

Meðhöndlun trúnaðarupplýsinga hjá löggæslustofnunum ríkisins

Kristín Guðmundsdóttir, MA, upplýsingafræðingur, sérfræðingur hjá ríkislögreglustjóra

Jóhanna Gunnlaugsdóttir, prófessor við Félags- og mannvísindadeild Háskóla Íslands

Útdráttur

Grein þessi byggir á niðurstöðum rannsóknar sem gerð var á meðferð trúnaðarupplýsinga meðal löggæslustofnana og löggæslutengdra stofnana. Markmiðið var að skoða hvernig meðhöndlun slíkra upplýsinga væri háttáð hjá stofnunum. Þá var tilgangurinn að varpa ljósi á skyldur og kvaðir varðandi meðferð trúnaðarupplýsinga og hvernig tókst að framfylgja þeim svo og að kanna þekkingu starfsfólks á viðeigandi lagaumhverfi. Meðferð trúnaðarupplýsinga hefur ekki áður verið rannsökuð á heildstæðan hátt hérlendis með hliðsjón af starfsemi og hlutverki umræddra stofnana.

Rannsóknin byggði á eigindlegri aðferðafræði, nánar tiltekið viðtalsaðferð. Helstu niðurstöður sýndu að viðmælendur höfðu lagalegar kvaðir um trúnað og þagnarskyldu í heiðri varðandi meðhöndlun upplýsinga. Þeir vísuðu til trúnaðaryfirlýsinga og stöðu ríkisstarfsmanna og ábyrgðar þeirra í tengslum við lögbundna þagmælsku. Skiptar skoðanir voru um það hvort gildandi lög og reglur um meðferð trúnaðarupplýsinga nægðu eða þörfuðust breytinga. Þá höfðu hefðir og venjur mótað vissar starfsaðferðir við ýmis hversdagsleg störf fremur en að um þær giltu fyrirfram skilgreindar reglur.

Efnisorð: Trúnaðarupplýsingar; þagnarskylda; persónuvernd; opinber stjórnsýsla.



Icelandic Review of Politics and Administration Vol. 13, Issue 2 (239-264)

© 2017 Contact: Kristín Guðmundsdóttir, kristingudmunds@hotmail.com

Article first published online December 14th 2017 on <http://www.irpa.is>

Publisher: Institute of Public Administration and Politics, Gimli, Sæmundargötu 1, 101 Reykjavík, Iceland

Stjórnmál & stjórnsýsla 2. tbl. 13. árg. 2017 (239-264) Fræðigreinar

© 2017 Tengiliður: Kristín Guðmundsdóttir, kristingudmunds@hotmail.com

Vefbirting 14. desember 2017 - Birtist á vefnum <http://www.irpa.is>

Útgefandi: Stofnun stjórnsýslufræða og stjórnmála, Gimli, Sæmundargötu 1, 101 Reykjavík

DOI: <https://doi.org/10.13177/irpa.a.2017.13.2.4>

This work is licensed under a Creative Commons Attribution 3.0 License.

Handling of confidential Information at law enforcement agencies

Abstract

This article is based on the findings of a research into the procedures regarding the handling of classified and confidential information at law enforcement agencies and related institutions. The aim was to examine how this information was being dealt with at these institutions. A secondary aim was to shed light on the duties and requirements regarding how confidential information should be handled and how the information were being enforced, in addition to examining the knowledge that the employees possessed regarding the legal environment. Procedures regarding the processing of confidential information have not been studied before in a comprehensive manner from the perspective of having the operation and purpose of these institutions in mind.

The research was based on a qualitative methodology, interviews to be exact. The main findings showed that the respondents honoured the legal requirements regarding confidentiality when they handled such information. They referred to declarations of confidentiality, obligations of State employees, and their responsibilities in connection with the legal requirements regarding discretion. There was a difference of opinion whether current laws and regulations regarding the handling of confidential information were sufficient or should be changed. Traditions and customs had furthermore created certain work procedures in the daily work, and proved more valid than predefined rules.

Keywords: Confidential information; classified information; data protection; public governance; law enforcement agencies.

Inngangur

Rannsóknin, sem hér er kynnt, er hluti af stærra rannsóknarverkefni (Kristín Guðmundsdóttir 2016; Kristín Guðmundsdóttir & Jóhanna Gunnlaugsdóttir 2016). Hún fjallar um meðferð trúnaðarupplýsinga meðal ríkisstofnana. Til þess að gefa verkefninu skýrari ramma var athygli beint að meðferð trúnaðarupplýsinga sem vörðuðu öryggi og vernd í almannabágu, það er löggæslu- og öryggismál. Aðalhöfundur greinarinnar hefur um árabíl starfað á vegum löggæslustofnunar og þótti efnið því áhugavert til frekari skoðunar. Starfsvettvangur og starfssvið þeirra, sem sinna öryggis- og löggæslustörfum, er mismunandi og efnislegt form þeirra upplýsinga, sem þeir meðhöndla, er margþætt. Almannaþarnir taka meðal annars til öryggis landsins, reksturs mannvirkja, borgaralegs/samfélagslegs öryggis svo og mikilvægra innviða eins og orku-, fjarskipta-, nets- og upplýsingaöryggis (Innanríkisráðuneytið 2015). Trúnaðarupplýsingar og viðkvæmar upplýsingar af ýmsu tagi eru því víða meðhöndlaðar innan stofnana. Gæta ber að rétttri meðferð upplýsinganna og tryggja að hún sé í samræmi við gildandi lög og reglugerðir, óháð eðli þeirra, hvort sem þær varða persónulega hagi einstaklinga, eru stjórnsýslulegs eðlis, varða öryggismál eða rannsóknarhagsmuni svo að dæmi séu rekin.

Markmið rannsóknarinnar var að skoða hvernig meðferð trúnaðarupplýsinga væri háttað innan löggæslu- og löggæslutengdra stofnana, lagalegar kvaðir og framkvæmd þeirra. Hvorki verður komið inn á útfærslu á öryggi tölvukerfa né tölvuöryggi almennt. Notast var við eiginlega aðferðafræði við gerð rannsóknarinnar og 13 viðtöl tekin hjá sjö stofnunum. Helstu niðurstöður sýndu að allir viðmælendur þekktu og virtu lagalegar kvaðir um trúnað og þagnarskyldu varðandi meðhöndlun upplýsinga. Aftur á móti voru starfsaðferðir eða reglur um meðferð trúnaðarupplýsinga ekki samræmdar og á köflum jafnvel ekki fyrir hendi.

Fræðilegum bakgrunni rannsóknarinnar er gerð skil í upphafi greinarinnar og í framhaldinu fjallað um aðferðafræði hennar. Niðurstöður eru settar fram í aðskildum þemaköflum, þá birtast umræður og samantekt um rannsóknina og að endingu eru lokaorð sett fram.

1. Fræðilegur bakgrunnur

Um fjöllun um upplýsingaleynd stjórnvalda hefur um aldir fylgt rekstri stjórnsýslunnar. Jeremy Bentham (1843) skrifaði árið 1791 að ekki væri hægt að gera allar upplýsingar hjá stjórnvöldum opinberar þar sem taka yrði tillit til aðstæðna á hverjum tíma. Hann taldi að leynd væri áhald samsæris og leyndin ætti ekki við innan stjórnsýslunnar. Hann var þeirrar skoðunar að einungis þrjár ástæður væru þess eðlis að þær gætu komið í veg fyrir upplýsingaskyldu stjórnvalda; að (1) upplýsingar kæmu óvinveittum að notum, (2) upplýsingar sköðuðu saklausa og (3) upplýsingar gerðu of mikið úr sekt hins seka (Bentham 1843).

Talið er að bandaríski herinn hafi fyrstur sett verklagsreglur um meðferð trúnaðarupplýsinga árið 1912 (Relyea 2008). Að mati Ferraiolo og Kuhn (1992) var ekki síður mikilvægt að borgaralegar stofnanir settu slíkar reglur enda þyrftu þær að vernda upplýsingarnar gegn rökun, þjófnaði og óæskilegri birtingu. Þannig má sjá að þörf fyrir skipulagt regluverk um meðferð upplýsinga og upplýsingaleynd stjórnvalda hafi fylgt rekstri stjórnsýslunnar um langt skeið.

1.1 Upplýsingavernd eða upplýsingaleynd

Fjölmargar rannsóknir og greinar má finna um skilgreiningu á leynd og leyndarmáli og meðferð upplýsinga því tengdu. Sissela Bok (1989) rannsakaði og fjallaði um leynd (e. secrecy) og friðhelgi (e. privacy). Að hennar mati líkjast hugtökin leynd og friðhelgi og því mikilvægt að greina þar á milli. Með „leynd“ sé átt við að upplýsingar séu faldar af ásettu ráði til þess að varna því að einstaklingar öðlist vitneskju um leyndarmálið eða fái á einhvern hátt vísbendingar um að það sé til. Slík aðgerð getur til dæmis verið í formi viðskiptaleyndar eða faglegs trúnaðar í starfi. Hins vegar að „friðhelgi“ sé að vernda eitthvað fyrir óæskilegum aðgangi óviðkomandi að því sem einstaklingur telur vera persónulegt yfirráðasvæði sitt (Bok 1989).

Fleiri hafa tekið undir sjónarmið Bok (1989) hin síðari ár. Martin, Bray og Kumar (2015) eru þeirrar skoðunar að einungis hluti þeirra upplýsinga, sem liggja hjá stjórnvöldum, séu þess eðlis að þær megi birta opinberlega og því hafi löggjafinn gert ráð fyrir.

Ákvæði um trúnað, þagmælsku og upplýsingaleynd er að finna í lögum og reglugerðum. Trúnaðarákvæðin eiga við í mismunandi tilvikum svo sem við meðferð persónu- og viðskiptaupplýsinga svo og öryggismál. Reginmunur getur verið þarna á en leynd í þágu persónuverndar og friðhelgi einkalífsins er oftast talin jákvæð í edli sínu en síður þegar upplýsingum er haldið leyndum innan stjórnsýslunnar. Þannig framganga er fremur litin neikvæðum augum enda stríðir hún gegn hugmyndinni um opna og gegnsæja stjórnsýslu (Martin o.fl. 2015).

Kim Lane Scheppele (1988) skoðaði hugtakið leynd og hvernig hún er skilgreind og réttlætt í vestrænum samfélögum. Eins og Bok (1989) skilgreinir Scheppele (1988) „leynd“ sem vitneskju eða upplýsingar sem einn eða fleiri einstaklingar viljandi leyna einum einstaklingi eða fleirum. Scheppele (1988) kom fyrst fram með skilgreiningu á tvískiptingu leyndar, það er „djúpri leynd“ (e. deep secret) og „grunnri leynd“ (e. shallow secret). Með grunnri leynd er átt við að einstaklingar viti að upplýsingum sé haldið leyndum en sé ekki kunnugt um innihald upplýsinganna. Djúp leynd felur í sér að einungis þeir einstaklingar, sem halda upplýsingunum leyndum, viti að þær séu til (Scheppele 1988).

Gutmann og Thompson (1996) þróðu kenningar Scheppele (1988) áfram, settu þær í víðara samhengi og heimfærðu meðal annars yfir á stjórnsýsluna. Að þeirra áliti er djúpa leyndin falin almenningi en hin grunna sú sem almenningur hefur takmarkaða vitneskju um en þekkir ekki nánar til um innihald hennar. Almenningur hefur möguleika á því að mótmæla grunnri leynd og fara fram á að upplýsingar verði gerðar opinberar. Djúp leynd er aftur á móti alfarið á valdi þeirra sem leyna upplýsingum og þess háttar leynd fylgir sá möguleiki að embættismenn misbeiti henni ef leyna á upplýsingum til þess að villa um fyrir almenningi. Þetta geti til dæmis verið gert með það fyrir augum að forðast gagnrýni og fela misgjörðir eða vafasamar aðgerðir (Gutmann & Thompson 1996; Jóhanna Gunnlaugsdóttir 2016).

Pozen (2010) rannsakaði einnig leyndina og skilgreininguna á djúpri og grunnri leynd. Að hans mati gilda önnur lögmál um leynd stjórnvalda en einkaaðila eða félagsleg leyndarmál eins og Scheppele (1988) lagði áherslu á í sínum rannsóknum. Hann fjallar um lagskiptingu stjórnsýslunnar og heldur því fram að leynd stjórnvalda sé ekki jafn einföld og Scheppele (1988) túlkar hana. Hann telur að í tilvikum ríkisleýndar sé upplýsingum haldið leyndum fyrir mun fleiri aðilum. Auk þessa getur almenningur krafist þess að stjórnvöld geri upplýsingar opinberar ólíkt því sem á sér stað þegar tveir einkaaðilar eiga í hlut. Þannig telur Pozen (2010) að ríkisleýndarmál séu djúp þegar opinberir starfsmenn, leyna samstarfsaðilum og almenningi upplýsingum. Hann telur að leyndarmál séu grunn þegar almenningur gerir sér grein fyrir að upplýsingum, sem hann hefur þó takmarkaða vitneskju um, sé leynt. Hann ræðir einnig hvernig rök hafa verið færð fyrir réttlætingu ríkisleýndar og þar vegi fjórir þættir þyngst; að (1) vernda ríkið, (2) fyrirbyggja að óæskilegir aðilar geti nálgast upplýsingar og þannig skaðað þjóðarhagsmuni og stefnu yfirvalda, (3) tryggja að persónuupplýsingum, sem ríkisstofnanir búi yfir í miklu magni, sem ríkisleýnd í formi friðhelgi, verði ekki miðlað eða þær birtar og (4) minni kostnaður fylgi því oft þegar upplýsingum sé leynt heldur en ómakinu við að reka gegnsæja stjórnsýslu.

1.2 Rannsóknir á meðferð viðkvæmra upplýsinga

Erlendar rannsóknir um hlutverk stjórnvalda við að tryggja öryggi upplýsinga er víða að finna. Sem dæmi má taka rannsókn Hitoshi Nasu (2015) sem skoðaði áskoranir ríkisins við verndun ríkisupplýsinga. Túlkun hugtaksins þjóðaröryggi, að hans mati, hefur víkkað á síðastliðnum árum, frá því að beinast að því að vernda ríkið í hernaðarlegum skilningi til þess að varða einnig öryggi tengdu efnahagi, fæðu, auðlindum, orku, umhverfi og netheimum. Allir þessir þættir kynnu að hafa neikvæð áhrif á þjóðaröryggi. Stjórnvöld þurfa fremur að huga að þeim nútímaógnum sem eiga við á hverjum tíma heldur en hefðbundnum ógnum svo sem stjórnmalalegum, efnahagslegum og félagslegum ógnum. Þannig tiltekur hann að hryðjuverkaógnir séu alþjóðasamvinna og miðlun leyndlegra upplýsinga mikilvæg í því samhengi. Hann bendir einnig á að með sívaxandi þróun tölvutækni geti almennar opinberar upplýsingar varðað þjóðaröryggi enda kynnu þær að ógna almannahagsmunum. Huga þurfi að fleiri áhættuþáttum við birtingu opinberra upplýsinga á tímum örrar tækniþróunar og hraða þar sem afleidd áhrif birtingar geta orðið alvarleg. Við rannsókn Nasu (2015) kom í ljós að í auknum mæli er upplýsingaöryggi orðið þáttur í þjóðaröryggi ríkja þar sem birting upplýsinga getur haft neikvæð áhrif á ríki, sérstaklega varnir þess eða allsherjarreglu og almannaöryggi. Lög ríkjanna eru að mati Nasu (2015) sniðin að því að stjórnvöld geti aðlagð gildissvið upplýsingaleyndar á hverjum tíma samfara örri þróun á umhverfi og ógnum sem stöðja að öryggi ríkisins. Ávallt þarf að taka mið af þeim skaða, sem getur hlotist við birtingu upplýsinganna, við stofnun og flokkun ríkisleyndarmála.

Að mörgu ber að hyggja þegar tryggja á öryggi persónuupplýsinga. Ný tækni og samfélagsmiðlar hafa í för með sér aukna hættu hvað slíkt varðar. Þá má geta þess að eftirlitsstofnanir á Íslandi hafa í auknum mæli hagnýtt sér persónuupplýsingar á Facebook við opinbert eftirlit með einstaklingum (Sigurður G. Hafstað & Jóhanna Gunnlaugsdóttir 2016). Warkentin, Johnston og Shropshire (2011) skoðuðu meðal annars hlutverk forstöðumanna við að tryggja upplýsingaöryggi og að starfsmenn fari eftir þeim reglum sem settar eru í þeim tilgangi. Þeir nefna að forstöðumenn þurfi ávallt að tryggja að allt starfsfólk, sem meðhöndlar persónuupplýsingar, hafi sama skilning á reglum sem um þær gilda sem og reglum sem gilda um að tryggja öryggi þeirra (Warkentin o.fl. 2011).

Almennt eru ríkar kröfur um að starfsmenn hyggi að upplýsingaöryggi við störf sín. Niðurstöður rannsóknar Albrechtsen (2007) sýndu að mikill munur var á skilningi starfsmanna á öryggisráðstöfunum og á raunverulegri framkvæmd þeirra á því að tryggja upplýsingaöryggi. Þetta taldi hann helst stafa af skorti á þekkingu og hvata til þess að beita öflugri öryggisráðstöfunum. Í ljósi vaxandi vinnuálags og kröfu um hraða og aukna framleiðni urðu aukin afköst gjarnan á kostnað öryggisins þar sem öryggisráðstafanir gátu dregið úr vinnuhraða og árangri (Albrechtsen 2007). Rannsókn á svokallaðri innri hættu (e. insider threat) sýndi einmitt að öryggisrof starfsmanna eru oft vanmetnir þættir þegar kemur að því að tryggja öryggi. Algengt er að notendur upplýsingakerfa, viljandi eða óviljandi, fylgi ekki settum reglum um upplýsingaöryggi (Dhillon 2001).

Rannsókn Theoharidou, Kokalakis, Karyda og Kiountouzis (2005) náði meðal annars til mikilvægi þjálfunar og vitundarvakningar varðandi meðferð upplýsinga. Í rann-

sókninni greindu þeir hvernig tekist er á við þær áskoranir í *ISO/IEC 17799* staðlinum um upplýsingaöryggi (nú *ISO/IEC 27001*). Í niðurstöðunum kom fram að hindrunarmáttur staðalsins fælist einkum í ákvæðum um agaferli starfsmanna sem brjóta öryggisreglur. Þar má nefna eflingu á aðgangsstýringu, þjálfun og aukna vitundarvakningu á öryggisreglum og kröfum (Theoharidou o.fl. 2005).

Niðurstöður rannsóknar Warkentin, Johnston og Shropshire (2011) sýndu fram á að þátttaka allra starfsmanna við að framfylgja reglum um upplýsingaöryggi hefur áhrif á heildaröryggi skipulagsheilda. Regluleg hópræðsla þarf að eiga sér stað en einnig er mikilvægt að starfsmenn miðli reynslu og þekkingu sín á milli.

Hér á landi hafa verið gerðar rannsóknir sem tengjast upplýsingalöggjöfni og formfestu í vinnubrögðum hvað skjalfestingu og skjalahald varðar. Þessar rannsóknir gefa meðal annars til kynna að skortur sé á formlegri meðhöndlun upplýsinga innan stjórnsýslunnar og samræmdum vinnubrögðum varðandi kerfisbundna stjórn á skjölum. (Jóhanna Gunnlaugsdóttir 2015; Jóhanna Gunnlaugsdóttir 2016). Víða virðist því pottur brotinn hvað varðar skjalamál opinberra stofnana. Í því sambandi er rétt að minna á nýlega grein um varðveislu gagna í stjórnsýslunni. Hún getur komið þeim, sem vinna með þess háttar gögn, að notum (Kristín Benediktsdóttir & Trausti Fannar Valsson 2016).

1.3 Trúnaðar- og þagnarskylduákvæði og meðferð upplýsinga

Finna má fjölda laga og reglugerða sem varða annars vegar trúnaðar- eða persónuupplýsingar og hins vegar trúnað eða þagnarskylduákvæði þeirra sem með þær fara. Ákvæðin má finna í almennum lögum og reglugerðum, sem ganga þvert á stjórnsýsluna, svo og í sérlögum og reglugerðum sem gilda um tiltekna stofnanir eða málaflokka. Ákvæðin eru margvísleg og misjöfn þó svo að tilgangurinn með þeim sé almennt sá sami.

Í íslenskum stjórnsýslurétti eru ákvæði um að ríkisstarfsmenn eigi að fara með skilgreindar upplýsingar sem trúnaðarmál. Þá er þeim víða uppálagður trúnaður og eru birtingarmyndir hans af ýmsum meidi. Hér á eftir verður farið yfir helstu lög og reglugerðir, sem varða meðferð trúnaðar- eða persónuupplýsinga, og falla undir starfsemi ríkisstofnana svo og á hvern hátt þagnarskyldan birtist í þeim. Auk þessara laga eru trúnaðar- og þagnarskylduákvæði í sérlögum þeirra stofnana sem rannsóknin náði til. Þeirra er látið ógetið hér með það fyrir augum að virða trúnað við viðmælendur og stofnanir.

1.3.1 Lög um réttindi og skyldur starfsmanna ríkisins

Lög um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, ná til allra opinberra starfsmanna óháð því hvaða sérstofnun þeir heyra undir. Í 18. gr. laganna segir að starfsmanni sé:

[...] skylt að gæta þagnarskyldu um atriði er hann fær vitneskju um í starfi sínu og leynt skulu fara samkvæmt lögum, fyrirmælum yfirmanna eða edli málsins. Þagnarskylda samkvæmt lögum helst þó látið sé af störfum.

Brot gegn þagnarskyldu getur varðað stjórnsýsluviðurlögum, það er áminningu í starfi eða uppsögn. Sé brotið þess eðlis, eða ítrekað, getur þagnarskyldubrot enn fremur varðað réttindasviptingu. Þagnarskyldubrot geta einnig varðað refsingu samkvæmt 136. grein almennra hegningarlaga, nr. 19/1940, sé um ásetningsbrot að ræða (Páll Hreinsson 1996; Páll Hreinsson 2013).

1.3.2 *Upplýsingalög*

Í upplýsingalögum, nr. 140/2012, er meðal annars kveðið á um rétt almennings til aðgangs að fyrirliggjandi gögnum stjórnvalda. Þó felst ekki í því réttur til aðgengis að skráum og gagnagrunnum hafi upplýsingar ekki verið gerðar að gögnum og frekar unnið úr þeim af hálfu stjórnvalda (Trausti Fannar Valsson 2015). Kröfur um öryggisráðstafanir eða aðrar lágmarkskröfur við meðferð persónuupplýsinga er ekki að finna í lögunum heldur varða þau upplýsingarétt almennings.

Í lögunum er ekki beint kveðið á um þagnarskylduákvæði gagnvart ríkisstarfsmönnum en í 2. mgr. 4. gr. laganna segir að þau gildi ekki um upplýsingar, sem trúnaður skuli ríkja um, í samræmi við þjóðréttarsamninga sem Ísland er aðili að. Þess háttar undanþáguákvæði er til að mynda að finna í 38. gr. laga um opinber skjalasöfn, nr. 77/2014.

1.3.3 *Lög um persónuvernd og meðferð persónuupplýsinga*

Lögum um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000, er meðal annars ætlað að tryggja friðhelgi einkalífs. Lögin ná ekki einungis til stjórnsýslunnar heldur gilda um alla vinnslu persónuupplýsinga óháð því hver á í hlut. Tiltekin ákvæði í lögunum gilda ekki um vinnslu persónuupplýsinga varði þær almannaöryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu.

Skilmálar um mögulegt þagnarskylduákvæði, sem ná til ábyrgðar- og vinnsluaðila leyfisskyldrar vinnslu persónuupplýsinga, sem og starfsmanna á vegum þeirra, ákvæði Persónuvernd svo, er að finna í 34. gr. laganna. Brot gegn þagnarskyldu varðar refsingu samkvæmt almennum hegningarlögum.

1.3.4 *Almenn hegningarlög*

Kveðið er á um refsingar við þagnarskyldubrotum opinberra starfsmanna í 136. gr. almennra hegningarlaga, nr. 19/1940:

Opinber starfsmaður, sem segir frá nokkru, er leynt á að fara og hann hefur fengið vitneskju um í starfi sínu eða varðar embætti hans eða sýslan, skal sæta fangelsi allt að einu ári. Hafi hann gert það til þess að afla sér eða öðrum óréttmæts ávinnings, eða noti hann slíka vitneskju í því skyni, má beita fangelsi allt að 3 árum.

Þá segir í 230. gr.

Ef maður, sem hefur eða hefur haft með höndum starf, sem opinbera skipun, leyfi eða viðurkenningu þarf til að rækja, segir frá einhverjum einkamálefnum, sem leynt eiga að fara og hann hefur fengið vitneskju um í starfi sínu, þá varðar það sektum eða fangelsi allt að 1 ári.

1.3.5 Reglugerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála

Reglugerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála, nr. 959/2012, er sett á grundvelli varnarmálalaga, nr. 34/2008. Sérstakur viðurlagakafli er í reglugerðinni en brot á henni getur varðað refsingu samkvæmt almennum hegningarlögum, nr. 19/1940, varnarmálalögum, nr. 34/2008, og/eða lögum um eftirlit með þjónustu og hlutum sem geta haft hernaðarlega þýðingu, nr. 58/2010.

Reglugerðin tekur til margra öryggisþátta sem taka þarf tillit til við meðferð trúnaðarupplýsinga. Hún varðar mannaúdsöryggi, raunlægt öryggi, upplýsingaöryggi og tölvuöryggi. Skilgreindar eru kröfur sem uppfylla þarf vegna meðferðar trúnaðarupplýsinga, bæði hvað varðar starfsfólk, umhverfi og þá aðstöðu sem þær eru meðhöndlaðar og/eða vistaðar í. Þá eru skilgreindar kröfur um tölvubúnað, sem upplýsingarnar eru unnar í, auk fleiri þátta sem varða heildaröryggi trúnaðarupplýsinganna. Þessi reglugerð er sú eina sinnar tegundar í íslenskrí stjórnsýslu.

1.4 Trúnaðar- og þagnarskylduhugtökin

Bein þagnarskylduákvæði, sem þó eru misafdráttarlaus, er að finna í íslenskum lögum og reglugerðum eins og fyrr er getið. Ákveðið ósamræmi má glöggst sjá í lögum og reglugerðum við skoðun á trúnaðarhugtökum enda er staðlaður orðaforði ekki fyrir hendi. Til dæmis segir; „... starfsmönnum sé óheimilt að miðla upplýsingum“, „... starfsmenn séu bundnir trúnaði“, „... þeim skylt að halda trúnað“, „... þeim beri að gæta trúnaðar“, „... þeir skuli undirrita eiðstaf“, „... fara beri með ákveðin mál sem trúnaðarmál“, „... ákveðin mál séu trúnaðarmál“, „... óheimilt sé að greina frá trúnaðarupplýsingum“, „... óheimilt sé að greina opinberlega frá“, „... starfsmenn séu bundnir þagnarskyldu“, „... sé skylt að gæta þagnarskyldu“ og „... þeir sem þrátt fyrir þagnarskylduákvæði láti af hendi trúnaðarupplýsingar eða greini frá nokkru er leynt á að fara skuli sæta ákveðnum viðurlögum“. Með frumvarpi til laga um breytingu á stjórnsýslulögum, nr. 37/1993 um einföldun og samræmingu þagnarskylduákvæða, sem birt var á vefsíðu forsætisráðuneytisins í nóvember 2013, var ætlað að skerpa á þeim þáttum er falla undir þagnarskylduna, kalla eftir frekari skilgreiningu á þeim upplýsingum er falla undir 136. gr. almennra hegningarlaga, nr. 19/1940 og hvað þagnarskyldunni er ætlað að vernda (Trausti Fannar Valsson 2015). Þess ber þó að geta að á Alþingi hefur frumvarpið enn ekki náð fram að ganga og það því ekki orðið að lögum.

Hér mun nánar fjallað um helstu trúnaðar- og þagnarskylduákvæði annars vegar og trúnaðarhugtök hins vegar sem gilda um löggæslu- og öryggismál. Þá verða trúnaðarhugtökin greind enn frekar.

Við framkvæmd rannsóknar var í febrúar 2016 framkvæmd leit í lagasafn á vef Alþingis og í reglugerðarsafni innanríkisráðuneytisins (Kristín Guðmundsdóttir 2016). Við leitina var tíðni sjö hugtaka (hér eftir hugtakaflokka) greind:

- Trúnaðarmál* (Trúnaðarmál/mála/málum o.s.frv.)
- Trúnaðarupplýsing* (Trúnaðarupplýsingar/upplýsingum o.s.frv.)
- Trúnaðarg* (Trúnaðargagna/gögn o.s.frv.)
- Trúnaðarskj* (Trúnaðarskjal/skjöl o.s.frv.)
- Trúnaðarstig* (Trúnaðarstig/stiga o.s.frv.)
- Trúnaðarflokk* (Trúnaðarflokkur/flokka o.s.frv.)
- Öryggisgráð* (Öryggisgráða/gráðun o.s.frv.)

Þá var leitað eftir hugtakinu „trúnaðarefni“. Sú leit skilaði engum niðurstöðum hvorki í lögum né reglugerðum. Ofangreind hugtök komu fyrir samtals 130 sinnum í 107 lögum og reglugerðum. Þó er rétt að geta þess að í einstaka lögum og reglugerðum komu fleiri en eitt hugtak fyrir. Til dæmis komu hugtökin „trúnaðarmál“, „trúnaðarupplýsingar“, „trúnaðargögn“, „trúnaðarskjöl“ og „trúnaðarstig“ öll fyrir í varnarmálalögum. Þau falla þannig í fimm mismunandi hugtakaflokka. Niðurstöður voru:

Trúnaðarmál: Birtist alls 68 sinnum í 29 lögum og 39 reglugerðum.

Trúnaðargögn: Birtist alls sjö sinnum í fimm lögum og tveimur reglugerðum.

Trúnaðarskjöl: Birtist alls sex sinnum í tveimur lögum og fjórum reglugerðum.

Trúnaðarupplýsingar: Birtist alls 43 sinnum í 22 lögum og 21 reglugerðum.

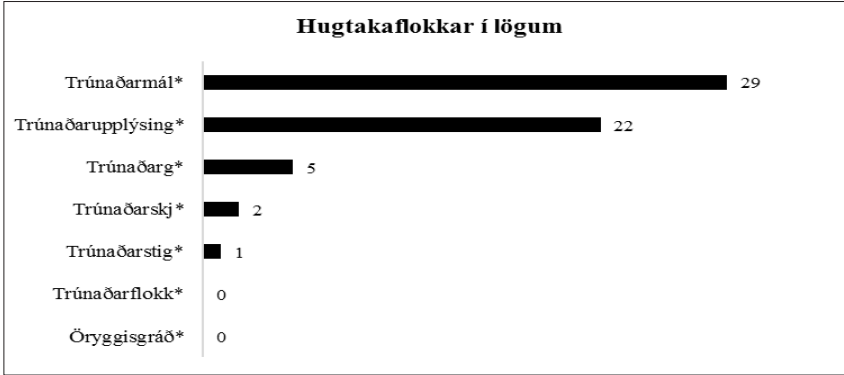
Trúnaðarstig: Birtist alls þrisvar sinnum í einum lögum og tveimur reglugerðum.

Trúnaðarflokkun: Birtist alls tvisvar sinnum í tveimur reglugerðum.

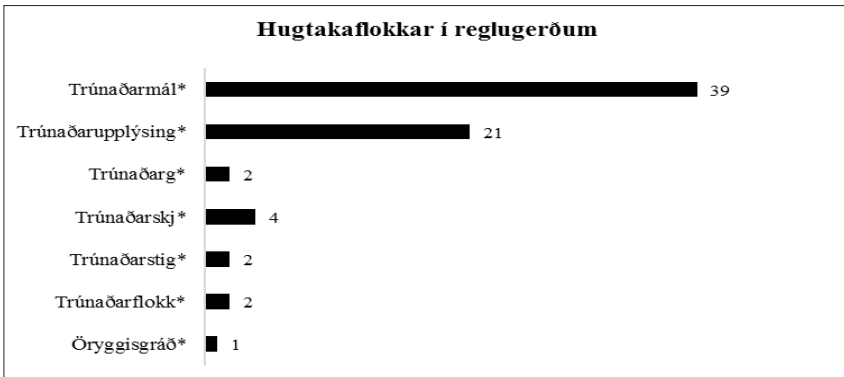
Öryggisgráðun: Birtist einu sinni í einni reglugerð.

Trúnaðarhugtökin komu alls 59 sinnum fram í 49 aðskildum lögum í lagasafni Alþingis. Hér er um að ræða lög, sem sett hafa verið eingöngu á grundvelli íslenskrar stjórnsýslu eins og um þingsköp Alþingis, svo og á grundvelli alþjóðasamstarfs til að mynda vegna innleiðingar tilskipana Evrópusambandsins (ESB). Fern lög af 49 flokkuðust síðan undir lögreglumál og/eda varnarmál í efnisorðaflokkun á vef Alþingis. Þó svo að kvaðir um trúnað í einhverri mynd væri að finna í 49 lögum var einungis í tveimur lögum, beinlínis vísað til 18. gr. laga um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, um þagmælsku.

Mynd 1. Tíðni trúnaðarhugtakanna sjö í gildandi lögum. Alls komu fimm af sjö hugtökum 59 sinnum fyrir í 49 lögum.



Mynd 2. Tíðni trúnaðarhugtakanna sjö eins og þau birtast í gildandi reglugerðum. Alls komu öll sjö hugtökin 71 sinni fyrir í 54 reglugerðum.



Ofangreind hugtök, eitt eða fleiri, komu fram alls 71 sinni í 54 aðskildum reglugerðum í reglugerðasafni innanríkisráðuneytisins. Það byggir á B deild Stjórnartíðinda. Hugtakið „trúnaðarmál“ var algengast, kom fyrir í 39 reglugerðum, og því næst hugtakið „trúnaðarupplýsingar“ í 21 reglugerð. Eins og í viðvíkjandi lögnum, voru reglugerðirnar settar á grundvelli íslenskrar stjórnarsýslu eingöngu auk alþjóðasamstarfs svo sem í tengslum við Evrópusambandið (ESB) og Atlantshafsbandalagið (NATO).

Hugtakið „öryggisgráðun“ kom aðeins einu sinni fyrir. Það var í reglugerð um greiningardeild ríkislögreglustjóra, nr. 404/2007. Þar segir að skilgreint hlutverk greiningardeildar sé meðal annars að hafa eftirlit með því að „reglum um meðhöndlun öryggisgráðaðra gagna sé fylgt“. Ekki er frekar greint frá hvaða reglum skuli hafa eftirlit með né kom hugtakið „öryggisgráðun“ fram annars staðar í löggjöfinni. Athyglisvert þykir að reglugerð um greiningardeild ríkislögreglustjóra var sett fimm árum fyrir en reglu-

gerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála, nr. 959/2012, tók gildi. Þar er ríkislögreglustjóri skilgreindur sem svokallað öryggisstjórnvald (e. national security authority) sem hefur meðal annars það hlutverk að vera eftirlitsaðili með trúnaðarupplýsingum gagnvart stofnunum sem meðhöndla trúnaðarupplýsingar á grundvelli reglugerðarinnar. Þetta hlutverk er einmitt í höndum greiningardeildar ríkislögreglustjóra (Lögreglan 2017).

Aðeins í einum lögum og tveimur reglugerðum þar sem hugtakið „trúnaðarupplýsingar“ kom fyrir var nánari skilgreining á því hvað eða hvernig trúnaðarupplýsingar flokkast eða hvernig skuli meðhöndla þær. Annars vegar var um að ræða reglugerð um framkvæmd siglingaverndar, nr. 265/2008, en þar er fjórði kafli helgaður meðferð trúnaðarskjala. Hann hefur að geyma fjórar greinar: trúnaður; aðgangur að trúnaðarupplýsingum; móttaka trúnaðarskjala og; geymsla og dreifing trúnaðarskjala. Kröfur eru ekki nákvæmar heldur fremur almennar og vísa fremur til aðgæslu en öryggis við meðferð upplýsinganna. Síðara tilvikið er að finna í reglugerð, nr. 959/2012, um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála sem þegar hefur verið nefnd. Í henni er ítarlega gerð grein fyrir þeim lágmarksöryggisráðstöfunum sem er krafist til meðhöndlunar trúnaðarupplýsinga.

Leitir varðandi þagnarskylduákvæðin skiluðu sér einnig í að minnsta kosti 134 gildandi lögum og 159 gildandi reglugerðum. Hugtakið „trúnaðareid“ kom fyrir í tveimur reglugerðum. Fleiri þagnarskylduákvæði kunna að vera fyrir hendi í lögum og reglugerðum enda ekki um staðlað hugtak að ræða. Þannig skilaði leitin „þagmælsk“ 57 gildandi reglugerðum. Nánari greining var ekki gerð á því hvort um endurtekningu laga og/eða reglugerða var að ræða, til að mynda hvort orðin „þagmælska“ og „þagnareidur“ væri að finna í sömu lögum og/eða reglugerðum. Víst er að hin lagalegu þagnarskylduákvæði eru af ýmsu tagi, ýmist alger í störfum starfsfólksins eða að hluta til. Vöntun á samræmdum orðaforða og stöðlun hugtaka gerði því erfitt um vik að fá nákvæmar heildarniðurstöður.

Hugtök þessi koma nú fyrir í auknum mæli í lögum og reglugerðum. Í bókinni *Upplýsingalögin: Kennslurit frá árinu 1996* segir að þagnarskylduákvæði hefði mátt finna í yfir 70 lögum (Páll Hreinsson 1996). Þremur árum síðar segir í skýrslu um starfsskilyrði stjórnvalda að þagnarskylduákvæði sé að finna í yfir 80 lögum og enn fremur í fleiri reglugerðum (Forsætisráðuneytið 1999). Í umræddum leitum, frá árinu 2016, birtust þagnarskylduákvæðin í ýmis konar formi, í að minnsta kosti 134 gildandi lögum og 159 gildandi reglugerðum.

2. Aðferðafræði

Markmið rannsóknarinnar var að skoða hvernig meðhöndlun trúnaðarupplýsinga væri háttað hjá löggæslustofnunum og löggæslutengdum stofnunum á Íslandi. Þannig náði rannsókn eingöngu til ríkisstofnana en ekki til sveitarstjórnareininga. Þá var tilgangurinn að beina sjónum að skyldum stofnananna og kvöðum varðandi meðferð trúnaðarupplýsinga og hvernig þær náðu að framfylgja þeim. Rannsóknarspurningarnar snérust einkum um:

- Hver geta stofnananna væri til þess að tryggja öryggi trúnaðarupplýsinga.
- Hvernig þekkingu starfsfólks stofnananna á lagaumhverfi um skyldur og trúnað hvað upplýsingar varðar væri háttáð.

Eigindleg aðferðafræði (e. qualitative methodology) var notuð við framkvæmd rannsóknarinnar og hálfstöðluð viðtöl (e. semi structured interviews) tekin við 13 einstaklinga hjá sjö stofnunum. Sú aðferð hentaði vel enda var ætlunin að fanga sjónarmið viðmælenda varðandi rannsóknarsefnið (Helga Jónsdóttir 2013; Hennink, Hutter & Bailey 2011; Silverman 2013). Viðtölin áttu sér stað í febrúar og mars 2016. Stofnanirnar voru ákvarðaðar markvisst (e. purposive sampling) með tilliti til lögbundinna hlutverka. Yfirleitt völdu yfirmenn það starfsfólk sem talað var við (Palys 2008; Þórólfur Þórlindsson & Þorlákur Karlsson 2003). Snjóboltaaðferð (e. snowball sampling) var notuð við val tveggja viðmælenda (Katrín Blöndal & Sigríður Halldórsdóttir 2013). Notast var við „gervinöfn“ til þess að tryggja trúnað og viðmælendur einfaldlega tilgreindir með bókstöfunum A, B, C og svo framvegis (Gorman & Clayton 2005). Helstu og stærstu löggæslustofnanir landsins tóku þátt í rannsókninni og var bæði forstöðumönnum þeirra og viðmælendum heitið nafn- og hlutleysi. Af þeim sökum verður stofnununum ekki gerð frekari skil. Rætt var við sjö sérmenntaða löggæsluaðila og sex borgaralegra starfsmenn, tíu karlmenn og þrjár konur. Meðalstarfsaldur viðmælenda var 18,2 ár.

Rannsóknargögnin voru greind með aðferð grundaðrar kenningar (e. grounded theory). Þá eru kerfisbundin viðmið notuð við söfnun og greiningu gagnanna þannig að setja megi fram kenningar sem grundvallast á gögnunum sjálfum (Charmaz 2014; Glaser & Strauss 1967; Schwandt 2007). Gögnin voru vandlega lesin með hliðsjón af grundarði kenningu og þreföld kóðun (e. coding) eða lykklun notuð. Viðtölin voru síðan þemagreind (Hermann Óskarsson 2000; Saunders, Lewis & Thornhill 2009) og meginþemum sem fram komu voru:

- Trúnaðar- og þagnarskylda.
- Lög og önnur ákvæði.
- Fræðsla og öryggisvitund.

Í niðurstöðuköflunum sem hér fylgja verður gerð grein fyrir efni þemanna.

3. Trúnaðar- og þagnarskylda

Kveðið er á um þagmælsku í 18. grein laga um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, og þagnarskyldan heldur þótt látið sé af störfum. Samkvæmt 136. gr. almennra hegningarlaga, nr. 19/1940, geta brot á þagnarskyldu varðað allt að þriggja ára fangelsi. Hér verður fjallað um niðurstöður viðtalanna og skoðanir viðmælenda á efninu.

3.1 Trúnaðaryfirlýsing og þagnareiður

Viðmælendur allra stofnananna höfðu staðfest þagnarskyldu með undirskrift í upphafi starfsferils. Gildi þagnarskyldu og lögbundins trúnaðar var í fyrirrúmi hjá viðmælendum meðal annars á grundvelli laga um réttindi og skyldur opinberra starfsmanna, nr. 70/1996. Þagnarskyldan var þeim jafnvel ofar í huga en sértækar reglur um meðferð og aðgang að viðkvæmum upplýsingum.

Í viðtölunum mátti greina að upplýsingamiðlun byggðist á gagnkvæmu trausti. Viðmælendur þekktu trúnaðarkvaðir sínar og treystu því enn fremur að samstarfsfólk væri jafnmeðvitað um skyldur sínar og kvaðir og virtist þeim vera eðlislægt að fara með allar upplýsingar sem trúnaðarupplýsingar.

Viðmælendum bar saman um mikilvægi þagmælsku, trausts og trúnaðar í störfum, orðum og gjörðum og komu gildi þessara þátta ítrekað í ljós á öllum stigum viðtalanna. Starfsfólk skrifaði undir þagnareid við ráðningu eins og fyrr greinir. Til dæmis sagði E:

Já þeir þurfa að skrifa undir. Þeir eru upplýstir um það þegar þeir eru ráðnir. Þeir hafa ákveðnar skyldur samkvæmt lögum hvað varðar trúnað. Það stendur í ráðningarsamningnum þeirra.

Hið sama kom fram hjá C: „Fólkið er að vinna í þessum störfum og það veit að það er að vinna með trúnaðarupplýsingar. Almennir starfsmenn undirrita eiðstaf og starfsmenn eru upplýstir um trúnaðarskyldu sem um störf þeirra gildir lögum samkvæmt.“

Þagnarskylduákvæðið kom upp í sambandi við margvísleg málefni og viðmælendur bentu á hversu rík þagnarskyldan væri í öllum daglegum störfum. Í samræmi við gildandi lagaumhverfi um meðferð trúnaðarupplýsinga taldi B meðal annars upp eiðstafinn sem hann skrifaði undir. D sagði: „Það er bara almenn svona þagnarskylda. Síðan erum við náttúrulega bara með hegningarlögin, lög um opinbera starfsmenn um trúnað og þagnarskyldu.“ Áður en starfsfólki á vinnustað F var gefin aðgangsheimild að upplýsingakerfum þurfti það að fylla út þar til gert eyðublað: „Og þar staðfestir fólk að það hafi kynnt sér þær reglur sem gilda um trúnaðarupplýsingar.“ Um lagaleg ákvæði varðandi vernd trúnaðarupplýsinga sagði F:

Maður undirritar heitstaf og þar kemur fram að maður ... þagnarskylda ... er ítrekuð þar. Og það, sem leynt á að fara, eigi að fara leynt, svo að maður upplýsi það ekki ... sú þagnarskylda, hún haldist eftir að maður hættir störfum.

J sagði um kröfur sem gerðar voru til starfsfólks sem veittur var aðgangur að trúnaðarupplýsingum: „Ég held að það sé, þú þarft líka að skrifa undir heitstaf þar.“ Í þessu sambandi nefndi M: „Þú náttúrulega þarft að skrifa upp á heitstaf, allir sem fá aðgang að kerfinu.“ H sagði þegar eftirlit með notkun upplýsinga kom til tals: „Og allir undirrita náttúrulega trúnaðaryfirlýsingu um að vera bara að grauta í þessu á grundvelli starfsins.“

Þá vísaði G til þagnarskyldunnar: „Og ég dett nefnilega alltaf inn í þagnarskyldu-
hlutann. Hann í raun er okkar leiðarljós í trúnaði.“ J lagði áherslu á trúnaðinn:

Ég held að náttúrulega númer eitt, tvö og þrjú er bara heitstafurinn. Það hefur verið hamrað svolítið á því. Allt sem við fáum að vita hér það fer ekkert lengra. Eða, ég held að maður þæli miklu frekar í því en að einhver skrifi *trúnaðarupplýsingar* skilur þú? Það hefur ákveðið gildi held ég.

Dæmi voru um að viðmælendur hefðu undirritað fleiri en einn þagnareið svo sem þegar um var að ræða aukinn aðgang að upplýsingum og/eða að mörgum upplýsingakerfum. Það átti meðal annars við í tilviki M: „Við þurfum þá að skrifa undir aukinn eiðstaf, ... ég man ekki hve ég er oft búinn að skrifa undir einhvern eiðstaf, fleiri en einn.“

3.2 Traust og trúnaður

Þagnarskylduákvæðin komu fram í ýmsum myndum eins og lýst hefur verið en einnig að miðlun viðkvæmra upplýsinga byggði á trausti og trúnaði. Viðmælendur vitnuðu í þær kröfur, sem til þeirra voru gerðar við framkvæmd starfa, og á þeim mátti heyra að þeir gerðu sjálfir sömu kröfur til samstarfsfólksins. D ræddi kröfurnar um trúnað og traust þegar hann var spurður út í auðkenningu upplýsinga:

Menn eru bara ráðnir hingað inn sem opinberir starfsmenn og á þeim hvílir mikill trúnaður ... og menn eru ráðnir í [starfsstöð] með það fyrir augum að þeir mega ekki segja frá því sem er að gerast. Þannig að meginreglan er að menn geti gengið út frá því í okkar starfi að þær upplýsingar sem þú færð, það er bara trúnaður sem hvílir á þessum gögnum.

J var spurður hvort hann teldi að nægjanleg úrræði væru fyrir hendi um að vernda öryggi upplýsinga. Í því samhengi vísaði hann í gagnkvæmt traust starfsfólks: „Eins langt og það nær. Ég bara treysti samstarfsfélögunum ... þeir eiga að vita nákvæmlega eins og ég að þetta er trúnaðarmál.“ Og einnig: „Maður bara treystir. Maður er alltaf með sama fólkinu.“ I hafði þetta um læsingar mála að segja: „Mennirnir eru náttúrulega bundnir trúnaði hvort sem er.“

4. Lög og önnur ákvæði

Allir viðmælendur voru bundnir þagnareið í samræmi við lög um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, eins og fyrr segir. Auk þess unnu þeir samkvæmt sér-
lögum og reglugerðum svo og öðrum reglum sem kveða sérstaklega á um þagmælsku og trúnað.

Reglugerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála, nr. 959/2012, gildir meðal annars um aðgang að trúnaðar-

upplýsingum, sem miðlað er á grundvelli alþjóðasamninga, milli Íslands og Atlantshafsbandalagsins (NATO) annars vegar og Evrópusambandsins (ESB) hins vegar. Þannig falla margvísleg stjórnsýsluverkefni og upplýsingamiðlun hérlandis undir reglugerðina. Þá er ekki einungis um að ræða varnartengd verkefni heldur einnig verkefni sem unnin eru á grundvelli ESB-samstarfsins. Þar á meðal eru verkefni og upplýsingamiðlun tengd Evrópulögreglunni (Europol). Í reglugerðinni eru settar fram lágmarkskröfur um öryggisráðstafanir sem varða til dæmis aðgangshemildir, vinnslu, vistun og varðveislu upplýsinga.

4.1 Lög og reglur

Allir viðmælendur voru spurðir um þau lög og reglur sem tengdust meðferð trúnaðarupplýsinga og þeim bar að hlíta. A nefndi að hann þekkti einna helst til þeirra reglna sem vörðuðu sérverkefni hans:

Já, ég þekki best [X] og þar gilda reglur sem eru skýrar, sem við höfum nýtt okkur aðeins. Svo verð ég bara að viðurkenna að ég þekki ekki bara nógu vel íslensk lög og reglur um trúnaðarupplýsingar.

B vísaði í reglur um notkun tölvupósts opinberra starfsmanna og eiðstafinn. H vísaði í sömu reglur svo og lög um meðferð sakamála. C kvað þagnarskylduákvæði vera í þeim sérlögum sem stofnun hans starfaði eftir og sagði enn fremur: „Síðan eru það bara persónuverndarlögin, upplýsingalögin, stjórnsýslulög og já, þessi lög sem við þurfum að gæta vel að.“ D sagði um lagaumhverfi vinnustaðar síns:

Já, það er þetta sem gildir um flestar þessar stofnanir fyrst og fremst upplýsingalögin ... meginreglan um það að gögn eru háð upplýsingarétti nema takmarkanir eigi við. Svo eru lög um meðferð persónuupplýsinga almennt. Það er almenn þagnarskylda ... [og] með hegningarlögin, um opinbera starfsmenn um trúnað og þagnarskyldu.

F vísaði meðal annars í lögreglulögin, lög um réttindi og skyldur starfsmanna ríkisins og persónuverndarlögin. Slíkt hið sama gerði I auk sakamála. J lagði aðaláherslu á heitstafinn og K á persónuverndarlögin.

Viðmælendur voru þannig meðvitaðir um að þeir störfuðu samkvæmt lögum sem kváðu á um tiltekna meðferð persónuupplýsinga og þagnarskyldu. Þeir voru almennt sammála um að fyrirliggjandi lagaumhverfi og regluverk væri nægjanlegt.

E áleit að í reynd væri varla hægt að hafa nákvæmar, staðlaðar verklagsreglur um meðferð upplýsinga. Fjölbreytt verkefni stofnunarinnar gerðu það illmögulegt:

Ef við værum með svona dags daglega afgreiðslu þar sem við værum bara alltaf með sömu erindin, með sömu verklagsreglum þá væri þetta kannski tiltölulega þægilegt og einfalt, að binda þetta niður í einhvers konar verklagsreglu. En, við erum bara alls ekki með þannig. Þetta

er ólíkt og aldrei eins. En við erum auðvitað búin að marka okkur ákveðna grunnlínu. Það er ekki þannig að þetta sé alltaf eitthvað sem kemur okkur í opna skjöldu í hvert skipti, heldur erum við með ákveðna grunnlínu sem við erum búin að marka okkur.

I var heldur afdráttarlausari í svörum: „Mér finnst þetta bara alveg vera skýrt.“ H var honum sammála: „Þetta er náttúrulega bara tiltölulega lítil eining, við erum bara ekkert að flækja þetta.“ F sagði:

Nei, ég er algjörlega sáttur við þetta kerfi eins og það er. Það er bara þetta þagnarskylduákvæði og það sem lögreglan er með. Það á að fara leynt. Og kannski er þetta líka bara eitthvað sem hefur heppnast vel í menntun lögreglumanna. Kannski er þetta hluti af menningunni í lögreglunni að það hefur heppnast vel.

Þó svo að viðmælendur teldu að regluverkið um meðferð viðkvæmra upplýsinga væri nokkuð skýrt komu fram atriði sem þeir álitu að mættu betur fara. M nefndi að hann vildi sjá skýrari reglur um meðferð viðkvæmra upplýsinga: „Það er ekki spurning. Ekki flóknar en stuttar og skorinorðar. Bara svona er þetta, punktur.“ L vildi einnig að skerpt yrði á þessum reglum: „Það bara veitir líka öryggi að hafa eitthvað ... þú átt að gera þetta svona og þú átt að fara svona með gögnin.“

D taldi hindranir við meðhöndlun viðkvæmra upplýsinga ekki aftra samstarfsfólki mikið: „Ekki beint íþyngjandi eða aftrandi heldur einhvern veginn bara laga menn sig eftir því umhverfi sem þeir eru í hverju sinni.“ Undir það tók I: „Nei ég meina, þetta er lögreglan, þú sækir um vinnu hérna og þú bara gengur inn í þær leikreglur sem gilda.“ G svaraði til um hindranir í regluverkinu á eftirfarandi hátt:

Ég hugsa já, það eru mannlegu þröskuldarnir eru meiri heldur en kannski ... Lög og reglur eru settar þannig að það er hægt að túlka það á mismunandi hátt og fara í allar áttir með það. Það er bara það umhverfi sem við vinnum við.

C áleit að skerpa mætti á kerfisbundinni söfnum persónuupplýsinga í sérlögum:

Ef við hefðum það þá væri þetta bara gangsaerra. Við erum með heimildirnar í persónuverndarlögum en það væri bara skýrara fyrir alla ef þetta væri í okkar sérlögum. Maður veltir fyrir sér hvort að það sé eðlilegt að það taki lögfræðinga langan tíma að plægja sig í gegn og skilja hvernig þetta virkar. Á þetta ekki bara að vera gegnsætt þannig að borgarinn geti líka séð í lögum að þetta séu heimildirnar sem [X] hefur? Það er eðlilegra að mínu mati.

Aðrir viðmælendur tiltóku minniháttar vanda sem orsakaðist af regluverkinu um meðferð viðkvæmra upplýsinga. F sagði: „Já, það eru ákveðnar hindranir kannski sem að segja okkur það að þetta sé svona meira tímafaktor.“ K var sömu skoðunar: „Nei, þetta bara hægir á, já, gerir okkur ekki eins auðvelt fyrir.“

4.2 Hefðir og skynsemishyggja

Viðmælendur svöruðu því játandi þegar þeir voru spurðir um hvort reglur væru til um framkvæmd verkefna og meðhöndlun tiltekinna upplýsinga. Þeim var þó í mörgum tilvikum ekki kunnugt um að skriflegar reglur væru fyrir hendi og vísuðu þá gjarnan til hefða og almennrar skynsemi. L sagði um ytra öryggi og trúnaðarupplýsingar að ákveðnar reglur giltu en bætti við: „Svo eru náttúrulega ákveðnar reglur sem mannskapurinn hefur sett sér og þú hefur sett þér sjálfur persónulega.“ L taldi að ekki væri að finna reglur um framkvæmd á aðgangsstýringu í upplýsingakerfum: „Ég held að það sé bara frekar venja.“

Þegar boðsendingar gagna komu til tals sagði M starfsfólk vinnustaðarins alltaf sinna þeim: „Það hefur alltaf tíðkast, ég hef nú aldrei séð reglur um það.“ Og um boðsendingar sagði B: „Ég hef aldrei séð þær reglur, nei.“ M vísaði jafnframt til þess að reynslan hefði einkum kennt honum að meðhöndla viðkvæmar upplýsingar:

Fræðslan er bara engin ... ég hef aldrei þurft að, aldrei verið kynnt fyrir mér hvað ég á að gera við skjöl, svona þegar maður var almennur lög-reglumadur. Það má segja að það lærðist ... bara, vissi að þetta voru viðkvæmar upplýsingar.

Meðal viðmælenda mátti greina að þrátt fyrir að lög, reglugerðir og í sumum tilvikum innanhússreglur giltu um meðferð upplýsinga var hvergi fjallað um nákvæma framkvæmd öryggisráðstafana. Svörin voru ekki jafnskýr þegar spurningar beindust að reglum um ákveðna og nákvæmari meðferð upplýsinganna.

Viðmælendur voru spurðir út í reglur um meðferð upplýsinga í snjallsímum. Í því sambandi svaraði L: „Nei það eru engar reglur um það. Ég fékk engin fyrirmæli eða það voru engar reglur settar. Það er bara held ég persónubundið. Ég alla vega sá ekki neinar reglur eða neitt.“ Og G sagði: „Það er ekkert sagt, ég megi ekki opna viðkvæman tölvupóst í símanum mínum.“ Varðandi þetta sagði I: „Engar almennar reglur um það. Það er bara svona almennar varúðarreglur, passa sig“. M svaraði: „Nei það eru engar reglur um það. Maður passar sig bara að vera ekki með símann opinn og póstin, hvar sem er.“ „Það hafa ekki verið gefnar út stífar reglur um hvernig megi nota tölvupósta,“ sagði F.

5. Fræðsla og öryggisvitund

Fjórir af 13 viðmælendum sögðu formlega fræðslu vera fyrir hendi á sinni starfsstöð. Hún varðaði þó ekki ávallt og beint meðferð trúnaðarupplýsinga fremur meðferð upplýsinga almennt svo og upplýsingakerfa. Á starfsstöð E voru námskeið haldin reglulega:

Við höldum námskeið fyrir starfsmenn til að fara yfir það hvað það þýðir að vera starfsmaður [starfsstöð]. Hvaða reglum og skyldum þér ber að fara eftir og þar auðvitað er komið inn á trúnaðinn og heimildir okkar til að veita upplýsingar og hverjir þá hafa þær heimildir.

K útskýrði eftirfarandi: „Það er farið yfir þetta með nýjum starfsmönnum ... svona fyrirlestur bara fyrir nýliðana hjá okkur þannig að ég hef ekki fengið þetta. En eins og ég segi ég hef ekki fengið þessa fræðslu þannig að ég hef ekki hugmynd um það.“

F nefndi varðandi sína starfsstöð: „Við vorum með nýliðanámskeið, stór námskeið varðandi meðhöndlun rannsóknarupplýsinga og uppbyggingu rannsókna. Það hefur ekki verið nein svona skyldufræðsla undanfarin ár.“ Að sögn C var reglulega haldin fræðsla fyrir nýja starfsmenn á hans vinnustað:

Í henni er lögð áhersla á að fólk kynni sér réttindi og skyldur opinberra starfsmanna og rætt um þá ábyrgð sem fylgir því að starfa hjá opinberu embætti og meðhöndla þau gögn sem unnið er með. Stefnt er að því að auka áhersluna á þennan þátt og verður tekið tillit til þess í endurskoðun á fræðslu fyrir nýliða. Hvort að það sé sí- og endurmenntun á því sviði? Ég hef svo sem ekki sérstaklega orðið var við það.

C sagði einnig: „Svo eru [starfsheiti], þeir fara í [X] og þá er farið mjög ítarlega yfir starfsheimildirnar, hvað þeir mega og hvað þeir mega ekki og farið yfir lögfræðina. Þar er farið meðal annars yfir upplýsingalögin og persónuverndarlögin.“ Viðmælandi A sagði:

Til dæmis í [upplýsingakerfi] þá hefur verið gerð krafa um námskeið. Það er mjög mikilvægt að þjálfari eða kennari fer yfir þessi málefni, að allir eru kunnugir um reglurnar sem gilda hjá [X] um þær. En með annað er þetta nánast villta vestrið. Sem þýðir að það sé ekki beint fræðsla í boðið að það er engin formleg kennsla. Við hefjum störf í deildinni, menn læra bara með því að sitja hjá einhverjum öðrum og sjá þá vinna. Og svo þegar það kemur eitthvað upp á það er það bara, þá er það leyst bara svona ad-hoc einhvern veginn.

A sagði um þá nýliðafræðslu sem hann sjálfur fékk: „Frá byrjun man ég bara að, mér var kynnt einhverjar reglur um lög og ég undirritaði eitthvert skjal.“ A var einnig í hópi þriggja viðmælanda sem kváðust hafa fengið sérstaka fræðslu um meðferð trúnaðarupplýsinga.

Og þessi kynning var líklega þá eitthvað að frumkvæði [yfirmaður]. Það var ekki skipulagt og fast. Og mér þætti það alveg mega vera þannig. Að það væru kannski reglulegir, áminningar um hvernig þetta er og svoleiðis.

Sömu fræðslu hafði L fengið í tengslum við verkefni sem hann sinnti. Þá fræðslu fengu ekki allir starfsmenn heldur hefði hún verið háð eðli verkefna starfsmannanna og að kröfur væru þar um:

Þegar ég fékk til dæmis [X] þá fékk ég fína fræðslu og hefur svo sem ekki reynt á það ennþá hvort að það sé endurmenntun í því. Það var mjög gott og mín persónulega skoðun er, það var mjög gott og tel að það ætti kannski að vera hjá hverjum starfsmanni einu sinni á ári því þarna vöknudu ýmsar spurningar sem maður fór að velta fyrir sér. Af því að maður á það náttúrulega til, maður er bara mannlegur, að þetta allt verður bara sjálfsagður hlutur.

Aðspurður taldi B sig sáttan við þá fræðslu um meðferð upplýsinga sem nýir starfsmenn fengu á hans starfsstöð: „Við byrjum á að svona fara yfir það helsta og svo er nýr starfsmaður bara látinn hanga í hverri vinnustöð fyrir sig.“ Þá kvað B að framkvæmd símenntunar fælist einnig í því að starfsmenn fræddu hvern annan.

H benti á ábyrgð yfirmanna við að tryggja að starfsmenn væru uppræddir um rétta meðhöndlun upplýsinga og notkun upplýsingakerfa: „Það er engin fræðsla eða símenntun en það er bara ætlast til að yfirmenn, varðstjórar og millistjórnendur og aðrir, að þeir bara hafi þessi mál í lagi, kenni bara viðkomandi á lögreglukerfið.“ Þannig útskýrði G:

Ég held að fræðslan á sér stað í grunnnámi eftir það kannast ég ekki við að það sé fræðsla nema þegar koma upp einhver mál og það fer eitthvað svona haveri í gang, þá kemur umburðarbréf sem segir [X]. Hvort að menn lesi það eða ekki? Nei það er ekki formleg fræðsla.

Viðmælendum bar flestum saman um að fræðsla væri ekki nægjanleg og að hana mætti bæta. Jafnvel þeir sem töldu fræðsluna hafa verið í góðum farvegi gátu þess að þörf væri á símenntun eða upprifjunarnámskeiðum.

D var spurður hvort hann teldi starfsmenn almennt meðvitaða um persónulega ábyrgð sína við meðhöndlun trúnaðarupplýsinga: „Þess vegna er þessi fræðsla og annað náttúrulega bara mikilvæg. Og halda hana kannski þá ört og til þess að það síust smám saman inn. Kannski til þeirra sem ekki hafa áttað sig á því að hver ábyrgðin er og hvar hún liggur.“ Sömu spurningu svaraði K: „Kannski vantar þessa fræðslu eða að þetta sé til á pappír.“

Að lokum vék E tali að eflingu faglegrar menntunar og fagskóla löggæsluáðila og sagði:

Það væri auðvitað skynsamlegast í staðinn fyrir að lögreglan væri að reka sinn sér og Tollurinn sér og Landhelgisgæslan sér og fangelsin sér, að þetta væri bara einn skóli ... Það er mín skoðun að minnsta kosti. Það er svo margt sem á við á öllum þessum stöðum sem ætti að hafa mun öflugra með því að hafa þetta sameiginlegt.

6. Umræður og samantekt

Hér að framan hefur verið gerð grein fyrir helstu niðurstöðum rannsóknar um meðferð trúnaðarupplýsinga hjá íslenskum löggæslu- og löggæslutengdum stofnunum. Tilgangur rannsóknarinnar var að skoða hvernig meðferð trúnaðarupplýsinga væri háttað meðal þessara stofnana, lagalegar kvaðir og framkvæmd þeirra. Nú verður sett fram samantekt um niðurstöður og ályktanir dregnar af þeim.

6.1 Trúnaðar og þagnarskylda

Trúnaðar- og þagnarskylda hvílir á öllum ríkisstarfsmönnum samkvæmt 18. grein laga um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, og enn fremur eru ákvæði í hinum ýmsu sérlögum og reglugerðum þar sem trúnaður er áréttaður. Samkvæmt 136. gr. almennra hegningarlaga, nr. 19/1940, geta brot á þagnarskyldu varðað allt að þriggja ára fangelsi.

Hjá viðmælendum mátti greina að þeir höfðu lagalegar kvaðir um trúnað og þagnarskyldu í heidri þegar kom að meðferð upplýsinga. Þeir höfðu trúnaðaryfirlýsingar og heit í hávegum og vísuðu gjarnan til stöðu ríkisstarfsmanna og ábyrgðar þeirra í sambandi við lögbundna þagmælsku. Viðmælendur tiltóku hversu algild þagnarskyldan væri í öllum daglegum störfum og trúnaður og traust ríkti meðal starfsfólks þegar að miðlun og meðferð upplýsinga kæmi. Má þannig ætla á viðtölunum að þagnarskylduákvæðin gegni veigamiklu, jafnvel meginhlutverki starfsmanna við meðhöndlun og miðlun upplýsinga.

Allir viðmælendur höfðu staðfest þagnarskyldu í upphafi starfa. Gildi þagnarskyldu og lögbundins trúnaðar, meðal annars á grundvelli laga um réttindi og skyldur opinberra starfsmanna, nr. 70/1996, var í forgangi hjá viðmælendum og var þeim jafnvel ofar í huga en sértækar reglur um meðhöndlun og aðgengi að viðkvæmum upplýsingum. Í ljósi lögbundinnar trúnaðar-, þagnar- og hollustuskyldu jöfnuðu viðmælendur gjarnan ákvæðunum við reglur um aðgangsstýringu og aðrar öryggisráðstafanir. Viðmælendur álitu þannig margir að þagnarskyldan uppfyllti þær kröfur, sem æskilegt þætti að starfsfólki sem færi með viðkvæmar upplýsingar, væru settar – að á grundvelli hennar væri starfsfólki settur skýr rammi um meðhöndlun upplýsinganna. Fróðlegt verður að sjá hvað áhrif fyrirhugaðar breytingar á þagnarskylduákvæðinu (Forsætisráðuneytið 2013) kunna að hafa á gildi þagnarskyldunnar í framtíðinni ef af þeim verður. Starfsmenn löggæslustofnana meðhöndla ýmiskonar viðkvæmar upplýsingar, allt frá upplýsingum sem varða almannaheill og öryggisþætti varðandi mikilvæga innviði landsins, til persónuupplýsinga svo að eitthvað sé nefnt. Þá ber einnig að hafa í huga að löggæsluaðilar fara með öryggis- og varnarmál hér á landi. Þannig eiga bæði skilgreiningar á leynd og friðhelgi við (Bok 1989; Pozen 2010; Martin, Bray & Kumar 2015; Scheppele 2015) þegar kemur að meðhöndlun löggæsluáðila á upplýsingum sem taka þarf tillit til við snið regluverks um þessa sameiginlegu en ólíku þætti.

Ósamræmi og hugtakaflokt í lagaverkinu, sem tengjast trúnaðarhugtökunum, mun verða ríkjandi við meðhöndlun trúnaðarupplýsinga í stjórnsýslunni á meðan kerfisbundnar og staðlaðar reglur eru ekki fyrir hendi.

Fram kom hjá viðmælendum að upplýsingamiðlun byggði á gagnkvæmu trausti. Þeir

voru meðvitaðir um trúnaðarkvaðir og treystu því jafnframt að samstarfsfólk væri jafnmeðvitað um sínar kvaðir og skyldur. Viðmælendum virtist vera eðlislægt að fara með allar upplýsingar sem trúnaðarupplýsingar og höfðu jafnvel hvorki leitt hugann að því né haft skoðun á því hvort þörf væri fyrir sérstakt regluverk um meðhöndlun upplýsinga.

6.2 Lög og önnur ákvæði

Viðmælendur störfuðu allir á einhvern hátt undir sameiginlegum lögum um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000, auk sérлага og reglugerða varðandi starfsemina. Þeir voru ekki á eitt sáttir um hvort gildandi lög og reglur væru nægjanlegar eða þörfnuðust breytinga. Margir þeirra töldu þó að regluverkið gagnaðist fjölbreyttum starfsvettvangi þeirra vel, að verkefnið rúmuðust vel innan lagarammans og frekari skorður þyrfti ekki. Aðrir töldu að nánari umgjörð skorti. Fram kom að hefðir og venjur hefðu í gegnum tíðina mótað tilteknar starfsaðferðir við dagleg störf fremur en að fyrirfram skilgreindar reglur giltu um þær.

Viðmælendur voru allir meðvitaðir um að meðhöndlun upplýsinga, sem þeir unnu með, væri háð takmörkunum þótt ekki væru til staðar lög eða reglugerðir í íslenski stjórnarsýslu sem fjölluðu beinlínis um meðferð trúnaðarupplýsinga. Slíkir starfshættir fara í bága við rannsóknir sem sýna fram á mikilvægi þess að allt starfsfólk, sem meðhöndlar viðkvæmar persónuupplýsingar, starfi samkvæmt sömu lögum/reglum og leggi sama skilning í regluverkið (Ferraiolo & Kuhn 1992; Warkentin o.fl. 2011). Almenn þekktu viðmælendur þó til þeirra grundvallarlaga og regna sem kveða á um ákveðna meðferð persónuupplýsinga. Þá voru þeir meðvitaðir um eigin kvaðir um þagnarskyldu eins og lög um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996, lög um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000 og upplýsingalaga, nr. 40/2012, segja til um.

Fram hefur komið að skiptar skoðanir voru á því hvort regluumhverfið væri fullnægjandi eða ekki. Þeir, sem töldu þörf fyrir frekari reglur, nefndu flestir að samræmdar reglur um merkingar upplýsinga skorti eða að vöntun væri á reglum sem skilyrtu notkun og dreifingu upplýsinga. Þessir viðmælendur álitu að vissu öryggi fælist í skýrum ramma um meðhöndlun upplýsinga og því að hægt væri að skilyrða hverjum upplýsingarnar væru ætlaðar og í hvaða tilgangi. Aðrir töldu regluverkið skýrt og óþarft að setja frekari reglur. Þá kom fram að í ljósi þess hversu fjölbreytt og ólík verkefni væru yrði erfitt að setja stífan ramma um framkvæmdina.

Kerfisbundin og stöðluð meðferð viðkvæmra upplýsinga er tiltölulega nýtt fyrirbrigði á Íslandi. Ólíkt aldalangri reynslu hernaðarþjóða af flokkunarkerfi trúnaðarupplýsinga, líkt og Relyea (2008) greindi frá, er fyrsta hérlenda sértæka reglugerðin, sem kveður á um slíkt, eingöngu frá árinu 2012. Sú reglugerð varðar öryggis- og varnarmál og hefur henni þegar verið lýst. Ákvæði af einhverju tagi er að finna um meðhöndlun viðkvæmra upplýsinga í íslenskum stjórnarsýslurétti til dæmis í upplýsingalögum, nr. 40/2012, lögum um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000, sér-lögum og reglugerðum. Lög þessi og reglugerðir taka þó einungis á rétti til söfnunar og miðlunar upplýsinga, hvaða upplýsingum megi safna og í hvaða tilgangi svo og aðgangs almennings að upplýsingum hins opinbera en ekki beinlínis til öryggisráðstafana um

að vernda trúnaðarupplýsingar, aðgangsstýringar, kröfur til starfsmanna sem þær meðhöndla og svo framvegis.

Sameiginlegt regluverk um trúnaðarupplýsingar og kerfisbundna meðferð og merkingu þeirra er ekki fyrir hendi, að undanskilyldum reglum sem snerta erlent samstarf á grundvelli öryggis- og varnarmála. Af þeim sökum gátu þær stofnanir, sem þó trúnaðarmerktu upplýsingar, ekki tryggt að móttakandi utan stofnunarinnar meðhöndlaði þær í samræmi við það. Rannsókn Ferraiolo og Khun (1992) sýndi einmitt fram á að borgaralegar stofnanir þurfi að vernda og tryggja upplýsingar á skipulegan og samræmdan hátt. Einnig var algengt að viðmælendur vísuðu í viðtekið verklag, hefðir og venjur þegar reglur um tilteknar aðgerðir eða verkefni voru rædd. Þar má aftur benda á að slíkt er andstætt rannsóknnum sem sýnt hafa fram á nauðsyn samræmingar og þess að starfsfólk hafi sama skilning á þeim reglum sem gilda (Ferraiolo & Kuhn 1992; Warkentin o.fl. 2011). Því má velta fyrir sér hvers vegna ekki hefur verið talin þörf fyrir sérstakt íslenskt regluverk um meðferð upplýsinga. Einkum þar sem þess er krafist í samskiptum við erlendar stofnanir og ríki, sem hafa langa reynslu af slíku regluverki, en þar þykir slíkt vera grundvallaratriði og gera kröfu til þessa við gagnkvæma miðlun viðkvæmra upplýsinga við íslensk stjórnvöld.

Reglugerð, sem gengur þvert á íslenska stjórnslu, með það markmið að tryggja öryggi upplýsinga, meðal annars um kröfur um merkingu, vistun, birtingu og aðgengi að trúnaðarupplýsingum, er ekki til í íslenskri stjórnslu. Slík reglugerð, nr. 959/2012, um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála eingöngu, er hins vegar fyrir hendi. Sambærileg reglugerð, sem nærði til allra málaflokka stjórnslunnar, ætti að geta tryggt samræmda meðferð upplýsinga og að sömu öryggisráðstöfunum yrði beitt við vernd upplýsinga sem stofnanir miðluðu sín á milli. Þá hafa rannsóknir sýnt fram á mikilvægi faglegrar skjalastjórnar í því samhengi (Jóhanna Gunnlaugsdóttir 2015; Jóhanna Gunnlaugsdóttir 2016; Kristín Benediktsdóttir & Trausti Fannar Valsson 2016).

6.3 Fræðsla og öryggisvitund

Fræðsla um meðferð trúnaðarupplýsinga var almennt lítil og voru viðmælendur flestir sammála um að hana mætti efla. Fram kom í rannsókn Warkentin o.fl. (2011) að fræðsla og þjálfun starfsmanna væri grundvallaratriði þegar kæmi að því að tryggja öryggi upplýsinga og virkja starfsmenn til þess að fylgja reglum um upplýsingaöryggi. Þó svo að viðmælendur hefðu fengið fræðslu í sínum sérfögum við löggæslunám eða þjálfun var bakgrunnur borgaralegra starfsmanna misjafn. Þeir meðhöndluðu margir daglega viðkvæmar upplýsingar og ekki tryggt að þeir hefðu þá undirstöðuþekkingu á lögnum sem skipaðir embættismenn eða löggæsluaðilar fengu í sínu námi. Út frá niðurstöðum viðtalanna má því álykta að leggja þurfi ríkari áherslu á fræðslu um meðferð viðkvæmra upplýsinga til handa öllum starfsmönnum. Ekki eingöngu þeirra sem fara með lögregluvald heldur einnig borgaralegra starfsmanna sem meðhöndla upplýsingarnar eða verða áskynja um þær í störfum sínum hjá löggæslustofnunum. Hafa ber í huga að orsakir öryggisrofs geta verið margvíslegar. Þótt starfsmenn séu meðvitaðir um gildandi reglur

geta slysin alltaf átt sér stað og því þarf sífellt að minna fólk á hætturnar. Dhillon (2001) sýndi fram á að öryggisrof starfsmanna ættu sér ekki eingöngu stað vegna ásetnings heldur einnig gáleysis. Enn fremur sýndu niðurstöður rannsóknar Stanton o.fl. (2005) að einföld mistök starfsmanna var ein af fjórum helstu ástæðum þess að öryggisrof ylli stofnunum skaða. Mistök, sem með fræðslu á grundvallarþáttum upplýsingaöryggis, væri auðveldlega hægt að koma í veg fyrir.

Þó svo að fræðsla um meðferð viðkvæmra upplýsinga væri takmörkuð virtist öryggisvitund viðmælenda rík á flestum sviðum. Þeir þekktu ábyrgð sína og skyldur við meðhöndlun upplýsinga. Þá voru flestir meðvitaðir um öryggisráðstafanir í nánasta umhverfi sem hafa bæri í huga við meðferð viðkvæmra upplýsinga. Þeir voru jafnframt meðvitaðir um öryggisveikleika í umhverfi sínu og hvað þeim fannst að betur mætti fara.

7. Lokaorð

Í rannsókninni, sem náði til 13 starfsmanna hjá sjö ríkisstofnunum sem fara með löggæslumál, kom fram að upplýsingaeign löggæslustofnana og löggæslutengdra stofnana var mikil og í ýmsu formi. Upplýsingamiðlun þeirra á meðal var mikilvæg og stór hluti þeirra upplýsinga, sem meðhöndlaðar voru hjá umræddum stofnunum, viðkvæmar trúnaðarupplýsingar.

Af niðurstöðum rannsóknarinnar má draga þá ályktun að ríkisstarfsmenn löggæslu- og löggæslutengdra stofnana séu fullmeðvitaðir um ábyrgð sínar og skyldur hvað þagnarskyldu og trúnað í starfi varðar. Þó má ætla að samræmd lög, reglur og verklag um lágmarksöryggisráðstafanir við meðferð trúnaðarupplýsinga séu ekki fyrir hendi.

Á Íslandi virðist skortur á samræmdum lögum og reglugerðum sem beinlínis og eingöngu fjalla um trúnaðarupplýsingar. Þá er átt við sérstakt regluverk þar sem kveðið er á um lágmarksöryggisráðstafanir og útfærslu á því hvernig vernda beri slíkar upplýsingar sem meðhöndlaðar eru innan stjórnsýslunnar. Þó má geta að stofnanir hafa margar sett sér verklagsreglur sem varða meðferð viðkvæmra upplýsinga á einhvern máta en þær ná ekki út fyrir stofnanirnar og eru því ekki samræmdar meðal ríkisstofnana eins og fram hefur komið. Mikilvægt er að yfirsýn náist yfir málaflokkinn og samræmt kerfi verði eflt sem tryggði rétta og ábyrga meðhöndlun trúnaðarupplýsinganna, þar á meðal viðkvæmra persónuupplýsinga, á öllum stigum. Rannsóknin gæti þannig gagnast sem vitundarvakning og innlegg til frekari umræðu um faglega meðferð þessara upplýsinga innan stjórnsýslunnar. Mikilvægur þáttur í upplýsingaöryggi er fræðsla starfsmanna á öryggismálum og hlítingu öryggisreglna. Ætla má að brot á öryggisreglum megi oft rekja til vanþekkingar starfsmanna á öryggisreglunum og skorti á þekkingu á því af hverju slíkar reglur eru settar. En skaðinn, sem getur hlotist af ótímabærri miðlun eða birtingu upplýsinga, er óháður því hvort birtingin sé gerð af ásetningi eða að um óviljaverk sé að ræða.

Evrópuþingið (e. European Parliament) og Evrópuráðið (e. European Council) samþykktu nýja löggjöf um persónuvernd og meðferð persónuupplýsinga (e. the European Data Protection Law) í apríl 2016. Gildistaka laganna er fyrirhuguð á fyrri hluta árs 2018. Ísland mun þurfa að gildistaka löggjöfina enda aðili að Evrópska efnahagssvæðinu (e. European Economic Area). Þessi nýja löggjöf felur í sér byltingarkenndar breytingar

hvað persónuvernd varðar. Niðurstöður rannsóknarinnar gætu verið upplýsandi í þessu sambandi og þannig auðveldað undirbúninginn að gildistöku þessara nýju laga.

Sambærilegar rannsóknir um meðferð trúnaðarupplýsinga í íslenski stjórnýslyu er ekki til að dreifa. Rannsókn þessi gæti nýst löggæslustofnunum og löggæslutengdum stofnunum svo og stjórnýslunni allri við að öðlast innsýn í umgjörð og meðferð upplýsinganna. Hún gefur jafnframt vísbendingar um reynslu og viðhorf starfsfólks hvað varðar þær viðkvæmu upplýsingar sem þeir meðhöndla og verða áskynja um. Rannsóknin getur enn fremur lagt grunn að þróun innan málaflokksins og grundvöll til frekari rannsókna innan upplýsingafræðinnar.

Heimildir

- Albrechtsen, E. (2007). A qualitative study of users's view on information security. *Computers & Security* 26(4). 276-289.
- Almenn hegningarlög, nr. 19/1940
- Bentham, J. (1843). *The Works of Jeremy Bentham: Exceptions to the rule of publicity*. Sótt af <http://oll.libertyfund.org/titles/bentham-the-works-of-jeremy-bentham-vol-2>
- Bok, S. (1989). *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage Books.
- Charmaz, K. (2014). *Constructing Grounded Theory* (2. útg.) London: Sage Publications.
- Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computer & Security* 20(2), 165-172. Sótt af <http://www.sciencedirect.com/science/article/pii/S0167404801002097>
- Ferraiolo, D.F. og Kuhn, D.R. (1992). Role-based access controls. *15th National Computer Security Conference: Proceedings Volume II*. Sótt af <http://csrc.nist.gov/publications/history/nissc/1992-15th-NCSC-proceedings-vol-2.pdf>
- Forsætisráðuneytið (1999). *Starfsskiðyrði stjórnvalda: Skýrsla nefndar um starfsskiðyrði stjórnvalda, eftirlit með starfsemi þeirra og viðurlög við réttarbrotum í stjórnýslyu*. Sótt af https://www.forsaetisraduneyti.is/media/Skyrslur/F0033_Oll_skor.pdf
- Forsætisráðuneytið (2013). *Drög að frumvarpi til laga um breytingu á stjórnýslyulögum, nr. 38/1993 (þagnar-skýlda)*. Sótt af <https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/frettir2/drog-frumvarp-breyting-a-stjornyslyulogum.pdf>
- Glaser, B.G. og Strauss, A.L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago: Aldine Publishing Company
- Gorman, G.E. og Clayton, P. (2005). *Qualitative research for the information professional: A practical handbook* (2. útg.). London: Facet Publishing
- Gutmann, A. og Thompson, D. (1996) *Democracy and disagreement*. Cambridge, Massachusetts; London: Belknap Press of Harvard University Press.
- Helga Jónsdóttir (2013). „Viðtöl í eiginlegum og megindlegum rannsóknum“, í Sigríður Halldórsdóttir (ritstj.), *Handbók í aðferðafræði rannsókna* (bls. 137-153). Akureyri: Háskólinn á Akureyri.
- Hennink, M., Hutter, I. og Bailey, A. (2011). *Qualitative research methods*. London: Sage Publications.
- Hermann Óskarsson (2000). *Aðferðafræði félagsvísinda: Undirbúningur rannsókna, framkvæmd og skýrslugerð*. Reykjavík: Iðnú.
- Innanríkisráðuneytið (2015). *Stefna í almannavarna- og öryggismálum ríkisins 2015-2017*. Sótt af https://www.innanrikisraduneyti.is/media/blai_bordinn/Almannavarnastefna.pdf
- Jóhanna Gunnlaugsdóttir (2015). “Government Secrecy: Public Attitudes toward Information Provided by the Authorities”, *Records Management Journal* 25(2), 197-222.
- Jóhanna Gunnlaugsdóttir (2016). “Reasons for the Poor Provision of Information by the Government: Public Opinion”, *Records Management Journal* 26(2), 185-205.

- Katrín Blöndal og Sigríður Halldórsdóttir (2013). Úrtök og úrtaksaðferðir í eiginlegum rannsóknum. Í Sigríður Halldórsdóttir (ritstj.). *Handbók í aðferðafræði rannsókna* (bls. 129-136). Akureyri: Áspret.
- Kristín Benediktsdóttir og Trausti Fannar Valsson (2016). Varðveisla gagna í stjórnsýslunni. *Stjórnmál & Stjórnsýsla* 12(2), 321-342. doi:10.13177/irpa.a.2016.12.2.7
- Kristín Guðmundsdóttir (2016). „Því beiti ég og legg við drengskap minn og heidur“: Meðferð trúnaðarupplýsinga í íslenskeri stjórnsýslu. Óbirt MA-ritgerð. Reykjavík: Háskóli Íslands: Félags- og mannvísindadeild.
- Kristín Guðmundsdóttir og Jóhanna Gunnlaugsdóttir (2016). „Meðferð trúnaðarupplýsinga meðal stjórnsýslustofnana: Fræðsla starfsmanna“. Í Helgu Ólafsdóttir og Thamar M. Jeijstra (ritstj.), *Þjóðar-spegillinn XVII: Rannsóknir í félagsvísindum – Félags og mannvísindadeild* (bls. 1-11). Sótt af <http://hdl.handle.net/1946/26384>
- Lög um opinber skjalasöfn, nr. 77/2014
- Lög um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000
- Lög um réttindi og skyldur starfsmanna ríkisins, nr. 70/1996
- Lögreglan (2017, 1. febrúar). Greiningardeild. Sótt af <http://www.logreglan.is/logreglan/rikislogreglu-stjori/skipurit-2/>
- Martin, G., Bray, R.S. og Kumar, M. (2015). Secrecy, Law, and Society. Í Martin, G., Bray, R.S. og Kumar, M (ritstj.), *Secrecy, Law, and Society* (bls. 1-20) Milton Park, Abingdon, Oxon: Routledge.
- Nasu, H. (2015). State secrets law and national security. *The International and Comparative Law Quarterly* 64(2), 365-404. doi:10.1017/S0020589315000056
- Palys, T. (2008). “Purposive Sampling”, í L. M. Given (ritstj.), *The Sage Encyclopedia of Qualitative Research Methods* (bls. 697-698). California: Sage Publication.
- Páll Hreinsson (1996). *Upphýsingalögin: Kennslurit*. Reykjavík: Forsætisráðuneytið.
- Páll Hreinsson (2013). *Stjórnsýsluréttur – málsmeðferð*. Reykjavík: Codex.
- Pozen, D.E. (2010). Deep Secrecy. *Stanford Law Review* 62(2), 257-340. Sótt af <https://www.law.upenn.edu/institutes/cecl/conferences/ethicsofsecrecy/papers/reading/Pozen.pdf>
- Reglugerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála, nr. 959/2012.
- Relyea, H.C. (2008). *Security Classified and Controlled Information*. New York: Nova Science Publishers Inc.
- Saunders, M., Lewis, P. og Thornhill A. (2009). *Research methods for business students* (5. útg.). Essex: Pearson Education Limited.
- Scheppele, K.L. (1988). *Legal Secrets: Equality and Efficiency in the Common Law*. Chicago: The University of Chicago Press.
- Schwandt, T.A. (2007). *The Sage dictionary of qualitative inquiry* (3. útg.). Los Angeles: Sage Publications.
- Silverman, D. (2013). *Doing qualitative research* (4. útg.). London: Sage Publication.
- Sigurður G. Hafstað og Jóhanna Gunnlaugsdóttir (2016). „Hagnýting persónuupplýsinga á Facebook hjá eftirlitsstofnunum“, *Stjórnmál og stjórnsýsla* 12(2), 343-367.
- Stanton, J.M., Stam, K.R., Mastrangelo, P. og Jolton, J. (2005). Analyzis of end user security behaviors. *Computer & Security* 24(2), 124-133. doi:10.1016/j.cose.2004.07.001
- Theoharidou, M., Kokalakis, S., Karyda, M. og Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computer & Security* 24(6), 472-484.
- Trausti Fannar Valsson (2015). Upplýsingaréttur og þagnarskylda. *Stjórnmál og stjórnsýsla* 11(2), 289-312. doi:10.13177/irpa.a.2015.11.2.9
- Upplýsingalög, nr. 140/2012
- Warkentin, M., Johnston, A.C. og Shropshire, J. (2011). *The influence of the informal social learning environment on information privat policy compliance efficacy and intention*. *European Journal of Information Systems* 20(3), 267-284. doi:10.1057/ejis.2010.72
- Þórólfur Þórlindsson og Þorlákur Karlsson (2003). Um úrtök og úrtöksaðferðir. Í Sigríður Halldórsdóttir og Kristján Kristjánsson (ritstj.), *Handbók í aðferðafræði og rannsóknum í heilbrigðisvísindum* (bls. 51-66). Akureyri: Háskólinn á Akureyri.

