Umsögn um “Öryggi net- og upplýsingakerfa mikilvægra innviða“
“416. mál, lagafrumvarp”

6.gr
liður 23. vantar líklega ',' milli
"Tengi- og skiptipunktar" og "þjónustuveitendur lénsheitakerfis"

Allavegna þá virðist sem RIX eigi að flokkast sem "stafræn grunnvirki" og það að þessi ',' vanti gerir það að verkum að hægt er að snúa útúr og segja að RIX sé ekki grunnvirki?

9.gr og 14. gr.
Væri betur komið sem hluti af lögreglu. Í staðinn fyrir að dreifa persónuupplýsingum.

12.gr
Verðlag hækkar, fyrirtæki þurfa að ráða þarf fólk (í fleirtölu) ef þetta verður mikið notað (misnotað).

Frekar skrýtið að eftirlits aðili sé að skipa fyrirtæki að vinna vinnu á þeirra kostnað? Ef fyrirtæki er ekki að standa sig ættu viðskiptavinir að beina viðskiptum sínum annað?

17. gr
Aukin kostnaður ef kaupa á búnað sem styður hleranir.

Hvað ef þessi gögn sem verið er að biðja um eru ekki til, ekki verið að safna þeim?

Einkafyrirtæki að láta netöryggissveit fá persónuupplýsingar væri ekki betra að þetta væri lögregla og/eða dómsúrskurður?

18. gr
Hægt að setja hvern sem er í samráðshóp og fara dreifa persónuupplýsingum sem er undanþegin aðgangsrétti almennings?
Ekkert eftirlit með?

21. gr
Þessi grein er ekki í anda persónuverndar og vinnslu persónuupplýsinga, þ.e.a.s. vegna "er einnig heimilt að miðla þeim upplýsingum til viðeigandi þriðju aðila,"
Hver á eiginlega að hafa eftirlit með þessu?

22. gr
Dagsekt uppá 500.000 fyrir að skila ekki gögnum sem mögulega eru ekki til?

23. gr
Hver á að ákveða hvort þessi gögn sem talin eru upp í II kafla fullnægjandi. Heimilt að senda manneskju í 2 ára fangelsi fyrir að senda ekki inn lýsingar á verkferlum?

Breytingar á öðrum lögum.
Samningar netöryggissveitar og fjarskiptafyrirtækja.

Að veita netöryggissveit aðgang að netumferð
 * Þetta eru hleranir, köllum þetta réttu nafni, er framkvæmt í dag af lögreglu og/eða dómsúrskurðum
 * Eykur árása fleti,
 * eykur líkur á leka frá netöryggissveitinni eða búnaði sem netöryggissveit velur
 * Veikir varnir með samning um uppsetningu búnaðar sem úreldist
 * Hafa heimildir til að dreifa persónupplýsingum án eftirlits
 * Ekkert eftirlit með þessu
 * Stendur "Hvorki er heimilt að persónugreina netumferð né skima einstaka netpakka" er á skjön við 21. gr. þar sem netöryggissveit er veitt heimild til vinnslu persónugreinanlegra gagna
 * "Netöryggissveit er þó heimilt að móttaka upplýsingar um almenna netumferð án dómsúrskurðar, þ.m.t. á samtengipunktum og í útlandagáttum, enda séu þær upplýsingar ópersónugreinanlegar." fullyrðing stenst ekki, þær eru persónugreinanlegar og það er sagt í umsögn
 * Hvað ef gögnum er ekki safnað? Á að skipa fyrirtækjum að byrja að safna svo netöryggissveit geti hlerað?
 * Hvað ef fyrirtæki neitar að gera samning?

25. gr.
Eru menn að falla á tíma? Mikil heimild veitt til ráðherra í framtíðinni til að gjörbreyta framkvæmd lagana.

Varðandi
GREINAGERÐ

3. Meginefni frumvarpsins.
  Ekkert talað um að megin efni sé stórauknar valdheimilidir netöryggissveitar til vinnslu persónuupplýsingar og dreifingar á þeim til þriðja aðila auk hlerana.

5. Samráð
"Mikilvægi þess að vel sé búið að netöryggissveit áréttast þó hér með, enda mun hún gegna lykilhlutverki í vörnum Íslands gegn netógnum í framtíðinni sem landsbundið öryggis- og viðbragðsteymi (CSIRT)" rangt netöryggissveitin er EKKI að gegna lykilhlutverki í vörnum heldur eru það varnir sem fyrirtæki/stofnanir eru með á þeim tíma sem gegna því lykilhlutverki.

6. Mat á áhrifum
Er þetta sé mikilvæg þjónusta sem netöryggissveitin veitir?
Þjónustan minnkar öryggi með því að dreifa búnaðir sem úreldist og eykur árásarfleti.
Er íþyngjandi og eykur verðlag.
Ímynd net umferðar á íslandi breytist þar sem hleranir stóraukast.

Um 6. gr.
"Megintilgangur kerfisins er þannig að umbreyta úthlutuðu léni, þ.e. vefslóð, yfir í IP-tölur."
Nei, úthlutað lén er ekki "þ.e. vefslóð".

"hnitgreina (e. resolver)" á þetta að vera hnitgreinir? myndi frekar nota uppfletti nafnaþjónn (e. resolver eða e. non authorative name server) til greiningar frá nafnaþjónn (e. authorative name server). Til hvers að skilgreina þetta er ekki notað í lögum?
og vinsamlegast laga á
http://www.hugtakasafn.utn.stjr.is/leit-nidurstodur.adp?leitarord=e+V&tungumal=en
í leiðinni

"til að umbreyta lénunum (vefslóðum) yfir í IP-tölur", aftur nei, taka út "(vefslóðum)"

lénsheitakerfi (e. domain name system eða DNS), ISNIC hefur þýtt þetta nafnakerfi hingað til
https://www.isnic.is/is/faq#q29

"netöryggissveitina CERT-ÍS á grundvelli fjarskiptalaga og býr starfslið hennar yfir yfirburðaþekkingu og -reynslu á sviði net- og upplýsingaöryggis hér á landi" citation needed :)
(hver skrifaði þetta, væri áhugavert að fá að vita?)

"Skráningarstofur höfuðléna hvers lands gegna svo því mikilvæga hlutverki að endurúthluta lénum til svokallaðra skráningaraðila undir þeirra höfuðléni (TLD). Skráningaraðilar sem fá úthlutað frá skráningarstofu höfuðléns hvers lands geta svo úthlutað lénum ef þeir kjósa að gera slíkt. "
Hér er líklega verið að þýða registrar sem skráningaraðili, ISNIC rekur ekki .is sem registry-registrar heldur úthlutar beint til rétthafa kjósi þeir það, þ.e.a.s. tekið er við beinum skráningum (e. direct registrations).

"þjónustuveitendur lénsheitakerfis" ath hér eru teign á lofti um að þetta flytjist til útlanda (takk smáís og hæstiréttur) og fari þá í DNS over HTTP. Svo líklega verður úrelt eftir nokkur ár að flokka “þjónustuveitandi lénaheitakerfis” væntanlega átt við resolvera sem “ 23. *Stafræn grunnvirki:* Tengi- og skiptipunktar þjónustuveitendur lénsheitakerfis og skráningarstofur höfuðléna. “

Þar er talað um "símstöðvarbúnað (e. switch)" þetta er líklega röng þýðing á að vera "skiptir"
https://www.visindavefur.is/svar.php?id=18687

Um 7. gr. og Um 12. gr.

Ef t.d. lítil fyrirtæki verða skylduð að taka upp ISO27001 þá þarf að ráða fólk og verðlag eykst.

Um 16. gr.
Segir
"Mikilvægt er að árétta að um er að ræða umferð við kerfi aðila, en ekki tilgangurinn að nema almenna netumferð notenda Netsins. Þá er innihald fjarskiptapakka svo sem innihald tölvupósts og HTML pakkar ekki hluti af þessum almennu samskiptum mikilvægra innviða og netöryggissveitarinnar."
Þetta er rangt engin munur á þessari umferð og innihaldi pakka.

Einnig segir
"Hér getur t.d. verið um að ræða vafasamar IP-tölur eða URL móttakanda utan kerfis"
Hvernig á að finna URL ef ekki á að hlera "almenna notendur netsins" og skoða "HTML pakkar".

"Lagt er til að endurgjald vegna tæknilegrar vöktunarþjónustu samkvæmt ákvæðinu taki einkum mið af útlögðum kostnaði vegna þjónustunnar, svo sem vegna uppsetningar og rekstrar skynjara eftir því sem við kann að eiga"
ATH búnaður verður úreldur á örfáum árum (1-3 ár).

Um 21. gr.
Segir
"Í 1. mgr. ákvæðisins er netöryggissveit einnig veitt heimild til þess að kanna innihald einstaka sendinga til og frá neti mikilvægra innviða, liggi fyrir rökstuddur grunur um að sending, svo sem tölvupóstur, innihaldi spillikóða. Er slík framkvæmd þó ávallt háð samþykki mikilvægra innviða, en er þó ekki háð samþykki hins skráða, t.d. starfsmanns mikilvægra innviða. Mikilvægt er að árétta að heimild þessa skal einungis nýta þegar rökstuddur grunur leikur á um að sending geti falið í sér ógn eða áhættu fyrir mikilvæga innviði. Þar sem tímarammi til viðbragða við ógnum og áhættum er mjög skammur er nauðsynlegt að veita netöryggissveitinni heimild til að kanna innihald sendingarinnar án samþykkis viðkomandi einstaklings."
stangast á við næstu setningu
"Árétta skal að heimild sem þessi getur aldrei falið í sér heimild til skoðunar á sendingum í almennum fjarskiptanetum fjarskiptafyrirtækja."

2 mgr. best væri að þetta væri á hendi lögreglu og/eða dómara einsog hleranir eru í dag.

"Í 1. málsl. 3. mgr." netöryggissveitin á ekki að dreifa persónugreinanlegum gögnum (í það minnsta ekki án eftirlits og skjölunar)

Um 27. gr.
"Starfslið stofnunarinnar býr yfir yfirburða þekkingu og reynslu á þessu sviði sem nýta má til vitundarvakningar í samfélaginu um net- og upplýsingaöryggi með þessum hætti, án þess að eigi að krefjast mikils tilkostnaðar. "
Bara 2.745 millj. kr? Og svo 648 milljónir á ári eftir það.

" Í b-lið greinir tillögur að fjórum nýjum ákvæðum, sem koma í stað gildandi 47. gr. a, og verða ný 47. gr. a–47. gr. d. Því skal haldið til haga að fjarskiptafyrirtæki falla ekki undir gildissvið tilskipunar (ESB) 2016/1148, enda er nú þegar í fjarskiptalögum og evrópsku regluverki á sviði fjarskipta að finna sambærilegar skyldur varðandi skipulag upplýsingaöryggis."

Nokkuð viss um að þetta sé miskilningur því fjarskiptafyrirtæki reka í dag uppfletti nafnaþjona og þeir stærstu myndu valda miklum usla ef þeir færu á hliðina eða ráðist yrði á þá og þeir færu að svara röngum fyrirspurnum.
(sjá 6. gr “29. Þjónustuveitandi lénsheitakerfis: Aðili sem veitir þjónustu fyrir lénsheitakerfi á netinu. “)

Axel Tómasson
Forritari hjá Internet á Íslandi hf.