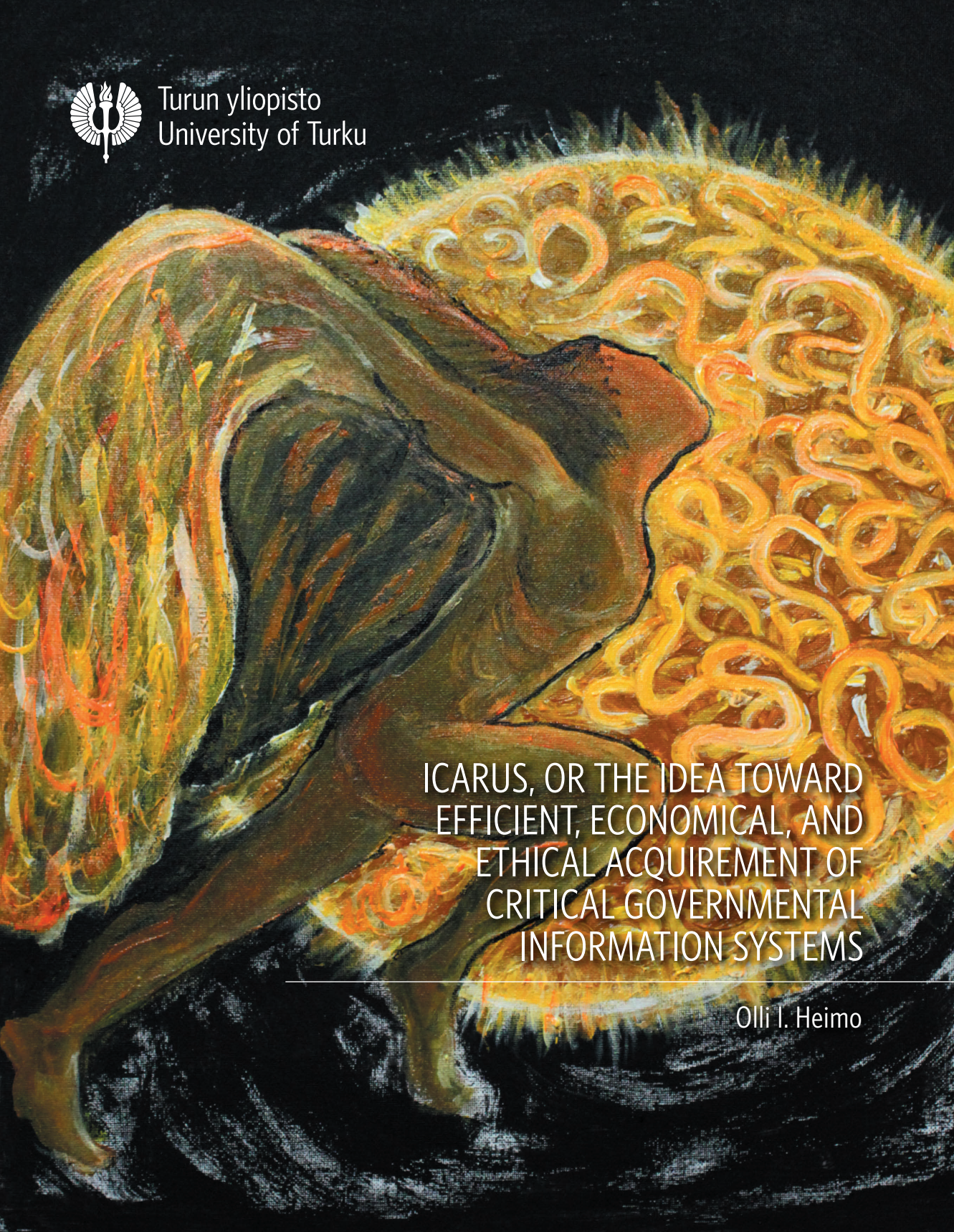
Turun yliopisto
University of Turku



ICARUS, OR THE IDEA TOWARD EFFICIENT, ECONOMICAL, AND ETHICAL ACQUIREMENT OF CRITICAL GOVERNMENTAL INFORMATION SYSTEMS

Olli I. Heimo

TURUN YLIOPISTON JULKAISUJA - ANNALES UNIVERSITATIS TURKUENSIS
Sarja - ser. E osa - tom. 43 | Oeconomica | Turku 2018

Turun yliopisto
University of Turku

ICARUS, OR THE IDEA TOWARD EFFICIENT, ECONOMICAL, AND ETHICAL ACQUIREMENT OF CRITICAL GOVERNMENTAL INFORMATION SYSTEMS

Olli I. Heimo

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
Sarja - ser. E osa - tom. 43 | Oeconomica | Turku 2018

University of Turku

Turku School of Economics
Department of Management and Entrepreneurship
Information Systems Science

Supervised by

Ph. D Kai K. Kimppa
Turku School of Economics

Professor Jukka Heikkilä
Turku School of Economics

Reviewed by

Professor Marty J. Wolf
Bemidji State University

Professor Richard Volkman
Southern Connecticut State University

Custos

Ph. D Kai K. Kimppa
Turku School of Economics

Opponent

Professor Richard Volkman
Southern Connecticut State University

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

Cover painting: Tiina Kimppa

ISBN 978-951-29-7507-5 (PRINT)
ISBN 978-951-29-7508-2 (PDF)
ISSN 2343-3159 (PRINT)
ISSN 2343-3167 (PDF)
Painosalama Oy - Turku, Finland 2018

Sofialle

Ex Ignorantia Ad Sapientiam; Ex Luce Ad Tenebras
—The motto of Miscatonic University

ABSTRACT

Critical governmental information systems are governmental information systems used by the administration to retain information and provide services that enable and safeguard the lives, well-being and security of citizens. These include public healthcare information systems, electronic voting systems, and border control information systems with biometric registers. As the ongoing digitalisation of our society advances, our dependence on information systems, their functionality and security continues to grow and the quality of work done with them increasingly intertwines with the daily lives of citizens. However, it has long been evident that IT projects in public administration are failing. Governmental information system projects often end up being astronomically expensive, unreasonably ineffective and ethically unsustainable. Therefore, much more attention should be paid to the procurement process for these systems.

The reasons for these problems are manifold. Often, simple political motivations and appeal to, among other things, national pride, are a simple way for politicians to attain support. The creation of large-scale system entities favours large-scale private-sector actors specialised on governmental information systems. These companies' impact on society's decision-making and operations should not be underrated. However, the lack of understanding of technology and socio-technical problems and the structure of the digitalisation in society are likely to be the biggest problems in procuring these systems. It must be understood that organisational behaviour changes when its information systems are changed - including the ethical basis.

To develop efficient, economical and ethical governmental information systems, a holistic approach is required. The ability to make decisions that take into account the needs and requirements of the citizens, employees, system vendors, and society at large in an ethically sustainable way is required. It should be noted that the decision makers, payers, suppliers, and the targets of the use are often different parties with their own desires, goals, and objectives. It is necessary to understand the functioning of the technology and its potential, but also to address the limitations of technology and potential threats created by it. The security required for these systems should not be diminished.

This dissertation is framed in the light of Ovid’s telling of the myth of Daedalus and Icarus and through the framework for Aristotle's virtue ethics to examine the responsibility of governmental information system procurement, the role of responsible actors in society, and their required capabilities. The dissertation demonstrates that the current approach in many situations, *the Icarian method*, whereby persons committed their lives to the virtue of scientific knowledge are dismissed on discussion and decision-making in a way that is economically, effectively and ethically unsustainable. The antithesis for this, *the Daedalus effect*, represents a desirable state where decision-making is guided by caution, as well as by scientific and ethical inspiration. The dissertation proposes that critical governmental information systems should be guided by a prominent actor cultivated to the virtue of holistic scientific wisdom.

TIIVISTELMÄ

Julkishallinnon kriittiset tietojärjestelmät ovat tietojärjestelmiä, joita hallinto käyttää säilyttämään tietoa sekä tuottamaan kansalaisten henkeä, hyvinvointia ja turvallisuutta mahdollistavia palveluita. Näihin järjestelmiin lukeutuvat muun muassa julkisen terveydenhuollon tietojärjestelmät, sähköiset äänestysjärjestelmät sekä rajavalvonnan tietojärjestelmät biometrisine tunnisterekistereineen. Yhteiskunnan digitalisoituessa riippuvuutemme tieto-järjestelmistä sekä niiden toimivuudesta ja turvallisuudesta jatkaa kasvamistaan ja näiden järjestelmien avulla suoritetun työn laatu on yhä tiukemmassa vuorovaikutussuhteessa kansalaisten jokapäiväiseen elämään.

On kuitenkin ollut ilmiselvää jo pitkään, että julkishallinnon IT-hankkeet epäonnistuvat taajaan. Julkishallinnon tietojärjestelmähankkeet ovat usein tähtitieteellisen kalliita, kohtuuttoman tehottomia ja eettisesti kestämättömiä. Siksi näiden järjestelmien hankintaprosessiin olisi syytä kiinnittää nykyistä selvästi enemmän huomiota.

Syyt näihin ongelmiin ovat moninaiset. Usein jo yksinkertaiset poliittiset motivaatiot sekä vetoaminen muun muassa kansalliseen ylpeyteen ovat poliitikolle yksinkertainen keino saavuttaa kannatusta. Suurikokoisten järjestelmäkokonaisuuksien tekeminen suosii julkishallinnon järjestelmähankintoihin keskittyneitä suuryrityksiä, joiden vaikutusta yhteiskunnalliseen päätöksentekoon ja toimintaan ei sovi väheksyä. Kuitenkin ymmärtämättömyys teknologiasta ja sosio-teknisistä ongelmista sekä digitali-soituvan yhteiskunnan rakenteista lienee suurimpia ongelmia järjestelmien hankinnassa. On otettava huomioon, että yhteisön toiminta muuttuu, kun sen tietojärjestelmiä muutetaan – myös eettisen toiminnan osalta.

Luodaksemme tehokkaita, taloudellisia ja eettisesti kestäviä tietojärjestelmiä julkishallinnon käyttöön on asiaa lähestyttävä kokonaisvaltaisesti. On osattava tehdä päätöksiä, joissa otetaan huomioon kansalaisten, työntekijöiden, järjestelmien toimittajien sekä yhteiskunnan tarpeet ja vaatimukset eettisesti kestävällä tavalla. On huomattava, että päättäjä, maksaja, toimittaja ja käytön kohde ovat kovin usein eri tahoja omine toiveineen, tavoitteineen ja päämäärineen. On ymmärrettävä teknologian toiminta ja sen luomat mahdollisuudet mutta myös käsitettävä

teknologian rajoitukset ja sen luomat uhat. Myöskään tietoturvan tarvetta näiden järjestelmien kohdalla ei sovi vähätellä.

Väitöskirjassa käsitellään Ovidiuksen kertoman Daedaluksen ja Ikaroksen myytin kautta Aristoteelisen hyve-etiikan viitekehyksessä julkishallinnon tietojärjestelmätilausten vastuuta sekä vastuuhenkilöitä, vastuuhenkilöiden asemaa yhteiskunnassa ja heiltä vaadittavia kykyjä. Väitöskirjassa osoitetaan, että monessa tilanteessa esiintyvä julkishallinnon toimintatapa, *Ikaroslainen metodi*, jossa tiedon hyveillä varustautuneet henkilöt sivutetaan keskustelusta ja päätöksenteosta on niin taloudellisesti, tehokkuudellisesti kuin eettisestikin kestämätön toimintatapa. Tämän vastavoima, *Daedalus-efekti*, taas edustaa tavoitetilaa, jossa päätöksentekoa ohjaavat varovaisuus sekä tieteen ja moraalifilosofian inspiroima toiminta. Väitöskirjassa esitetään, että julkishallinnon tietojärjestelmätoimintaa pitäisi ohjata laaja-alaisen tieteellisen viisauden hyveen kultivoinut näkyvä toimija.

ACKNOWLEDGMENTS

This work would not have been possible without the support from numerous people and organisations. First I must express my deep gratitude towards my supervisors, Dr. Kai K. Kimppa and Professor Jukka 'Jups' Heikkilä. Kai, you gave me the possibility and the tools to make this happen. You have been a mentor, teacher, colleague, and a dear friend during this process. May our friendship and collaboration continue and ever strengthen. Jups, you have enabled me to have scientific freedom and possibilities to write the thesis as I see best as well as made me feel that my work is appreciated. Thank you both for your invaluable help! I also want to give my most sincere thanks to both my pre-examiners, Professor Marty J. Wolf and Professor Richard Volkman for their invaluable contributions as reviewers of this thesis. Your comments improved this thesis to a significant extent. I also look forward as having Professor Volkman as my opponent as I assume the defence will be a strict but an interesting contest.

I am thankful for all the co-authors of the original papers, N. Ben Fairweather, Antti Hakkala, Ville Kainu, Jani Koskinen, Kai K. Kimppa, and Professor emeritus Markku I. Nurminen. Ben, I want to thank you for your invaluable contribution to my first (!) article and your guidance as well as your friendship along the years. Antti, we have been through a lot together and the academic careers are just one of many aspects of our friendship and I want to thank you for all the good things you have brought to my life. You are a perfect combination of a friend and a colleague. Ville, it has been an honour to work with you and spend time with you. Your sharp mind and wits have made many discussions as well as writing papers very pleasant and interesting. Jani, thank you for being there all the times I have needed wisdom, guidance, and help. Co-authoring papers as well as collaborating with you has been a pleasure and I wish to keep the good work going. Kai, thank you again. Thank you for being the best man possible for supervising this thesis as well as co-authoring articles with me. Thank you for being there when I have had the dark moments with this thesis. Most of all, thank you for knowing when to be a supervisor, when to be a colleague, and when to be a true friend, for you have succeeded there like no other can. Markku, I want to express my gratitude helping us younger scientists to find the joy of doing

science. Working and discussing with you has always been an educative moment made joy. Your method of sharing wisdom, conversing, and guiding others is a rare and precious talent indeed. It has been an honour to work with all of you.

I am also thankful all my colleagues in the departments of Management and Entrepreneurship, Future Technology, former TRC, and former IT. Thank you, Professor Ari Paasio, Professor Timo Knuutila, Professor Jukka Heikkilä, Teijo Lehtonen, Tuomas Mäkilä, Timo Leino, and Tero Säntti for your guidance and giving me opportunities to work with you. These years have been excellent time to learn new things and collaborate in different projects and challenges. I offer my thanks to all the members of Future Ethics Group (i.e. 'the Dolphins'), Juhani Naskali, Ville Kainu, Kai K. Kimppa, Jani Koskinen, Minna Rantanen, and Anne-Marie Tuikka, for your continuous support, wisdom, and insights, as well as the developing of our research group, a joint scientific safe-haven. May our dolphinarium live long and prosper. I also want to thank Professor emeritus Simon Rogersson, Professor Emeritus Don Gotterbarn, Professor emeritus William Fleischman, Professor emeritus Ahti Saarenpää, Professor Charles Ess, Professor Tero Vartiainen, Professor J. Tuomas Harviainen, Penny Duquenoy, Diane Whitehouse, David Kreps, Antti Tuomisto, Tapani Joelsson, Kaapo Seppälä, Leo Sakari, Timo Korkalainen, Tomi 'bgt' Suovuo, Sami Hyrynsalmi, Ville Harkke, Jonna Järveläinen, Matti Mäntymäki, Seppo Helle, Lauri Viinikkala, Laura Yli-Seppälä, Polaris Koi, and Jouko Kiesiläinen for the wisdom and encouragement during the adventures we have had. I also wish to thank Jenni Heervä for her administrative toils. I have not been the easiest doctoral student, have I?

I wish to express gratitude for all my friends who have supported me and been there for me during this project. Especially I wish to thank Antti Airola, Olli Ala-Hakula, Tomi Gratschew, Antti Hakkala, Katri Haverinen, Jouko Kiesiläinen, Kai K. Kimppa, Lauri Lehikoinen, Tuomas Lehtovaara, Henry Lintula, Jani Mäki-Opas, Esa Moilanen, Janne Metsänperä, Minna Rantanen, Eero Stürmer, Tero Säntti, Janne Tuomisto, Juho Vepsä, and Björn Westberg. I also wish to thank Otto Haaki, Lassi Loijas, Sami Saksi, Anna Hatakka and Tuomas Niemelä from Proffan Kellari for making 'Proffa' to be a perfect place to write this thesis.

I also thank my parents Marja-Liisa and Jukka as well as my brother Juha-Pekka for the support they have altruistically offered during my studies as well as during my life. Thank you for being there for me whenever I have needed it the most.

Last, but definitely not least, I wish to express my deepest gratitude to the light of my life, my wife Jenni, who has offered her never-ending encouragement, support, and patience toward this project. This thesis is a part of our journey together and is not my but our achievement. I love you Jenni, always.

TABLE OF CONTENTS

List of Figures

List of Original Papers

Paper I — Heimo, O. I., Fairweather, N. B., & Kimppa, K. K. (2010, April 14–16). *The Finnish eVoting Experiment: What Went Wrong*? Paper presented at Ethicomp 2010, Tarragona, Spain.

Paper II — Heimo, O. I., Hakkala, A., & Kimppa, K. K. (2012). How to abuse biometric passport systems. *Journal of Information, Communication and Ethics in Society*, Volume 10, Issue 2 (pp. 68–81).

Paper III — Heimo, O. I., Koskinen, J. S. & Kimppa, K. K. (2013, June 12–14). *Responsibility in Acquiring Critical Governmental Information Systems: Whose Fault is Failure?* Paper presented at ETHICOMP 2013: The possibilities of ethical ICT. University of Southern Denmark, Kolding, Denmark.

Paper IV — Heimo, O. I., Koskinen, J. S., Kainu, V., & Kimppa, K. K. (2014). Problem of Power: The Missing Agent. *Proceedings of CEPE 2013 - Ambiguous Technologies: Philosophical Issues, Practical Solutions, Human Nature*. Autónoma University of Lisbon, Lisbon, Portugal (2013, July 1–3).

Paper V — Heimo, O. I., Kimppa, K. K., & Nurminen, M. I. (2014, July 25–27). *Ethics and the Inseparability Postulate*. Paper presented at ETHICOMP 2014. Pierre & Marie Curie University, Paris, France.

Paper VI — Heimo, O. I. (2018). *Procuring Critical Governmental Information Systems: A Virtue Ethics Approach* (Unpublished manuscript). Department of Management and Entrepreneurship, Turku School of Economics, University of Turku.

1 INTRODUCTION

Digitalisation is an ongoing phenomenon. We can compare this digital revolution to the industrial revolution in regard to changes in work, productivity, economics, security, well-being, and the realisation of possibilities. As work and the economy change, the demands brought for those working, dividing those who can adjust to digitalisation from those who cannot. Because productivity is tied more and more to automatisation, humans are left only the tasks that machines cannot yet do as cheap as humans (European Economic and Social Committee, 2017, pp. 11–14).

At best, this transformation leads to more and more people contributing to the well-being of everyone, yet the possibility for dystopias, such as those suggested by Huxley or Orwell, are still present. When society allows automatization more power over personal information, the citizens empower the government with their detailed personal information, responsibility for our security and safety, tasks to keep us healthy, and more possibilities to use the aforementioned information and tasks against them. That is, the citizens may become more reliant on the government, not vice versa, giving the government increased power over their citizens thus lessening the citizens' power over their own life.

These information systems controlling our society are not actors themselves but mere tools for someone. In the context of this thesis these actors are the government and its citizens. These systems pose a threat because, whoever controls them, controls the information flow in society, that is the citizens (i.e. the individuals) and the societal infrastructure, and, therefore, controls the society (i.e. the citizens and the infrastructure around them). Thus when these systems are paid for by the society, acquired or implemented by the government and forced to be used by the government (i.e. the entity consisting on politicians and officials who govern the society, usually divided to different offices, and in the end, to the government officials as individuals), the control over society is also given to the government. This of course does not mean that there is – necessarily – one person controlling over the citizens with the CGISs, but to analyse in a larger scheme of things where the balance of power is moving between the those who govern and those who are governed. When the citizens give this control to the

government, who guards the government to see that these systems are used for the benefit of the citizens? Or as Juvenal (6.O29-34) posed, “But who is to guard the guards themselves?”

The process of developing government information systems should be as open as possible and the responsibilities for using them should be clearly defined. This thesis focuses on government-controlled information systems, referred to as *critical governmental information systems* (CGIS). These systems are critical to holding the information and implementing functions that protect the lives, security, and well-being of citizens. Examples of these systems include eHealth, eDemocracy, police databases, and information security systems, such as physical access rights to paper archives (Heimo et al., 2013).

This study is a theoretical analysis of critical governmental information systems that are made to serve and protect the society. The study concludes that Aristotelian virtue ethics are an effective way to analyse the virtues that are required for the procurement process of the efficient, economical, and ethical CGISs. As the resources are limited, the members of society, the individuals, should be the utmost priority in regard to their lives, security, and well-being. To understand this we must monitor the development of digital infrastructures – especially how to monitor the digital-age government. Vartiainen, Heimo, and Kimppa (2016) describe an increased concern about, and frustration toward, the development of governmental information systems (GIS). In their study of Finnish information technology (IT) specialists, the specialists reported frustrations from observing unethical procurement and development practices. For example, they reported procurement issues that included mandatory lying and biased selection of providers. On the development side, they reported poor quality of work and services, and higher fees that were charged by the contractors from the government as a result of intentionally increasing the amount of work. According to Vartiainen et al., the underlying reasons for bad client-vendor relationships should be considered to even start improving the systems. Responsibility in the public sector information systems lies with the governmental office (2016; see also Heimo, Koskinen, and Kimppa, 2013).

Laws and regulations directly mandate the activities of government offices, giving them different motivations from private organisations. Vartiainen et al. (2016) found in their survey that the relationship between a developer of an information system (IS) and a government office was missing critical factors (e.g. trust into the procurement process and trust to the functionality of these systems) that are required for IT specialists to be

satisfied. Their research showed that governments should choose the best vendor for procurement and development based only on the technology that is needed. However, the IT specialists claimed that developers are chosen unethically and that the procurement, development, and management processes have major problems.

This thesis is focuses on *Ethics*, the study of *morals, morality – everyday morals* (Feldman, 1978), form *IT-ethics* perspective (formerly known as computer ethics). It differs from *information ethics* perspective (see e.g. Floridi, 2010, pp. 39–48) by not focusing on the information but bringing the technology and society to the focal points for a more holistic approach. IT-ethics is a part of ethics of technology (or technology ethics) but with a more social twist as IT has become an indistinguishable part of modern society and its' functions.

IT ethics is a branch of philosophy focused on ethical issues in IT, with a strong connection to IT, sociology, economics, psychology, and other relevant sciences; it might also be a branch of IT with a strong connection to philosophy, especially ethics. The American Engineers Council for Professional Development first addressed the ethical issues with computer science and technology in 1966. The Association for Computing Machinery (ACM) adopted their ethics as a set of guidelines for professional conduct.[1] Early in the field of computer ethics, the issues of concern were unauthorized use of services and information, information ownership, responsibility and intimidation, and deception done with computers (Parker, 1979).

According to Moor (1985), computer ethics is "the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology." Moor focused on solving the problems where "computer technology essentially was involved" and "there was uncertainty about what to do and even about how to understand the situation." Weckert and Adeney (1997) point out that computer ethics should concern both IT professionals and society as a whole.

The dynamic and complex field of IT ethics must consider the relationships among facts, conceptualizations, policies, and values (Moor, 1985). The characteristic features of IT ethics use a descriptive reality of technology, especially for IT, to raise issues about the state and direction of society's digitalisation process and derive judgements for these policies through normative ethics. Johnson (2001) argues that the policy requirements

[1] More on the subject: https://inroads.acm.org/article.cfm?aid=3204466

and the lack of policies are the ethical part of Moor's description in computer ethics. Johnson (pp. vii – viii) also states that technology should follow ethics, not vice versa, at least in some situations.

Also characteristic for IT ethics is that studies are only a quick peek into a larger issue from the point of technology and normative ethics. Often, the result leads to fractilised studies made in IT ethics. Although most of the scientists in the field generally agree upon the same issues (e.g. it is unethical to produce IS which endanger people's lives because of one's own financial gain), the bigger picture is hard to gather and combine from the small different pieces of research from the multitude, some of them being in contradiction with each other. Therefore it can be argued that the field of study is a sum of these pieces and one general theory of IT ethics does not exist. Nonetheless, IT ethics does not usually produce a fixed set of rules but rather a set of skills and tools to evaluate the nature of the IT that is used and a general theory of IT ethics could easily interfere with this. From a philosophical perspective, IT ethics produces concepts to understand the science; it provides tools and policies for the science to understand the philosophy, yet being a discipline on its own right (Moor, 1985). Ess (2009) describes ethical thinking as an important skill for making well-informed judgements, which Socrates and Aristotle referred to as *phronesis* or practical wisdom. This practical wisdom is needed when facing new situations, including the challenges of digitalisation.

Some excellent IT ethics guides (see e.g. Stamatellos, 2007), where the writers are philosophers themselves, give only descriptions of the setting and the questions without answers. The writers might have done this because they did not have concrete answers, which is probable, or perhaps they wanted to be more pedagogical? Nonetheless, when the discourse aims to entertain the mind and make an impact on society, the great majority requires answers, not riddles.

IT ethics is the scientific offspring of early science fiction literature. For example, Shelley's *Frankenstein*, Huxley's *Brave New World*, Lovecraft's *Herbert West—Reanimator*, and Orwell's *1984*, provided warnings for the scientific community and society about the problems of science without ethics. Luckily, today's scientists do not have to use mere fiction but also have tools provided by science to tackle with these issues, although fiction remains a good tool for teaching IT ethics. The field of IT ethics has filled this gap with both philosophical deduction and scientific method. However, the relationship with IT ethics to early science fiction is a general style of narrative in IT ethics, where the phenomena of technology is criticized with

both dystopia-like narrative structures and clear warnings to both the scientific community and society.

The problem with IT ethics often occurs with timelines. It is easy to focus on a phenomenon, for example, automation and artificial intelligence (AI) (e.g. automated stock markets) and combine (or confuse?) it with science fiction (e.g. robots that walk and talk like humans), which might not be probable for the next two decades. To clarify, the timelines of these two aforementioned AI-related cases do not match and thus when discussing around these current and futuristic issues a timeline must always be clarified and described. The descriptive state of technology as described in this thesis is based on current affairs or what is happening in the next couple of years.

As mentioned earlier, the field of IT ethics suffers from fractalisation and a lack of cohesion. Several scientific works give instructions (e.g., Johnson, 2001; Duquenoy, Jones, and Blundell, 2008; Stahl et al., 2014) on what to do and how to act in complex ethical situations. However, some published works on this topic describe a problem and treat the solution as so obvious or trivial that the researcher should not address it (cf. most ETHICOMP or CEPE conference proceedings), which is not usually the case in a real environment. As digitalisation advances, those citizens or groups who oppose it must provide reasons not to digitalise and present alternatives and guidelines on what to do–in contradiction to traditional burden of proof. For example, opposition to a specific advance in digitalisation might be due to its expected cost-benefit ratio.

The implementation of technology also includes problems that concern society as a whole because technology can be used to diminish, disregard, and dismiss certain groups and individuals. We need ideas to make the information age work for the benefit of society and the individuals.

This thesis is written with the aim to provide answers and ideas to use technology to do good. It consists of traditional IT ethics articles that critique certain aspects of the digitalisation phenomenon. It is also based on articles that describe problems in-depth and that give ideas and advice on how to possibly correct the problems. This thesis is highly theoretical because empirical studies from the field give light only to *mores*, or opinions of the people, rather than the ethical justifications for the phenomena (e.g., see Vartiainen et al., 2016). Also, proper empirical studies with CGIS require a nation state, such as Uruguay, to conduct tests on how the theory works in practice and several nations to conduct A/B testing, that is, simultaneous tests between two or more countries.

The thesis aims to avoid certain philosophical "razors"; the hypothesis of this thesis were selected that has the fewest assumptions but is not always open for *empirical* testing, only philosophical testing (Wigosky, 2004, pp. 30 – 32). It dismisses statements with no evidence by arguments with no evidence (Hitchens, 2007). It does not attribute malice when the situation can be adequately explained with ignorance (Wigosky, 2004, pp. 30 – 32) and by stating only something that can be falsified (Popper, 1959), yet with the power of deduction due to the theoretical framework.

To emphasise, the goal of this thesis is not to declare all CGISs as inherently bad nor is it to criticise governments, information systems, or technology. This thesis highlights both malpractices and the tools and methods that might help solve such problems that have arisen with the technology positive attitude towards rapid digitalisation during the said digitalisation. Although much of the research focuses on Finland, the problems, values, and solutions can be applied to governments around the world.

This thesis focuses on the current situation and problems with CGIS and presents possible directions and guidelines on how to improve them. It includes the following terms:

- *eVoting* refers to casting and counting votes with, or aided by, electronic devices during the voting process. The focus is on elections that are "important enough" in regional, national, or international level and thus not concerned with, for example, student union elections or Internet polls.
- *Biometric passports* refers to travel documents, which, in addition to normal passport information, contain additional machine-readable biometric data about the person they are issued to.
- *eHealth* refers to healthcare practices that are supported by electronic processes, communication, or devices. It also refers to the digitalisation and upgrading and upkeep of digital healthcare information systems.

Starting in Chapter 2, this thesis focuses on the terminology and philosophy regarding critical governmental information systems. As shown later in the thesis, terminology is not just a tool to communicate but is needed to enable meaningful discussion about the subject (e.g., see Rantanen and Heimo, 2014). Chapter 3 presents several examples that show how different processes surrounding CGISs are handled. They include examples of system failures and poor system designs in addition to examples of issues surrounding ongoing pre-procurement CGIS. Chapter 4 explains possible

solutions to the problems from Chapter 3 based on a wide range of analysis and discussion.

Finally, Chapter 5 outlines requirements for CGIS procurement, through a virtue ethics-based analysis. In this chapter a discussion through Aristotelian virtue ethics the procurement process of the efficient, economical, and ethical CGISs could be procured by the lead of *Archons*, philosopher-scientiests proficient in the field of required sciences, skill, and knowledge required to guide us through these vast socio-technical challenges.

As mentioned earlier, IT ethics has a strong connection to science fiction. Therefore, during this thesis, we follow the tale of Icarus and Daedalus (*Metamorphoses* 8), a science fiction epic from ancient Greece written by Publius Ovidius Naso (also known as *Ovid*), who wrote the Metamorphoses series. As these narratives go hand-in-hand, they show how the development and adaptation of technology still follows this ancient Greek poem, where hasty adoption and adaptation of technology causes misfortune to those who do not heed the warnings of the wise.

Meanwhile Daedalus, hating Crete, and his long exile, and filled with a desire to stand on his native soil, was imprisoned by the waves. “He may thwart our escape by land or sea” he said “but the sky is surely open to us: we will go that way: Minos rules everything but he does not rule the heavens.”
—*Metamorphoses 8 by Ovid*

2 CRITICAL GOVERNMENTAL INFORMATION SYSTEMS

A critical governmental information system is an information system that is provided by the government and differs from other government information systems, e.g. government websites, due its critical nature: its failure can cause endangerment or loss of something valuable to society, such as life, health, democratic process, or security. Heimo et al., (2013) define CGIS as follows:

> A critical governmental information system (CGIS), by definition, is an information system developed for governmental needs including data or functionality which is critical in nature to the security or wellbeing of individuals or the society as whole. It is a system where something invaluable can easily be compromised. These kinds of systems include eHealth, eDemocracy, police databases and some information security systems e.g. physical access [rights] control.

To emphasise, CGISs are by nature more vulnerable to different kinds of threats from user error to malicious activity and the consequences when these threats actualise are dire due to the nature of information and functionalities they are entrusted with. The *easiness* in this context does not refer to the amount of effort required to compromise (hopefully vice versa) but rather the easiness to compromise security, safety, and wellbeing via poor procurement, design, implementation, and upkeep decisions. Thus CGISs require more meticulous approach in their lifecycle of the said type of ISs compared to other ISs.

CGISs serve and secure the critical functions that are required for a modern society to function properly and to maintain the required level of safety for its citizens to live their lives without excess fear. The government can outsource some of the critical services (e.g., passport control) to a third-party supplier the system still being a governmental system.

In an ideal situation, CGISs play a major role in modern society by providing the primary digital infrastructure that helps society to function efficiently and without interference. In practice CGISs due to system vulnerabilities often predispose a society to various social and technical attacks and abuses that diminish the security of the society. The power to determine the kind of CGISs that are introduced or used implicitly include the power to determine how to manage society. These decisions address many questions, for example: (a) are the health services a public or private domain (i.e. is healthcare paid by the government), (b) who can read patients' medical data, (c) who can apply for certain jobs, and (d) who is driving their own private vehicles, when are they driving, and where are they driving to (i.e. vehicle surveillance). The digital decisions of the society lead to possibilities of building "digital platforms" over the formerly analogue society. Society must limit the information system and imbue it with its inherent values, not vice versa.

Any digital platform transforms to a CGIS when sensitive information about the society or its' members are included in the system. This information can include healthcare data, locations, timestamps, biometrics, voting behaviour, or personal connections and desires. A CGIS can contain information and even fragments of information that, when mined, can be harmful to the individuals or society and therefore, must be protected by society – and by the government.

To protect these kinds of data, it would be ideal not to collect it at all. For example, in Germany, the legislature found that the national biometric database contradicted the rights of informational self-determination that were provided by the German constitution (Hornung, 2007, p. 256). On the other hand, in some situations data must be collected for the sake of a person, their identity, their safety, or their well-being, and in some cases for the sake of others. These situations bring to mind yet another problem. Because the information must be accessed by some and not by others, who gets access to it?

In this digital age, a lot of personal information is given to – or collected by – various commercial actors. Legislation limits the legal possibilities of how to use this data, which is an issue that is not enforced all the time because of local and international legislation. However, the governments, which follow different legislation concerning information gathering, have not stood idly by with the development of digitalisation and information sharing (e.g.,

see BBC, 2010; Fildes, 2010; Langner, 2010; Schneier, 2010; F-Secure, 2011; Sanger, 2012; Heimo and Kimppa, 2013; Hakkala, Heimo, Hyrynsalmi, and Kimppa, 2017). Moreover, after Edward Snowden's revelations[2] in 2014, governments around the world have decided to arm themselves with cyber capabilities (i.e. capabilities of waging war in cyberspace), with budgets higher than ever (Hyppönen, 2017). These revelations give a glimpse on how widespread the digital warfare armament phenomenon was. The current situation remains a mystery and thus it is hard for an individual – even for a scientist – to know what information concerning them is stored and by whom – and how do the governments store, share, and (ab)use the information they have gathered to their systems.

It is important to understand that these systems are CGISs. They are made by the government for the government, but hopefully at least in Western democracies for the citizens. The data stored to the servers include various personal and private data about both citizens and foreign people and can be used against them if a need arises. One could question should a government have that kind of power over their citizens.

Many CGISs are provided as the only system for a citizen to use, such as for passport processing, and thus "monopolized" by the government for a reason[3]. CGISs and governmental information databases at large can create problems with the government-citizen relationship because of the increased possibility for governmental control and surveillance (Heimo et. al., 2012). Even though it is ethically justified for the government to monopolize some of the functions in society, e.g. military or border security, the government should not have this level of power without accountability.

Private sector functions, such as electric networks, mobile networks, bank systems, and Internet services, are critical for society in the same ways as CGISs. However, the *economic philosophy* is different. That is, they are regulated by the government and paid for by customers in exchange for services, but have profits that go shareholders. In comparison with critical private sector information systems, CGISs have two clear differences: (a) they are provided by the government and, therefore, paid for by the citizens to

[2] See e.g. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

[3] In this context, made something a government monopoly, e.g. having a military is a common government monopoly.

serve them, and (b) the government usually monopolizes them. This does not mean that the electric or mobile networks could not be a CGIS if governments choose to provide them to their citizens. Rather, the distinction is about who provides these services. In any case, society requires critical information systems. The difference is whether the government regulates them or the government has direct control over them. Competition provides a possible sanction against serious malfeasance, but government actors can enforce a monopoly that protects them from consequences.

All publicly held and many if not most private companies and corporations have only one purpose: to generate a profit to their shareholders (unless otherwise specified). For example, banks serve their shareholders by making systems *secure enough.* The assumption is that some of the money is lost with the process, but a lower level of security is more advantageous in the means of creating more capital (Fairweather & Rogerson, 2002). This, of course, reflects on responsibility.

Usually a company constructs a network of responsibility between employees and management and between management and shareholders. If the shareholders best interests are to serve the customer with a functional and usable information system, management and employees are responsible for creating and maintaining that system. The customer can choose whether to use the system and whether to pay the company. To maintain the quality in eGovernment systems, a network of interest and responsibility must be built. Later, this thesis explains the field of responsibility and the improvements that are related to it.

Poor eGovernment solutions have even resulted in the loss of lives. One of the most classic examples is when the whole emergency healthcare system in London, England, went down because of the IS. Ambulances were sent to wrong sites causing several deaths and injuries (Avison & Torkzadeh, 2008, pp. 292 – 293)[4]. Also, numerous eVoting solutions worldwide have resulted in elections that were compromised numerous times (Mercuri, 2001, pp. 13 – 20; Heimo, Fairweather, & Kimppa, 2010; Robison, 2010; Heimo, Kimppa, and Nurminen 2014).

[4] And more recent the ransomware attacks against NHS. See e.g. https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

By the description alone, functioning CGISs are a necessity for governments and their people as a value of life, well-being and security. The next chapter provides more examples of poorly designed CGISs.

So saying he applied his thought to new invention and altered the natural order of things. He laid down lines of feathers, beginning with the smallest, following the shorter with longer ones, so that you might think they had grown like that, on a slant. Then he fastened them together with thread at the middle, and bees'-wax at the base, and, when he had arranged them, he flexed each one into a gentle curve, so that they imitated real bird's wings. His son, Icarus, stood next to him, and, not realising that he was handling things that would endanger him, caught laughingly at the down that blew in the passing breeze, and softened the yellow bees'-wax with his thumb, and, in his play, hindered his father's marvellous work.
—*Metamorphoses 8 by Ovid*

3 CASES OF CGIS

3.1 Electronic Voting

During the 1990s and 2000s, the Western world saw numerous experiments in electronic voting (eVoting), either to supplement or to replace existing systems. After several trials and many errors, several nation states have abandoned their eVoting projects (Heimo et al, 2010). Various arguments have been used to justify procuring eVoting systems, including cost savings, activating passive voters, speed, efficiency, and reliability of counting votes, and staying in the front line of information and communication technology (ICT)-using nations (Heimo et al, 2010). This section analyses these goals and the methods for acquiring an eVoting system.

eVoting systems have proved to be expensive (Verzola, 2008) and have not been shown to activate more people to voter. They are not be especially fast or efficient. At least in the Finnish case, the possibility of reducing the four-hour vote tally calculation to 30–60 min can be questioned altogether – a saving the value of which can be questioned. eVoting systems also tend to be more unreliable in counting votes than manual systems (Mercuri, 2001; Fleichman 2010; Heimo et al., 2010).

eVoting systems as a whole seem to have a few problems in common. Mainly, every system in use has not proved to be functional or has proved to be dysfunctional. Consider the following examples in the United States (US):

- In 2003, a candidate in the state of Virginia lost 100 votes due a programming error (Schneier, 2004; Effi, 2009).
- In 2001, in the state of California, because of a programming error, votes had to be recounted by hand, using paper copies (Schneier, 2004; Effi, 2009).
- In the 2000 U.S. presidential election, Al Gore was initially attributed minus 16 022[5] votes in a voting district in Florida (Schneier, 2004; Effi, 2009).

[5] Yes, you read that correctly. That is a negative number of votes.

- In 2003 in Boone county, Indiana, with 20,000 voters, 140,000 votes were accounted for (Schneier, 2004; Effi, 2009).
- In the 2008 elections in Florida, 3400 votes were lost[6] (Schneier, 2004; Effi, 2009).
- In the US, a group of researchers demonstrated that a voting machine can be hacked in less than 7 minutes (Appel et al. 2009; Effi, 2009).

Other countries and geographic regions have experienced their own problems with eVoting machines:

- In 2007, automated elections in Scotland cost GB£40 million. Elections in 2003 cost GB£17 million (Verzola, 2008).
- In 2008 in Finland, eVoting try-outs lost 2.3% of votes (Heimo et al., 2010).
- In 2007 in the Netherlands, a group of activists proved that the voting machine was hackable while in use (Gonggrijp & Hengeveld, 2007).
- In Ireland (population of 4 million), a five-year eVoting project cost over EU€52 million (Verzola, 2008).

eVoting systems are vulnerable to various attack methods. One of these methods entails tampering with a single voting machine, such as the hack done by Appel and his research group (Appel et. al., 2009). They proved that a Sequoia Pacific AVC Advantage can be turned *Turing complete*[7] in under 7 minutes, including the required lock picking. Also the Dutch activist group Wijvertrouwenstemcomputersniet made a commonly used Nedap/Groenendaal ES3B play chess (Gonggrijp and Hengeveld, 2007). These hacks are rather easy to produce, but even easier hacks can be found from 2018 Defcon Conference, where the security of 13 different U.S. voting systems was tested against children. 11-year old boy could hack a system in 10 minutes and overall 30 children could hack into the systems in 30 minutes.(Regan, 2018) Another possible form of attack includes information warfare-style attacks of the core system. While these methods have not been discovered against eVoting systems, but their potential impact could be huge.

Mercuri (2001) states in her study that the underlying problems of direct recording electric (DRE) voting machines, voting machines that are fully digital, are critical because they record and handle the votes only digitally and hence fraud might be difficult to detect. A fair number of those problems also recurred.

---

[6] See also https://www.theregister.co.uk/2008/09/04/missing_florida_votes/

[7] A computer that can simulate a universal Turing machine and thus execute all possible programs. See e.g. https://link.springer.com/chapter/10.1007/978-1-4615-0237-1_1

Most of the eVoting systems, including AVC Advantage, AVC Edge, Tieto Voting System, and Nedap ES3B, use a black-box security method, also known as *security through obscurity*. In this method, the blueprints or design of the systems are kept secret, making it harder to evaluate the system and create an attack (Heimo et al., 2010). German constitutional court ruled eVoting as unconstitutional in 2009 (Bundesverfassungsgericht, 2009).

Mercuri also stated that mobile or Internet-based voting systems (mobile voting, mVoting, voting conducted with the voters' own computers/mobile devices), due to the mobile nature, do not fulfil the requirements of democratic elections, such as privacy of the ballot or integrity of elections. To implement mVoting, ballot privacy must be broken (Mercuri, 2001; Heimo et al., 2010; Merimaa, 2017). However, many countries, including Finland, are preparing their own mVoting systems (e.g., see Merimaa, 2017). Estonia, the forerunner in mVoting, has used its mVoting system for several years (Mercuri, 2001; Heimo et al., 2010).

Yet there is a solution. The Voter Verified Paper Audit Trail (VVPAT) method, also referred to as the *Mercuri method* after Rebecca Mercuri, is a modification to DRE voting machines so that it provides a paper trail. The benefits of the DRE, mainly efficiency, are included along with trust in the authenticity of the results because they can be verified. In the VVPAT method, the DRE device is implemented with a transparent cover where the voter can see their printed vote and verify its correctness. Votes are cast after the voters verify them, and the physical records are stored inside the machine where they are gathered after the election. After the preliminary results, which are faster to gather when DRE machines are used, the election results can be verified by counting the paper votes (Mercuri, 2001). The only downside of this method is the price, which is roughly the cost of a paper ballot and DRE voting machine combined.

Both theoretically possible and actual problems still exist in using modern eVoting systems. Systems are developed and deployed into use without a burden of proof where the proposer of the change must prove the systems' validity. Scientists, civil activists, and non-governmental organizations invest huge amounts of work to prove that systems are being designed and implemented incorrectly. However, governmental offices are leaving out technical, social, economic, and ethical issues and, at best, are outsourced to members of the public (Heimo et al., 2010).

3.2 Biometric Passports

At the dawn of the 21st century, the 9/11 terrorist attack in the United States shocked the world. As an outcome of this event, Western nations came to a consensus on the need to identify travellers more thoroughly. In Finland, the Ministry of Internal Affairs implemented the biometric passport application to protect its citizens from international terrorism, illegal immigrants, and international criminals (Finnish Ministry of Interior, 2011). Recent scientific advancements in IT and biometrics had created a possibility to fulfil this demand.

The number of errors during the development and implementation of the biometric passports is still unclear, but current knowledge from past five years shows no negative consequences from implementing this system. However, some questionable decisions can lead to both direct and collateral consequences that are harmful to both individuals and society (Heimo, Hakkala, & Kimppa, 2012).

This section is based on the Finnish biometric passport control system reform as a part of European passport reform and its possible direct and collateral consequences. For collateral consequences, the related ethical questions are harder to find, examine, and analyse, making the outcome of the transition from non-biometric to biometric passports unclear (Heimo et al., 2012).

Biometric passports are similar to traditional passports but contain additional machine-readable biometric data from the person they are issued to. This additional biometric data can be read from the passport at border and can be used for automatic biometric recognition of the traveller (Heimo et al., 2012).

The International Civil Aviation Organization (ICAO) has defined the standard for biometric passports to include biometric traits including the face, fingerprints, and iris. A picture of the passport holder's face is stored on all biometric passports, and the other biometrics are optional (ICAO, 2006). The first phase of Finnish biometric passports contained only the photograph in a machine-readable form, and the second phase introduced fingerprint data. Some countries have implemented iris data, while others have left it as an option.

All biometric passports also contain sensitive, personal information such as the holder's date of birth and social security number. The initial standard for biometric passports issued by the ICAO (2006) contained technical measures for limiting access to the embedded radio-frequency identification (RFID) chip.

Heimo, Hakkala, and Kimppa (2012) list the following possible issues with biometric passports, which can be used for…

- gathering undeniable proof that a person has been in a particular place at a certain time by a third party (Monnerat et al., 2007, pp. 21 – 2);
- identifying passports by their response behaviour to a read request;
- identifying the nationality of a passport of certain nationals by this behaviour by a third party (Monnerat et al., 2007, p. 19), but not U.S. passports because of the Faraday cage that is implemented in the passport (Vaudenay, 2007, p. 61);
- fingerprinting and tracking of RFID chips for which a signature is known (Danev, Heydt-Benjamin, & Čapkun, 2009); and
- signature tracking, which is probably more practical for detecting counterfeit passports than tracking people (Chothia & Smirnov, 2010, pp. 26 – 32).

Chothia & Smirnov (2010) also presented a technique for tracking a passport without breaking security protocols. By listening to a transaction between a reader and a passport, it is possible to identify a passport holder's home country based on the passport's response to ill-formed read requests. Richter, Mostowski, & Poll (2008) pointed out various different vulnerabilities which may result in the loss of location privacy or anonymity for the passport holder. The most notable failure still seems to be that all the security protocols are optional (Chaabouni & Vaudenay, 2009, p. 7; Heimo et al., 2012). As stated earlier, adopting biometric passport systems can be divided into direct consequences and collateral consequences.

Examples of *direct consequences* include:

- erosion of document security (as explained previously);
- the leaking of personal information, which can be used in identity theft (Hoepman et al., 2005, p. 5; Juels et al., 2005, p. 15) through eavesdropping or skimming personal information from the passport (Ramos et al., 2009); and
- decreased security at borders due to inefficiency or errors in the socio-technical information system.

When a system is designed in haste due to tight schedules or budget, critical phases of the design process may not be done properly. For example, the security system implementation might be inadequate, or work processes in border security are incorrectly understood.

According to Leavitt (1964) and Nurminen and Forsman (1994), when technological solutions change, the work also changes. That is, when passport

technology changes, the tools that are used by border control agents and their whole work process must change. Biometric passports have automated border control and this surely is not an addition, as was told when the biometric passports were introduced, but a substitution to the border control workflow. It is debatable whether biometric passports increase border security as was intended (Heimo et al., 2012). Automation of border control procedures will eventually diminish the tacit knowledge and professional skills of border officials. Therefore, the concept of *increased security* will turn into a *change in security procedures*. While automation will bring more reliable methods for identifying travellers, other required border control security skills, such as identifying smugglers, can eventually be lost (Heimo et al., 2012).

Biometric passports also enable the possibility of building explosive devices to detonate near citizens of a specified nationality (Juels et al., 2005, p. 5; Zetter, 2006) or to be triggered by a certain number of foreign nationals. The ability to recognize certain nationalities, or foreigners in general, in a crowd could increase the efficiency of pickpockets to find targets or mark foreigners for kidnapping (Lockton & Rosenberg, 2005).

If national cryptographic keys are leaked, an irreversible denial of service (DoS) attack is possible[8]. Also, all passports that support Extended Access Control (EAC) and grant access for the country in question could be read at will by those in possession of the keys, giving access to any information in the passports and any saved biometric data (Grunwald, 2007; Heimo et al., 2012).

Collateral consequences include the erosion of privacy through the different registries that local and foreign governments keep. In Finland, the first phase of the biometric passport system started with the passport reform in 2006. The second phase started in 2011. The system incorporated fingerprint verification in accordance with European Council (EC) Regulation No. 2252/2004 (p. 2). During the second phase, the Finnish Government decided that the fingerprints gathered from passport applicants would be stored in a national fingerprint registry, an addition that EC Regulation does not require (EC, 2004, HE 234/2008). This registry contains all gathered biometric identifiers of Finnish passport holders and allows fingerprint and facial picture matching. It allows, for example, location detection of persons with two or more different official identities, unlike other systems (e.g., see Helsingin Sanomat, 2010a), making it a major ethical concern. Unfortunately the advantage is overshadowed by issues such as decreased privacy, false

[8] A big if, but very bad consequences if realised.

positives in criminal investigation and framing innocents to crimes, and compromising the border security (Heimo et al., 2012).

The Finnish Ministry of Internal Affairs justifies the registry because it holds the possibility to identify persons who have lost their passports (Finnish Ministry of Interior, 2011). The government has not revealed any specifications about the registry in its publications, meaning the system is an example of security-by-obscurity. The negative possibilities of biometric registries are taken seriously in some countries. For example, the German legislature ruled out the creation of a national biometric database because it contradicted the *right of informational self-determination* that is provided in the German constitution (Hornung, 2007, p. 256; Heimo et al., 2012).

During the legislative process, high-ranking Finnish police officials and politicians repeatedly demanded authorisation to use the database be included in the legislation. The system was opened to identify the deceased as well as to identify the living (given their consent). However, the demand for forensic use of the system was ultimately ruled out by the Finnish government in 2010 (HE 234/2008; Kerkelä, 2008a; Kerkelä, 2008b; Happonen, 2010; Lehto, 2010; Heimo et al., 2012; Nelonen.fi, 2012; Reinboth, 2014).

Yet no guarantee exists in law to prevent opening the biometric database for forensic use. Because Finland does not have a constitutional court, but rather a constitutional committee selected from the MPs, the issue is not settled but can be brought forth to parliamentary voting after every election. Eventually parliament might accept the use of the biometric database for purposes other than originally purported. This kind of registry might be built retroactively with only a subset of accepted passport applications: if the applications are stored or the database is retroactively constructed from the travel documents read at borders, airports, and other locations (i.e. if a passport is used, all information it contains is stored and inserted to a database). If passport application data are not destroyed, a database can be constructed in a matter of hours from the aforementioned data. Also, the registry can be constructed during the passport validity check of the border security process by saving data from the passports (Heimo et al., 2012). The retroactively constructed database inherits all the ethical dilemmas with a "traditional" fingerprint registry.

Having fingerprints stored can create problems like those surrounding the 2004 Madrid bombings, where an innocent American citizen was erroneously identified as the perpetrator based on the fingerprints found in forensic investigations. The Spanish police later connected the fingerprints to a

different person, and the FBI was forced to admit their mistake (Cherry & Imwinkelried, 2006, p. 336 – 337).

Evidence has shown that innocent people can be marked as suspects (and face a loss of freedom) with little to no actual evidence, especially in high-profile cases. The Finnish government has stated that its citizens should be worried about the effectiveness and cost of catching criminals. What Finnish citizens, and citizens of all countries, should be concerned about is the government being more than interested in gaining personal data about their citizens. (Heimo et al., 2012)

The problems with Finnish biometric passport systems are not limited to Finland but indicate a clear possibility of intentional international harm. Although a citizen of a certain state might trust the handling of their biometric data by their own country's officials, with foreign officials, the situation changes. When authorised border officials of other countries are authenticated to open the biometric data, the citizen owners of the data do not know when or where that data are stored or used afterwards (Singel, 2004; Heimo et al., 2012). The concept of massive storage of biometric data is at least a possible, if not even a probable, threat, which makes it important to ponder the potential consequences of these scenarios.

The actual implementation documents of biometric passports are not generally available for study by academics, making it difficult to ascertain whether they conform to the standards. Nation states do not usually publish the details of their implementations. Therefore, dealing with privacy and security issues must be reverse-engineered (Mostowski & Poll, 2010, p. 2). Because of trade secrets and security-through-obscurity methods, the openness of society and its implemented technology is lacking. Analysing and comprehending the changes in the border workflow is a challenge (Heimo et al., 2012).

No open public review or source of key information for any biometric passport system seems to exist. All analysable information is gained by examining and reverse-engineering passports and the technology that are currently in use. Yet with only these sources, the results of the analyses have raised numerous problems and security flaws, some of which have been fixed.Access to design documents prior to implementation might allow some of these flaw to be identified by experts. When the work of border officials is automated, we can presume that not all the changes in the given processes are beneficial to the citizens. Yet the border work process is one of the key functions of a secure society, if not at a national level, then at least at the outer borders of a border alliance. Altering this process without tacit consideration of the consequences and without open examination can decrease security for

both individuals and society alike. Moreover, the gathering of biometric data seems to be a problem where the interest of individuals or even of the society is placed behind the interest of their government (Heimo et al., 2012).

3.3 eHealth

Healthcare is a divided ensemble with separate special requirements for information systems. In addition the traditional challenges of IS development, healthcare IS must support the work processes and procedures in a fragmented healthcare system. Fragmentation and the resulting compartmentalisation in the healthcare sector is innate and unavoidable.Thus, healthcare imposes requirements and added costs for system development, and when those requirements and costs are not acknowledged, theyhealthcare IS can reduce, rather than increase, the amount of utility that the system provides (Danzon and Furukawa, 2001).

Rantanen and Heimo (2014) argue that the discussion around healthcare information systems (HCIS) in Finland seems to follow Plato's Theory of Forms, where the idea should be in everyone's mind (e.g., see Theaitetos, pp. 184 – 186; Republic, IX – X, pp. 589 – 599), but no one actually agrees with even the most basic terminology. In Finnish public rhetoric, *patient information systems* should be clear to everyone, but the interpretation of such systems varies widely (Rantanen & Heimo, 2014). Rantanen and Heimo (2014) state: "Whilst an engineer can see the problem as a technical one, a sociologist or economist has quite a different view about the subject. Therefore whilst the reflected idea is subjective, we need something more clear to have a discussion upon."

Heimo, Kimppa, and Nurminen (2014) argue that an information system should be viewed in larger context that consists of "[…] not only the technology nor the communications of the actors within the technology, but actually from any communication and delivery of information between the actors in real time or in stored format for their work tasks." That means the communication can happen in real life or using non-digital media as well as by communicating with technological solutions – both with the system core or with a communication tool, e.g. VoIP or mobile phone. Moreover the digital trace is not always visible – and the communication flows can be a tricky thing to follow by an outsider.

Therefore, HCISs are not only electronic patient records, electronic health records (EHR), or computerised patient records but something much larger –

yet the distinctions are unclear at best (see Rantanen & Heimo, 2014) . According to Nurminen (1986a), they are a combination of software, electronics, papers, doctors, nurses, patients, stored patient data, knowledge, and communication. They are not technical problems and should not be viewed as such. Instead, they should be viewed as a complex combination of workers and their tools intertwined with communication between them.

The technical and economic decisions seem to play a much larger role in the discussion and procurement than they should (e.g., see Kivekäs, 2012; Niilola, 2012; Peltomäki, 2012; Helsingin Sanomat, 2013; Iranto, 2013; Juntunen, 2013; Kasvi, 2013; Liimatainen, 2013; Lindstedt, 2013; Pitkänen, 2013; YLE, 2013; Rantanen and Heimo, 2014).

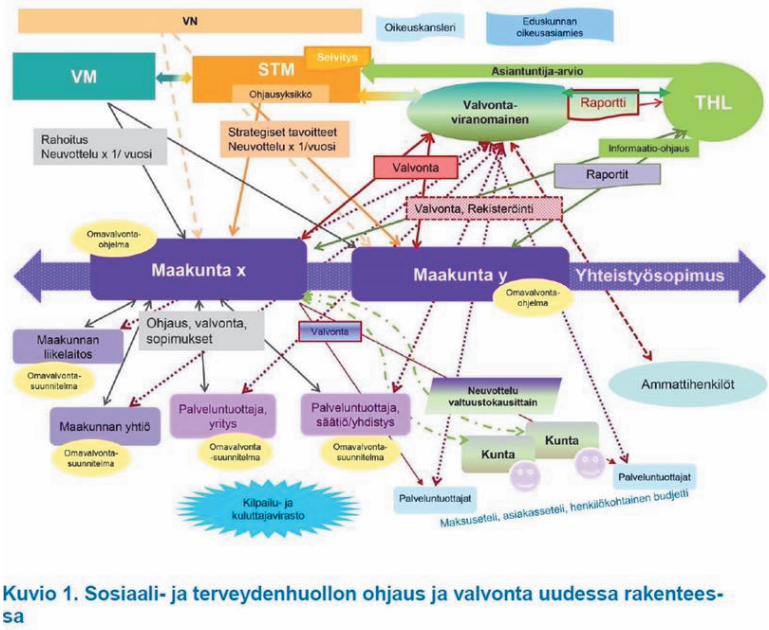
Rantanen and Heimo (2014) propose a common set of terms for HCIS so that everyone can understand them and partake in the discussion. They argue that to have a meaningful discourse about these complex multidisciplinary information systems, we must have a common language. The main focus of their study was just one term: *patient information systems*, which is commonly used in Finnish HCIS discussions. They noticed no consensus when using this single term. The meaning differed from a healthcare database to a whole hospital, including the people who use these systems. Therefore, a meaningful discussion about the price of a patient information system becomes impossible.

Numerous examples exist of situations where the language is even more unclear. While patient information system can be defined for every situation before the situation starts, sometimes language is actually used to confuse the reader and to intentionally (or with extreme incompetence in clarifying one's thoughts) make discussions about the subject more difficult. If the digital divide was not bad enough to separate those who can understand digital realm and those who do not, writing deliberately more complex (and vaguer) texts surely divides those who are both interested in the subject and capable of understanding, from those who are not. In the following example a description on how the secondary use of patient information will be executed in the near future and serves as a good example on how overly complex language is used:

> The development and resourcing of the secondary use of the knowledge: The development and gathering of social- and healthcare (sote) action-knowledge is set a national and regional goals and a national plan for a new sote-infrastructure will be made according to executing and action-requirements. Knowledge gathering and analyzing will be transformed to match the needs of the requirements, accessibility, productisation, tracking and

> development. Social- and healthcare services are described by classifications and metrics (content of services and use, accessibility, service processes, quality, efficiency and effectiveness) will be unified and developed through knowledge architecture. Coordination responsibility: national.[9] (STM, 2017)

To clarify: the text above describes the methods on how the government will proceed in selling citizens' healthcare information can be sold to outsiders. In addition public HCIS development publications provide yet another fine example of poor communication by introducing a new county-lead healthcare structure, as shown in Figure 1 by THL (Finnish Institute of Health and Welfare):



Kuvio 1. Sosiaali- ja terveydenhuollon ohjaus ja valvonta uudessa rakentees-sa

Figure 1. *An example of complex government information, Supervision and control of social and healthcare in a new structure. From Nykänen, Kovasin, Liukko, Blomqvist, Krohn, Ahola, Nurmi-Koikkalainen and Jonsson, 2017.*

---

[9] "Tiedon toissijaisen käytön kehittäminen ja resursointi: Sosiaali- ja terveydenhuollon toimintatiedon keräämiselle ja hyödyntämiselle asetetaan kansalliset ja alueelliset tavoitteet ja laaditaan kansallinen suunnitelma uuden sote-rakenteen toimeenpanon ja toiminnan vaatimusten mukaisesti. Tiedon keruu ja analysointi muutetaan vastaamaan sote-palveluiden tarpeen, saatavuuden, tuotteistuksen, seurannan ja kehittämisen tarpeita. Sosiaali- ja terveyspalveluita kuvaavat luokitukset ja mittarit (palveluiden sisältö sekä käyttö, saatavuus, palveluprosessit, laatu, tehokkuus ja vaikuttavuus) yhdenmukaistetaan ja kehitetään tietoarkkitehtuurin avulla. Koordinaatiovastuu: kansallinen"

In the future, more research will be conducted on the topic of language used in Finnish public-sector HCIS development. The difference between good governance and bad governance might just be in the discourse (e.g., see Heimo, Koskinen, Kainu, & Kimppa, 2014). A good discourse demands honest conversation and, moreover, a common and understandable language (e.g., see Rantanen & Heimo, 2014).

Functionality is a key element when creating a successful HCIS. Therefore, when evaluating a HCIS, the procurement process must verify and validate that these CGISs are functional. To be successful in this process, validation and verification must be easy to do and optimally be done without doubt (Koskinen, Heimo, & Kimppa, 2018).

Because the validation and verification processes are citizens' last line of defence before the systems are implemented, a lot is at stake for this process to be done correctly. To produce efficient, economical, and ethical HCISs, all of these viewpoints (efficiency, economical and ethical) must be taken into account, and ease of verification process must be considered when procuring the system (Koskinen, Heimo, & Kimppa, 2018).

This verification process cannot function without having discourse on the subject.

Heimo, Koskinen, & Kimppa (2013) promote the idea of Habermasian rational discourse on the subject of procuring CGIS. They argue that this should be done in such a way that the "strategic games" are ruled out from the discussion and everyone participating in the discussion has an equal say on the matter. Thus if a participant in the discussion tries to promote their own advantage over others they are shut down from the discussion.

Habermasian discourse is an ideal state and cannot function *as is* in the real world, but it can be applied in certain levels to counter the effects on irrational and unvirtuous arguments. In the discourse there are for instance problems of definition on what are strategic games, who is benefiting from the status quo, and who is in advantageous position and when. It must be understood that no perfect answer can be found to these questions but only answers that can be derived in a high abstraction level which is a clear limitation in the Habermasian discourse. Nevertheless there is a possibility to have a discourse about the subject and to gain knowledge from different interest groups and their needs, hopes, and recommendations on the process of CGIS lifecycle.

To work – even on a theoretical level – the Habermasian rational discourse must indeed be rational and promote the rationality as well as common benefit. Heimo, Koskinen, Kainu, & Kimppa (2014) suggest *a discourse on*

discourse, which is a discourse to set limits and define terminology before discussing the actual subject of procuring the CGIS. Hence, according to them, we should have a discussion – on the societal level – on how to discuss these problematic questions. We must be aware of who are promoting and what – but most of all why – to make the connections to different interest groups public and monitor that the proper moral lines are not overstepped. A representative example of this was when in the middle of the Finnish Social Welfare and Healthcare Reform one nominated expert – professor Hiilamo – was found be employed by a large private healthcare organization just after he changed his mind on how and when the new system should be implemented (Iltalehti, 2018).

For this we need people who are able to lead the discussion and guide us through this problematic field and approximate the arguments from a rational perspective. That person – or those persons – should be able to understand the limitations of the rational discourse, the possibilities to produce rational information for instance, and relate the arguments to the real world. If we actively monitor the strategic games – "lobbying" – it could be possible to at least cut off the worst cases of the discussion.

3.4 Social Welfare and Healthcare Reform

The National Institute for Healthcare and Welfare of Finland (THL) states that social welfare and healthcare reform are:

> An overhaul of the structures of the social welfare and health care services system has been going on in Finland for several years. The need for this reform emerged from problems in ensuring equal and adequate social welfare and health care services for the population under the existing municipality-based service structure as the dependency ratio changes. Small and financially weak municipalities have encountered significant difficulties in organising and producing services. In the present reform, responsibility for providing social welfare and health care services is being transferred to larger and hence stronger administrative entities.
>
> The Government has outlined the creation of autonomous areas for the purpose of organising social welfare and health care services. The objective in this operation is not only to create financially more viable bodies as service organisers, but also to achieve complete horizontal

> and vertical integration of social welfare and health care services. (THL, 2018)

This process started in 2011 when the municipality and service reform—the PARAS[10] project—which had similar goals, was cancelled. The next two governments, during 2011 and 2015, aimed to reform the social welfare and health care system (SoTe-reform) on a large scale. Finland is a welfare state where social welfare and healthcare are trusted mainly to the government. The current percentage of social welfare and healthcare done by the government is over EU€31 billion (from the total of EU€64 billion of taxes) (Raivio, 2006; Laki kunta- ja palvelurakenneuudistuksesta, 9.2.2007/169).

The goal of the project is to move the creation of social welfare and healthcare services to the counties, although they do not yet exist (Finnish Government, 2018). The ongoing project has faced numerous difficulties, such as in the number of counties because opinions vary about the number of counties that exist. The number ranged from 5 to 18 counties, but 18 was selected. Other difficulties include identifying specific responsibilities, the main municipalities in which the services will be located, and rising inequality due to centralisation, among other difficulties (Shikeben, 2014; Finnish Government, 2016; Kärki, 2016; Demokraatti.fi, 2017; Pantsu, 2017).

The information system solutions that are tied to reform are only in high-level planning (Finnish Ministry of Social Affairs and Health, 2017) because the national healthcare database is one of the backbones of the system (Finnish Ministry of Finance, 2015). Therefore, having a more detailed discourse about IS solutions is not necessary at the moment. However, there are more intriguing aspects in the public discourse, which is not listening to the experts. This project has created such a fuss in Finnish media that experts are constantly interviewed by the media. Those entities who are leading the project seem to bypass the expert opinions (Merikanto, 2017a, 2017b, 2017c; Paulavaara, 2017).

The Supreme Administrative Court of Finland has criticized the process because it seems to forget the social welfare part of the reform and is focusing only on the healthcare sector (KHO, 2017). This perception does not mean that the reform itself is bad. Finnish national social welfare and healthcare costs have increased by almost 2% annually[11] and it is obviously this trend

[10] Paras means “the best” in Finnish.

[11] During last 10 years over 19%, when inflation was taken into account. See http://budjetti.vm.fi/

cannot continue for long. However, this reform might not cut the spending, and it might increase spending, according to the experts (Heikinheimo et al., 2017; MTV3.fi, 2017).

3.5 New Finnish Intelligence Legislation

Digitalisation has evolved in societies to yield a ubiquitous information presence, where information and communication are delivered over national borders in mere milliseconds. As a result, traditional intelligence operations and the legislation around them have been a rising concern in the Western world. In some countries, such as the US, China, and Russia,intelligence agencies have traditionally had more rights and resources to act than in the smaller countries like Finland.

As more of these operations require breaking into information systems, and as physical and digital worlds are more and more intertwined, it is harder to draw line between information warfare and intelligence operations. A significant problem is that the Internet makes it difficult to differentiate between users and targets, making everyone a target, which leads to mass surveillance.

Information warfare weapon systems (IWWSs) are becoming a more commonplace form of government armament around the world. Nation states and various military alliances are developing IWWSs for defensive, counter-offensive, and offensive purposes (U.S. Department of Defense, 2005; Wu, 2006; YLE, 2009). However, there are major differences between IWWSs and traditional military equipment. The discussion about IWWS has been more about the use of an IWWS with traditional weaponry, for example, surveillance before missile attacks, rather than substituting for it (Heimo & Kimppa, 2013).

A few large warfare-like conflicts have emerged. In 2007, the Estonian internal conflict, which was labelled as “the bronze soldier conflict,” escalated to an international conflict between Estonia and Russia. This conflict led to Russia (although it was not proven to be the Russian Federation) attacking several Estonian information services with an effective blow to the infrastructure. The attack was one of the largest information warfare attacks ever made, lasting three weeks with a focus on governmental services, banks, and the media. Russia accused the nationalistic youth movement Nashi, which is heavily supported by Kremlin (*The Guardian*, 2007; Ottis, 2008). Another information warfare attack occurred in 2008 during the Georgian conflict. A

large distributed DoS attack separated the whole country from the Internet, while Russia began a physical invasion. The conflict was reported by *The Guardian* as the first possible modern cyberwar (The White House, 2009; Heimo & Kimppa, 2013).

Not all information warfare requires a warrior behind the keyboard. A strike malware commonly known as *Stuxnet* was considered a military grade smart weapon that was designed to seek and destroy a target in the real world (BBC 2010; Fildes, 2010; Langner, 2010; Schneier, 2010). It was a precisely programmed to use Siemens SIMATIC S7 logic controllers against an Iranian nuclear facility in Natanz. The Iranian enrichment program was successfully delayed due to broken centrifuges for an extended period (F-Secure 2010/1, F-Secure 2010/2). The the *Flame* malware (e.g., see Nakashima, Miller, and Tate, 2012), which like Stuxnet, is cyber intelligence malware that scouts the terrain and gathers military intelligence, possibly for Stuxnet (Heimo & Kimppa, 2013).

In addition, individuals and non-governmental organisations (NGOs), such as Anonymous and Lulzsec, have taken to acts of hacking and *hacktivism* (e.g., see Heimo & Kimppa, 2013). These hackers who have different goals, including breaking into and deriving information, or disturbing systems . Some of these organisations, such as Nashi, have more clear connections to nation states and their goals. For other groups, the aim can be fiscal, political, or just for entertainment (Heimo & Kimppa, 2013).

Because of these examples and recent terrorist activity in the Western world, governments are trying to focus on intelligence and increasing their rights to counter any harm to their nations and citizens. They are trying to create defences to protect against hacking of their systems by increasing intelligence work and government control over the local Internet and the information that passes through it. This task is difficult because of the rights of the targets of the intelligence operations. Giving more power to government takes more power from its citizens. Moreover, intelligence operations are, by nature, obfuscated for the purpose of efficiency. That is, the misdeeds done with these systems and their true nature and capabilities are not clear to citizens. For example, the Snowden revelations (e.g., see Landau, 2013; Hakkala, 2017, pp. 54 – 58), turned U.S. cyber capabilities from science fiction to an ugly truth in just one day.

This *security through obscurity* –while probably increasing capabilities for acting, is alarming for the common citizen, even though it can keep the tactical advantage with the military. Citizens can be assured of their security by the numbers their military provides and their own government's capability

to use the traditional military might, but to trust (or protect oneself from) something they do not know exists is a much harder task (Heimo & Kimppa, 2013).

In Finland, the discussion has been about increasing the capability of the military and civil intelligence operations of the Finnish Defence Forces and Finnish Security Intelligence Service (SuPo). The discussion is in regard to both new rights to do intelligence mainly in a digital environment and to clearly outline the field of responsibilities between the organisations in the field of intelligence. The new intelligence legislation requires changing the Finnish constitution related to problems in the wording about the legislation of the secrecy of messages. Changing the constitution in normal order requires a two-thirds majority in parliament during two separate election cycles. In accelerated order, a five-sixths majority is required in parliament during one election cycle (Finnish Constitution). The latter has never been done (Ilta-Sanomat, 2017; Niilola, 2017; Pitkänen, 2017). The new legislation is seen as important nearly unanimously by all government officials and NGOs. The problem is the content and execution of the legislation process (Järvinen, 2017).

The primary objective of the law is to protect national security, which according to the Ministry of Interior officials is a goal that the majority of the consulting comments agreed upon (Finnish Ministry of Interior, 2017). The Ministry of Interior justifies the legislation with following:

> The security environment in Finland has changed rapidly. The Government has proposed the adoption of intelligence legislation in Finland, with the aim of improving our protection capabilities against serious threats to national security. Such threats include terrorism, espionage by foreign states or disruption of critical infrastructure. (Finnish Ministry of Interior, 2017)

While it seems to be clearly beneficial to upgrade the legislation to match the digital era and clarify the legislative powers and actors under one law, the patterns of poor CGIS procurement are again visible. Even the Finnish Ministry of Internal Affairs acknowledges the problem with the feedback that it received from consulting groups. Moreover the project has had its share of critique in the media.

Because the legislation is only at it's earliest phases – planning – it is not feasible to analyse the IS solutions made. Yet the process where the creation of the guidelines – the laws – can be analysed. Although the evaluation of the

legislation and the information systems following it is an ongoing process and with the limited information available some patterns shown in previous chapters can be seen in the legislation process as well.

Critiques of the legislation include the obvious problems with citizen privacy. Scheinin (2017), amongst others, has criticised the legislation to allow mass surveillance of Internet traffic and, therefore, is against a legitimate proportionality principle (Scheinin, 2017). That is, the proportionality of the punishment should mach the crime as well as the proportionality of the criminal act taken[12] when fighting crime should be in line with the severity of the level and harm of the criminality[13]. Many experts, including Scheinin, oppose the timeframe of the proposed legislation and demand that changing the constitution should be in normal, not accelerated, order (Ahtokivi, 2017; Järvinen, 2017; Niilola, 2017; Scheinin, 2017).

However, in this case, the Ministry of Interior has listened to some of the critique that has been given and increased limitations on intelligence operations. It has also created a position for a high official, an intelligence supervisor under the Office of Data Protection supervisor, to monitor the intelligence operations (Happonen, 2017). Also, a parliamentary intelligence committee has been proposed (Finnish Government, 2017). However, these requirements are quite vague as the power of the high official might be too limited. This problem also leads to trust issues, for example, how to verify that the guardians are properly guarded.

Other questions remain, such as whether these limitations work and whether the government will find an official who is proficient to succeed in this enormously critical task (e.g., see Heimo, 2018). The future will determine how this legislation, if passed and at what pace, will be formulated and combined into the CGISs.

[12] "One does not hang a cabbage thief." – A Finnish proverb
[13] "One does not send an army to find a cabbage thief." – An application of the former.

When he had put the last touches to what he had begun, the artificer balanced his own body between the two wings and hovered in the moving air. He instructed the boy as well, saying “Let me warn you, Icarus, to take the middle way, in case the moisture weighs down your wings, if you fly too low, or if you go too high, the sun scorches them. Travel between the extremes. And I order you not to aim towards Bootes, the Herdsman, or Helice, the Great Bear, or towards the drawn sword of Orion: take the course I show you!” At the same time as he laid down the rules of flight, he fitted the newly created wings on the boy’s shoulders. While he worked and issued his warnings the ageing man’s cheeks were wet with tears: the father’s hands trembled.

—*Metamorphoses 8 by Ovid*

4 REASONS AND FIXES

4.1 Politics and National Pride or Humility

As explained previously, functionality is a key element in CGIS success. As Nurminen (1986a) states, the success of a system is more of a combination of different elements and how they correspond with each other than a single design decision. Yet, sometimes the technical and economic decisions seem to dominate the discussion of the procurement process. The economic decisions make a framework around the procurement process, that is, how much the system should cost and what the cost-benefit ratio is around the system. Where the limited resources in society dictate the possibilities around the procurement and development, technology should be seen as a tool, not as an end in itself. However, this does not seem to be the case (e.g., see Kivekäs, 2012; Niilola, 2012; Peltomäki, 2012; Helsingin Sanomat 2013; Iranto, 2013; Juntunen, 2013; Kasvi, 2013; Liimatainen, 2013; Lindstedt, 2013; Pitkänen, 2013; YLE, 2013; Rantanen & Heimo, 2014).

The problem of nations holding leadership in ICT usage as an end itself seems to have something in common with national pride. Europe and the US have both recently seen some nationalistic movements. This national pride seems to have a common rhetoric, at least in Finnish discussions, that mainstream politicians use from all political perspectives (e.g., see MTV3, 1999; Valtioneuvosto, 1999; Himanen, 2004; Kauppakamari, 2013; Kasvi, 2014; Katainen, 2014; Harjuhahto-Madetoja, 2016; Kauppalehti, 2017). Being in the forefront of ICT-using nations is seen as an end in itself, not as a means to improve society. Possible negative outcomes that professionals point out are often dismissed as dystopian(?) science fiction (Heimo, Fairweather, and Kimppa, 2010).

In political rhetoric, the term *information society* seems to arise from time to time as a value in itself. An information society reflects efficiency, electronic government practices, and generally a modern society in all positive ways. What it really seems to mean is *the whole third industrial revolution for good and bad* (e.g., see SCF Associates Ltd., 2009). While rhetorically being at the technological forefront might be appealing, nothing

about technology means that being an early adopter is a good thing, and therefore, justification for the value itself is needed. A high proportion of technologies, from supersonic airliners, to Betamax video, to pagers, and to using Gopher to retrieve information from the Internet offered opportunities to be at the technological forefront until the technology came to be seen as a dead-end (Heimo et al., 2010).

Many nation states that had committed to eVoting, such as Norway, Ireland, Netherlands, and UK, have since abandoned it. This is understandable because of costs, for example, at least EU€54 million in Ireland (Melia and Byrne, 2012) and GB£40 million in Scotland (Verzola, 2008). Another reason is public resistance after trials (e.g., see Oikeusministeriö, 2009). In the UK, unaddressed issues of security and transparency were the main reasons to abandon eVoting (Electoral Commission, 2007, p4). It seems that it is not inevitable to turn to eVoting, but rather it is inevitable to try it. For some reason, many nation states have enough nationalism, stubbornness, or lobbying to not learn from others' mistakes (Heimo et al., 2010).

This phenomenon does not apply to many other CGIS, such as eHealth systems, which seem to have become mandatory in most of the digitalised world. Nonetheless, cases like Kanta[14] and Apotti[15] show a clear indication on how a governmental actor wants to show power by doing larger projects than it actually seems able to (e.g., see Alaranta, 2013; Storås, 2015; Nykänen 2014; Turtola, 2015).

van den Hoven (2013) spoke about inserting values into design. For example, a low door where a person must bow to enter implements value-based design to the architecture. Similarly, we should identify these kinds of values before design in the procurement process. Therefore, instead of pride, more humility could be incorporated into the design of these systems. They are procured to safeguard us from harm, maintain our health and well-being, and maintain and improve our society with the values we have decided.

Procuring these systems is not only an implementation or an improvement to our current society but a transformation from one state to the next. The moment we start making changes, something else changes (e.g., see Nurminen, 1986a). To increase the possibility that the change is a positive one requires meticulous work that cannot be done when we are over-estimating our capabilities and not being humble.

---

[14] see http://www.kanta.fi/
[15] see http://www.apotti.fi/

4.2 Closed Monolith or Modularity and Open Source

Many eHealth solutions in Finland are built as big monoliths that consist of many different subroutines. For example the Apotti project is now approximated to cost circa 575 million euros (Kolehmainen, 2016). The functionalities of health care areas differ because the healthcare is a large collection of interlinked areas. Therefore, the healthcare sector can be seen as fragmented. For example, in addition to the most basic information, a dentist requires different information (and differently parsed information) from an HCIS human-computer interface than a radiologists or an ER nurse. The motives of the governmental office could be questioned when making only one monolithic system that is designed to solve all these separate problems. The alternative is to divide the problem into smaller modules.

In this context, modularity stands for the idea that information system are constructed out of separate, interchangeable modules that do not fully depend on other modules but have relationships with the other modules. Moreover, modularity implies a procedure for separating different parts of the information system into stand-alone modules that can be procured, developed, maintained, and changed without endangering the functionality of the whole system. For healthcare, this means defining a focus on one process for a specific purpose or activity.

A key problem in big monoliths is vendor lock-in, where the user of the system is tied to the services of one IS producer. That is, when problems occur with the IS, only the designated system provider can support it whereas when the system is in smaller modules, a substitute for ordering a fix for the system can be ordering a module from a different producer thus generating an incentive for the original producer to lower their bug-fixing and updating prices. In many agreements between the service provider, such as a government office, and the system provider, bug-fixes, for example, can be free-of-charge. If the procurer left off a key work element outside the list of required system functions, the client is required to buy that functionality from a certain vendor, regardless of price. In a modular system, the missing module can be acquired from another vendor, but with bigger monolithic ISs, this is not possible.

When done modularicly the competition is in lower levels and thus more competition can occur in the field – the smaller enterprises are also allowed to compete! Moreover the big companies can provide different quality of products to different fields (e.g. Company A can have an excellent dentistry software but their x-ray analyser is worse than one made by their

competitors). Therefore even a single-buyer organisation can have choice and cherry-pick the best solutions for different situations instead of being forced to choose one overall set of solutions and services.

Using a modular approach to develop solutions for strictly defined problems could avoid issues with the complexity of the solution. The system could be analysed and verified with more ease, increasing the likelihood of success of the HCIS development. If the modularity of HCIS is done correctly, the system implementation could better meet the demands of the aforementioned fragmentation of healthcare.

Koskinen, Heimo, and Kimppa (2018) state that ethical viewpoints of the design must also be verified and validated to ensure the safety, health, and well-being of patients. They argue that the implications with modularisation are clear enough to promote it because the ease of IS verification and validation is both functional and ethical. They also argue that:

> Modularisation in wider sense, especially in the eHealth – and eGovernment in general – can ease the challenge of procuring, developing and implementing these systems, but it can be argued that the main contribution of the modularisation is the easier control of the system. (Koskinen, Heimo & Kimppa, 2018)

With modularisation comes the possibility for open source development. While more complex solutions tend to be single-provider monoliths, more modularised sets can be handled by various producers. Open source, in many cases, would abolish most of the secrecy from the system because it would be easy enough for any professional or proficient amateur to review the system. Kimppa (2004) states:

> “If IPR’s [Intellectual property rights] didn’t exist, any party could use advances of another party, and instead of these monstrous development projects (be they in software or other immaterial) we could instead advance by multiple smaller steps. This is specifically beneficial in software development where modularity would often time [sic] (see e.g. many F/OSS projects, most predominantly GNU/Linux development (Raymond, 2001)) work much better than grandiose projects that try to answer all problems in one centrally organized software.”

Open source code should be a prerequisite to meet the appropriate standards of transparency (see e.g. Wolf, Miller and Grodzinsky, 2008). However, it does not solve the fundamental tensions between trust and extensive security, universal access, and strict privacy. Indeed those tensions have caused one previous advocate of open-source eVoting to recant (Kitcat, 2004; Heimo et al., 2010). Wolf, Miller and Grodzinsky (2008) argue that "[a]nyone wishing to be critical of government's operations and analysis would have access to the same software tools as the government and could therefore explore alternative analyses and operations." Yet there are situations where it would be crucial to know whether the said program is running in the system or some alteration of it.

Some open source solutions have been available for a while, such as the U.S. Veterans' VistA (U.S. Department of Veterans Affairs, 2009). Also a call for universal adaptation of an EHR was made in the United States House of Representatives (H.R. 3124, 111th congress). It aimed to pass the Health Information Technology Public Utility Act of 2009, which aims to:

- create a new federal Public Utility Board within the Office of the National Coordinator for Health IT to direct and oversee formation of this HIT Public Utility Model, its implementation, and its ongoing operation;
- implement and administer a new 21st Century Health IT Grant program for safety-net providers to cover the full cost of open source software implementation and maintenance for up to five years (with the possibility of renewal for up to five years if required benchmarks are met);
- facilitate ongoing communication with open source user groups to incorporate improvements and innovations from them into the core programs;
- ensure interoperability between these programs, including as innovations are incorporated, and develop mechanisms to integrate open source software with Medicaid and Children's Health Insurance Program (CHIP) billing;
- create a child-specific EHR to be used in Medicaid, CHIP, and other federal children's health programs; and
- develop and integrate quality and performance measurement into open source software modules (Healthcare Informatics, 2009).

The proposal died the same year (H.R. 3124).

Modular open source CGIS solutions could solve some problems in an efficient, economical, and ethical sense. There should be no need to re-invent

the wheel, so that, when a solution for a particular problem is developed, other developers can develop it further, saving some time. Therefore, the coders and their employers would not compete with each other but rather co-operate to improve the system for everyone. Current economic realities do not fully support this approach because people usually require monetary compensation for their intellectual property rights.

Thus, when someone has to pay for development, the government could order smaller modules or make open or closed bids to develop and improve current modules instead of ordering only “big solution A” or “big solution B”. The development cost could also be paid by smaller actors than the government, such as hospitals and municipalities. In a best-case scenario, these solutions are bought as open source; the cost could be distributed amongst many, done partly as pro bono and in a manner in which others could develop the software further. This approach can also improve the HCISs in developing countries, giving them access to functioning software and saving them healthcare costs for their citizens. This of course does not extend to many national security software.

At a minimum, the base infrastructure for the modules to connect should be open source and the system designed so that the modules are small, and only the backbone of the system is designed separately. This infrastructure should make it possible for small solutions for specialised problems to truly compete with each other, at least with systems as complex as eHealth. This approach differs from the current practice where a system might have an open interface that is built by one developer. Therefore, these interfaces are directed from outside of the system, where all the important parts of the system are implemented as an inseparable part of the system.

With the former method, however, one developer could produce software for an ER and another program for radiology. Without the basic infrastructure, only big system developers can implement solutions to their system, making it consist on only their solutions. A modular open-interface frame, however, could aid smaller software developers to come up with more efficient, economical, and ethical solutions for the public to utilise. This concept also holds true for eVoting and biometric passports, keeping in mind the principle limitations of those fields.

The main problem with open source is knowing who is checking that the program is running in the system. For example, workers, administrators, hackers, or even the government might have installed secret components. It is easier to check the source code, but to verify the actual binary files or the electronic components as the correct ones on every computer separately is a

difficult task. One somewhat cumbersome solution is to use checksums to verify that the executable file matches the executable file that was made in a controlled environment from an uninfected source code.

The problems with modularity come from the contract of how to store and transfer data between the modules. The interfaces between the modules must be programmed so that the data integrity is secured. When technology advances the program modules can produce different style of data than previously designed – e.g. larger and more accurate image files – thus demanding the interface to be updated. This in some cases can lead to the requirement to update all the interfaces – and reprogram many of the modules. Thus when designing modular systems, the backbone of the system – the databases and the interfaces – must be designed meticulously to diminish the amounts of updates required as well as the modules must be procured keeping in mind that there might be changes in the interface.

4.3 Indifference or Responsibility and Accountability

Responsibilities for the actions required for CGIS must be allocated. It is important to understand who could be responsible and how to manage their responsibility in these situations. In many cases, it seems that responsibility is either not defined or it not actualised (Heimo et al., 2010; Heimo, Koskinen and Kimppa, 2013; see also Vartiainen, Heimo and Kimppa, 2016). Indifferent attitudes about responsibility can easily affect the results and generate negative impacts for the society.

CGIS development should be done responsibly and requires the identification of a responsible actor to counter the indifferent attitudes toward the outcomes. Best practice dictates that during any IS project, a stakeholder analysis should be done. However, in this situation, the discussion is about responsibility. The situation also requires an understanding of the difference between responsibility and accountability. Even though an actor may be responsible, but they might not be held accountable (Heimo, Koskinen, Kainu, and Kimppa, 2013). That is, if one is responsible, they are seen as having an obligation of fulfilling a task. If, on the other hand, they are held accountable for the failure, they have (legal) consequences. One can be responsible for a task beforehand but they can be held accountable for it only after they have failed to perform the task. And if no one is ever held accountable for their actions, the idea of being responsible for the actions may lose its' ground.

If no one is accountable, a plan must be defined as to whom to direct the demand for efficient, economical, and ethical CGIS. Heimo et al. (2013) divide the possible responsible CGIS parties into four basic interest groups:

- the government office, whose task is to formulate the solutions to fulfil the needs of the society;
- the producer, who delivers the requested system;
- the end-user group, which consists of the people who will use the system; and
- the citizens, who are the targets of the system usage (Heimo et al., 2013).

Any or all of the groups can overlap. Heimo et al. (2013) argue that "the fundamental responsibility rests with the authorities" because "[t]hey hold the monopoly to the services they have been nominated to produce, control and upkeep and are in superior position in relation to others and thus with great power comes great responsibility." Therefore, citizens are unable to choose an alternative (Heimo, Koskinen, Kainu, and Kimppa, 2013). The end-user group possesses professional knowledge of their trade, not the skills to understand IT and they are most likely unable to verify the CGIS system as a whole. Therefore, assigning the burden of proof for the system functionality to the end-user group is unfair, leaving the system producer or governmental office, the procurer, to take that responsibility.

Rawls (1997) states that in society any change in the procedure must be to the advantage of the weakest parties, which in this case are the end-users and citizens. With the power to decide for the public comes a responsibility to the public. Therefore, responsibility must be either with the procurer or the supplier. The supplier's responsibility is in fulfilling the requests of the customer, that is, the governmental office. If the supplier fails at this task, the supplier is responsible to the authorities for their failure for not fulfilling the requirements they agreed upon. If the supplier of the CGIS fulfils its obligations, only one party remains for being assigned responsibility (Heimo, Koskinen, and Kimppa, 2013).

The authorities have a monopoly in supplying CGIS. They are in a supplier role in relation to citizens. That brings forth the responsibility to provide a functioning product. If the system is put into use, the final responsibility lies with the last supplier of the system, which is the government office, the procurer (Heimo, Koskinen, and Kimppa, 2013). If the developer of the system does not fulfil its obligations, the problem is between the supplier and the procurer. Therefore, the procurer must have specified

possible penalties for not fulfilling the obligations in such a manner that minimal harm comes to the public.

The situations of private organisations versus public organisations seem partly similar, partly different. In a private organisation, at least in theory, someone who is responsible to the stockholders (e.g., CEO, CIO, the board) is in charge of the actions. In a public organization, the responsibility seems to disappear into the system. This does not mean that IS procurement in the private sector does not have any problems, but rather they differ in this way (Vartiainen, Heimo, and Kimppa, 2016).

A representative of a governmental office or the system provider is unable to give reliable information due to the certainty trough (MacKenzie, 1990). It is impossible to reasonably give accountability to those who are unable to hold the responsibility due the problem that they cannot affect the outcome in the first place. Only those who can perform the actions can be accountable for the actions. It seems that no stakeholder can take the responsibility to verify the system against design errors. For a system to be considered a secure system, a verification process by a specific outside party who verifies the system development and upkeep process is required (e.g., see Heimo, Koskinen, and Kimppa, 2013). Those who are auditing CGISs must be accountable for the audit. As the watchmen require someone to watch them (see Juvenal) when they have erred in their job, they must be made accountable. In any other case, this façade of trust is quickly dismantled.

4.4 Security through Obscurity and Forcing the Trust, or Security through Trust

Secrecy, while being justified by security, easily diminishes it. The scientific community usually sees security through obscurity solutions differently. French mathematician Kerckhoffs defined the basis for (military) information security. Kerckhoffs' (1883) second rule states that security cannot be built upon any basis other than the encryption key, and the system designer must make an assumption that the enemy *knows* the system that is being used (Shannon, 1949). Therefore, security through obscurity cannot be accepted as a scientifically acknowledged and valid security method (Kerckhoffs, 1883; Shannon, 1949; Schneier, 1996, pp. 5 – 7; Molnar & Wagner, 2004; Gonggrijp and Hengeveld, 2007; Hoepman & Jacobs, 2007). It seems that this

method is used as a security measure (e.g. in Finnish eVoting and Passport registry cases).

As stated by Kerckhoffs (1883), Shannon (1949), and Schneier (1996), systems must be built in such manner that everything, except the cryptographic keys (crypto keys) are public. The public can evaluate system security and be ensured that the system is built properly. While security through obscurity can slow possible intrusion for a while, it does not remove all possible security threats.

Many of the security through obscurity systems are audited. Even so, in many cases, only some parts of the system are audited, the rest remains a mystery, and in some cases, auditing is done to silence the opposition. For example, the many auditors who were invited to audit the eVoting software in Finland declined because of the non-disclosure agreement (NDA) placed by TietoEnator. It was described as too restrictive. “The agreement is not designed to protect trade secrets, but to silence all criticism” (Tarvainen, 2008).

If a system is designed with security through obscurity, people tend to trust it as explained in Section 5.3 or because of *the certainty trough* idea (Mackenzie, 1990). With a certainty trough, people are more likely not to trust intercontinental ballistic missile (ICBM) technology when they: (a) are directly connected to ICBM development, or (b) do not have enough knowledge about any technology, as illustrated in Figure 2. Those who have knowledge about technology, but not expertise on ICBMs, are the most trusting about these doomsday machines and their safety (Mackenzie, 1990).

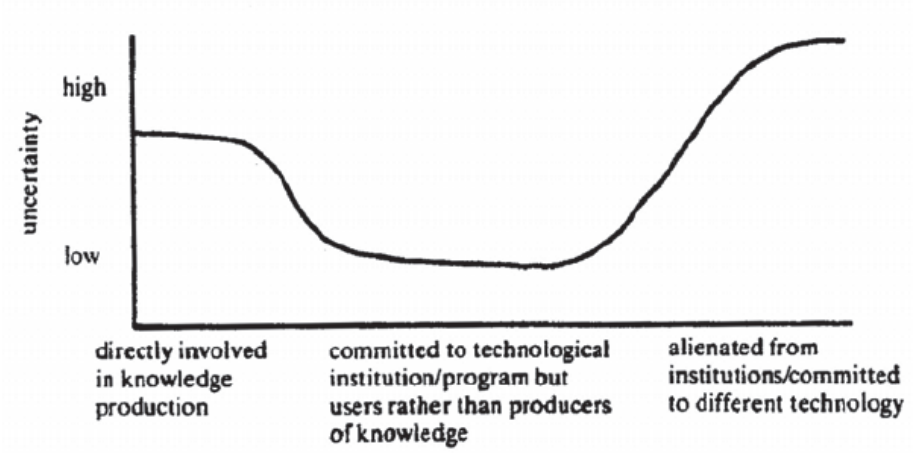


Figure 2. *Certainty Trough. From Mackenzie, 1990, p. 371.*

Pantzar (2002) generalizes this theory to all technology. He also claims that the marketers of the product, those who represent the producer, are denied their right to be uncertain about the product they are selling. In a wider sense, this includes the suppliers' representatives and anyone with technological savvy. Therefore, even a university professor of mathematics can state that what is impossible is possible (e.g., see Mölsä, 2008).

When a government is designing or procuring a system for the public, government representatives cannot appear to be uncertain of the product that it introduces to its citizens. In a situation where this risk is actualised, the information that government officials give to the public is misleading (e.g., Woolgar, 1994; Mackenzie, 1990; Pantzar, 2002).

Hakkala et al. (2017) discussed trust and forced trust. They define forced trust as "a situation where a user is dictated to use and to trust an information system or an ICT product." Hakkala et al. (2017) state that

> '[F]orced trust' concept depict a situation where an entity– whether a customer, an organization or even a governmental agency–does not have a privilege to choose but is instead mandated to use a dictated information system.

They argue that the most important trust issue is to understand where the trust is forced. If the system forces trust from any of the stakeholders, the stakeholders are subject to use power. When the trust is forced, the enforcer must have some external power that they can rely upon. If this power is lost, the forced trust is lost. The perceived power and the possible consequences must be greater than the probable gain from breaking the trust (Hakkala et al., 2017). Schneier (2012) divides trust into moral, reputational and institutional pressures, and security systems.

For CGIS, the requirement for trust is to verify the correctness of an IS at least at some level. Without these mechanisms, trust turns into belief. Therefore, the trusted party may "fulfil the needs of the person or organisation in question and not the needs of users" (Hakkala et al., 2017). The key element with trust is a panopticon that is designed to reveal at least some malpractices; that is trust with occasional verifying.[16] The main problem amongst security through obscurity of CGIS designs is the lack of openness and the possibility to conceal potential malpractices within the system (Hakkala et al., 2017).

[16] "Trust, but verify." – A Russian proverb

The resources that are given to organisations are finite, as are the results that they are required to produce. When these limited resources are scarce enough, the trust towards the CGIS – it's producer, functionality, security etc. – must be forced. Without watchmen, we must trust others, even when malpractice is a possibility. When these malpractices are not too grievous, the system still works (see e.g., Fairweather and Rogerson, 2002, p. 30). The key issue is understanding, and therefore, balancing the where, when, and how to dismantle the forced trust and when to pay for increased security (Hakkala et al., 2017).

With CGIS, the magnitude and probability of malpractices are key elements in understanding the problem. For example, the patients might give wrong information about their symptoms to acquire (otherwise legal) drugs, or a developer might leave a backdoor to the system to sell patient information to the highest bidder. Although the former example is not desired, the latter is clearly of a different magnitude and must be countered. Resource allocation to check the system against the worst possibilities, at least with some form of a panopticon-style solution, is a necessity. Not all trust can be forced, but not all security issues can be countered either. The procurer of these systems, therefore, must balance between them. That is, verify at least what is of utmost importance. This of course is the worst plausible situation – if it is plausible.

4.5 Inseparability Postulate: the Ethical Version

During the digital revolution, memos, sticky notes, and traditional mail were replaced by digital information systems, email, mobile phones, databases, search engines, and so on. This revolution not only filled our lives with gadgets, but it changed the way we store, analyse, organise, and deliver information to each other. The inseparability postulate is a product of the research tradition of the Scandinavian information system, where socio-technical and humanistic approaches of research emphasises that the IS is an inseparable part of any work process. The IS is no longer seen as an entity by itself but as a tool that allows for and simplifies work processes and the communication between people, creating more than just automating what already existed. In this tradition, ISs are seen to lack any goals other than what the people using the system have (e.g., see Järvinen, 1983; Nurminen, 1986a; Nurminen, 1986b; Bødker, 1989; Nurminen & Eriksson, 1999; Heimo, Kimppa and Nurminen, 2014). The inseparability postulate is:

You cannot _____ the information system and the way it functions without _____ the way the organisation functions (and vice versa).

The system is part of work processes. The users of the system do work with the system and are part of that system. The goals of the users of the system should be the goals of the system (Nurminen 1986a, pp. 84, 99 – 101).

The inseparability postulate extends Leavitt's (1964) idea that structure, task, technology, and people areas interconnected. It defines the inseparable nature of technology and the organisation better than Leavitt. It states that the IS is inseparable from an organization and that, when the way in which the organisation functions changes, the information system and the way it functions automatically changes. Yet, what these changes are is – at least partly – unknown. Also, when the IS is destroyed, the way in which the organisation functions is destroyed. The IS is not an actor and has no goals of its own. Moreover, the goals that form when the system is used should meet the goals of the user. Because users are both actors and part of the IS, the organisation that consists of the users is inseparable from the IS (Nurminen 1986a, pp. 84, 99 – 101).

Using an IS has consequences for its users, the organisation, for other organisations, and especially for the targets of the system. The targets of the system are the people whose lives the system impacts. When designing ISs, it is important to consider that every design decision that changes the system also changes the effects of the system on those who it is used upon (Johnson 2001, p. 5). The goals of the designer are required to be good and the consequences proper (e.g., see Moor, 1999; Tavani, 2007, pp. 64 – 66) (Heimo, Kimppa, and Nurminen, 2014).

CGIS can have grave consequences to its intended targets. For example, if a passport system has a fault, people can have their identities stolen; if an election system has a fault, democracy might stop functioning; or if a healthcare system has a fault, people can lose their lives (Heimo, Fairweather, and Kimppa, 2010; Heimo, Hakkala, and Kimppa, 2012; Heimo, Koskinen, Kimppa, 2013; Heimo, Kimppa, and Nurminen, 2014).

As Koskinen, Heimo, and Kimppa (2012) argue, systems should be built to serve the ethical principles of the customer organisation, not to emphasize the ethical principles of the producer. The ethical principles are, as Heimo, Kimppa, and Nurminen (2014) state: "not only included into the system to support the work process but as a model of the work process itself: the ethical values of the information systems are therefore inseparable of the ethical values of the work process."

Values are always designed into a system. If there is no purpose for the system, there is no reason to design it. Purpose brings values. The design values might differ from the values of the users of the system. For example, the values connected to an IT designer's work (as an IT professional) are different than the values that are connected to a medical doctor's work (as a medical professional) (Heimo, Kimppa, and Nurminen, 2014; see also Gillon, 1994; Koskinen, Heimo, & Kimppa, 2012).

CGISs have a purpose of maintaining a critical parts of our security (e.g. border security, police, military, and traffic control), health (e.g. hospitals and ambulances), and wellbeing (e.g. food, electricity, and fuel). Analysing the requirements, designing meticulously, and enforcing the desired values on the system are imperative for the system to fulfil its part in the process of securing and maintaining that critical service or infrastructure to society and its members. These systems support work processes that are loaded with goals, values, and ethical codes of the critical services that they serve. These values should be integrated during system development (Heimo, Kimppa, and Nurminen, 2014). Similar conclusions have been made by van den Hoven (2013) and Stahl et al. (2014), for example.

According to the inseparability postulate, if the IS is poorly designed, it does not support the goals of the work processes of the organization's users or target population as it should (Nurminen and Forsman, 1994). Heimo, Kimppa, and Nurminen (2014) state that this problem stands for both practical and moral goals. They argue that the ethical principles that the IS is founded upon cannot change without changing the ethical process of the IS that the organisation supports and is mainly founded upon.

Heimo et al. (2014) also argue that, to guarantee the security, health, and wellbeing of the public, this postulate should be taken into account throughout the whole lifecycle of the CGIS. Whenever an IS is modified, the possibility exists that the ethical principles of the IS are altered, modified, or destroyed. Modifying an IS means improving, altering or destroying the functionality of

the whole information system and vice versa. The ethical principles of the organisation must be taken into account in the lifecycle of the IS to ensure that the system supports the ethical principles of the organisation.

He gave a never to be repeated kiss to his son, and lifting upwards on his wings, flew ahead, anxious for his companion, like a bird, leading her fledglings out of a nest above, into the empty air. He urged the boy to follow, and showed him the dangerous art of flying, moving his own wings, and then looking back at his son. Some angler catching fish with a quivering rod, or a shepherd leaning on his crook, or a ploughman resting on the handles of his plough, saw them, perhaps, and stood there amazed, believing them to be gods able to travel the sky.
—*Metamorphoses 8 by Ovid*

5 THE ICARIAN METHOD OR THE DAEDALUS EFFECT

Currently, the core process to procure, procure, develop, and implement many CGIS is somewhat flawed. In this thesis, the shortcomings are Icarian in nature. Icarian refers to Icarus, the son of a protagonist in an ancient Greek poem that is narrated by the Roman poet Publius Ovidius Naso, who is commonly known as Ovid, in his book *Metamorphosis.* In this epic, Daedalus, an inventor, gave his son Icarus the newest technology to escape from the island of Crete. Instead of heeding his father's warnings, Icarus decided to use the new technology beyond its limits and perished because of his actions. The current practices seem to reflect this story, where technology is not only being developed but putting its users at risk.

In this thesis, the Icarian method in CGIS means: To implement possibly dangerous systems into use without heeding the advice of the professionals, without considering the possible consequences, or neglecting the overall responsibility of the governmental office towards the society. As described in this thesis, the Icarian method seems to be – if not a common practice – at least somewhat usual way to procure CGIS. In this chapter the issue is discussed through the ancient philosopher Aristotle's ethical framework.

According to Aristotle, to reach Eudaimonia, one must be virtuous in their everyday life. A good person fulfils his or her telos by avoiding vices, achieving their virtues, and most of all, developing their character – by flourishing in what they do. Implementing virtues is part of everyday life, and doing so develops character, which is a sum of a person's deeds. By following virtues, acting virtuously becomes a natural aspect of ones actions so that the character develops itself to be virtuous (Heimo, 2017). Vallor (2013) states that moral skills are necessary for moral virtue:

> Someone could have moral skills in the sense of practical moral knowledge but fail to be virtuous because they are unreliable in acting upon this knowledge, or because they act well only for nonmoral reasons. Still, moral skills are a necessary if not a sufficient condition for moral virtue. Without the requisite

> cultivation of moral knowledge and skill, even a person who sincerely wishes to do well consistently and for its own sake will be unsuccessful.

Virtue ethics does not generate a set of norms for normative ethics, to improve both people and society. Moreover virtue ethics generates guidelines both by promoting the virtuous actions and by encouraging people to avoid vice. The normativity comes from the level of ideas rather than from a strict set of rules. According to Aristotle, only through virtues can a person generate true value and vice versa with vices. Humans should aim for a virtuous life, which in the Aristotelian sense requires aiming for their telos, having virtuous friends, and navigating vices to arrive at virtue. A character is not virtuous by following virtue alone, since one might follow virtue reluctantly and in the face of temptation. Rather, when a person automatically aims toward all virtues, the character can become virtuous. (EN I, 9 – 10; 1098a, 15 – 21; 1098b 5 – 30; 1100a31 – 1101a21, II, 1; 1103a31 – 1103b25, 1104a10 – 1105a16; McPherson, 2013). Or as Vallor (2009) explains:

> […] the moral development of individuals cannot be assessed or predicted simply by looking at what they think, feel or believe—we also have to know what kinds of actions they will get in the habit of doing, and whether those actions will eventually promote in such persons the development of virtues or vices.

Being virtuous then is not a situational choice but a life choice, and only through a life choice can a human enjoy a happy and good life. Yet socially valued virtues might not equal ethical virtues (Beauchomp & Childress 2001, p. 27). At work, humans are often expected to follow socially valued virtues even though they conflict with their moral virtues (e.g., Murphy, 1999). Being good at one's work does not equal being virtuous. The totality of human life, which is not divisible into parts that can then ignore other parts, needs to be taken into account and built virtuously (MacIntyre, 2004, pp. 240 – 241; 2007, p. xv).

A problem that Aristotelian virtue ethics brings forth is the dictation of only higher-level abstraction, for example: be brave; do not act cowardly, foolhardily, or rashly. Therefore, more in-depth analysis is required, such as to answer the question of what it means to be truthful, as in the following example:

> Let us discuss them both, but first of all the truthful man. We are not speaking of the man who keeps faith in his agreements, i.e. in the things that pertain to justice or injustice (for this would belong to another virtue), but the man who in the matters in which nothing of this sort is at stake is true both in word and in life because his character is such. (EN IV, 7, 1127a33 – 1127b2.)

Churchland (2011, p. 115) on the other hand turns the higher abstraction-level as a favourable position to virtue ethics, as the higher-level concepts – ideas rather than rules – tend to work better with the human mind. Rathermore Churchland implies that there cannot be universal categorical laws by which we can tell the right from wrong all the time and we are more able to understand the right from the wrong – truthful from the false – better than via complex set of norms or rules. (Churchland, pp. 114-116.) Aristotle states that not only words and actions define truthfulness or honesty, but life itself defines whether an actor is indeed truthful or honest. Moreover, over time the repeated practice of truthfulness can lead the person to understand the concept of honesty, see the value in it and embody it better and with more ease. Or as Vallor (2013) explains, those who have cultivated themselves in the virtue of honesty have "[…] learned how to excel at truth-telling in any situation that might arise: who to tell the truth to, when and where, in what way, and to what extent."

A virtuous CGIS procurer or developer both fulfils stated promises and legalities and aims for the right choices because they are right and virtuous and develops their character towards better skill, knowledge, and virtue. If NDAs are used only to justify actions and choices in a legal sense and to avoid responsibility, they might not always be described as ethical, as in Finnish eVoting case (e.g., see Tarvainen, 2008). To ensure virtuous CGIS development, the actors must be virtuous, and the ethical basis for the system must be sound (Heimo et al., 2014).

MacIntyre (2004) points out that, to interpret Aristotle, humans must not just study Aristotle, but comprehend that he wrote for his time, where the world, linguistics, and culture were much different from today. The ideas of social beings and norms, and even the meaning of the words, have surely changed. To comprehend the relevance of Aristotle's texts, we must understand and interpret the virtues that are required in relation to the modern world (MacIntyre, 2004).

According to MacIntyre (2004), language and society are bound to each other. We live in quite a different society today than the ancient Greeks did.

Therefore, to understand Aristotle, we must reflect on how the virtues in that society were understood. Aristotle aimed to be understood by other educated Greeks, not by barbarians who lived in the northern part of the continent and over two millennia later. To truly comprehend the virtues and vices, we must focus on the translation and modernisation of the term and understand the virtue itself, that is, to understand how to be a good procurer and a good person.

Aristotelian virtue ethics does not solve all problems. Virtues and analysing them alone cannot guide professionals toward making CGIS because they cannot be used like mathematical calculations, but they can serve as a practice – even a best practice. Virtuousness serves to improve the individual(s) and thus make the society a little better.

Aristotle teaches that the balance for action is somewhere between the extremes (Churchland, 2011), or as Daedalus advices in the epic: *"If low, the surges wet your flagging plumes; If high, the sun the melting wax consumes: […] But follow me: let me before you lay"* (Ovid, 8). Where the Icarian method is about acting without heeding advice, acting before thinking, acting without humility toward the enormity of the task, and acting without virtues, there must be another extreme. That extreme is a direct opposite in which all advice is taken in account, where people think and ponder, but no one gets anything done. Inaction is at the other end of the problem. While there is not always a need for a new CGIS, in many cases, there is a need, and it is justifiable to procure one. The virtue then is to understand where, between inaction and the Icarian method, one should stand. The virtue where a person (or an organisation) does what is necessary but with humility is a counterforce for both – a virtue between the extremes – the inaction and Icarian method. Let us call that the *Daedalus effect*.

In the epic, Daedalus offered guidelines for gaining advantage from a new technology. In the modern era the scientists who study computing artifacts and the philosophers who describe the possible utopias and dystopias urge and warn us that we should heed to these ideas. Where the ideas seem likely, on some scale, the ideas of the scientists and philosophers must be taken into account. This does not mean any philosopher because the word *philosopher* in later times seems to have suffered some inflation. The word *philosopher* comes from the ancient Greek word *philosophia*, "φιλοσοφία", meaning love of wisdom. This term is too broad for the use in CGIS development. Nor does the statement mean any scientist, but a scientist with understanding of CGIS development and philosophy. Now we can think of a philosopher, a lover of wisdom, who has proven knowledge in both the technological and scientific

field of CGIS and the skill in philosophy, IT ethics especially. To ease our discussion, let us call that person *an archon*.

Heimo (2017) introduces a list of requirements for this archon (all required). An archon:

- understands the technical limitations of the current available technology (see also Mercuri, 2001; Heimo et al., 2010);
- finds the societal needs for the new system (if any) (see also Mercuri, 2001);
- has communication skills to define the terminology and frame of discourse to enable the public discussion about the subject (e.g., see Heimo et al., 2013; Rantanen & Heimo, 2014);
- comprehends the work process of the people who are working with the (future) CGIS (see also Leavitt, 1964; Nurminen, 1986a; and Heimo et al., 2012);
- sees the needs of citizens who are forced to use the CGIS (see also Heimo et al., 2012; Heimo et al., 2013; Heimo and Kimppa, 2014);
- desires to protect citizens from overly eager gathering of their information (see also Heimo et al., 2012);
- bravely pushes only those systems that are clearly better than the systems they replace, and requires suppliers to improve the systems wherever the system might pose a threat (see also Heimo et al., 2013);
- has the wisdom to understand the overall responsibility that they are entrusted with (see Heimo et al., 2014); and
- accepts the accountability of their failures (see also Heimo et al., 2014).

An archon could also be a person who monitors and moderates the discourse about CGIS (and how the discourse on the aforementioned discourse should be conducted) as mentioned before when discussing eHealth, and derives the meaningful and rational arguments from the public discourse – both citizens and experts alike. Archons should be the society's shield against irrationality.

Therefore, we define the Daedalus effect as: *When a scientist who is directly involved in the technology or an archon warns of possible misconducts with a technology and those who develop the information system heed the warning.*

The Daedalus effect is in place where the warnings of those who focus their life on knowledge or wisdom make a difference, where reason triumphs over politics. It is the moments when virtues rule over profits, or when the people who are responsible did their job not for fear of punishment but because it was the right thing to do.

The balance this virtue seeks requires a lot of work. People should be proficient in understanding both the social and technical (and socio-technical) aspects of the change and have the courage to pursue the best solutions. They should also have proper ambition and pride (not over-ambitious nor unambitious), be patient (not irascible nor lacking in spirit), and be truthful (not boastful nor understating), and so on. To fulfil the requirements of such a large set of virtues, they should dedicate their lives to the pursuit of the aforementioned virtues. According to Aristotle, this pursuit requires higher virtues of practical wisdom and contemplative wisdom (EN I 9 – 10, 1098a15 – 21, 1098b5 – 30, 1100a31 – 1101a21, IV, 7, 1127a33 – 1127b2, VI, 12, 1144b01 – 1145a13, X, 7, 1177a11 – 1177b03).

Practical wisdom is not theoretical wisdom, but instead is "a true and reasoned state of capacity to act with regard to the things that are good or bad for man" (EN VI 5, 1140b). Aristotle claimed that it is impossible to be practically wise without being good. Therefore, a good leader (or a good procurer or developer) can benefit from having practical virtue. Political wisdom also shares the same state of mind, but it differs in essence:

> Of the wisdom concerned with the city, the practical wisdom which plays a controlling part is legislative wisdom, while that which is related to this as particulars to their universal is known by the general name "political wisdom;" this has to do with action and deliberation, for a decree is a thing to be carried out in the form of an individual act. This is why the exponents of this art are alone said to "take part in politics;" for these alone "do things" as manual labourers "do things." (EN VI, 12, 1144b01 – 1145a13)

Aristotle stated that the highest form of virtue is *contemplative wisdom*, meaning that the person enjoys thinking, and while thinking, he[17] is enjoying. This kind of person is, therefore, driven to think about things happily while

[17] Can be applied to both sexes.

learning and enjoying new ideas and comparing them to old ideas. By achieving the supreme virtue of contemplative wisdom, a person becomes inseparable from achieving all the virtues of the character (EN X, 7, 1177a11 – 1177b03).

To have virtue that leads to the Daedalus effect, which requires the love of knowledge to be in action, a person should indeed be proficient in the highest virtues, the virtues of practice and wisdom. That is, even Aristotle knew the best CGIS procurers are philosophers.

According to MacIntyre (2004), Aristotelian texts require some interpretation. While the philosophers of ancient Greek were scholars, wise men, and aristocrats who spent their days debating and arguing, the philosophers of today can easily fill their days with administrative reports and funding applications – if their workplace does not support the research. To understand the concept of the philosopher, we must go deeper into the subject. The best description of philosophers of the ancient world could be that they were people who by definition loved wisdom, were driven to acquire knowledge, and aimed to create a better society. They were philosophers who were proficient in their field or archons. In this sense, it would be wise to give CGIS procurement and development to them.

However tempting it might be to say this, it does not mean that the person who procures or develops the CGIS must be a wise person. It means that this person should be driven to knowledge and aim for higher understanding, which in time develops their character for all the virtues and virtue of knowledge. The virtue of knowledge does not come cheaply. Therefore, archons are, for the sense of the society, of great value for getting a proper CGIS for the benefit of everyone.

And now Samos, sacred to Juno, lay ahead to the left (Delos and Paros were behind them), Lebinthos, and Calymne, rich in honey, to the right, when the boy began to delight in his daring flight, and abandoning his guide, drawn by desire for the heavens, soared higher. His nearness to the devouring sun softened the fragrant wax that held the wings: and the wax melted: he flailed with bare arms, but losing his oar-like wings, could not ride the air. Even as his mouth was crying his father's name, it vanished into the dark blue sea, the Icarian Sea, called after him. The unhappy father, now no longer a father, shouted 'Icarus, Icarus where are you? Which way should I be looking, to see you?' 'Icarus' he called again. Then he caught sight of the feathers on the waves, and cursed his inventions. He laid the body to rest, in a tomb, and the island was named Icaria after his buried child.

—*Metamorphoses 8 by Ovid*

6 CONCLUSIONS

The procurement of CGIS requires the wisdom to listen to different sciences and to follow wisdom. Because human life is an end in itself and of infinite value (e.g., see Kant, 1785), it seems impossible to actualise the responsibility towards one person – or even a group of people – as a means to repay mistakes. That is, one cannot give a lost life back or truly make amends of equal value – and that is one of the factors that makes these systems critical. Therefore, we need discourse on how to realise the responsibility and for what ends.

The problem of privacy should be considered in-depth before limiting the possibilities of personal privacy. While systems can, at least on paper, offer easy solutions to difficult problems, in reality it is not always like that. To foresee the implications of today's decisions on tomorrow's privacy is a task that requires a particular kind of wisdom. Saying "no" when asked perform a task is a skill indeed.

Moreover, it is important to discuss the aforementioned problems. Analysing, rephrasing, and defining terms in a small scientific community is a possibility, but in larger communities and in societies, this type of discussion is not an option. The language can and will be used as a tool to get more power over others. Society must safely keep CGISs by enabling a proper discussion about them.

Open and modular thinking and design, open discourse, and free-to-inspect systems are a way to help people trust these systems. Moreover, these methods are a way to keep procurement, design, implementation, and maintenance of a CGIS for a society open, fair, and transparent.

CGISs are a prime example of an area where ethics should be built in. Because many CGISs function well, their nature requires meticulous examination to diminish or negate the possibility of failures. CGISs do not keep us out of harm's way, but make safety possible. Many professionals work with these systems, which are the products of the tools of their trade. They make our lives as good as they are now. Although the information system and the work done with it are inseparable, these systems might allow or interfere with these esteemed servants of society as they work toward our common goal of a secure and healthy society where citizen well-being is an utmost priority. To produce a poorly designed CGIS is to harm their work for the common good.

The goal of this thesis is not to prove that digitalisation and the use of technology is inherently bad but moreover to promote good practices when creating these systems. The validity of the technology is about the values that are embedded to the system, where the system is used, and how it is used. For example, electronic voting can be used in various situations, but suitable ideas to implement it on a larger (national) scale are not viable. At a higher level, the risks are greater than, for example, in a student election because the values of the voting and the nature of these values are not compatible, with reasonable cost efficiency. Biometric passports can help to tighten security and ease travel, but only when they are designed and implemented correctly. The trend of changing security methods and using passports' data for other reasons requires a serious discussion about the nature of any change in the socio-technical system. The best examples of a good CGIS are in the eHealth cases, where technology saves both lives and money every day.

These information systems all serve a purpose. That purpose must always be kept in mind in order to ethically developing information systems. The system requirements must be analysed from the viewpoint of the purpose of the system and reflect the ethical values and requirements that are embedded in the system. Because the purpose and ethical values are tied together, failing to understand one is most likely to lead to failure in the other and ultimately failure with the whole system procurement.

Most importantly, we should be humble in front of these immense creations of mankind. These systems can help keep us healthy and safe, save our loved ones, and protect us from chaos that could occur if they were to stop functioning. These systems and their designers deserve our respect. That respect should also go to the ones who do the difficult task of ensuring that the systems do their intended tasks – for those who watch the watchmen.

Not all hope is lost in CGIS procurement, at least in Finland. All cases in Chapter 3 that showed a lack of proper discussion and discounting of expert opinions for the process of intelligent legislation now show signs for the better. Delegation of responsibility, checking mechanisms, and public discourse have been implemented and sometimes even heeded (see e.g. the case of Intelligence legislation). It just might be possible in the future to have more *Daedalian* CGIS procurement in Finland and maybe even globally.

CGIS procurement is not an easy task and obviously requires skills that not everyone possesses. When a task is both important and arduous, we should value those who are willing and able to do it. We need virtuous people who can guard us from possible harms and guide the CGIS development, allowing communities and nations to enter a new age of prosperity.

REFERENCES

Ahtokivi, I. (2017, July 31). Valtiosääntöoikeuden tutkijat Ylelle: Tiedustelulakien kiirehtimisen perusteet puuttuvat [Constitutional Law Researchers to YLE: There are no grounds for hurrying up the intelligence legislation]. *Verkkouutiset*. Retrieved from https://www.verkkouutiset.fi/valtiosaantooikeuden-tutkijat-ylelle-tiedustelulakien-kiirehtimisen-perusteet-puuttuvat-68364/.

Alaranta, M. (2013, January 20). Apotti on liian suuri riski [Apotti is too big of a risk]. *Talouselämä*. Retrieved from http://www.talouselama.fi/tebatti/apotti-on-liian-suuri-riski-3434141.

Appel, A. W., Ginsburg, M., Hursti, H., Kerninghan, B. W., Richards, C. D., Tan, G., & Venetis, P. (2009). *The New Jersey Voting-Machine Lawsuit and the AVC Advantage DRE Voting Machine*. Paper presented at USENIX Security 2009. Retrieved from https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/appel.pdf.

Avison, D. & Torkzadeh, G. (2008, August 22). *Information Systems Project Management*. SAGE Publications, Inc.; First edition.

British Broadcasting Company (BBC; 2010, 22 November). Stuxnet 'hit' Iran nuclear plans. BBC. Retrieved from http://www.bbc.co.uk/news/technology-11809827.

Bissett, A. K. (2003, June 25–27). Carl von Clausewitz and high technology war. *Proceedings of CEPE 2003* (pp. 14–26), Boston College; Boston, MA, US.

Bundesverfassungsgericht (2009, March 03). *Use of voting computers in 2005 Bundestag election unconstitutional*. Press Release No. 19/2009. Retrieved from https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html.

Bødker, S. (1989, September). A human activity approach to user interfaces. *Human-Computer Interaction* 4, 3 (pp. 171–195).

Chaabouni R. & Vaudenay S. (2009). *The Extended Access Control for Machine Readable Travel Documents*. BIOSIG 2009, Biometrics and Electronic Signatures, LNI vol. 155 (pp. 93–103). Gesellschaft für Informatik (GI), Bonn, Germany. Retrieved from: https://eprint.iacr.org/2010/103.pdf.

Cherry, M. & Imwinkelried, E. (2006, May/June). Cautionary Note about Fingerprint Analysis and Reliance on Digital Technology. *Judicature*, Volume: 89, Issue: 6 (pp. 334–338). Retrieved from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=236592.

Chomsky, N. (2002, February). *Distorted Morality: America's War on Terror?* Paper presented at Harvard University. Retrieved from https://chomsky.info/200202__02/.

Chothia, T. & Smirnov, V. (2010). A Traceability Attack against e-Passports. Financial Cryptography and Data Security, *Lecture Notes in Computer Science*, vol. 6052, (pp. 20–34). Springer Berlin/Heidelberg. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-642-14577-3_5.

Churchland, P. S (2011) *Braintrust : What Neuroscience Tells Us about Morality*, Princeton University Press, 2011.

Constitution of Finland (11.6.1999/731). *Suomen perustuslaki*. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/1999/19990731#a731-1999.

Danev B., Heydt-Benjamin, T. S., & Čapkun S. (2009). Physical-layer identification of RFID devices. *Proceedings of the 18th conference on USENIX security symposium (SSYM'09)* (pp. 199–214). USENIX Association, Berkeley, CA, US. Retrieved from https://www.usenix.org/legacy/events/sec09/tech/full_papers/danev.pdf?CFID=915221657&CFTOKEN=61369210.

De George, R. T. (2003). Post-September 11: Computers, ethics and war. *Journal of Ethics and Information Technology*, Volume 5, Issue 4 (pp. 183–190).

Demokraatti.fi (2017). *Kritiikki leviää: "sote-uudistus uhkaa pahentaa eriarvoisuutta"* [*Critique spreading: "sote-renew threatens to increase inequality*]. Retrieved from https://demokraatti.fi/kritiikki-leviaa-sote-uudistus-uhkaa-pahentaa-eriarvoisuutta/.

The Electoral Commission (2007, May). *Key issues and conclusions: Electoral pilot schemes*. Retrieved from http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0015/13218/Keyfindingsandrecommendationssummarypaper_27191-20111__E__N__S__W__.pdf.

Duquenoy, P., Jones, S., & Blundell, B. G. (2007, November 30). *Ethical, Legal and Professional Issues in Computing*. Cengage Learning EMEA, first edition.

Effi (2009), Electronical Frontier Finland, Sähköäänestys-FAQ [eVoting FAQ]. Retrieved from http://www.effi.org/sahkoaanestys-faq.html

Ess, C. (2009, March 16). *Digital Media Ethics*. Polity Press.

European Council Regulation (EC) (2004, December 13). Standards for security features and biometrics in passports and travel documents issued by Member States. No 2252/2004. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R2252&from=EN.

European Economic and Social Committee (2017), Impact of digitalisation and the on-demand economy on labour markets and the consequences for employment and industrial relations, Published by: "Visits and Publications" Unit EESC-2017-71-EN, European Union. Retrieved from https://www.eesc.europa.eu/resources/docs/qe-02-17-763-en-n.pdf

Fairweather, N. B. & Rogerson, S. (2002). *Technical Options Report*. The Implementation of Electronic Voting in the UK project. Jointly

commissioned by the Department for Transport, Local Government and the Regions, Office of the e-Envoy, Electoral Commission, LGA, IDeA, and Solace.

Fildes, J. (2010, October 23). Stuxnet worm 'targeted high-value Iranian assets.' BBC. Retrieved from http://www.bbc.co.uk/news/technology-11388018.

Finnish Government (2016) Alustavat ehdotukset sote- ja maakuntauudistuksen lainsäädännöksi [Preliminary suggestions for sote- and county renew legislation]. Retrieved from http://alueuudistus.fi/documents/1477425/2969580/Tiivistelm%C3%A4+hallituksen+lakiluonnosten+keskeisist%C3%A4+asioista+29.6.2016+sote-+ja+maakuntauudistus.

Finnish Government (2017). *Tiedustelutoiminnan valvonta. Työryhmän mietintö* [*Surveillance of intelligence. Working group report*]. Retrieved from https://julkaisut.valtioneuvosto.fi/handle/10024/79758.

Finnish Government (2018). *Mikä on sote-uudistus?* [*What is sote renew?*]. Valtioneuvosto [Finnish Government]. Retrieved from http://alueuudistus.fi/mika-on-sote-uudistus.

Finnish Ministry of Interior (2011). *Miksi tarvitaan biometrinen passi?* [*Why biometric passport is needed?*].

Finnish Ministry of the Interior (2017). *Civilian intelligence legislation considered necessary and worth supporting*. Retrieved from http://intermin.fi/en/artikkeli/-/asset_publisher/siviilitiedustelulainsaadantoa-pidetaan-tarpeellisena-ja-kannatettavana.

Finnish Ministry of Social Affairs and Health (2017). *Sote- ja maakuntauudistuksen digitalisaatio tehdään yhdessä - tietojärjestelmät rakennetaan vaiheittain* [*Digitalisation of the sote and county reform is done together - information systems are being built in stages*]. Retrieved from http://stm.fi/artikkeli/-/asset_publisher/sote-ja-maakuntauudistuksen-digitalisaatio-tehdaan-yhdessa-tietojarjestelmat-rakennetaan-vaiheittain.

Fleischman, W. M. (2010). Electronic Voting Systems and The Therac-25: What Have We Learned? *Proceedings at Ethicomp 2010*.

F-Secure (2010/1) (2010, September 1). Stuxnet Questions and Answers. *News from the Lab.* Retrieved from http://www.f-secure.com/weblog/archives/00002040.html.

F-Secure (2010/2) (2010, November 23). Stuxnet Redux: Questions and Answers. *News from the Lab*. Retrieved from http://www.f-secure.com/weblog/archives/00002066.html.

F-Secure (2011, August 23). Chinese Government Launching Online Attacks. *News from the Lab*. Retrieved from http://www.f-secure.com/weblog/archives/00002221.html.

Gillon, R. (1994). Medical ethics: four principles plus attention to scope. *British Medical Journal*. Vol 309 (6948).

Gonggrijp, R. & Hengeveld, W-J. (2007). Studying the Nedap/Groenendaal ES3B voting computer, a computer security perspective, Wijvertrouwenstemcomputersniet. *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology 2007*. Retrieved from http://wijvertrouwenstemcomputersniet.nl/images/c/ce/ES3B_EVT07.pdf.

Grunwald, L. (2007). *Security by Politics – Why it will never work.* Paper presented at the DEFCON15 conference. Riviera Hotel and Casino, Las Vegas, Nevada, US (2007, August 3–5). Retrieved from https://www.dc414.org/download/confs/defcon15/Speakers/Grunwald/Presentation/dc-15-grunwald.pdf.

The Guardian (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia*. Retrieved from http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

HE 234/2008. Hallituksen esitys laiksi passilain ja eräiden siihen liittyvien lakien muuttamisesta [Government's proposal for changing passport act and certain other related laws]. *Finlex*. Retrieved from http://www.finlex.fi/fi/esitykset/he/2008/20080234.

Healthcare Informatics (2009). *Legislation Calls for Universal EHR Adoption*. Retrieved from http://www.healthcare-informatics.com/news-item/legislation-calls-universal-ehr-adoption.

Hakkala, A. (2017). *On Security and Privacy for Networked Information Society: Observations and Solutions for Security Engineering and Trust Building in Advanced Societal Processes* (Doctoral thesis, University of Turku). Retrieved from http://www.utupub.fi/bitstream/handle/10024/144070/TUCSSDissertationD225.pdf?sequence=1.

Hakkala, A., Heimo, O. I., Hyrynsalmi, S., & Kimppa, K. K. (2017, June). Security, Privacy‘); DROP TABLE users; -- and Forced Trust in the Information Age? *ACM SIGCAS Computers and Society: Special Issue on Ethicomp*. TBA.

Happonen, P. (2010, August 03). Poliisi haluaa suomalaisten sormenjäljet rikostutkintaansa [Police requests Finnish fingerprints to criminal investigation]. *YLE* [Finnish National Broadcasting Company]. Retrieved from http://www.yle.fi/uutiset/kotimaa/2010/08/poliisi_haluaa_suomalaisten_sormenjaljet_rikostutkintaansa_1870808.html.

Happonen, P. (2017, December 08). Kiisteltyyn tiedustelulakiin tulossa tiukennuksia – Yle sai salaiset lakipykälät etukäteen nähtäväksi [Controversial Intelligence Act is getting harder - Yle got secret legislation proposals]. *YLE* [Finnish National Broadcasting Company]. Retrieved from https://yle.fi/uutiset/3-9967517.

Harjuhahto-Madetoja, K. (2016). *Kohti koko kansan tietoyhteiskuntaa* [*Toward an information society of everyone*]. Retrieved from https://suomidigi.fi/wp-content/themes/suomidigi/assets/attachments/digitaalinen-suomi-1995-2015/osa1/4%20Kohti%20koko%20kansan%20tietoyhteiskuntaa.pdf.

Heikinheimo, M., Huttunen, J., Kekomäki, M. Kontula, K., Mustonen, P., Raivio, K. & Rapola, J. (2017). Ehdotettu valinnanvapausmalli uhkaa palvelujärjestelmämme perusteita [The proposed model of choice threatens the basis of our service system], *Finnish Medical Journal Duodecim* 2017; 133(21):1975–6. Retrieved from http://www.duodecimlehti.fi/duo13975.

Heimo, O. I. (2018). *Procuring Critical Governmental Information Systems: A Virtue Ethics Approach* (Unpublished manuscript). Department of Management and Entrepreneurship, Turku School of Economics, University of Turku.

Heimo, O. I., Fairweather, N. B., & Kimppa, K. K. (2010, April 14–16). *The Finnish eVoting Experiment: What Went Wrong*? Paper presented at Ethicomp 2010, Tarragona, Spain.

Heimo, O. I., Hakkala, A., & Kimppa, K. K. (2012). How to abuse biometric passport systems. *Journal of Information, Communication and Ethics in Society*, Volume 10, Issue 2 (pp. 68–81).

Heimo, O. I. & Kimppa, K. K. (2013, June 12–14). *Information Warfare – Are We Already at War*? Paper presented at ETHICOMP 2013: The possibilities of ethical ICT. University of Southern Denmark, Kolding, Denmark.

Heimo, O. I., Kimppa, K. K., & Nurminen, M. I. (2014, July 25–27). *Ethics and the Inseparability Postulate*. Paper presented at ETHICOMP 2014. Pierre & Marie Curie University, Paris, France.

Heimo, O. I., Koskinen, J. S., Kainu, V., & Kimppa, K. K. (2014). Problem of Power: The Missing Agent. *Proceedings of CEPE 2013 - Ambiguous Technologies: Philosophical Issues, Practical Solutions, Human Nature*. Autónoma University of Lisbon, Lisbon, Portugal (2013, July 1–3).

Heimo, O. I., Koskinen, J. S. & Kimppa, K. K. (2013, June 12–14). *Responsibility in Acquiring Critical Governmental Information Systems: Whose Fault is Failure?* Paper presented at ETHICOMP 2013: The possibilities of ethical ICT. University of Southern Denmark, Kolding, Denmark.

Helsingin Sanomat (2010). *Vesipiipputupakan tuonnista vankeutta ja 400 000 euron lasku* [*Prison sentence and 400 000 € fine from illegal import of waterpipe tobacco*]. Helsingin Sanomat, 2010.

Helsingin Sanomat (2011). Sisäministeri sallisi passien sormenjälkien käytön rikostutkinnassa [Minister of Interior would accept passport fingerprints for criminal investigation]. *Helsingin Sanomat.* Retrieved from http://www.hs.fi/politiikka/art-2000002506491.html.

Helsingin Sanomat (2013, September 19). Professori: Perusterveyden-huollon romahtamisen syynä keikkalääkärit ja tietojärjestelmät [Professor: Reasons for collapse of primary healthcare are freelance doctors and information systems]. *Helsingin Sanomat*. Retrieved from http://www.hs.fi/kotimaa/art-2000002675260.html.

Himanen, P. (2004). VÄLITTÄVÄ, KANNUSTAVA JA LUOVA SUOMI Katsaus tietoyhteiskuntamme syviin haasteisiin [Caring, encouraging and creative

Finland, Review of our information societys deep challenges]. *Eduskunta Riksdagen*. Retrieved from https://www.eduskunta.fi/FI/tietoaeduskunnasta/julkaisut/Documents/ekj_4+2004.pdf.

Hitchens, C. (2007). *God Is Not Great: How Religion Poisons Everything* (p. 150). New York, NY: Twelve Books.

Hoepman J-H., Hubbers E., Jacobs B., Oostdijk M., & Schreur R. W. (2006). Crossing Borders: Security and Privacy Issues of the European e-Passport, Advances in Information and Computer Security. *Lecture Notes in Computer Science*, Vol. 4266/2006 (pp. 152–167), Springer Berlin/Heidelberg. Retrieved from https://link.springer.com/content/pdf/10.1007%2F11908739.pdf.

Hornung, G. (2007). The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards. *SCRIPTed* Vol. 4, Issue 3/246. Retrieved from https://script-ed.org/wp-content/uploads/2016/07/4-3-Hornung.pdf.

H.R. 3124 (111th) (2009). Health Information Technology (IT) Public Utility Act of 2009. *GovTrack.us*. Retrieved from https://www.govtrack.us/congress/bills/111/hr3124.

Hyppönen, M. (2017, March 09). *The dark side of the net*. Guest Lecture at University of Turku.

Iltalehti (2018) Sote-asiantuntijaryhmään kuuluvalla professori Hiilamolla kytkös terveysbisnekseen - istuu Terveystalon ison omistajan hallituksessa [Sote-expert group member professor Hiilamo has a connection to health care business - has a seat in Terveystalo's big owner company's board, Iltalehti 16.3.2018, https://www.iltalehti.fi/politiikka/20180316220081 6758_pi.shtml

Ilta-sanomat (2017, April 19). Suojelupoliisin päällikkö kertoo, mistä uudessa tiedustelu-laissa on kyse [The chief of the security police says what the new intelligence legislation is about]. *Ilta-Sanomat*. Retrieved from https://www.is.fi/kotimaa/art-2000005175971.html.

Iranto, A. (2013, May 08). Apotti järjestelmäkehittyyvuorovaikutuksessa [Apotti system is being developed in interaction]. *YLE* (Finnish National Broadcasting Company). Retrieved from http://yle.fi/uutiset/apotti-jarjestelma_kehittyy_vuorovaikutuksessa/6633702.

Johnson, D. G. (2001). *Computer Ethics*. New Jersey: Prentice Hall.

Juels A., Molnar D., & Wagner D. (2005). *Security and Privacy Issues in E-passports* (pp. 74–88). First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM 2005). Retrieved from https://eprint.iacr.org/2005/095.pdf.

Juntunen, E. (2013, August 26). Apotti-järjestelmä tulee kaikkien kukkarolle [Apotti system will be expensive for everyone]. *Helsingin Sanomat*. Retrieved from http://www.hs.fi/kaupunki/a1377399301286.

Juvenal (c. 115), Satire VI. Retrieved from https://www.gutenberg.org/files/50657/50657-h/50657-h.htm.

Järvinen, P. (1983). A role of a user in the development and maintenance of an information system: Empirical and theoretical findings. *Proceedings of the Twentieth Annual Computer Personnel on Research Conference (SIGCPR '83)* (pp. 134–144). Elias M. Awad (Ed.). ACM, New York, NY, US.

Järvinen, P. (2017, September 11) Kiirehditty tiedustelulaki lykkääntyi yllättäen [The rushed intelligence legislation postponed unexpectedly]. *TIVI*. Retrieved from https://www.tivi.fi/Kaikki_uutiset/kiirehditty-tiedustelulaki-lykkaantyi-yllattaen-6675163.

Kant, I. (1785). *Grundlegug zur Metaphysik der Sitten* [*Groundwork of the Metaphysic of Morals*]. Several Translations used.

Katainen, J. (2004, October). *KESKUSTELUALOITE 10/2004 vp*. Discussion initiative. Retrieved from https://www.eduskunta.fi/FI/vaski/EduskuntaAloite/Documents/ka_10+2004.pdf.

Kasvi, J. J. J. (2013). Apotinsynti [The sin of Apotti]. Blog post. Retrieved from http://jyrkikasvi.puheenvuoro.uusisuomi.fi/131025-apotin-synti.

Kasvi, J. J. J. (2014) Jotain uutta, jotain vanhaa, jotain sinistä [Something new, something old, something blue]. Blog post. Retrieved from http://jyrkikasvi.puheenvuoro.uusisuomi.fi/171063-jotain-uutta-jotain-vanhaa-jotain-sinista.

Kauppakamari [Finnish Chamber of Commerce] (2013, May 30). *Kauppakamarin pikagallup: Suomesta tulee tietoyhteiskunnan edelläkävijä, uskoo yli ¾ digitalisaation asiantuntijoista* [*Chamber of Commerce quick poll: Finland will be a forerunner as an information society, believes ¾ of digitalisation experts*]. Retrieved from http://kauppakamari.fi/2013/05/30/kauppakamarin-pikagallup-suomesta-tulee-tietoyhteiskunnan-edellakavija-uskoo-yli-neljannes-digitalisaation-asiantuntijoista/.

Kauppalehti (2017, February 7). *Sipilä: Suomesta tekoälyn ykkösmaa* [*Sipilä: Finland to be the best country in artificial intelligence*]. Retrieved from http://www.kauppalehti.fi/uutiset/sipila-suomesta-tekoalyn-ykkosmaa/AStJsdj3.

Kerkelä, L. (2008a) (2008, February 22). Poliisi haluaa passien sormenjäljet rikostutkijoille [Police request passport fingerprints to criminal investigation]. *Helsingin Sanomat*. First edition. Retrieved from http://www.hs.fi/kotimaa/art-2000004549942.html.

Kerkelä, L. (2008b) (2008, November 27). Rikostutkijat eivät saa vielä passien sormenjälkiä käyttöönsä [Criminal investigators do not acquire passport fingerprints yet]. *Helsingin Sanomat*. First edition. Retrieved from http://www.hs.fi/kotimaa/art-2000004615726.html.

KHO [High Administrative Court] (2017). *KHO pitää esitystä Soten valinnanvapauslainsäädännöksi oikeudellisesti ongelmallisena* [*The KHO*

regards the proposal for the right to freedom of choice as a legally problematic one]. Retrieved from http://www.kho.fi/fi/index/ajankohtaista/tiedotteet/2017/03/khopitaaesitystasotenvalinnanvapauslainsaadannoksioikeudellisestiongelmallisena.html.

Kimppa, K. K. (2004). *Consequentialist Considerations of Intellectual Property Rights in Software and other Digitally Distributable Media in Ethicomp 2004*. Presentation to Challenges for the Citizen of the Information Society. University of the Aegean, Syros, Greece (2004 April 14–16).

Kivekäs, O. (2012, June 08). *Epic fail, eli sairaaloiden IT eilen, tänään ja huomenna* [*Epic fail, i.e. hospitals' IT yesterday, today and tomorrow*]. Blog post. Retrieved from http://otsokivekas.fi/2012/06/epic-fail-eli-sairaaloiden-it-eilen-tanaan-ja-huomenna/.

Kolehmainen, Aleksi (2016), Tämän takia Apotti-hanketta luultiin 150 miljoonaa euroa halvemmaksi [This is why Apotti-project was thought to be 150 million cheaper], Tietoviikko 10.6.2018, https://www.tivi.fi/Kaikki_uutiset/taman-takia-apotti-hanketta-luultiin-150-miljoonaa-euroa-halvemmaksi-6558668

Koskinen, J. S. S., Heimo, O. I., & Kimppa, K. K. (2012). *A viewpoint for more ethical approach in healthcare information system development and procurement: the four principles*. Well-being in the Information Society (WIS 2012), 22.8.2012– 24.8.2012, Turku, Finland.

Koskinen, J. S. S., Heimo, O. I., & Kimppa, K. K. (2014). Rawls' view in context of datenherrschaft over personal patient information. *Proceedings of CEPE 2013 - Ambiguous Technologies: Philosophical Issues, Practical Solutions, Human Nature*. Autónoma University of Lisbon, Lisbon, Portugal (2013, July 1–3).

Koskinen, J. S. S., Heimo, O. I., and Kimppa, K. K. (2018). *Ethics as a common Language in Healthcare Information System Development and Procurement: The Four Principles*. Unpublished manuscript. Department of Management and Entrepreneurship, Turku School of Economics, University of Turku.

Kärki, A. (2016, March 12). Jälleen viisi sote-aluetta! [Again five sote areas!]. *Keskisuomalainen*. Retrieved from https://www.ksml.fi/paakirjoitus/nimella/J%C3%A4lleen-viisi-sote-aluetta/743604.

Laki kunta- ja palvelurakenneuudistuksesta [Law on the reform of the municipal and service structure]. *Finlex*, 9.2.2007/169. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2007/20070169.

Landau, S. (2013, July/August). Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy*, vol. 11, no. 4 (pp. 54–63). doi: 10.1109/MSP.2013.90. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6573302&isnumber=6573290.

Langner, R. (2010, November 19). The big picture. Blog entry. *Langner*. Retrieved from http://www.langner.com/en/2010/11/19/the-big-picture/.

Larsen E. & Elligsen G. (2010, August). Facing the Lernaean Hydra: The Nature of Large-Scale Integration Projects in Healthcare. In Kautz K & Nielsen P. *Proceedings of the First Scandinavian Conference of Information Systems, SCIS 2010*. Rebild, Denmark.

Leavitt H. J. (1964) Applied Organization Change in Industry: Structural Technical and Human Approaches, in Cooper, W. W., Leavitt H. J. & Shelly, M. W. (eds.): New Perspectives in Organizational Research. Wiley, New York, USA.

Lehto, T. (2010, August 16) Poliisi saattaa saada passien sormenjäljet [Police may acquire the passport fingerprints]. *TIVI*. Retrieved from http://www.tivi.fi/Arkisto/2010-08-16/Poliisi-saattaa-saada-passien-sormenj%C3%A4ljet-3135928.html.

Lindstedt, S. (2013, January 3). Apotti-hankevaatiitehohoitoa [Apotti Program needs intensive care]. *TIVI*. Retrieved from = http://www.tivi.fi/Arkisto/2013-03-14/Apotti-hanke-vaatii-tehohoitoa-3146608.html.

Liimatainen, K. (2013, September 7). It-järjestelmän tilaaminen on taitolaji [Ordering information technology systems is skill based]. *Helsingin Sanomat*. Retrieved from http://www.hs.fi/talous/art-2000002672619.html.

Lockton, V. and Rosenberg, R. S. (2005). RFID: The next serious threat to privacy, Ethics and Information Technology. *Springer*, 7:221–231. Retrieved from https://link.springer.com/article/10.1007/s10676-006-0014-2.

Mackenzie, D. A. (1990). *Inventing accuracy: a historical sociology of nuclear missile guidance*. MIT Press.

Melia, P. and Byrne, L. (2012). €54m voting machines scrapped for €9 each. *Independent.ie*. Retrieved from http://www.independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each-26870212.html.

Mercuri, R. (2001). *Electronic Vote Tabulation: Checks and Balances*. PhD thesis, University of Pennsylvania.

Merikanto, T. (2017a). Professorit: Vapaudesta valita tuli mahdoton yhtälö – "Talon voi polttaa vain kerran" [Professors: From freedom to choose came an impossible equation – "House can only be burned once"]. *YLE* [Finnish National Broadcasting Company]. Retrieved from https://yle.fi/uutiset/3-9477663.

Merikanto, T. (2017b). Viisi professoria luki hallituksen valinnanvapaus-paperin, eivätkä hekään ota selvää, mitä valinnanvapaus käytännössä tarkoittaisi [Five professors read the governments freedom of choice paper and they do not find out what the freedom of choice would actually mean]. *YLE* [Finnish National Broadcasting Company]. Retrieved from https://yle.fi/uutiset/3-9972792.

Merikanto, T. (2017c). Analyysi: Viime kierroksella sote-asiantuntijat jätettiin katsomoon, ja tietoa on pantattu tälläkin kertaa [Analysis: Over the last round, the sote experts were left in the stand and the information was concealed this time]. *YLE* [Finnish National Broadcasting Company]. Retrieved from https://yle.fi/uutiset/3-9871352.

Merimaa, J. (2017, February 27). Nettiääni voi tulla paperisen rinnalle – jotta vilppi voitaisiin varmasti estää, vaalisalaisuutta pitäisi lieventää [Net vote can soon be alongside with paper vote. In order to prevent cheating, secrecy of ballot must be mitigated]. *Helsingin Sanomat.* Retrieved from http://www.hs.fi/tiede/art-2000005103948.html.

Monnerat, J., Vaudenay, S., and Vuagnoux, M. (2007). *About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferrable Data Authentication* (pages 15–28). International Conference on RFID Security.

Mostowski W. and Poll E. (2010). *Electronic Passports in a Nutshell*. Technical Report ICIS-R10004. Radboud University Nijmegen, the Netherlands. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.167.2807&rep=rep1&type=pdf.

Moor, J. H. (1999). *Just consequentialism and computing, Ethics and Information Technology*. 1: pp. 65–69.

MTV3 (1999) Ahtisaari: Suomalainen tietoyhteiskunta edelläkävijä Euroopassa [Ahtisaari: Finnish information society a forerunner in Europe]. Retrieved from http://www.mtv.fi/lifestyle/digi/artikkeli/ahtisaari-suomalainen-tietoyhteiskunta-edellakavija-euroopassa/5449830.

MTV3.fi (2017, November 20). Kuntien asiantuntijat: Sote-uudistus ei hillitse kustannusten nousua tai kavenna terveyseroja [Municipality experts: Sote reform does not curb rising costs or decline health inequalities]. Retrieved from https://www.mtv.fi/uutiset/kotimaa/artikkeli/kuntien-asiantuntijat-sote-uudistus-ei-hillitse-kustannusten-nousua-tai-kavenna-terveyseroja/6664410#gs.WI0_Sbo.

Mölsä, J. (2008, January 31). Professori pitää tietoturvaa riittävänä [Professor thinks the information security is adequate]. *Helsingin Sanomat*. Retrieved from http://www.hs.fi/kotimaa/art-2000004544495.html.

Nakashima, E., Miller, G. and Tate, J. (2012, September 19). U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, *Washington Post*. Retrieved from http://www.washingtonpost.com/world/ national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

Nelonen.fi (2012). Sormenjälkirekisteri voi avautua poliisille [Fingerprint registry can open to police]. Retrieved from http://www.nelonen.fi/uutiset/kotimaa/ 258154-sormenjalkirekisteri-voi-avautua-poliisille.

Niilola, M. (2012, May 21). Terveydenhuollon it-hankinnoissa lähes kaikki mennyt pieleen [In healthcare IT procurement almost everything gone wrong]. *YLE* (Finnish National Broadcasting Company). Retrieved from http://yle.fi/uutiset/terveydenhuollon_it-hankinnoissa_lahes_kaikki_on_mennyt_pieleen/6103664.

Niilola, M. (2017, July 31). Tutkijat nihkeinä tiedustelulakien kiireelliselle säätämiselle – "En näe Suomeen kohdistuvaa poikkeuksellista uhkaa tai kriisiä" [Scientists lament to urgent intelligence legislation changes – "I do not see an exceptional threat or crisis facing Finland"]. *YLE* (Finnish National Broadcasting Company). Retrieved from https://yle.fi/uutiset/3-9738553.

Nurminen, M. I. (1986a). *People or Computers: Three Ways of Looking at Information Systems*. Studentlitteratur, Cartwell Brat Ltd. Lund, Sweden.

Nurminen, M. I. (1986b). Information Systems Quality versus Quality of Work: Is there any Difference? Nissen H-B., Sandstrom G. (eds.): *Report of the 9th Scandinavian Research Seminar on Use and Development of Information Systems*. University of Lund.

Nurminen, M. I. & Eriksson, I. V. (1999). Information systems research: The 'infurgic' perspective. *International Journal of Information Management*, 19, pp. 87—94.

Nurminen M. I. & Forsman U. (1994). Reversed Quality Life Cycle Model. *Human Factors in Organizational Design and Management - IV*, pp. 393–398. Elsevier Science B.V., North-Holland, Amsterdam.

Nurminen M. I. & Torvinen V. (1996, May). *Role-based Interpretation of ISs, TUCS Technical Report No 9*.

Nykänen, E., Kovasin, M., Liukko, E., Blomqvist, P., Krohn, M., Ahola, S., Nurmi-Koikkalainen, P., and Jonsson, P. M. (2017). *Vaikuttava valvonta osana sosiaali- ja terveydenhuollon uudistusta* [*Effecting surveillance as a part of social and healthcare renewal*]. Retrieved from http://tietokayttoon.fi/documents/10616/3866814/29_vaikuttava-valvonta-osana-sosiaali-ja-terveydenhuollon-uudistusta.pdf/ffe32373-6827-4ce2-a22a-60469ffff2c9?version=1.0.

Nykänen, H. (2014, February 6). Valtava ja kallis urakka viimein toteutumassa – kansallinen potilasarkisto käyttöön keväällä [Huge and expensive task is at last being made true - a national patient registry is being taken into use in spring]. *YLE* (Finnish National Broadcasting Company). Retrieved from http://yle.fi/uutiset/3-7070869.

Oikeusministeriö [Ministry of Justice] (2009). *Sähköisen äänestyksen pilottihanke vuoden 2008 kunnallisvaaleissa: Kokemuksia ja opittuja asioita* [Electronic voting pilot project in the municipal elections 2008: Experiences and what was learned].

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth*. Reading: Academic Publishing Limited, pp. 163–168.

Ovid (8). *Metamorphoses, Book VIII*. [Translation by A. S. Kline.] Retrieved from http://etext.lib.virginia.edu/latin/ovid/trans/Ovhome.htm

Pantsu, P. (2017). Rajua kritiikkiä hallituksen sote-esitykselle: Katso 20 suurimman kaupungin kannat valinnanvapausmalliin [Heavy the criticism for the government's sote presentation: See the opinions of the 20 largest cities about the freedom of choice model]. *YLE* (Finnish National Broadcasting Company). Retrieved from https://yle.fi/uutiset/3-9529905.

Parker, D. B. (1979). *Ethical conflicts in computer science and technology*.

Paulavaara, P. (2017). Sote-uudistus on täynnä suden-kuoppia, sanoo professori Jussi Huttunen – Riskejä ovat verorahojen hassaus, pompottelun lisääntyminen ja maailman parhaan hoidon romuttuminen [Sote reform is full of pitfalls, says Professor Jussi Huttunen – Risks are wasting tax money, increased bureaucracy and the destroying the best treatment in the world]. *Helsingin Sanomat*. Retrieved from https://www.hs.fi/kotimaa/art-2000005455978.html.

Peltomäki, T. (2012, September 12). Uutisanalyysi: Apotti-hanke saa maksaa tietotekniikan vanhoista synneistä [News analysis: Apotti programwillpay for the old sins of computing]. *Helsingin Sanomat*. Retrieved from http://www.hs.fi/kotimaa/a1347361544072.

Pitkänen, P. (2013, May 30). Viron potilasjärjestelmän kehittäjä pilkkoisi HUS:in Apotin osiin [The Estonian patient information system developer would modularise Apotti]. *Ilta-sanomat*. Retrieved from http://www.is.fi/digitoday/art-2000001797734.html.

Pitkänen, P. (2017, April 11). Kaleva: Pääministeri Sipilä haluaa tiedustelulain poikkeuskeinolla kiireellisesti voimaan [Kaleva: Prime Minister Sipilä wants the Intelligence Act to be expectionally urgently accepted]. *Ilta-Sanomat*. Retrieved from https://www.is.fi/digitoday/art-2000005166115.html.

Popper, K. (1959). *The Logic of Scientific Discovery*. Retrieved from https://archive.org/details/PopperLogicScientificDiscovery.

Raivio, K. (2006). *Paras-hanke Suomea muokkaamassa*. Yhteiskuntapolitiikka 71. Retrieved from https://www.julkari.fi/bitstream/handle/10024/100631/062raivio.pdf?sequence=1.

Rantanen, M. & Heimo, O. I. (2014, July 30 – August 1). *Problem in Patient Information System Acquirement in Finland: Translation and Terminology*. HCC11 ICT and Society. University of Turku, Turku, Finland.

Regan, Michael D. (2018) An 11-year-old changed election results on a replica Florida state website in under 10 minutes, PBS News Hour,

https://www.pbs.org/newshour/nation/an-11-year-old-changed-election-results-on-a-replica-florida-state-website-in-under-10-minutes

Reinboth (2014). Passien sormenjälki-rekisteriä ei avata rikostutkinnalle [The passports fingerprint register will not be opened for criminal investigation]. *Helsingin Sanomat*. Retrieved from http://www.hs.fi/kotimaa/art-2000002738728.html.

Rhem, Kathleen T. (2005, May 20). China Investing in Information Warfare Technology, Doctrine. U.S. Department of Defense. Retrieved from http://archive.defense.gov/news/newsarticle.aspx?id=16594.

Richter, H., Mostowski, W., and Poll, E. (2008). *Fingerprinting passports*. NLUUG spring conference on security (pp. 21–30). Citeseer. Retrieved from https://cs.ru.nl/E.Poll/papers/nluug.pdf

Robison, W. L. (2010). *Voting and Mix-And-Match Software.* Ethicomp.

Sanger, D. E. (2012, June 01). Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all.

Sanger, D. E. and Broad, W. J. (2017, April 03). Trump Inherits a Secret Cyberwar Against North Korean Missiles. *New York Times*. Retrieved from https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=span-ab-top-region&region=top-news&WT.nav=top-news&_r=3.

SCF Associates Ltd. (2009, September). *A Green Knowledge Society: An ICT policy agenda to 2015 for Europe's future knowledge society.* Retrieved from http://www.ifap.ru/library/book444.pdf.

Scheinin, M. (2017, June 16). Martin Scheinin: Kommentteja mietinnöstä siviilitiedustelua koskevaksi lainsäädännöksi [Martin Schein: Commentary on the report on civilian intelligence legislation]. *PERUSTUSLAKIBLOGI*. Retrieved from https://perustuslakiblogi.wordpress.com/2017/06/16/martin-scheinin-kommentteja-mietinnosta-siviilitiedustelua-koskevaksi-lainsaadannoksi/.

Schneier, B. (2004, November 10). The Problem with Electronic Voting Machines. Blog post. *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html.

Schneier, B. (2010, September 22). The Stuxnet Worm. Blog post. *Schneier on Security*. Retrieved from http://www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html.

Schneier, B. (2012, February 01). *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Wiley (pp. 69–70).

Shikeben, S. (2014). Sote-uudistuksen suurin kritiikki Vaasasta ja Seinäjoelta [Sote-renew gets the biggest critique from Vaasa and Seinäjoki]. *YLE* (Finnish National Broadcasting Company). Retrieved from https://yle.fi/uutiset/3-7152886.

Singel, R. (2004, October 21). American Passports to Get Chipped. *Wired*. Retrieved from http://www.wired.com/politics/security/news/2004/10/65412.

Stamatellos, G. (2007),Computer ethics – A Global Perspective, Jones and Bartlett, Sudbury, USA

STM (Ministry of Social affairs and Health) (2017). Tieto hyvinvoinnin ja uudistuvien palvelujen tukena [Knowledge as a support for well-being and renewing services]. Retrieved from http://stm.fi/julkaisu?pubid= URN:ISBN:978-952-00-3548-8.

Storås, N. (2015, January 06). CGI:lle ropisee miljoonia Apotin myöhästymisestä [CGI earns millions for the delays in apotti]. *TIVI*. Retrieved from http://www.tivi.fi/Uutiset/2015-01-16/CGIlle-ropisee-miljoonia-Apotin-my%C3%B6h%C3%A4stymisest%C3%A4-3152165.html.

Tarvainen, T. (2008). Salassapitosopimuksen anatomia [The anatomy of the nondisclosure agreement]. Blog entry. *effi.org*. Retrieved from https://effi.org/blog/2008-03-20-Tapani-Tarvainen.html.

Tavani, H. T. (2006, October 27). *Ethics & Technology: Ethical Issues in an Age of Information and Communication Technology* (2nd ed.). John Wiley & Sons, Inc.

THL (2018). SOCIAL WELFARE AND HEALTH CARE REFORM IN FINLAND. THL [National institute for health and welfare]. Retrieved from https://www.thl.fi/fi/web/social-welfare-and-health-care-reform.

Turtola, I. (2015, April 09). Terveydenhuollon jättihanke etenee: Helsinki sanoi Apotti-tarjouspyynnölle kyllä [A giant healthcare project is progressing: Helsinki said yes for Apotti invitation to tender]. *YLE* (Finnish National Broadcasting Company). Retrieved from http://yle.fi/uutiset/3-7919237.

U.S. Department of Defense (2011). Department of Defense Cyberspace Policy Report. Retrieved from http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf.

U.S. Department of Veterans Affairs (2009, July 14). The Honorable Roger W. Baker

Assistant Secretary for Information and Technology Department of Veterans Affairs before the House Committee of Veterans' Affairs Subcommittee on Oversight and Investigations. Retrieved from https://www.va.gov/OCA/testimony/hvac/soi/090714RB.asp.

Vallor, S. (2009), Social networking technology and the virtues, *Ethics and Information Technology* (2010) 12:157–170, Published online: 11 August 2009 Springer Science+Business Media B.V. 2009, DOI 10.1007/s10676-009-9202-1 Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs10676-009-9202-1.pdf0

Vallor, S. (2013) The future of military virtue: Autonomous systems and the moral deskilling of the military, 2013 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, 2013, pp. 1-15.

Valtioneuvosto (The Council of State of Finland) (1999). Pääministeri Paavo Lipposen II hallituksen ohjelma 15.4.1999 [The Prime minister Paavo Lipponen's second governments' program 15.4.1999]. Retrieved from http://valtioneuvosto.fi/hallitusohjelmat/-/asset_publisher/67-paaministeri-paavo-lipposen-ii-hallituksen-ohjelma.

Vaudenay S. (2007, November/December). *E-Passport Threats, IEEE Security & Privacy*, Vol. 5, No. 6 (pp. 61–64).

Van den Hoven, J. (2013). Value Sensitive Design and Responsible Innovation. Owen, R., Bessant, J. and Heintz M., eds. *Responsible Innovation*, John Wiley and Sons, Ltd., pp. 75–83. Retrieved from http://ieeexplore.ieee.org/document/4402450/.

Verzola, R. (2008). *The Cost of Automating Elections*. Retrieved from http://ssrn.com/abstract=1150267.

The White House, Office of the Press Secretary (2009). *Remarks by the President on Securing Our Nation's Cyber Infrastructure*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Wu C. (2006). An Overview of the Research and Development of Information Warfare in China. Edward F. Halpin, Philippa Trevorrow, David C. Webb, and Steve Wright (eds.). *Cyberwar, Netwar and the Revolution in Military Affairs* (pp. 173–195).

Weckert, J. & Adeney, D. (1997). *Computer and Information Ethics*. Greenwood Publishing Group Inc.

Wolf, M.J., Miller, K. and Grodzinsky, F. (2008) Free, Source-Code-Available, or Proprietary: An ethically charged, context-sensitive choice, *Tenth ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communication Technologies*

YLE (2009). Puolustusvoimat panostaa informaatiosodankäyntiin [The Finnish Defence Forces are investing on information warfare]. *YLE* (Finnish National Broadcasting Company). Retrieved from http://yle.fi/uutiset/teksti/kotimaa/2009/01/puolustusvoimat_panostaa_informaatiosodankayntiin_495397.html.

YLE (2013, May 07). IT-asiantuntija: Husin uusi potilastietojärjestelmä menossa pahasti pieleen [IT specialist: Hus' new patient information system going terribly wrong]. *YLE* (National Finnish Broadcasting Company). Retrieved from http://yle.fi/uutiset/3-6630873.

Zetter, K. (2006, March 08). Hackers Clone E-Passports. *Wired*. Retrieved from http://www.wired.com/science/discoveries/news/2006/08/71521.

Annales Universitatis Turkuensis

Turun yliopisto
University of Turku

Painosalama Oy, Turku, Finland 2018

ISBN 978-951-29-7507-5 (PRINT)
ISBN 978-951-29-7508-2 (PDF)
ISSN 2343-3159 (PRINT) | ISSN 2343-3167 (PDF)