvæmt almennum reglum skaðabótaréttarins.

Í úttektinni kemur fram að í fjarskiptalögum, nr. 81/2003, sé að finna kafla um viðurlagaheimildir, kafla XVI, sem ber heitið Viðurlög o.fl. Kaflinn geymir tvær lagagreinar.

Höfundur úttektarinnar telur ekki þörf á að herða viðurlagaákvæði fjarskipta- eða persónuverndarlaga, en ljóst sé að samkvæmt drögum að evrópskum reglum megi búast við hertum viðurlögum á sviði almennrar persónuverndar þegar fram í sækir. Telur hann farsælla að eftirlitsaðilar sinni leiðbeiningar- og samræmingarhlutverki sínu á sviði net- og upplýsingaöryggismála með setningu fyrirframreglna og tilmæla (ex ante) fremur en að eftirlitið snúist um hörð viðurlög við brotum í fortíð (ex post).

c. Eftirlit opinberra stofnana.

Fram kemur í úttektinni að PFS og Persónuvernd hafi almennu eftirlitshlutverki að gegna þegar kemur að net- og upplýsingaöryggi. Eftirlitshlutverk Persónuverndar snúi m.a. að áhættumati, gæðum og öryggi persónuupplýsinga. PFS sé hins vegar falið almennt eftirlitshlutverk með fjarskiptafyrirtækjum og snýr eftirlit stofnunarinnar á sviði net- og upplýsingaöryggis einkum að ákvæðum IX. kafla laganna, um vernd persónuupplýsinga og friðhelgi einkalífs. Að þessu leyti beri að líta á ákvæði fjarskiptalaga um vernd persónuupplýsinga í starfsemi fjarskiptafyrirtækja sem sérákvæði sem ganga framar almennum ákvæðum laga um persónuvernd. Þau síðarnefndu séu hins vegar sérákvæðum fjarskiptalaga til skýringar og fyllingar.

Bent er á að til viðbótar hinu almenna eftirlitshlutverki hafi PFS, sem fyrr greindi, einnig hlutverki að gegna þegar kemur að starfsemi netöryggissveitarinnar. Þannig segi í 1. málsl. 1. mgr. 47. gr. a fjarskiptalaga að PFS skuli starfrækja netöryggissveit sem gegna skuli hlutverki öryggis- og viðbragðshóps til verndar ómissandi upplýsingainnviðum gegn netárásum.

Fram kemur í úttektinni að opinberir starfsmenn geti við rækslu starfsskyldna sinna, í þessu tilviki hinu almenna og sértæka eftirlitshlutverki, bakað sér bæði refsi- og bótaábyrgð. Ekki var fjallað sérstaklega um mögulega refsiábyrgð í úttektinni, hins vegar var bent á að opinberir starfsmenn geti valdið tjóni vegna mistaka eða vanrækslu við opinbert eftirlit. Bent var á að í fræðiritum hafi mikið verið fjallað um þetta atriði og hafi verið leidd að því rök að ábyrgð hins opinbera í þessum tilvikum sé vægari en á öðrum sviðum.

Þá er vísað til þess að embætti ríkislögreglustjóra hafi lögbundnu hlutverki að gegna í tengslum við net- og upplýsingaöryggi. Þannig sé kveðið á um í orðskýringarákvæði 27. tölul. 1. mgr. 3. gr. laga nr. 81/2003, um fjarskipti, að ríkislögreglustjóri skilgreini ómissandi upplýsingainnviði. Þá sé mælt fyrir um í 5. mgr. 47. gr. a sömu laga að netöryggissveitinni sé heimilt að tilkynna til ríkislögreglustjóra um meiri háttar netárásir gegn netumdæminu og um alvarleg eða útbreidd öryggisatvik sem valdið hafa tjóni eða hættu á tjóni á ómissandi upplýsingainnviðum, í þeim tilvikum þar sem þjóðaröryggi og almannaheill er í húfi. Að beiðni ríkislögreglustjóra skuli netöryggissveitin viðhafa samstarf um varnir og viðbrögð. Að mati höfundar er sem fyrr segir lagt til að færa embætti ríkislögreglustjóra enn ríkara hlutverk, þ.e. að færa Cert-ÍS til almannavarnadeildar ríkislögreglustjóra.

d. Gæði lagarammans.

Í úttektinni kemur fram það mat að löggjöfin hér á landi um net- og upplýsingaöryggi sé um margt ítarlegri en víðast hvar í þeim löndum sem við berum okkur gjarnan saman við. Að mati höfundar fæst því ekki séð að knýjandi þörf eða nauðsyn sé á viðamiklum breytingum

á löggjöf til að hrinda ábendingum úttektaraðila í framkvæmd. Þó koma fram í úttektinni tillögur varðandi mögulegar breytingar á núgildandi löggjöf, þær eru eftirfarandi:

1. Breyta þarf ákvæði 47. gr. a í fjarskiptalögum ef starfsemi CERT-ÍS verður færð til almannavarnadeildar ríkislögreglustjóra í tengslum við stofnun GOV-CERT-hóps hér á landi.
2. Breyta þarf eða fella niður og setja nýja reglugerð í stað reglugerðar nr. 475/2013, um málefni CERT-ÍS netöryggissveitar. Við þá vinnu þarf m.a. að gæta samræmis milli þess hvort ákvarðanir netöryggissveitar séu bindandi stjórnvaldsákvarðanir sem sæti kæru til æðra setts stjórnvalds eða leiðbeinandi tilmæli sem ekki hafi bindandi áhrif og því ekki kæranlegar.
3. Til álita kemur að setja á laggirnar sérstakt netöryggisráð og að starfsemi þess verði formbundin að því leyti að það starfi á grundvelli lagaheimildar.
4. Huga þarf að nauðsynlegum breytingum á löggjöf í tengslum við tillögu að tilskipun Evrópuþingsins og ráðsins „concerning measures to ensure high common level of network and information security across the Union“. Í ljósi þess að tilskipunin er enn á undirbúningsstigi og ekki komin í EES-samninginn er íslenska ríkið ekki skuldbundið þjóðréttarlega til að innleiða reglurnar. Hins vegar er lagt til að nú þegar verði öllum rekstraraðilum ómissandi upplýsingainnviða gert með lagafyrirmælum að gera áhættumat og grípa til nauðsynlegra ráðstafana til að tryggja net- og upplýsingaöryggi. Þessum aðilum verði gert skylt að tilkynna til hinnar nýju netöryggissveitar atvik sem setja net- og upplýsingaöryggi í hættu.
5. Huga þarf að breikkun á gjaldstofni vegna reksturs á GOV-CERT hér á landi, sem jafnframt fari með núverandi hlutverk CERT-ÍS. Fram til þessa hafa einungis fjarskiptafyrirtæki fjármagnað rekstur CERT-ÍS gegnum svokallað rekstrargjald. Þykir eðlilegt að rekstraraðilar ómissandi upplýsingainnviða taki allir þátt í starfseminni en fram til þessa hafa ekki verið gerðir þjónustusamningar við slíka aðila, sbr. 14. gr. reglugerðar nr. 475/2013. Að fenginni þeirri reynslu kann að vera heppilegra að rekstraraðilar ómissandi upplýsingainnviða verði sjálfvirkt þjónustuaðilar breyttrar netöryggissveitar. Með því að breikka gjaldstofninn væri samtímis unnt að lækka álagningarprósentuna. Þannig væri viðkomandi fyrirtækjum og stofnunum ekki íþyngt um of. Lítil og meðalstór fyrirtæki, sem ekki reka ómissandi upplýsingainnviði, t.d. mörg aðildarfélög Samtaka verslunar og þjónustu, gætu síðan gert þjónustusamninga við netöryggissveitina kjósi þau það.
6. Lagt er til að fyrirmæli um að rekstraraðilar ómissandi upplýsingainnviða styðjist við tiltekna staðla og fái vottun á grundvelli þeirra verði bundin í lög í rýmri merkingu. Kemur einkum til álita að tilteknir kaflar ISO/IEC 270001 staðalsins (Stjórnkerfi upplýsingaöryggis) verði færðir í lög eða reglugerð en jafnframt koma aðrir staðlar til skoðunar. Til að íþyngja ekki smærri einkaaðilum þyrfti að miða slíka skyldu við veltu hlutaðeigandi og útfæra þröskulda þannig að einungis stærri fyrirtæki féllu þar undir. Við þetta mundi hlutverk sérfróðra og óháðra úttektaraðila úr einkageiranum aukast og eftirlitshlutverk opinberra aðila minnka.
7. Til álita kemur að lögbinda sérstaka undanþáguheimild frá samkeppnislögum til að greiða fyrir samstarfi tæknimanna sem starfa að net- og upplýsingaöryggismálum, enda þarf að óbreyttum lögum að öðrum kosti að sækja sérstaklega um undanþágu fyrir slíku samstarfi á grundvelli 15. gr. samkeppnislaga, nr. 44/2005.
8. Til álita kemur að lögfesta skýra lagaheimild til að unnt sé að gera kröfur til þeirra sem reka ómissandi innviði, t.d. til að mæla fyrir frágang við brunna í orkukerfinu í því skyni

að tryggja varaafl í raforku og mæla fyrir um frágang við landtökustaði sæstrengja. Þá er bent á að hér á landi skortir almennt regluverk um merkingu skjala eftir öryggisstigi, vottun persóna o.s.frv.

9. Huga þarf að nauðsynlegum breytingum á almennum hegningarlögum til að íslensk refsilöggjöf samrýmist Búdapest-samkomulaginu eins og það hefur verið túlkað og skýrt (sjá hér kafla 8.6 í stöðuskýrslu starfshóps um net- og upplýsingaöryggi). Sérstaklega þarf að huga að því að láta brot gegn 228. gr. almennra hegningarlaga sæta almennri opinberri rannsókn og ákærumeðferð.

e. Réttarstaða neytenda.

Hinn almenni borgari getur einkum sótt rétt þegar kemur að net- og upplýsingaöryggi í fjarskiptum á grundvelli ákvæða IX. kafla fjarskiptalaga, um vernd persónuupplýsinga og friðhelgi einkalífs, sbr. einnig fyrrnefnd ákvæði persónuverndarlaga, sem eru til skýringar og fyllingar. Þá geta neytendur sem telja sig hafa orðið fyrir fjárhagstjóni sótt skaðabætur á grundvelli almennra reglna. Jafnframt hafa neytendur það úrræði að höfða einkarefsimál í tilefni af broti gegn 228. gr. almennra hegningarlaga, sbr. 142. gr. sömu laga. Sönnunargagna úr tölvukerfum verður hins vegar alla jafna ekki aflað nema með opinberri rannsókn. Neytendum er því tæpast kleift að leita réttar síns vegna tölvubrota á grundvelli gildandi laga.

2. Hefur verið gripið til einhverra ráðstafana í kjölfar úttektarinnar?

Í kjölfar úttektarinnar var unnið frumvarp í ráðuneytinu þar sem lagður var grunnur að flutningi Cert-ÍS-sveitarinnar. Það frumvarp var sem fyrr segir lagt fram á Alþingi sl. vor. Frumvarpið hlaut ekki afgreiðslu og verður lagt fram nýtt frumvarp á haustþingi.

Megintilgangur frumvarpsins er að heimila færslu starfsemi netöryggissveitar frá PFS til almannavarnadeildar ríkislögreglustjóra. Við samningu frumvarpsins var m.a. byggt á tillögum sem fram komu í fyrrnefndu minnisblaði Páls Ásgrímssonar hdl. til innanríkisráðuneytis.

Enn fremur er rétt taka fram að unnið er að stefnumótun um net- og upplýsingaöryggismál á vegum ráðuneytisins þar sem litið er til erlendra fyrirmynda, alþjóðlegra skuldbindinga og stefnumarkandi yfirlýsinga. Samráðsferli þetta er nú þegar hafið og búið er að funda með helstu hagsmunaaðilum. Mun það samráð verða grundvöllur að stefnu og sérstakri netöryggisáætlun. Gert er ráð fyrir því að stefnumótunin geti einnig falið í sér tillögur að breytingum á lögum og/eða reglugerðum.

3. Hvenær og á hvaða vettvangi verða niðurstöður úttektarinnar gerðar opinberar?

Meginþorri niðurstaðna úttektarinnar er gerður opinber í svari þessu. Þá hefur hluti hennar áður verið gerður opinber, m.a. í greinargerð með áðurnefndu frumvarpi til laga um flutning Cert-ÍS-netöryggissveitarinnar. Ekkert er því til fyrirstöðu að birta niðurstöður úttektarinnar í heild sinni og er stefnt að því innan skamms.

Auk þess, sem að framan greinir, verða niðurstöðurnar nýttar í vinnu hóps um stefnumótun í net- og upplýsingaöryggi sem starfar á vegum ráðuneytisins. Verkefni hópsins er að móta langtímastefnu stjórnvalda í netöryggis- og upplýsingaöryggismálum. Hópurinn á að setja fram langtímastefnu fyrir tímabilið 2014–2025 og aðgerðaáætlun 2014–2017 varðandi net- og upplýsingaöryggi. Verkefnaáætlun hópsins miðar að því að aðgerðaáætlunin og langtímastefnan verði tilbúnar í sumar. Þá á hópurinn að hafa samráð um framkvæmd verkefna er falla undir viðfangsefni hópsins og sem eru tilgreind í framangreindum áætlunum og stofnanir fulltrúa í hópnum koma að.