

Reykjavík, 14. ágúst 2018

Samgöng- og sveitarstjórnarráðuneytið

Efni: Mál nr. S-79/2018 – Drög að frumvarpi til laga um öryggi net- og upplýsingakerfa mikilvægra innviða – Umsögn Samorku samtaka orku- og veitufyrirtækja

Tilgangur og markmið

Í kynningu á málinu kemur fram að um er að ræða drög að frumvarpi til nýrra laga um öryggi net- og upplýsingakerfa mikilvægra innviða þar sem m.a. er lagt til að innleidd verði tilskipun Evrópuþingsins og ráðsins nr. 1148/2016/ESB um ráðstafanir til að ná sameiginlegu öryggisstigi í net- og upplýsingakerfum innan EES, oft skammstöfuð NIS tilskipuni.

Tilskipunin kveður á um vernd net- og upplýsingakerfa tiltekinnna aðila, þ.e. rekstraraðila þeirra nauðsynlegu þjónustu sem tilskipunin skilgreinir og stafræna þjónustuveitendur með það að markmiði að tryggja hátt öryggisstig fyrir net- og upplýsingakerfi innan Evrópusambandsins og EES-ríkja.

Meginmarkmið frumvarpsins er að auka öryggi net- og upplýsingakerfa og bæta viðbrögð við öryggisatvikum enda sé áreiðanleiki og öryggi net- og upplýsingakerfa grundvöllur efnahags- og samfélagslegrar starfsemi og netöryggi sé mikilvægt fyrir trúverðugleika þjónustunnar, bæði innanlands og utan.

Núverandi staða og kröfur NIS

Nokkur reynsla er komin rekstur CERTIS hér á landi og þar með þær lausnir sem byggt hefur verið á hingað til og þar með talið samstarf við erlenda aðila. Ekki er dregið í efa mikilvægi þess að

Ísland, Stjórnarráðið, stofnanir ríkisins, fyrirtæki sem sinna mikilvægum samfélagslegum innviðum og þjónustuveitendur taki alvarlega þær grundvallar áskoranir sem máli skipta um öryggi net og upplýsingakerfa. Bendir enda flest til þess að svo hafi verið hingað til, þótt vafalaust megi gera enn betur á ýmsum sviðum. Mikilvægt er að hafa þetta í huga þegar horft er til leiða að lausn þeirra verkefna sem bíða okkar. Í því samhengi er mikilvægt að fyrir liggi gapgreining á þeim kröfum sem koma fram í NIS-tilskipuninni og núverandi stöðu hjá okkur Íslendingum. Jafnframt að fram komi hvar leiðir að markmiðum eru valkvæðar og hvar aðferðir eða leiðir eru skyldubundnar.

Samkvæmt þessum drögum að lagafrumvarpi og greinargerðar með þeim er ljóst að stefnt er að verulegri fjárfestingu sem og stórauknum kostnað við rekstur á eftirliti og vöktun til allrar framtíðar. Koma á upp viðtækum eftirlitsheimildum um leið og hægt verður að leggja ýmsar skyldur og kvaðir á þau fyrirtæki sem undir væntanleg lög falla. Lagt er til að en ein eftirlitsstofnun ríkisins verði stækkuð og “efldi” til mikilla muna og sem meira er, henni er ætlað að starfa allan sólarhringinn alla daga ársins. Er enda gert ráð fyrir að kostnaðurinn við innleiðinguna verði tæpir þrír milljarðar á fimm ára tímabili og ljóst að framtíðar fjárfestingar- og rekstrarkostnaður getur orðið mjög mikill miðað við það hvernig ætlunin er að sinna vöktun og eftirliti.

Í þessu samhengi má nefna að ekki er í frumvarpsdrögunum að sjá að metin hafi verið sá kostur, að sólahringsvöktun væri betur komin hjá t.d. Aðþjóðadeild Ríkislögreglustjóra eða öðrum sambærilegum aðilum sem þegar reka sólahringsvöktun sem ætti að vera auðvelt að fella að þörfum CERTÍS fyrir slíka vöktun. Í þessu samhengi þarf ekki að orðlengja að sólahrings vöktun með tilheyrandi vaktaskipulagi, bakvöktum o.s.frv. er gríðalega kostnaðarsöm eins og áður er nefnt. Hér má einnig nefna að reynslan sýnir að alvarleg netöryggisbrot, netárásir o.s.frv. verða fljótt að almannavarnar atvikum þar sem nauðsynlegt er að virkja hlutaðeigandi deildir hjá Ríkislögreglustjóra.

Að teknu tilliti framangreindra hugleiðinga þykir skorta verulega á að fram komi hvernig komist er að þeirri niðurstöðu að þær leiðir sem frumvarpsdrögin gera ráð fyrir séu þær sem best sameina hagkvæmni og leiðir að fullnægjandi árangri við að ná þeim markmiðum að er stefnt.

Það hlýtur að vera eðlilegt þegar taka á upp kostnaðarsöm og yfirgripsmikil kerfi að fyrir liggi greining ólíkar sviðsmynda og þar með leiða að þeim markmiðum sem ætlað er að ná. Hér mætti þá einnig draga fram hvaða ólíku leiðir aðrar þjóðir í Evrópu stórar og smáar, hafa farið við að koma upp vöktun og eftirliti.

Þá er einnig mikilvægt huga vel að því með hvaða hætti opinbert regluverk og þar með eftirlitsstofnanir og -kerfi, opinberir sérfræðingar o.s.frv. geta unnið með sjálfstæðum rannsóknarstofnunum, háskólum og fyrirtækjum á markaði. Um þetta má einmitt finna dæmi víða í Evrópu og fyrir lítið land eins og Ísland hlýtur þetta að vera mikilvægt og þá einnig sá möguleiki að samstarf við erlenda aðila í grunnrekstri eftirlitsins sé hluti af leiðinni að settum markmiðum. Því er ekki sjálfgefið að það sé slæmt að CERTÍS “þurfi að reiða sig á” samstarf við erlenda samstarfsaðila við þau verkefni sem vinna þarf að hverju sinni, svo vitnað sé til orða greinargerðar með frumvarpsdrögunum. Slíkt kann beinlínis að vera skynsamlegt bæði út frá faglegum og rekstrarlegum forsendum. Hér þarf líka að hafa í huga að ráðningar í tæknigeiranum og þar með fjárfesting í þekkingu starfsfólks fela í sér miklar áskoranir sem oft á tíðum er auðveldara að leysa í samstarfi eða með samningum við þriðja aðila en innan viðkomandi stofnunar. Þá er einnig vandséð hvernig á að rökstyðja að slík þekking sé byggð upp hjá mörgum stofnunum ríkisins þegar augljóslega er hægt að fara í samnýtingu eins og getið er um hér að framan.

Innra eftirlit og gæðakerfi fyrirtækja

Eins og áður segir er með frumvarpsdrögunum stefnt að mjög viðamiklu eftirlitskerfi og stórauðnum valdheimildum til handa eftirlitsstofnuninni og þar með skyldum og kostnaði sem falla eiga á þau fyrirtæki sem undir fyrirhuguð lög falla. Er hér m.a. vísað til ráðgerðrar skyldu aðildarfyrirtækja Samorku til þess að gera samninga við CERTIS um viðamikla og kostnaðarsama þjónustu.

Í þessu samhengi er mikilvægt að draga fram að hægt er að einfalda eftirlit og draga úr kostnaði með því t.d. að gera ráð fyrir eigin innra eftirliti hjá viðkomandi fyrirtækjum sem eru þá jafnframt hluti af vottuðu gæðakerfi þeirra. Er hér vísað til þess að stór hluti fyrirtækja í orkuframleiðslu, flutningi, dreifingu og veitustarfsemi sem undir lögin falla eru með vottuð gæðakerfi sem auðvelt er að fella innra eftirlitið að. Þessi kerfi eru síðan tekin út með reglubundnum hætti af óháðum ytri eftirlitsaðilum. Með þessum hætti er hægt að lágmarka opinbera eftirlitið og þar með þann kostnað sem af því hlýst. Sem dæmi um þessa leið í opinberu eftirlitskerfi má nefna eftirlit Neytendastofu með sölumælum þar sem sett er inn jákvæð heimild til handa Neytendastofu til þess að heimila og viðurkenna innri eftirlitskerfi viðkomandi fyrirtækja. Þá má nefna að nú þegar eru nokkur fyrirtæki innan Samorku með vottað stjórnunarkerfi samkvæmt ISO 27001 staðlinum og vitað er að Fjármálaeftirlitið tekur slíka vottun gilda í stað reglubundins eftirlits þeirrar stofnunar. Ekki er að sjá þess stað í frumvarpsdrögunum að gert sé ráð fyrir slíkri leið.

Fleiri valkostir – einfaldari leiðir

Með allt framanritað í huga er mikilvægt að lögð sé frekari vinna í að greina ólíkar leiðir og/eða gera grein fyrir þeim leiðum öðrum sem hafa verið skoðaðar en ekki er gerð grein fyrir í drögum að greinargerð og þá afhverju þær koma ekki til álita við leiðir að þeim markmiðunum sem að er stefnt með frumvarpsdrögum.

Ber í þessu samhengi sérstaklega að gjalda varhug við þeim miklu og matskenndu valdheimildum eftirlitsaðilans sem fyrirhugaðar eru í drögum að frumvarpinu, en jafnframt að ætlunin virðist að skilja eftir nánari útfærslu þeirra í reglugerð án þess að valdmörkin séu skilgrein nægilega í lagafrumvarpinu sjálfu.

Athugasemdir við einstakar greinar

Samorka er aðili að Samtökum atvinnulífsins og viljum við taka undir þær ábendingar og athugasemdir sem koma fram í bréfi þeirra og lagt hefur verið inn í Samráðsgáttina um málið.

1. gr.

Hér er talað um að „*samþykkja stefnu*” stjórnvalda. Betur færi á því að tala um að marka stefnu og uppfæra hana með reglubundnum hætti, sjá til samanburðar orðalag í 7. gr.

Sérstakt er að setja í lagatexta ákvæði um að „efla hlutverk netöryggissveitar” eins og að sé stöðugt framtíðarhlutverk að hún verði stærri og öflugari með hverju árinu sem líður. Þetta orðalag beinlínis ýtir undir áhyggjur sem að framan er lýst um óhóflegt og kostnaðarsamt eftirlit.

2. gr.

Í **fjórdða lið** er talað um eftirlitsstjórnvöld, *sjá nánar í umfjöllun um 8. gr.*

Orðalag í **tíunda lið** er mjög sérstakt. Þegar talað er um „stefnuáætlun” er þá verið að tala um stefnu stjórnvalda á hverjum tíma? Hvað er átt við þegar talað er um að „rammi komi einhverju á fót”? Sjá hins vegar til samanburðar orðalag og nálgun í 7. gr. sem er miklu skiljanlegra.

Í **átjandaánda lið** er fjallað um orkuveitur og tilvitunun til hlutaðeigandi tilskipunar, *sjá einnig nánar í umfjöllun um 8. gr.*

5. gr.

Í 1. tl. er talað um orkuveitur, *sjá nánar í umfjöllun um 8. gr.*

8. gr.

Í greininni er fjallað um eftirlitsstjórnvöld á hverju sviði og þar m.a. vísað til Orkustofnunar vegna orkuveitna og Umhverfisstofnunar vegna vatnsveitna. Orkuveitur eru síðan skilgreindar í átjándi tölulið 2. gr. og vatnsveitur í þrítugasta tölulið sömu greinar. Rekstraraðilar mikilvægra samfélagslegra innviða eru síðan taldir upp í 5. gr., orkuveitur og vatnsveitur.

Samkvæmt nefndum 35. lið og 19. lið 2. gr. tilskipunar 2009/72/EB má því segja að hér sé um að ræða alla aðila keðjunnar nema kaupendurnar („endanotendur”). Framleiðendur, flutningsfyrirtækið, dreifiveitur, þeir sem áhrif hafa á framboð og eftirspurn, svo sem með kaupum og/eða endursölu á raforku og þeir sem bera ábyrgð á viðskiptalegum, tæknilegum eða viðhaldslegum þáttum sem áhrif geta haft á afhendingu vörunar, svo tekið sé mið af orðalagi ákvæðisins.

Í ljósi aðstæðna á Íslandi þar sem stærstur hluti orku til húshitunar kemur frá hitaveitum er mikilvægt að umrædd ákvæði taki einnig til þeirra enda ljóst að þær hljóta sömuleiðis að teljast til mikilvægra samfélagslegra innviða. Hér ættu þá að falla undir allar hitaveitur hvort sem þær nýta jarðhitavatn, jarðhitagufu, rafmagn eða varmaskipta eins og í fyrirhugaðri sjóvarmaveit í Vestmannaeyjum.

Með hliðsjón af ofanrituðu kann að þurfa rýna betur hvort öll hlutaðeigandi eftirlitsstjórnvöld eru talin upp í 8. gr. frumvarpsdraganna. Með sama hætti kann að vera nauðsynlegt að meta sjálfstætt hvort gera þurfi breytingar á þeim lagaákvæðum sem um viðkomandi eftirlitsstjórnvöld gilda.

Tekið er undir með ábendingu Samtaka atvinnulífsins um nauðsynlega samræmingu eftirlitsreglna milli hlutaðeigandi eftirlitsaðila.

Loks má benda á hvort ekki sé rétt að leita umsagnar ráðgjafanendar um opinberar eftirlitsreglur um frumvarp þetta.

9. gr.

Umrædd grein lætur ekki mikið yfir sér en greinargerðin með því er öllu yfirgrípsmeiri og þar fjallað í löngu máli um fyrirhugað eftirlit og vöktun og að mikil vinna sé í raun eftir við að útfæra

Það til hlýtar þó vissulega sé tæpt á ýmsum atriðum í væntanlegri framkvæmd þess. Miðað við texta greinargerðarinnar er ljóst að því er ætlað að verða umfangsmikið og kostnaðarsamt. Gjalda verður sérstakan varhug við þessu og leggja áherslu á einfaldleika og skilvirkni og þá m.a. vísað til þess sem kemur fram í inngangsköflum umsagnar þessarar.

10. gr.

Hér er fjallað um Netöryggissveitina og hlutverk hennar. Í inngangsköflum umsagnar þessarar er fjallað um ýmsa þætti sem lúta að því að horft sé til fleiri möguleika á framkvæmd þeirra verkefna sem NIS-tilskipuninn fjallar um á sviði eftirlits og vöktunar. Ítrekað er að í ljósi smæðar landsins og hagkvæmnissjónarmiða er mikilvægt að allar leiðir séu skoðaðar til þess að lágmarka kostnað við framkvæmd umræddra verkefna. Hér má minna á að í Noregi er sveitin hluti af “Nasjonal Sikkerhetsmyndighet” og í Bretlandi “Homeland Security” og því spurning hvort t.d. Ríkislögreglustjóri og Almannavarnadeild hans væru hentugir vistunaraðilar þar sem verulegur hluti nauðsynlegra innviða er þá þegar fyrir hendi.

11. gr.

Ljóst er að það er ærið verkefni að stofna og halda utan um samráðshóp eða hópa og sviðahópa fyrir alla þá aðila sem sinna samfélagslega mikilvægum innviðum. Hér má velta fyrir sér hvort ekki sé skynsamlegra að viðkomandi svið haldi sjálf hvert um sig utan sína hópa og eigi síðan samráð og veiti upplýsingar til Netöryggissveitar þegar þörf er á. Slíkt gæti verið til mikillar einföldunar og byggir þá m.a á formi sem þegar er til, sbr. t.d. Netöryggishóp Samorku.

IV. Kafli – Öryggi net- og upplýsingakerfa.

Hér er ástæða til þess að ítreka enn og aftur þau atriði sem koma fram í inngangsköflum þessarar umsagnar og lúta að einföldun, skilvirkni og nýtingu á þeim gæðakerfum sem mjög mörg fyrirtæki hafa þegar komið sér upp með tilheyrandi vottun og ytri úttektum. Má að sumu leyti segja að hluti þeirrar upptalningar sem kemur fram t.d. í **14. gr.** styðji við þessa nálgun.

Í **15. grein** og sömleiðis í **20. gr.** eru settar upp mjög víðtækar heimildir til eftirlits og kröfur um afhendingu á upplýsingum. Ljóst er að eins og ákvæðin eru orðuð er mjög auðvelt að missa sig í eftirliti og vöktun sem eftir atvikum getur verið lagt umfram tilefni eða þörf. Mikilvægt er því að

lagatextinn setji eftirliti, vöktun og gagnaöflun mjög skýr mörk og þar með um tilefni. Hér ríður mikið á að skapa fremur traust og umgjörð, fremur en ágengt eftirlit og gagnaöflun. Enn og aftur ríður á að inn komi ákvæði um jákvæða heimild um nýtingu gæðakerfa fyrirtækjanna og þar með innra eftirlit þeirra sem grunn til einföldunar.

19. gr.

Hér er gert ráð fyrir skyldu rekstraraðila mikilvægra innviða til þess að gera samning eða samninga við Netöryggissveitina og þar með að veita aðgang að upplýsingum, heimild til upplýsingasöfnunar, heimild til að koma fyrir vöktunarbúnaði o.s.frv. eins og nánar er lýst í greingarerð með 19. gr.

Ljóst er að hér er um gríðarlegt inngrip að ræða í rekstur viðkomandi fyrirtækja sem erfitt er að sjá fyrir hvað nákvæmlega þýðir. Hér virðist eiga að setja upp „hlerunarbúnað“ á öll samskipti rekstraraðila út frá því sjónarhorni að Netöryggissveitin búi á hverjum tíma yfir einhverjum tilteknum upplýsingum um aðsteðjandi hættur sem aftur byggir á því að sveitin sé með víðtækt neteftirlit í gangi. Með þessu móti eigi síðan að fyrirbyggja eða greina í tíma netárásir gagnvart rekstraraðilum. Hér þarf að hafa í huga að viðkomandi rekstraraðilar eru auðvitað með sinn búnað og sínar varnir stöðugt í gangi og vandséð með hvaða hætti Netöryggissveitin ætlar að láta þessa hluti vinna með sjálfstæðu eftirlit sínu. Má þannig spyrja hvernig tryggja á að búnaður Netöryggissveitarinnar auki ekki beinlínis áhættu í rekstri upplýsingakerfa viðkomandi rekstraraðila. Með hvaða hætti er ætlunin að skoða netumferð? Með hvaða hætti er ætlunin að fara inn í gögn rekstraraðila? Hér þarf að svara því hvort sé ekki hægt að nálgast þetta verkefni með öðrum hagkvæmari og áhættu minni hætti eins og áður er vikið að. Mætti þannig hugsa sér að skilgreind upplýsingaskil úr fyrirbyggjandi búnaði gæti komið í stað sjálfstæðrar vöktunar Netöryggissveitarinnar. Með þeim hætti væri sveitin að vinna í samstarfi við fyrirtækin og sérfræðinga þeirra með það að markmiði að verja mikilvæga innviði þeirra.

Varðandi ætlun frumvarpsdraganna að samningar verði skyldubundnir og þá væntanlega að greitt verði fyrir þjónustuna, þá er mikilvægt að leggja sjálfstætt mat á það hvort slíkt fyrirkomulag standist grunnreglur stjórnsýsluréttarins.

20. gr.

Hér er ætllunin að koma upp galopinni heimild Netöryggissveitarinnar til þess að kalla eftir mjög ýtarlegum gögnum úr hendi fyrirtækjanna og án þess séð verði að nokkrum andmælum eða málsmeðferð sé við komið telji fyrirtækin að gagnaöflunin sé ekki í nauðsynleg og til þess fallinn að gagnast Netöryggissveitinni. Grundvallaratriði um friðhelgi við gagnaöflun, málsmeðferð o.s.frv. eru síðan en og aftur skilin eftir til nánari útfærslu í reglugerð.

21. og 26. gr.

Hér er ljóst að um mjög þýngjandi aðgerðir getur orðið að ræða fyrir rekstraraðila. Ákvæðin eru mjög matskennt og vafasamt að þau séu nægur grundvöllur að setningu reglugerðar. Ekkert er kveðið á um skyldu eftirlitsstjórnvalda um nánari framkvæmd tilmæla og bindandi fyrirmæla og þar með réttindi rekstraraðila. Óljóst er með hvaða hætti stjórnvald á að láta vinna verk á kostnað rekstraraðila og með hvaða hætti og formerkjum það ætti að fá nauðsynlegan aðgang að kerfum rekstraraðila.

Hér getur augljóslega verið um mjög umfangsmikil inngrip að ræða og því mikilvægt að laga-grundvöllur og nánari framkvæmd sé skýr í lagatextanum sjálfum og þá tekið mið af meðalhófs-sjónarmiðum og að andmælaréttur og málsmeðferðarréttur sé tryggður.

27. gr. og 28. gr.

Tekið er undir með athugasemdum í umsögn Samtaka atvinnulífins og einnig áréttað það sem fram kemur hér að ofan um 26. gr.

f.h. Samorku

Baldur Dýrfjörð lögfræðingur