



RÍKISLÖGREGLUSTJÓRI

Reykjavík 16. maí 2022

Tilvísun: 2022040193

Tilvísun yðar:

Alþingi
Nefndasvið.
Kirkjustræti
150 REYKJAVÍK

Umsögn um frumvarp til laga um fjarskipti , 461. mál

Embætti ríkislögreglustjóra (RLS), vísar til beiðni nefndasviðs Alþingis um beiðni um umsögn um frumvarp til laga um fjarskipti, 461. mál.

Í 100. gr. frumvarpsins er fjallað um fjarskipti á hættutímum og í neyðartilvikum. Að mati embættis ríkislögreglustjóra verður að vera skýrt að ákvæðið nái einnig til þess þegar þær aðstæður koma upp að takmarka verði og trufla fjarskipti á tilteknu svæði, s.s. vegna lögregluaðgerða sem ráðast verður í. Getur það átt við um þegar aftengja þarf mögulegar sprengjur eða annan búnað sem hægt er að ræsa með þráðlausum fjarskiptum. Skýr heimild verður að vera til staðar fyrir lögreglu að trufla fjarskipti þegar slíkar aðstæður koma upp og er þá litið til öryggis almennings og öryggis þess starfsfólks lögreglu sem kemur að þeim lögregluaðgerðum. Slíkt getur einnig átt við í þeim aðstæðum þegar gíslataka stendur yfir, að hægt verði að takmarka með skjótum hætti þráðlaus fjarskipti á milli gíslatökuaðila. Einnig má nefna öryggisgæslu í tengslum við heimsóknir erlendra aðila sem og hótanir og öryggisgæslu innlendra aðila þar sem fyllsta öryggis verður að vera gætt. Lögreglu verður að vera veitt tilhlýðilegar heimildir til að reka og eiga búnað er getur truflað fjarskipti á mismunandi tíðnisviðum, vegna þeirra verkefna sem að framan hafa verið nefnd. Setja þarf inn ákvæði þess efnis að lögreglu sé heimilt að nema og takmarka fjarskipti með sérstökum tæknibúnaði svo unnt sé að framkvæma inngríp og afstýra hættu. Slíkt þarf að vera framkvæmanlegt með afar skjótum hætti, enda er það í því skyni að afstýra hættuástandi sem komið er á. Framangreint yrði útfært nánar í reglugerð settri af ráðherra.

Bent er á í þessu samhengi að í 29. gr. frumvarpsins er fjallað um takmörkun fjarskipta vegna truflana eða sérstakra aðgerða. Þannig er í 5. mgr. ákvæðisins kveðið á um að

RÍKISLÖGREGLUSTJÓRI

Fangelsismálastofnun geti að undangenginni beiðni til Fjarskiptastofu, truflað þráðlaus fjarskipti innan sérstaklega afmarkaðs svæðis vegna framkvæmdar á öryggis- og refsigæslu. Úrræði lögreglu þurfa þó að geta komið skjótar til og getur ekki verið háð tímafreku ferli.

Embætti ríkislögreglustjóra vill sérstaklega vekja athygli á 3. mgr. 89. gr. frumvarpsins, en um er að ræða mikilvægt ákvæði þar sem fjallað er um skyldu fjarskiptafyrirtækja til að varðveita lágmarksskráningu gagna um fjarskiptaumferð notenda í sex mánuði. Lögreglan getur þá með undangengnum úrskurði héraðsdóms krafist þess að fjarskiptafyrirtækin afhendi lögreglu slík gögn til rannsóknar sakamála. Umrætt ákvæði er mikilvægt úrræði fyrir lögreglu við rannsókn skipulagðrar brotastarfsemi þar sem internetið kemur við sögu. Ef umrætt ákvæði er ekki til staðar, eru úrræði lögreglu til rannsóknar slíkra mála nánast engin.

Sem dæmi um mál eða brotaflokka þar sem þessar upplýsingar nýtast með afgerandi hætti, má nefna netglæpi almennt, t.d. fjársvik, tælingarmál gagnvart börnum, kynferðisbrot, hótanir á netinu, hatursglæpir og skipulögð brotastarfsemi í heild sinni sem hefur færst yfir á netið. Í raun er ekki hægt að lista upp brot með tæmandi hætti þar sem þessar upplýsingar gagnast.

Skráningar sem þessar falla undir það sem kalla má „*stafrænt spor*“ með vísan í að það inniheldur rekjanleika til upprunans, líkt og fingraför gera þegar við snertum eitthvað.

Reynsla lögreglu af því að geta sótt slík gögn á framangreindum forsendum er almennt góð, þótt auðveldlega mætti færa rök fyrir því að kröfur yrðu settar á lengri varðveislutíma IP-talna líkt og gert er í nágrannaríkjum okkar sem er allt að eitt ár. Þannig var lengi vel að varðveisla á IP-tölum í Noregi var að hámarki þrjár vikur. Í júní 2021 var fjarskiptalögum þar í landi breytt og eru IP-tölur (IP-logs) varðveittar í 1 ár til að lögreglan geti nálgast upplýsingar til að verjast alvarlegum glæpum. Aðgangur er bundinn ákveðnum skilyrðum, svo sem vegna rannsókn máls, bundið við nauðsyn og brot er varðar þriggja ára fangelsi. Í Danmörku eru upplýsingar um IP tölur allra viðskiptavina og „port number“ varðveittar áfram í 1 ár.

Embætti ríkislögreglustjóra telur mikilvægt að líta til þeirrar þróunar sem hefur orðið í þessum löndum, en ljóst er að brot eða mál koma oft ekki inn á borð lögreglu fyrr en að nokkrum tíma liðnum frá því að brot átti sér stað. Því er mikilvægt að þessar upplýsingar séu gerðar aðgengilegar lengur, líkt og gert er t.d. í Noregi og Danmörku.

Benda má á tillögur til úrbóta er koma fram í kafla 6.1 í áhættumatsskýrslu Europol 2021 um skipulagða netglæpi (e. *Internet Organized Crime Threat Assessment, IOCTA*) „... sökum lagalegra hindrana er varða varðveislu og deilingu fjarskiptafyrirtækja á [stafrænum] umferðar- og staðsetningargögnum, þá séu gögn séu oft ekki varðveitt nægilega lengi, sem þá geti leitt til þess

að möguleg sönnunargögn fari forgörðum. Skýrari reglur um skráningu IP númera og léna gætu aukið á gagnagæðin.^[1]

Við þetta er að bæta sbr. frétt sem hefur verið á heimasíðu dómsmálaráðuneytisins að þá hefur verið undirrituð önnur viðbótarbókun við samning Evrópuráðsins um tölvubrot um aukið samstarf og upplýsingagjöf fyrir rafræn sönnunargögn. Markmiðið er að koma á skjótvirkara og skilvirkara samstarfi vegna upplýsingaöflunar löggæsluyfirvalda um notendur, áskrifendur og fjarskiptaumferð í þágu rannsóknar sakamála.

Í 2. mgr. 92. gr. frumvarpsins er fjallað um skyldu fjarskiptafyrirtækja til að setja sér verklagsreglur um aðgang lögreglu að persónuupplýsingum notenda fjarskiptaþjónustu. Í lokamálsgrein ákvæðisins er kveðið á um að ráðherra getur sett reglugerð um skyldur fjarskiptafyrirtækja varðandi varðveislu upplýsinga og aðgang lögreglu að fjarskiptasendingum og upplýsingum samkvæmt þessari grein. Mikilvægt er að mati ríkislögreglustjóra að það liggi skýrt fyrir að lögreglu sé ekki gert að afhenda fjarskiptafyrirtækjum dómsúrskurði né úrskurðarorð sem liggja fyrir varðandi rannsóknaraðgerðir. Það er að mati lögreglu mögulega til þess fallið að spilla yfirstandandi rannsókn, sem og mögulega framtíðarrannsóknum tengdum sömu aðilum séu slíkar upplýsingar varðveittar hjá fjarskiptafyrirtækjum. Nóg ætti að vera að einungis verði afhent númer úrskurðar ásamt kröfu um tilteknaðgerðir. Í þessu samhengi er bent á að lögreglan lýtur eftirliti ríkissaksóknara vegna aðgerða sem þessara sbr. 3. mgr. 85. gr. laga nr. 88/2008 um meðferð sakamála. Ítrekað er að það getur ekki verið háð mati fjarskiptafyrirtækja hverju sinni hvernig rannsóknum sakamála er hátað hverju sinni út frá verklagsreglum sem fyrirtækin setja sér. Skýrt verður að vera að umræddar verklagsreglur taki einvörðungu til innri ferla sem verða að fara af stað þegar beiðni lögreglu berst. Að mati embættisins er þetta ekki nægilega skýrt og getur í framkvæmd valdið vandkvæðum.

Hvað öryggisvottun lögreglu varðandi starfsmenn fjarskiptafyrirtækja sem annast tengingar á símhlustun lögreglu, er mikilvægt að mati RLS að skilgreining á hugtakinu öryggisvottun liggja fyrir, samkvæmt tilgangi þessa frumvarps. Að mati RLS þýðir öryggisvottun samkvæmt þessu frumvarpi að bakgrunnskoðun lögreglu hafi farið fram og að viðkomandi hafi staðist hana. Mikilvægt er að þessa atriðis sé geti í orðskýringum eða mögulega í greinargerð með frumvarpinu. Bent er á að t.d. er öryggisvottun á grundvelli varnarmálalaga, annarskonar öryggisvottun en hér um ræðir.

Í 95. gr. frumvarpsins er fjallað um neyðar- og öryggisfjarskipti, en að mati embættisins þurfa þar að vera talin upp fleiri atriði sem nauðsynlegt er að kveða á um í reglugerð. Þar má nefna atriði

[1] [internet organised crime threat assessment iocra 2021.pdf \(europa.eu\)](#) „Legal barriers around the retention and sharing of data persist. Data is often not retained for long enough with ISPs, which can lead to a loss of potential evidence. Investigations would benefit from longer data retention, but also from faster and higher quality data exchange with service providers. Clearer rules for registering IP addresses and domains could increase this data quality.“

RÍKISLÖGREGLUSTJÓRI

hvað varðar hlutfallslegan uppítími neyðar- og öryggisfjarskiptakerfis eftir mismunandi kerfiseiningum, viðmið um flokkun fjarskiptastaða út frá öryggissjónarmiðum, ráðstafanir til að tryggja öryggi í viðkomandi flokki, þar með talið varðandi varaleiðir og lágmarks varaafli í rafgeymum eða vararafstöðvar eftir mismunandi flokkun fjarskiptastaðarins, kröfur til gerðar og tegundar fjarskiptabúnaðar ásamt kröfum sem gerðar eru til framleiðenda búnaðar fyrirkomulag innra eftirlits, tilkynningar til Fjarskiptastofu um öryggisatvik, úttektir og prófanir af hálfu Fjarskiptastofu og aðgengi stofnunarinnar að upplýsingum, þátttöku í samhæfingu fjarskiptafélaga og Fjarskiptastofu er varðar öryggi og almannavarnir sem og skilyrði fyrir samstarfi rekstraraðila neyðar- og öryggisfjarskiptakerfis við önnur fjarskiptafyrirtæki um starfrækslu einstakra fjarskiptastaða, eða kerfishluta.“

Mikilvægt er að koma því á framfæri að trygg neyðar- og öryggisfjarskipti er forsenda þess að hægt sé að hefja og samræma aðgerðir viðbragðsaðila þegar vá ber að höndum. Neyðarfjarskiptakerfi eru þau fjarskipti sem þurfa að vera til staðar á tímum neyðar vegna slysa, náttúruhamfara eða hamfara af mannavöldum til að tryggja svo sem öryggi almennings, rekstur grunnþjónustu, varna tjóni á mannvirkjum, virkni samgangna á landi, sjó og lofti. Rekstur neyðar- og öryggisfjarskiptakerfis þarf að hvíla á grunni öruggs rekstrar.

Í því felst að þjónustustigið þurfi að vera hátt og rekstraröryggið mikið, m.a. varðandi tvöföld kerfi og leiðir, varakerfi og varaafli o.s.frv. Þetta kallar einnig á kröfur um reglubundið viðhald og stuttan viðbragðstíma vegna viðgerða. Í neyðar- og öryggisfjarskiptakerfi þurfa að vera innbyggðar varnir gegn vá og truflunum og byggir kerfið á tæknilegum eiginleikum sem ekki eru til staðar í almennum fjarskiptanetum. Neyðarfjarskiptakerfi er því ætlað að halda fullri virkni þótt almennu fjarskiptanetin verði að einhverju leyti óvirk um lengri eða skemmri tíma. Ákvæði þetta gerir ráð fyrir því að sú umgjörð sem gildir um almenn fjarskiptanet taki jafnframt til neyðar- og öryggisfjarskiptakerfa. Þannig skal beita sömu aðferðum og verkferlum til að skjalfesta fyrirkomulag öryggisskipulags og uppfylla sömu viðmið og kröfur um áhættustýringarumgjörð þegar neyðarfjarskiptakerfi eiga í hlut, sbr. 78. gr. frumvarpsins og reglugerða sem kunna að vera settar með stoð í því ákvæði.

Rétt er að ítreka að markmið með þessari lagasetningu, getur ekki verið að hrófla við þeim atriðum sem snúa að neyðarfjarskiptakerfum samkvæmt lögum um almannavarnir nr. 82/2008. Sem dæmi má nefna að sú reglugerð sem dómsmálaráðherra setur samkvæmt 34. gr. laganna er af öðrum toga, þ.e. lýtur ekki að tæknilegum öryggisráðstöfunum til að tryggja samfellda virkni, eins þessu lagaákvæði er ætlað að gera. Reglugerðarheimild samkvæmt almannavarnarlögum snýr fremur að inntaki og umfangi á nýtingu neyðarfjarskiptakerfa.

Að öðru leyti vísar embætti ríkislögreglustjóra til áður innsendra umsagna bæði ríkislögreglustjóra og annarra lögregluembætta um frumvarpið. Má sérstaklega benda á umsögn embættisins dags. 5.

RÍKISLÖGREGLUSTJÓRI

nóvember 2020, sem og umsagnar embættis lögreglustjórans á höfuðborgarsvæðinu dags. 11. júní 2020 svo dæmi séu nefnd. Mikilvægt er að þau sjónarmið sem þar eru reifuð verði raungerð í því frumvarpi sem nú liggur fyrir þinginu, hafi það ekki þegar verið gert.

F.h. ríkislögreglustjóra



Helgi Valberg Jenson,
yfirlögfræðingur.