RÍKISSAKSÓKNARI

Alþingi
Erindi nr. Þ 132/1600
komudagur 11.4.2006

HMG/jhb

Reykjavík 10. apríl 2006

Umsögn um frumvarp til laga um breyting á almennum hegningarlögum o.fl. (samningur Evrópuráðsins um tölvubrot) Þskj. 905, 619. mál

Ríkissaksóknara barst til umsagnar með bréfi ritara alsherjarnefndar Alþingis dags. 27. mars sl., frumvarp til laga um breyting á almennum hegningarlögum, lögum um meðferð opinberra mála og lögum um fjarskipti, (Samningur Evrópuráðsins um tölvubrot)

Umsögn um einstakar greinar frumvarpsins:

1. gr. frumvarpsins - Refsiábyrgð lögaðila– Kafli 3.12. og 12. gr. CC

Það er ekki gerð athugasemd við að brot gegn almennum hegningarlögum verði lýst refsiverð fyrir lögaðila einnig. Aðferð sú sem notuð er til þess í frumvarpinu orkar tvímælis þar sem í 1. gr. er gert ráð fyrir nýju ákvæði í II kafla A almennra hegningarlaga 19. gr. d, en í henni segir; „Ef skilyrðum ákvæða þessa kafla er fullnægt..." o.s.frv. Kafli II A í hegningarlögum er byggður þannig upp að 19. gr. a gerir ráð fyrir að í lögum þurfi að vera sjálfstæð lagaheimild til að refsa lögaðila.

Réttara væri að fara að hætti Dana sem hafa sett sambærileg ákvæði við kafla II A sem er 5. kafli dönsku hegningarlaganna. Þeir hafa svo þar fyrir utan sett sérstakt refsiákvæði sem gildir um ábyrgð lögaðila samkvæmt hegningarlögum og er í 306. gr. laganna en vísar til 5. kafla um framkvæmdina en ekki heimildina eins og skilja má að gert sé með framangreindri tilvísun í 1. gr. frumvarpsins. Einnig mætti umorða ákvæðið og segja; Heimilt er að láta lögaðila sæta refsiábyrgð fyrir brot á lögum þessum, í samræmi við ákvæði þessa kafla. Ríkissaksóknari telur umrædda breytingu nauðsynlega til að fullnægja skyldum Íslands samkvæmt sáttmálanum og leggur til að greinin verði samþykkt þó með framangreindum fyrirvara.

2. gr. frumvarpsins – Barnaklám – Kafli 3.9 og 1. mgr. 9. gr. CC

Ríkissaksóknari telur umrædda breytingu nauðsynlega til að fullnægja skyldum Íslands samkvæmt sáttmálanum og leggur til að greinin verði samþykkt óbreytt.

Póstfang: Hverfisgata 6, 150 Reykjavík
Sími: 530-1600
Netfang: rsak@tmd.is
Bréfsími: 530-1606
Kennitala: 530175-0229

3. gr. frumvarpsins – Röskun fjarskipta – Kafli 3.5. og 5. gr. CC

Ríkissaksóknari telur umrædda breytingu nauðsynlega til að fullnægja skyldum Íslands samkvæmt sáttmálanum og leggur til að greinin verði samþykkt óbreytt.

4. gr. frumvarpsins – Aðgangur að samskiptagögnum – Kafli 4 og 14. – 21. gr. CC

Ríkissaksóknari telur þá breytingu nauðsynlega sem lögð er til á b. lið 2. mgr. 87. gr. oml. Nauðsynlegra sönnunargagna um brot framin með tölvum verður í mörgum tilfellum ekki aflað án aðgangs að gögnum um samskipti tölva, (s.k. loggskrár) Refsirammi þeirra ákvæða sem í hlut eiga eins og t.d. 249. gr. a, og 257. gr. hgl. nær ekki því lágmarki refsingar sem nú gilda samkvæmt b. lið 2. mgr. 87. gr. þ.e. átta ára fangelsi. Í sumum tilfellum hefur verið talið heimilt á grundvelli ríkra almanna- eða einkahagsmuna að heimila lögreglu aðgang að gögnum, en slíkt er undantekning.

Rétt er að leggja áherslu á að 4. gr. frumvarpsins útvíkkar heimild lögreglu til að fá úrskurð til öflunar upplýsinga um tengingar milli fjarskiptatækja, sbr. b. lið 1. mgr. 86. gr. oml. Með því að lækka áskilin refsiramma samkvæmt b. lið 1. mgr. 87. gr. oml. úr átta árum niður í tvö ár nýtist úrræðið til rannsóknar stórs hluta allra refsilagabrota í stað fárra og sérstaklegra alvarlegra áður. Það verður þó að árétta að ekki er gerð nein breyting á skilyrðum fyrir símhlustun. Eðlilegt er að líta svo á að persónuupplýsingar um tengingar milli fjarskiptatækja þ.e. hvaða síma eða tölvu viðkomandi tengist á ákveðnum tíma, krefjist ekki jafn ríkra takmarkana og upplýsingar um efni og innihald samskiptanna. Ríkissaksóknari telur umrædda breytingu nauðsynlega til að fullnægja skyldum Íslands samkvæmt sáttmálanum og leggur til að greinin verði samþykkt óbreytt.

5. og 6. gr. frumvarpsins – Fyrirmæli um varðveislu gagna – Kafli 4 og 16. gr. CC

Við framkvæmd rannsókna tölvutengdra brota hefur lögregla hingað til þurft að treysta á velvilja starfsmanna fjarskiptafyrirtækja um varðveislu samskiptagagna og trúnað um fyrirspurnir sínar, meðan aflað er dómsúrskurðar um afhendingu þeirra. Þetta getur ekki talist ásættanlegt hvorki til að tryggja að sönnunargögn spillist ekki né til að tryggja þagnarskyldu sem er mjög mikilvæg til að koma í veg fyrir spillingu sönnunargagna hjá sakborningi sjálfum. Eins eru fjarskiptafyrirtæki sett í afkáralega stöðu gagnvart viðskiptavininum ef lögregla óskar þagnar þeirra um rannsókn á brotum viðskiptavinar þeirra án þess að þau geti réttlætt þögn sína með tilvísun til lögbundinnar þagnarskyldu. Ríkissaksóknari telur umrædda breytingu nauðsynlega til að fullnægja skyldum Íslands samkvæmt sáttmálanum og leggur til að greinin verði samþykkt óbreytt.

7. gr. frumvarpsins – Hækkun refsiramma vegna brota gegn fjarskiptalögum

Hvergi er eins líklegt að rannsóknir brota krefjist öflunar samskiptagagna frá fjarskiptafyrirtækum en þegar brotið er gegn fjarskiptalögum og væri því mjög afkáralegt ef refsirammi þeirra brota næði ekki tilskyldu lágmarki, sbr. 4. gr.

frumvarpsins. Þó verður að benda á að refsirammi brota getur ekki eingöngu tekið mið af þeim takmörkunum sem eru á öflun sönnunargagna um brotin. Refsirammi upp á allt að tveggja ára fangelsi er þó í samræmi við refsiramma í mörgum sérrefsilögum. Ríkissaksóknari telur umrædda breytingu nauðsynlega og leggur til að greinin verði samþykkt óbreytt.

Umsögn um ákvæði sáttmálans sem ekki eru taldar kalla á lagabreytingar.

Kafli 3.2. í athugasemdum við frumvarpið - 228. gr. hgl. og 2. gr. CC um ólöglegan aðgang

Brot gegn 228. gr. hgl. sæta hvorki opinberri rannsókn né opinberri ákæru, sbr. 242. gr. hgl. Breyting sem gerð var með 4. gr. laga nr. 30, 1998, í því skyni að láta greinina ná yfir tölvubrot er með öllu ófullnægjandi og nýtist fáum ef einhverjum brotaþolum. Heimildir 86. og 87. gr. laga nr. 19, 1991, um meðferð opinberra mála standa ekki einkaðilum til boða við rannsókn þeirra á brotum gegn 228. gr. hgl.

Sönnunargagna úr tölvukerfum verður ekki aflað með öðrum úrræðum. Einkaðilum sem hyggjast leita réttar síns er það því fyrirmunað, enda nýtur sjaldan við annarra sönnunargagna, um hver var að verki, en þeirra sem geymd eru á tölvutæku formi í formi annála hjá fjarskiptafyrirtækjum. Svo virðist sem í frumvarpinu sé uppi misskilningur um að ákvæði 228. gr. hgl. sé fullnægjandi úrræði í skilningi 2. gr. sáttmálans, sem það er í raun ekki. Gera verður breytingar á þessu fyrirkomulagi enda eru engin úrræði fyrir lögreglu til að bregðast við hreinum tölvuinnbrotum, „hacking", í núverandi lögum. Þó kemur til greina, og kann að vera eðlilegt, að opinber rannsókn og ákvörðun um saksókn verði háð kröfu þess sem misgert er við.

Enn fremur kann að vera eðlilegt að þyngja refsingu við brotum þessum þannig að hún verði allt að 2ja ára fangelsi svo nota megi úrræði 86. og 87. gr. oml. til gagnaöflunar sbr. 4. og 7. gr. frumvarpsins. Tölvuinnbrot eru bagaleg og kostnaðarsöm fyrir þá sem fyrir þeim verða þrátt fyrir að ekki sé hægt að sanna eignarspjöll eða ásetning til auðgunarbrota og því nauðsynlegt að lögregla hafi heimild til að rannsaka þau brot. Danir leggja allt að 18 mánaða fangelsi við þessum brotum en við öðrum brotum sem talin eru upp í 228. gr. hgl. einungis 6 mánaða fangelsi, sbr. 263. gr. dönsku hegningarlaganna. Rök standa til þess að þyngja refsingar vegna tölvuinnbrota þar sem þær upplýsingar sem í hlut eiga geta varðað meiri verðmæti, t.d. atvinnuleyndarmál, en þau sem greininni var upphaflega ætlað að vernda, þ.e. einkamál annars manns. Bent er á að samkvæmt 3. mgr. 263. gr. dönsku hegningarlaganna er lagt allt að 6 ára fangelsi við grófum brotum gegn 1. eða 2. mgr.

Kafli 3.3. í athugasemdum við frumvarpið - 228. gr. hgl. og 3. gr. CC ólögleg hlerun

Sama misskilnings gætir um ágæti 228. gr. hgl. Vísað er til umfjöllunar hér að framan.

Kafli 3.6. í athugasemdum við frumvarpið - 6. gr. CC um misnotkun búnaðar

Tilvísun til 20. og 22. gr. hgl. um hlutdeild og tilraun eru byggð á misskilningi og nægja þau engan veginn til að fullnægja skuldbindingum 6. gr. sáttmálans. Tilgangurinn með 6. gr sáttmálans er að gera refsivert að framleiða, selja, afla, flytja inn, dreifa eða að gera aðgengilegan tiltekinn búnað sem samkvæmt gerð sinni og eðli er fyrst og fremst ætlaður til tölvubrota sem og sömu meðferðar á lykilorðum og aðgangskóðum.

Það er langur vegur frá því að maður sé tekinn með forrit sem einkum er notað til tölvuinnbrota til þess að hægt sé að sanna að hann hafi haft ásetning til að brjótast inn í tölvukerfi. Í mörgum tilfellum má gera líklegt að forritið hafi átt að nota til að prófa innbrotsþol eigin tölvu. Til eru dæmi um að illa fengin lykilorð og notendanöfn gangi manna á milli á netinu. Þrátt fyrir að maður sé tekinn með slík lykilorð og notendanöfn, án þess að hann hafi aðhafst nokkuð til að nota þau eða undirbúa notkun þeirra í refsiverðum tilgangi, verður trauðla sannaður, gegn neitun hans, ásetningur til notkunar þeirra. Ákvæði 6. gr. má líkja við þau bönn sem eru við meðferð og eign ákveðinna vopna sem fyrst og fremst eru ætluð til líkamsmeiðinga eða eru sérstaklega hættuleg. T.d. er bannað að flytja inn, framleiða, eignast eða hafa í vörslum sínum hnúajárn sjá um þetta e-lið 1. mgr. 2. gr., c.-lið 2. mgr. 6. gr., sbr. 36. gr. vopnalaga nr. 16, 1998. Þrátt fyrir að maður sé tekin með slíkt vopn í fórum sínum, sem eingöngu er ætlað til að valda auknum áverka á öðrum mönnum af völdum hnefahögga, verður sá maður ekki ákærður eða sakfelldur fyrir tilraun til líkamsmeiðinga, nema eitthvað meira komi til.

Til greina kemur að setja í lög sérstakt bann byggt á 6. gr. sáttmálans og lögð verði refsing við vörslu þeirra hluta sem þar eru taldir með. Þess verði þó gætt að gerður sé fyrirvari um að hluti þeirra forrita sem einkum eru notuð til tölvuinnbrota eru einnig notuð í löglegum tilgangi t.d. til að prófa öryggi tölvukerfa og þeir sem starfa á því sviði kunna að hafa lögleg not af slíkum forritum. Nauðsynlegt kanna að vera að sett verði heimild í lög til að dómsmálaráðherra geti kveðið á í reglugerð um hvaða tæki og tól falla undir bannregluna. Svipuð leið kemur til greina og farin er með reglugerð 233/2001, um ávana- og fíkniefni og önnur eftirlitsskyld efni. Tækni á þessu sviði fleytir fram og sífellt spretta upp ný forrit sem falla undir skilgreininguna í 6. gr. CC. Í þessu efni er nauðsynlegt að leita álits fagmanna á tölvusviði.

Rétt er þó að benda á að það kann að vera rétt niðurstaða að gera ekki sérstakar ráðstafanir í tilefni af 6. gr. sáttmálans og líta í staðinn á þann vanda sem ákvæðinu er ætlað að leysa sem öryggisvanda sem ekki skapi mikla hættu, heldur verði leystur með þeim öru framförum sem orðið hafa í aðgangsstýringum og öryggisráðstöfunum til varnar tölvukerfum. Þetta verður þó að vega og meta en það mun hafa verið niðurstaðan í Danmörku að setja ekki í lög sérstök ákvæði að þessu tilefni með vísan til þess að tæknin leysi þann vanda sem að steðjar. Niðurstaðan í Danmörku er ekki fengin með þeim rökum að ákvæði um tilraun og hlutdeild leysi vandann. Niðurstaða

frumvarpsins er þó eftir sem áður röng, þótt farin yrði sú leið sem Danir kusu, þar sem hún byggir á miskilningi varðandi sönnunarkröfur í opinberum málum og gildissvið ákvæða 20. og 22. gr. hgl.

Um 17. gr. CC

Í umfjöllun um réttarfarsúrræði er ekki vikið að ákvæði 17. gr. sáttmálans. Í b.-lið 1. mgr. 17. gr. CC er gert ráð fyrir að fjarskiptafyrirtæki skuli afhenda lögbærum yfirvöldum í flýti samskiptagögn til að bera kennsl á viðkomandi þjónustuveitendur. Með samskiptagögnum er meðal annars átt við frá hvaða IP tölu tengst er og við hverja og á hvaða tíma. Allar tölvur á internetinu hafa sérstakar IP tölur sem geta verið fastar eða breytilegar. Upplýsingar um IP tölur er hægt að finna á þar til gerðum heimsíðum á internetinu þar sem haldið er utan um skráningu þeirra eftir svæðum í heiminum. Þar kemur fram hvaða þjónustuveitendur eru skráðir fyrir ákveðinni IP tölu. Þegar tölvur eiga samskipti eru skráðar, eða hægt er að skrá, upplýsingar um m.a. IP tölu þess sem tengist, tímasetningu, tímalengd tengingar, hverjum er tengst áfram o.s.frv. Slíkar upplýsingar kallast samskiptagögn, e. Traffic Data.

Þegar lögregla rannsakar brot getur þurft að rekja fjarskiptin, tengingar tölvunnar, frá brotavettvangi þ.e. þeirri tölvu þar sem brot er framið eða kemur fram, til baka til þess sem liggur undir grun eða öfugt. Slík samskipti geta farið vítt og breytt um heiminn frá einum þjónustuaðila til annars þannig að hjá einum slíkum í keðjunni liggi bara upplýsingar um þá IP tölu sem er næst á eftir og undan í keðjunni. Þegar svo háttar til þarf að afla með dómsúrskurði upplýsinga hjá hverjum og einum þeirra sérstaklega. Ef einungis er leitað til eins í einu líður langur tími þar til rannsókn leiðir til niðurstöðu.

Ákvæði 17. gr. er ætlað að gera það mögulegt að tryggja að allir þjónustuaðilar sem koma að tengingu varðveiti eða sjái til þess að aðrir þjónustuaðilar sem koma við sögu í fjarskiptunum, tengingunni, varðveiti nauðsynleg samskiptagögn. Þetta er gert til að öruggt sé að upplýsingar um leið samskiptanna liggi fyrir þegar lögregla kemur til að sækja þær. Eða eins og það er orðað í ákvæðinu „átta sig á þeirri leið sem boðin voru send eftir". Nauðsynlegt er að tryggja að lögregla geti snúið sér beint til allra, eða sem flestra, þjónustuaðila sem í hlut eiga, á sem skemmstum tíma og lagt fyrir þá að varðveita gögn um tengingar meðan leitað er dómsúrskurðar. Án þessa er líklegt að búið verði að eyða gögnum hjá einhverjum þeim þjónustuaðilum sem í hlut eiga áður en lögregla fær upplýsingar um þá og nær að tryggja gögnin. Þetta er skjól tölvuþrjóta sem nýta með þessum hætti að fara flóknar leiðir við tengingar til að koma í veg fyrir rakningu.

Það er því nauðsynlegt að taka, með einhverjum hætti, á þessum vanda sem 17. gr. CC er ætlað að leysa en það hefur ekki verið gert. Öruggasta leiðin til að tryggja umrædda rannsóknarhagsmuni er að skylda þjónustuveitanda til að gefa lögreglu, án úrskurðar, upplýsingar um hvaða aðrir þjónustuveitendur koma við sögu þannig að lögregla geta beint því til þeirra að varðveita gögnin meðan aflað er dómsúrskurðar.

Einnig þurfa þeir að afhenda upplýsingar sem nægja til að aðrir þjónustuveitendur geti borið kennsl á fjarskiptin s.s. IP tölu og tímsetningu. Vísað er til enskrar útgáfu af „ Explanatory Report“ með Convention on Cybercrime af þeim kafla sem fjallar um 17. gr. CC.

Frumvarpið tekur ekki á þessum vanda sem 17. gr. CC er ætlað að leysa og verður að bæta úr því.

saksóknari

Nefndasvið Alþingis

Alsherjarnefnd

b.t. Elín Valdís Þorsteinsdóttir nefndarritari

Hjálagt.

Ensk útgáfa úr „ Explanatory Report" með Convention on Cybercrime. Slóðin þar sem alla skýrsluna er að finna er:

http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

Expedited preservation and partial disclosure of traffic data (Article 17)

165. This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications. "Traffic data" is defined in Article 1.

166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).

167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

168. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. The article does not specify the means by which this may be achieved, leaving it to domestic

law to determine a means that is consistent with its legal and economic system. One means to achieve expeditious preservation would be for competent authorities to serve expeditiously a separate preservation order on each service provider. Nevertheless, obtaining a series of separate orders can be unduly time consuming. A preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This comprehensive order could be served sequentially on each service provider identified. Other possible alternatives could involve the participation of service providers. For example, requiring a service provider that was served with an order to notify the next service provider in the chain of the existence and terms of the preservation order. This notice could, depending on domestic law, have the effect of either permitting the other service provider to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandating the preservation of the relevant traffic data. The second service provider could similarly notify the next service provider in the chain.

169. As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. The competent authorities should specify clearly the type of traffic data that is required to be disclosed. Receipt of this information would enable the competent authorities to determine whether to take preservation measures with respect to the other service providers. In this way, the investigating authorities can trace the communication back to its origin, or forward to its destination, and identify the perpetrator or perpetrators of the specific crime being investigated. The measures in this article are also subject to the limitations, conditions and safeguards provided in Articles 14 and 15.