



**LUND UNIVERSITY**  
Faculty of Social Sciences

Graduate School

Master of Science in Global Studies

Major: Political Science

Course: SIMV07

Term: Spring 2016

Supervisor: Astrid Hedin

## E-Government in Singapore: strengthening political control over society

Author: Ievgen Iaroshenko

## Abstract

Developing an e-government in a state has become a new trend in the world of political reform. However, e-government itself as a way of public service digitalization does not incline that political regime of the state will be democratic and inclusive. When e-government has been usually researched in the democratic setting, question marks remain of how it works in the non-democratic one. This paper tries to find out consequences e-government implementation have on the citizens' privacy in the hybrid regime like Singapore. The used material consists of both Singapore's laws, governmental stats and official documents, as well as outside reports and statistics provided by international organizations and think tanks. The outcome of the analysis suggests that the implementation of e-government in the non-democratic state leads to the increased capacity and cases of the unrestricted surveillance of citizens by government that includes either gathering private data, or using it against the citizens or social actors that are considered to be dangerous to the monopoly of ruling elites power.

**Key words:** E-government, non-democracy, privacy, political power, ICT, Singapore

## Table of Contents

<b>1 Introduction</b>	6
1.1. Why e-government and non-democracy?	6
1.2. Thesis Design	8
<b>2 Previous research in the field</b>	10
2.1. Non-democratic political regime and e-government	10
2.2. Citizen and his privacy: e-government perspective	12
<b>3 Methodology</b>	15
3.1 Selecting the case	17
3.2. Data	18
3.3. Independent and dependent variables	19
3.4. Approach to case analysis	21
3.5. Research limitations	22
<b>4 Political regime of Singapore</b>	24
4.1. Theoretical perspective on measuring country's democracy level	25
4.2. Analysis of the political regime of Singapore	26
<b>5 The concept of e-government: theoretical perspective</b>	33
5.1. E-government and society of control	33
5.2. E-government and network society	37
<b>6 How Singapore is e-governed</b>	43
6.1. Ministry of Communications and Information: structure and goals	43
6.2. E-government in Singapore from the state's budget viewpoint	48
<b>7 State of citizen's privacy in Singapore</b>	53
7.1. Legal background of personal data protection in Singapore	53
7.2. Practice of using surveillance technologies by the state	58
7.3. SingPass - instrument of the power of control	61
<b>8 Conclusion</b>	64
8.1. Further research	65
<b>The list of references</b>	66

## Abbreviations

CSA	Cyber Security Agency of Singapore
EUI	European Intelligence Unit
GovTech	Government Technology Agency of Singapore
ICCPR	International Covenant on Civil and Political Rights
ICT	Information communication technologies
IMDA	Info-communications Media Development Authority of Singapore
MCI	Ministry of Communications and Information
PAP	People's Actions Party
RAHZ	Risk Assessment and Horizon Scanning
SingPass	Singapore Personal Access
UN	United Nations

## List of Figures and Tables

<b>Figure 1.</b> Aggregated scores of the freedom status of the political regime of the Republic of Singapore, Freedom House (2006 - 2016).....	27
<b>Figure 2.</b> Accumulated rankings of the political participation, electoral process, and civil liberties indicators of the political regime of the Republic of Singapore, Economist Intelligence Unit (2006 - 2016).....	28
<b>Figure 3.</b> Accumulated rankings of the political participation, electoral process, and civil liberties indicators of the political regime of the Republic of Singapore, Economist Intelligence Unit (2011 - 2016).....	30
<b>Figure 4.</b> Organizational structure of the Ministry of Communications and Information.....	45
<b>Figure 5.</b> Development Expenditures of the Ministry of Communications and Information, 2006 - 2017.....	48
<b>Figure 6.</b> Operating Expenditures of the Ministry of Communications and Information, 2006 - 2017.....	49
<b>Figure 7.</b> Divided operating Expenditures of the Ministry of Communications and Information by purpose, 2013 - 2017.....	50

# 1 Introduction

## 1.1. Why e-government and non-democracy?

Aldous Huxley wrote in his famously notorious novel 'Brave New World' (Huxley, 2007: 18): 'A really efficient totalitarian state would be one in which the all-powerful executive of political bosses and their army of managers control a population of slaves who do not have to be coerced, because they love their servitude'. Even though the tone is highly novelistic and exaggerated, the main idea seems quite realistic - what if such circumstances in the society are created, when the majority of population voluntarily and neglectfully lose their hold on privacy and freedom to the political elites for the sake of comfort and the feeling of security? The idea is not very far-fetched, as stable authoritarian regimes like Qatar are creating such circumstances for citizens in the sphere of social values and material benefits that give the power holders ability to expand the reach of their 'oppressive legislative arsenal and the draconian system of censorship' (Reporters Without Borders, 2016).

However, with the rise of the Internet, the process of political rule strengthening has become much more latent. Instead of giving away material goods to guarantee the loyalty of country's citizens, powerholders received a new instrument of control that transits the margins of public and private in a very covert way. However, information and communication technology (ICT) in the political spectrum is not a one-sided concept, while it can either empower the civic society to participate in the country's governance or oppress it under the dictatorial rule. While the common belief states that modern means of communication bring freedom and weaken the state's monopoly on power, I would like to analyze the problem and bring up the «what if» question - what if state is using the benefits of ICT to strengthen its political power?

To answer this question is a task that cannot be tackled in terms of our thesis scope, while there are a lot of sides of the story that could be analyzed from different angles. From the one point, this study can examine the usage of Internet and the reasons why there are restrictions among the countries for people in terms of accessing the service, as well as a range of possibilities while using ICT in public space. From the other point, the study can investigate whether cyberspace is ultimately an efficient dimension for the establishment of democracy, giving voice and political strength to NGOs, social movements, different social groups etc. to lobby their interests and protect their rights. Or, if discussion of the theoretical concepts is the central task of the scientific approach to the investigation, research of what is the Internet and how it is integrated into the social process may shed light on the dangers and pitfalls of the massive usage of this technology.

Therefore, there are many things that could and should be discussed in the discourse of political power and ICT, and there is a lot of work for everybody interested in understanding the transformation modern society is undergoing. To avoid being superficial, I will concentrate on the other side of the collaborative nature between ICTs and political power that I have encountered personally, and the name of this side is electronic government or e-government. Having lived and studied in Europe for my whole life, establishment of the e-government has always been a positive trend, a new wave of the liberalization of the bureaucratic political system and an example of shortening the distance between powerholders and citizens, similarly to the utopian images of Agora in Ancient Greece. However, after I spent half a year studying in Singapore - the country that is regarded as a leader in e-government initiatives implementation - my perspective has changed drastically. The main shift lies in the awareness that e-government is a method, a technology, that can be implemented in both democratic and non-democratic settings differently and bring very different consequences for citizens. While democratic state proposes a transparent way of integrating digital

technologies into the public policy process, there a lot of question marks of how similar process takes shape in a non-democratic regime, where governing elites are primarily interested in using all available instruments to hold the monopoly on power. Hence, my research interest adheres to finding answers to the problem of e-government implementation in the non-democratic country - what are the repercussions of such policy for common citizens? To follow this perspective, our research question will sound in the following way:

***Does the establishment of e-government by the state make citizens' privacy more vulnerable to the government's interference under the non-democratic regime, and if so, to what extent?***

By answering this question, I will be able to put a stepping stone for the further research of the relationship between non-democratic states and the establishment of e-government. The main goal is to scrutinize the symbiosis between these two concepts, and the best way to understand it is through putting citizens and their rights in the center of the study.

In terms of our research a clear distinction between e-government and e-governance is made. E-government refers to the use of ICT by the government to enhance efficiency and increase quality of the public service (Grönlund, 2002), whereas e-governance can be defined as a totality of technically mediated formal and informal interactions combined with institutional arrangements in which public and private actors participate in the policy-making process (Makarava, 2011: 14). The latter is a feature of a democratic setting where citizens can actively participate and influence the political agenda of the government, but perspective of my research is quite different - I want to look at the political environment that is created in the process of the establishment of e-government in the non-democratic country. Hence, discussion of the concept of e-governance is omitted in the scope of the research.



## 2.2. Thesis design

To answer a research question, my thesis is going to have the following structure. An academic literature review concerning the connection between e-government and political regime, as well as the problem of privacy in the digitalized societies, will be conducted in Chapter 2. In Chapter 3 I discuss why I have chosen case study as my methodological approach to achieve the goal of the research, from the one point, and why Singapore was selected as the case I investigate, from the other. Chapter 4 will present a democratic assessment of the Singapore based on Dahl's (1989) theoretical viewpoints on democracy and the comparison of reports on the democracy level of the political regime of Singapore presented by the Freedom House and Economic Intelligence Unit (EIU). Chapter 5 will focus on studying the place of e-government in the power setting of the state, offering a theoretical perspective on the concept from the point of view of the society of control and network society. Examination of the political structure of the executive bodies of the Singaporean government responsible for e-government establishment will be done in Chapter 6. In Chapter 7 I will study contextually the problem of privacy by analyzing legal mechanisms of personal data protection that exist in the country, from the one point, and ways privacy rights are interfered and violated by the governmental institutions of Singapore, from the other.

This structure will help us understand the building blocks of the research question and reach meaningful conclusions that may encourage further interest and discussions in academia.

## 2 Previous research in the field

While browsing through the articles and analytical reports concerning e-government, I found little research on the correlation between political regime and e-government, from the one point, and the transformation of the shape of power as a result of the new digital dimension emergence of the social reality, from the other. It is a field that needs our attention, because technology itself is an objective and rational essence, while the side that uses it - in our case, the government - decides how to exploit this technology according to the established status quo and interests of the political elites. Consequently, when I speak about e-government in its broad way of using ICTs in the public sphere by the government, my attention will be driven the shape and goals the establishment of e-government will have under the Singaporean political regime, from the one point, and what repercussions does the digitalization of public serve progression have on the privacy of common citizens, from the other.

But, before doing the actual work, I should look at the research that has been done earlier in this thematic field. I have divided the reviewed literature into two categories: the first category is those articles that have discussed the connection between the political regime and the way e-government is established. Second category examines the problem of state's expanding intrusion into citizens' privacy by the means of digital technologies.

### 2.1. Non-democratic political regime and e-government

Fukuyama, famous political scientist who in his essay «The End of History?» confidently declared that with the spread of globalization liberal democracy is going to be the final universal form of human government (Fukuyama, 1989), recently has stated that democracies can and are actually going

backwards towards the right-wing nationalism, and there are overall many evident cases of the internal crisis of previously stable liberal regimes in the world (Tharoor, 2016). However, this backward effect has not stopped the technological revolution and massive integration of ICTs into the governmental practices. Some studies (Lee 2011; Paulin, 2014; Kollar, 2016) seem to be under the illusion that e-government equals democracy and the reign of human rights, as the study of the literature has highlighted.

Nevertheless, in the past years, one can witness an evident growth scholars who investigate the models of non-democratic e-governments. These studies support the idea that the establishment of e-government does not lead directly to democracy (Kardan & Sadeghiani, 2011), as well as the fact that political elites of the autocratic regimes comfortably apply ICTs to strengthen their hold on power in their respected countries (Johnson & Kolko, 2010), or to improve the overall image of effective public policies and high national development ratings (Stier, 2015). A quantitative investigation conducted by Kneuer & Harnisch (2016) suggested that non-democratic regimes are prone to use e-participation instruments as a substitution for the lack of military, business or party actors. In addition, Maerz (2016), by analyzing e-government initiatives in the post-Soviet countries, has also concluded that a huge influence on digitalization plays the internal legitimation pressure and the need to stimulate support of the population through new channels.

Hence, some researchers agree and prove that e-government does not correlate directly with a democratic political regime, because it is merely an instrument that serves the interests of the powerholders. Another case study of the political regime in China, that some researchers call IT-backed authoritarianism due to the applied mass surveillance and Big Data technologies (Meissner & Wubbeke, 2016), has shown that the Communist Party of China is inclined towards using digital technologies for strengthening the control over the society without the reverse movement for civic engagement (Baguero-Hernandez, 2012).

This trend of a top-down approach to e-government instruments is common among non-democratic countries that are using selectively e-participation mechanisms and implementing complex surveillance technologies to filter or to suppress Internet content for the sake of legitimacy and economic growth (Åström & Karlsson, 2012).

Consequently, a number of studies argue that non-democratic regimes apply e-governance as successfully as democratic regimes. However, those studies do not answer the question of whether there is a shift in the governmental structure and if there is a change in the power balance between private IT actors and political elites - a question that may shed light on the different practices and form of bureaucratic state machinery.

## 2.2. Citizen and his privacy: e-government perspective

Citizenship and the status of a citizen itself has a multidimensional orientation. From the one point, citizenship functions as a social closure, meaning it operates as a mechanism of social inclusion or exclusion. From the other point, citizenship has a formal legal layer and a moral layer, where the latter includes active participation of a citizen in the political sphere (van Houdt, 2008: 2). The same multidimensional approach works with the introduction of a new layer of citizenship in the form of digital citizens, or, according to Mossberger, Tolbert and McNeal (2008, 1), 'eCitizens' - those who use ICT regularly and effectively on the daily basis, especially while communicating with public institutions of the state.

In this context, the main goal of the state is to guarantee the loyalty of the subjects of power, and with the rise of ICT, governmental institutions received a new effective instrument for evaluating and monitoring citizens' private lives. Government has an unmatched power to centralize all the private data that is being generated in the society, and, what is important, the division between

government and private sector is fading rapidly ( Stanley & Steinhardt, 2014: 275) with wide programs of collaboration and sharing of the databases across the globe, and there are consequences of such collaboration. According to the research conducted by Bannister (2005), the technological invasion on privacy can be divided into and analyzed from the perspective of four categories: watching (physical observation/monitoring), intercepting, reading (accessing existing private data), interpreting (data mining and data interpretation). Thus, with myriad of possibilities to get private data about the citizen, state enters into the new era of managing society, especially in the non-democratic regimes, where legality is closely connected to the political will of the powerholders, and those operations, that were described by Bannister, become closely connected to the way state is governed.

Going further, it could be argued that state is becoming more adept at managing people's identities by shaping 'digital shadows' of its own citizens (Shorff & Fordham, 2010: 304-305) through a number of services and positions in the cyberspace of modern public sphere. For example, Bozbeyoglu (2011) looked at the case of the introduction of electronic ID cards in Turkey, proposing administrative efficiency and security, the way the data is collected and connected to other relative databases opens the possibility to use personal data for other purposes than the record collection and maintenance. Researcher also refers to other papers that state that ID card systems are considered as an 'unacceptable extension of state surveillance' (Lyon and Bennett, 2008: 13-15, 18).

Other studies have put emphasis on the fact that ICT technologies are de facto surveillance technologies, so tendencies towards surveillance 'should always be considered on the development of ICT' public services (Webster, 2012: 262). This surveillance perspective puts inevitability of breaking the boundaries of human rights and human privacy, the majority of e-government studies have overlooked.

Restricting the ability of the state to access and use private data may lead to the security pitfalls and weakened organizational possibilities of the political institutions in times of so many digital dangers and uncertainties (Taylor, 2002: 73). With a high risk in terms of cyber security and possible uncertainties ICT bring to the stability of political regimes, it is logical that state extends its power concerning private issues of its citizens. Moreover, another study that looked at the technology as a mediator between policymakers and citizens, pointed out that citizens are able to use surveillance technologies like a virtual globe to influence the former directly, concerning the issues of their neighborhood (Verplanke, 2010). By promoting both the idea of e-participation and a possibility to take part in the decision-making process (Kukovic, 2015: 29), surveillance technologies may actually open up the way for citizens to be more active in the political life of the society. However, breaking privacy may threaten a citizen's relationship with the government and lead to a loss of trust (Taylor, 2002: 76), so that is the problem state should always consider.

### 3 Methodology

This thesis has a form of a case study design, as it opens up a possibility to investigate specific situation or phenomenon in depth, retaining ‘the holistic and meaningful characteristics of the real-life events’ (Yin, 2003: 2). Generally, our goal of using this method is similar to the goals all scientific methods have in social sciences - develop logically consistent models or theories, derive observable implications from these theories, test them, and use the results to influence the theories or existent perspectives in the social realm (Bennett, 2005: 19). By looking at the problem researchers have not thoroughly investigated - the role and influence of ICT on citizen’s privacy in the non-democratic setting, I am eager to develop a theoretical model as a way of explaining the problem, and gather, analyze and contextualize the explanatory empirical data to find whether our perspective has the legitimate right to live.

Definitely, it is possible to tackle the question I have in hand using other methodological approaches. However, not all methodologies could offer us the most efficient path to this research goal - for example, conducting quantitative or qualitative research on the national or governmental levels will be a very reliable way to check the validity of our assumptions, but not affordable in terms of the existent time span and material resources. On a smaller scale these instruments will not have enough explanatory power and contextual connection to interpret scientifically the triangle of ICTs, political regime and privacy.

Therefore, I decided to stop on the case study for two reasons. Firstly, case studies offer conceptual validity, meaning that by identifying a case or number of cases, researcher is able to contextualize and make analytically equivalent the indicators and concepts that best explain the theoretical basis of the study (Bennett, 2005: 19). For us that means that I can concentrate solely on doing practical research, without going deep into philosophical discussion of what is

democracy, state, political regime etc., and then explain why I have chosen these definitions and not the others. Essentially, I am trying to be practical in the way I analyze and give meaning to the real data, building first a solid foundation for our model of highly digitalized non-democratic society, that could be later cross-compared with other models and scientific concepts.

Secondly, case study design is useful in terms of learning about new environments and settings (Yang, 2014: 161) that have never studied from a chosen perspective. It is very important, because with our research question it is impossible to use the traditional data or other research results that have been already accumulated or given meaning to. In our setup, it is imperative to be more independent and intuitive, investigating the little known social territory with the scientific instruments I have. Because little research has been conducted in the sphere of e-government as a new instrument of power in the modern society, case study became an evident choice for the examination of the validity of such theoretical trajectory, giving insights for the research areas which were barely studied before (Eisenhardt, 1989: 548). So, in other words, case study offers us a territory where research scientific perspectives can be tested.

Therefore, case study will serve as a research guidance for our strive to an answer to whether e-government in the context of non-democratic regime brings more dangers to the common citizens than positive outcomes. Last but not least, as our study is oriented towards discovering and exploring the social realm, such nature of our thesis design requires a similar category for a case study. Our task is to open up the door for scientific discussions and similar investigations in other countries. Hence, our research is going to stick to the exploratory case study design that investigates distinct phenomena characterized by a lack of detailed preliminary research, and that is often applied as a preliminary step before conducting a more sophisticated research (Mills, 2010). In the exploratory setting, our goal is to find the connection between the e-government under the non-democratic regime, from the one point, and higher vulnerability of the citizens due



to the expanding nature of the state's political power, from the other. By looking into the real-life data and building bridges between theoretical viewpoints and acquired data, exploratory case study will help us check the validity and potential of the theoretical model I will use in the process of our investigation.

### 3.1. Selecting the case

While there are many countries in the world that are on the advanced level of ICTs integration into the political system, and countries that are not considered to be democratic, there are not so many that have combination of both. Reducing our research choices to a developed non-democratic state that is actively pushing forward the digitalization of the political system, options narrowed down to a limited amount of countries that could potentially hold our interest. When choosing a case, the main principle is 'to maximize what we can learn' (Stake, 1995: 4), and this principle of the maximization of the potential knowledge was a prevailing factor in the scope of the case study design when choosing case of a non-democratic country. According to the United Nations top-50 rating of the world e-government leaders with a high E-Government Development Index - average of three scores: scope and quality of online services, status of the development of telecommunication infrastructure, and the human capital (UN E-Government Survey, 2016) - there are a number of countries that correspond to our demand - Singapore (4), Bahrain (24), United Arab Emirates (25), Kazakhstan (33), Russian Federation (35), Kuwait (40), Saudi Arabia (44), Qatar (48). Any country from the above-mentioned ones may be chosen. Personally, for me it would be also easier to investigate Russian case because of the language. However, for the maximization of the potential knowledge, Singapore is the case that will help to find the answer to our research question for two reasons.

Firstly, Singapore is a leading reformist in the sphere of e-government in the world. Besides the above-mentioned UN E-Government Development Survey

(2016), according to the famous World Economic Forum Global Information Technology Report (2016), Waseda University World e-Government Ranking (2017), Singapore was ranked on average in top five as the best prepared country in the world for the new digital economy, getting high results in such dimensions as political and regulatory environment that enables ICT implementation, infrastructure and digital content (mobile network coverage, Internet bandwidth), and individual usage. Moreover, the e-government in Singapore towards has had a long history and gives a lot of insights and raw data about the way political system operates in this new environment.

Secondly, being a highly developed modern country, Singapore is not a democracy. Reports of such organizations and think tanks as Freedom House (2016), Reporters without Borders (2017), the Economist Intelligence Unit (2016) point out that Singapore has a long road to go to become a full-fledged democracy. Consequently, high level of e-government development and non-democratic political system may be the prerogative to the 'crucial' or 'most likely' case that, according H. Eckstein, 'must closely fit a theory if one is one to have confidence in the theory's validity' (1975). In terms of our thesis, Singapore can be the case that will help us to conduct an exploratory case study and give us the answer to our question: «Does e-government implementation makes citizens more vulnerable to the state's interference under the non-democratic regime?».

### 3.2. Data

Success of our case study research mostly depends on the sources that will be used in order to find answer to whether the e-government implementation in the non-democratic regime makes citizens actually more vulnerable to the state's interference, and, consequently, less secure - both privately and socially. Having narrowed down our question to this simple statement and by choosing Singapore as our research target case, a manually closed context is created I could solely

concentrate and work on without interference from any discourses and points of view that may undermine our perspective. On this stage of our study the main thing that will definitely higher the potential success of our research are the sources our theoretical analysis will be based on. Therefore, by gathering multiple sources that cover the same phenomenon, case study findings are more convincing and accurate, thus increasing the validity of our research (Yin, 2014: 47). Moreover, with the possibility to acquire both quantitative and qualitative data, I receive the full coverage of the societal picture I have in hands, thus opening space for a better understanding of the case I investigate as a researcher.

Following this logic, a number of diverse empirical sources have been gathered: Singaporean official (political initiatives, statutes of the Ministries) and legal documents (Singaporean laws, acts, declarations, orders) that formulate the political order of the country; political programs, frameworks of the e-government reform, provided by Singaporean Ministries or expert organizations; nationwide statistical data provided by the Department of Statistics Singapore and Data.gov.sg; previous research and reports of the international organizations, NGOs engaged in human rights protection, sustainable and urban development, and public policies implementation. By analyzing these empirical sources, I will not only have a better understanding of Singapore in terms of the case study, but will also be able to look more critically at the research question.

### 3.3. Independent and Dependent Variables

My research question has a casual relationship in its core, so it is impossible to analyze data without having independent and dependent variables of the social phenomenon I am looking at. Bennett had emphasized dependent and independent variables as the essential case study design task (Bennet, 2005: 26), and for a right reason: to give sense to the empirical data, I should describe abstract generalized theoretical concepts that in some way relate and depend on

each other, and that serve as the gathering points for the data that is collected. In this way, our focus is set on supporting those concepts with empirical data, getting rid of all the information noise in the process of investigation.

Our independent variable is a grouped variable with the name of political regime of Singapore, because it consists of smaller diverse variables that define whether and to what extent the political regime is democratic or non-democratic. In terms of our research, our focus is not on the comparison between political regime of Singapore and other countries, but on how non-democratic state of affairs in the country shapes our dependent variables. So, in order to understand this influence, our task would be to describe the political regime of Singapore through those small variables, so that our research has a clear understanding of the context and its potential influence on our dependencies.

Another independent variable is the e-government reform. The extent and level of its implementation on the nationwide scale solely depends on the political regime and its interests. E-government reform is a policy that has been carried out by the government, because the former has been closely aligned with the Singapore's national interest of building an information society. Without this, it is very unlikely that the e-government would be at such an advanced stage in Singapore. Moreover, the nature and shape of the e-government initiatives implementation depend on the political frameworks and priorities set by the executive body. To investigate the variable, I am going to look at it from two sides. The first side is theoretical one - what is the role of e-government in changing the shape and concept of political power? What is the place of e-government in the evolution of power? How does e-government transform the bureaucratic model of political management?

The second side is a practical one - I will analyze how e-government initiatives are implemented in Singapore, starting from the executive structure of the digital side of governance, and ending with the current programs and set goals of the Singaporean e-government policies.

Privacy as the ability of citizen to seclude information about himself will be our dependent variable. It is the fundamental human right that is recognized by the UN Declaration of Human Rights. It is possible to measure the citizen's ability to ensure his privacy safety, by going from the opposite - examining how much information that can be used against a common citizen Singaporean political institutions collect. In this regard, the level of authoritarianism and the advancement of ICT technologies may have a defining influence on the level of secured privacy of citizens, including their private information as an asset, and the ability to protect this asset, both de facto and de jure. Through studying the potential dangers the state poses to citizen's privacy, as well as by analyzing real facts of privacy abuse by governmental institutions, it will become possible to answer my research question.

Because our research will reach privacy variable in our last chapter, it will be our most pivotal part of the thesis. Building on our previous work, created political environment in Singapore will be critically analyzed to understand the influence and potential harm e-government has on the security of citizen's privacy. The environment itself and its relation to privacy will be inspected from the two points - Singaporean legal framework of the personal data protection, as well as programs and instruments, including e-governmental ones, executive bodies use on a massive scale and which have potentially a negative impact on the citizen's privacy.

### 3.4. Approach to Case Analysis

Having defined the main inputs for our case study design, the last that is left is to choose the approach that will help us conceptualize our variables and connect them to our theoretical framework. Bennett (2005) has defined a number of methods for a within-case analysis like congruence testing that focuses mainly on comparing the actual and expected composition of the independent and

dependent variables, or counterfactual analysis that looks if negation of investigated variables changes the dependent ones. However, in terms of my research, I am going to analyze at how those variables that were defined above are connected to each other, how they influence each other, and, in the end, explain the casual relationship between political regime and e-government, from the one side, with the citizens' privacy matters, from the other. In this way, case study will give me a practical understanding of the core relationships between the concepts that are the basis of my research question.

### 3.5. Research Limitations

The main limitation of our research is that I concentrate only on one case. Surely, investigation of different cases across political cultures would perhaps be more valid. However, my main priority is to concentrate on the task of the thesis which is to conduct an investigation within the scope of this paper and time given, therefore, it would be difficult to examine more than one case on the national level. Moreover, many countries in the world lack the basic organizational structure, resources and infrastructural possibilities to implement e-government, making cross-country comparison invalid.

Another limitation of this study is that I am not a Singaporean or a permanent resident of the country. As a result, I cannot gather as much data and information, as I would like to. In contrast, with English as an official language, a lot of previous and actual reports on the state of e-governance of Singapore, my task becomes much simpler in terms of data collection, so I would be able to concentrate more on the theoretical work and analysis of the acquired data.

Lastly, limitation of the ambitiousness of the research lies in the idea of the political perspective on the digitalized governance in the period of its establishment. Eventually, such situation may result in more of a journalist report with a loud conclusions about digital dictatorship (Economist, 2016), rather than a

full-fledged research. To cope with this issue, Singapore was chosen as one of the most developed countries in the world with ICT implementation in the political sphere.

## 4 Political regime of Singapore

Located on the small island in the Indian Ocean, the Republic of Singapore with population of 5 million people is one of the most well-known and highly developed countries in the world. After gaining independence in 1965, the newly established state under the leadership of Lee Kuan Kew took the road towards building economic prosperity that turned out to be one of the biggest miracles in the modern world history.

However, with rapid economic development, achieving the status of a truly 'exceptional' place as the world's only fully functioning city-state, and a global hub of finance and commerce, Singapore has also fallen under the shadow of non-democratic political rule that undermines the rights and freedoms of citizens in the 'democratic' political system that has never changed its ruling party for the whole country's history (The Economist, 2015). Therefore, the logical question arises: what is the human value of having high economic indicators, when people do not have possibility to protect their rights and have independent political stance in their own country? Technology in this question plays also a pivotal role - what if the actual beneficiary of the liberating innovations is not an individual in the first place, but a state that innovatively insures the stability of its rule in the established non-democratic setting? This is the question that pushed me towards exploring the connection between political regime and e-government as a political pro-democratic reform. Thus, before looking at the way technology has any connections of the scope and range of the government's power, it is important to understand the essence of the Singaporean political regime, so our findings correlate with the realistic picture of the state of affairs I investigate in the first place.



## 4.1. Theoretical approach on measuring country's democracy level

Democracy as a concept has been discussed since the start of the European philosophical tradition itself, starting from Plato and Sokrates centuries ago. While our goal is not to discuss how democracy can be defined from the comparative perspective of many researchers that have looked at the topic, I am going to apply the classical understanding of democracy presented by the famous political theorist Robert A. Dahl to analyze the Singaporean political regime. The main strength of Dahl's conceptualization of democracy is his practical stance of identifying if a state is democratic or non-democratic. This sort of position opens for us the possibility to apply our results in the practical part of our research, leaving behind the struggles of philosophical uncertainties.

American researcher in his book *Polyarchy* (1971) explained two main prerogatives for a state to conceptually be democratic. The first prerogative is contestation - when citizens have «unimpaired opportunities to 1) formulate their preferences 2) signify their preferences to their fellow citizens and the government by individual or collective action 3) to have their preferences weighed equally in the conduct of government» (Dahl, 1971: 2). Citizens have actual or potential ability lobby or outline their interests, protect them in public space through instruments like media, NGOs, political parties etc. The second prerogative is participation or inclusiveness - «proportion of the population entitled to participate on a more or less equal plane in controlling and contesting the conduct of the government... the larger the proportion of citizens who enjoy the right, the more inclusive the regime» (Dahl, 1971: 4). Dahl was talking about the electoral side of political regime, of being able not only freely address issues to the government, but also of taking part in deciding in which direction - politically, economically, culturally - the country is moving.

Even though some might say that these two criteria are leaning towards abstractness, because there are no ideal democratic systems where every person has the equal voice in the public sphere, or where citizens have no obstacles of taking part in elections and then management of the country, they are the basic refer points for understanding of how democratic the country is. If there are no free elections, or the public sphere is controlled and repressed by the majority or the ruling elites, than I can clearly say that the country is non-democratic, despite the economic development or declared democratic rights in the country's main law.

## 4.2. Analysis of the political regime of Singapore

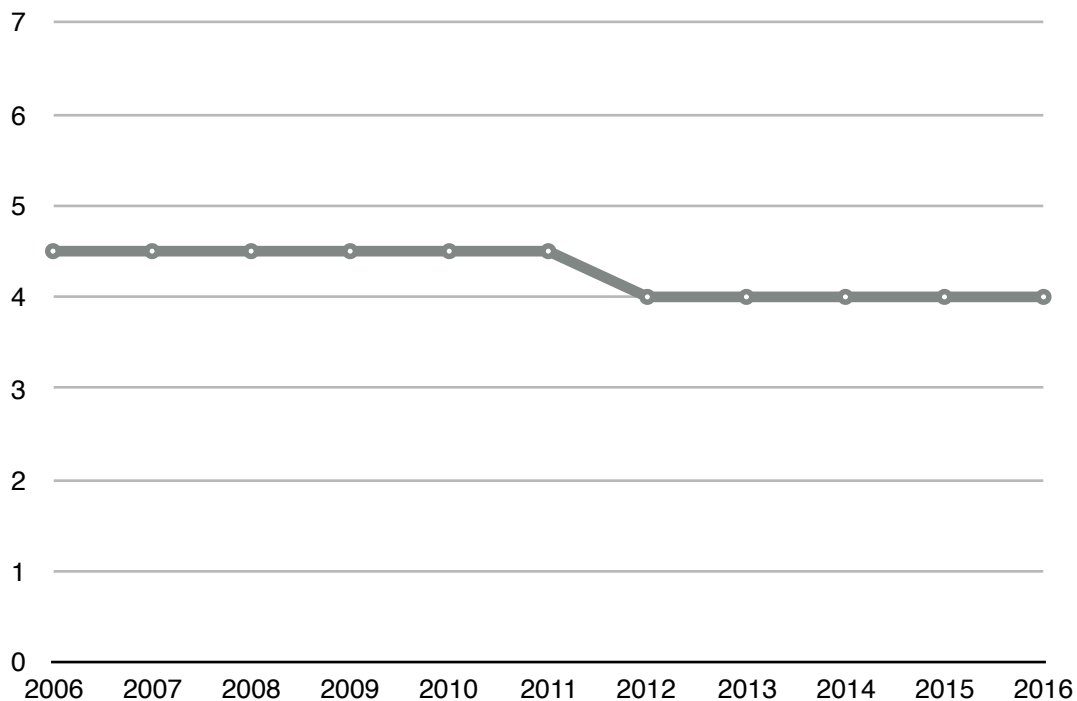
Having in mind those two points - contestation and participation - our investigation is getting rid of the bias of measuring the 'democracy level' of the country - the problem not only academics, but also many think tanks and research centers are bumping into when applying complex methodology instruments for identifying how democratic/undemocratic the country comparing to other countries, leaving alone the bias of the published results due to some background influences or other undisclosed reasons.

However, what those reports are good at is at detecting the trending change in a number of analyzed indicators throughout the researched years. Moreover, in its essence in those ratings it is possible to find those ones that entirely or partly describe the contestation and participation indicators. Therefore, I will comparatively investigate the Singaporean results in terms of these two compound parameters presented by the most famous ratings - Freedom House and their 'Country Reports', as well as the Economist Intelligence Unit and their Democracy Index respectively. The time span of our retrospective analysis is 2006 - 2016, because, from the one point, EIU's Democracy Index first started in 2006,

and for the sake of comparable results it is essential to have the comparable data. Secondly, I am interested in the tendencies of the last decade in the 21st century, rather than what happened 20 years ago and is irrelevant in terms of our research.

Both Freedom House and EIU describe Singapore as Partly Free (Freedom House) or Hybrid regime (EIU), while it combines democratic traits with non-

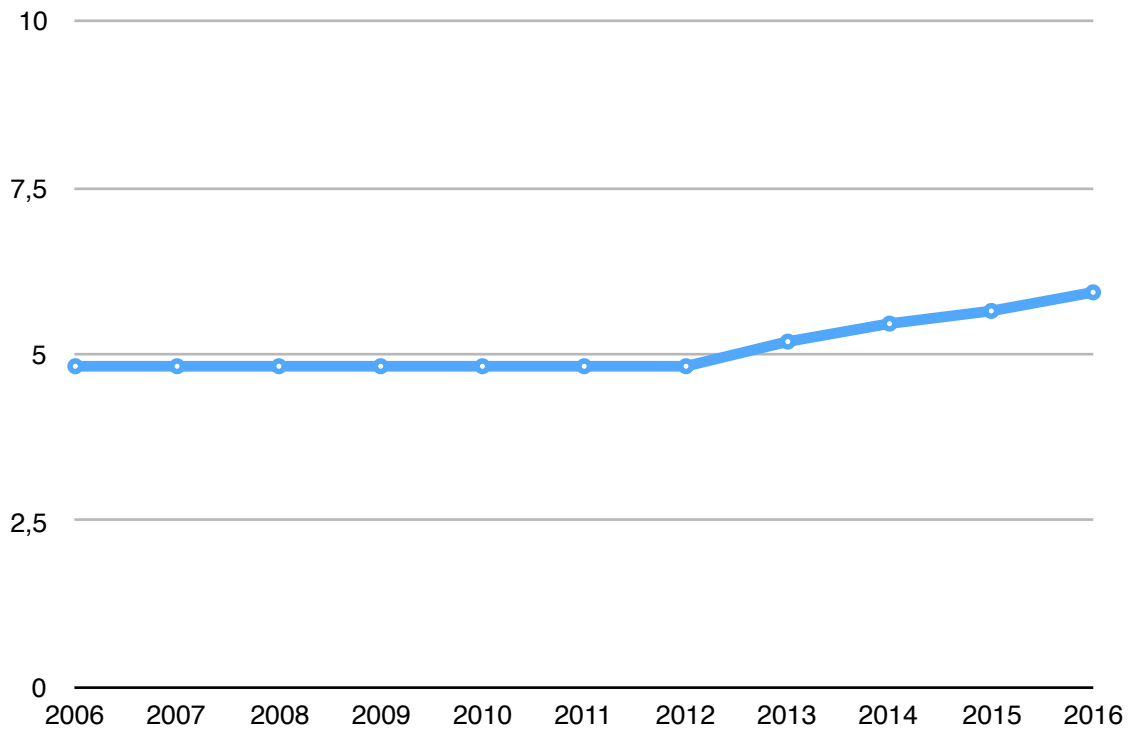
Figure 1. Aggregated scores of the freedom status of the political regime of the Republic of Singapore, Freedom House (2006 – 2016)



○ Freedom House accumulated rating (0 - Free, 7 - Not Free)

democratic ones. If we look at the charts (Figure 1 & 2) of the way both political institutions have evaluated political regime of Singapore during the last 10 years, the picture is very similar: both Freedom House and EIU have reported a declining authoritarian tendency of the political regime. However, there is a slight difference in the dynamics of that change, as the EIU a much rapid change in the recent years. To understand such discrepancies, let us go step by step in terms of the way presented ratings evaluated political contestation and participation in Singapore.

Figure 2. Accumulated rankings of the political participation, electoral process, and civil liberties indicators of the political regime of the Republic of Singapore, Economist Intelligence Unit (2006 – 2016)



● EUI accumulated rankings (0 - Authoritarian regimes, 10 - Full Democracies)

Both Freedom House and EUI put a lot of emphasis on the electoral process of the political regime, which has both contestation and participation sides. Results of their investigation have an unchanged medium estimate for Singapore throughout the years - 4 and 4.33 respectively. Legally, electoral rules of Single Member Constituency and Group Representation Constituency in the political structure of Singapore have always worked for the benefit of the ruling party, overpowering the strength of popular vote and financial capabilities of the small political organizations. According to the Freedom House investigation, the political climate in terms of contestation has in practice remained the same during the decade: People's Action Party (PAP), dominant political force in Singapore since independence, grasp on power has been untouched by the opposition parties, which have been formal rather than real contestants; because the court, as well as the media are dominated by the pro-governmental groups of interests (Freedom House, 2006), reiterative cases of politically motivated trials of opposition

leaders, independent bloggers have taken place throughout the years (Freedom House, 2010); elections have been repeatedly used as referendums on the prime minister's and government's popularity, organized spontaneously and outside the expected normative proceedings (Freedom House, 2007).

Generally successful for opposition were Singaporean general elections 2011 and 2015, when most (the former case) or all seats in Parliament were contested between the PAP and the Worker's Party - first time since the independence (Kok, 2015). However, the outcome itself was far from optimistic, when PAP has retained in both cases more than 90% of the seats in the Parliament.

Concerning elections in terms of participation, legally every Singaporean citizen older than 21 has the right to vote, but more importantly - every Singaporean citizen is obliged to vote as 'part of the responsibility of being' Singaporean (Singapore Elections Department, 2017). Abstaining from voting means public shame and inability to vote during next elections (Charlene, 2015). So, the number of voters is not representative of the active participation. What matters is that public space as a forum for ideas and discussion has been strictly confined in Singapore: opposition parties have been repressed by the ban on taking part in and producing political films, televised programs, expressing political opinion freely; most of the domestic newspapers, radio stations, and television channels belong to the governmental actors (Freedom House, 2011); high level of censorship of political, religious and racial issues for the sake of Singapore's multi-racial society balance has blocked not only highly abusive or criminal cases, but also very neutral or politically motivated ones (Southeast Asian Press Alliance, 2013). Increasing use of social media by Singaporeans has opened up possibilities for opposition, NGOs and individuals to build their own different discourse from the dominant one, but due to Internet legal regulations (Kirsten, 2016) and content blocking through governmental directives to licensed service provider (Freedom House, 2016) those movements have not drastically changed the electoral field in Singapore.

However, the strength of the EUI's Democracy Index is that it evaluates the opinion of experts and civic public leaders, offering a subjective view on the political situation in the country, overcoming in that way the narrowness of isolated historical facts and numbers. As table shows (Figure 3), from 2011 until today there is a growing liberalization movement in Singapore, and more specifically, in the index of political participation - the number has risen more than two times!

Figure 3. Accumulated rankings of the political participation, electoral process, and civil liberties indicators of the political regime of the Republic of Singapore, Economist Intelligence Unit (2011 – 2016)

	2011	2012	2013	2014	2015	2016
Electoral process	4.33	4.33	4.33	4.33	4.33	4.33
Political participation	2.78	3.33	3.89	5.00	5.56	6.11
Civil Liberties	7.35	7.35	7.35	7.06	7.06	7.35

Singaporean government has created legal and repressive obstacles for opposition to has any influence or saying in ruling the country. Other organizations and opinion leaders have been surveilled and pressed by the dominant media and centralized censorship. Going further, freedom of public assemblies has also been restricted by the officials, as it requires police permission to organize public assembly (Freedom House, 2009), including the need to apply for such permit 28 days in advance (Amnesty, 2017) - rarely an option for a protester to present effectively his position. Despite all these restrictions, during the last years a huge democratic wave of civil society activities was evident in Singapore. Public protests on a variety of topics - water prices rise (Ungku, 2017), Prime Minister's alleged abuse of power (Ungku, 2017), Singapore government's horrendous treatment of detainees without trial (The

Online Citizen, 2017), against governmental immigration policies (BBC News, 2013) - are only the tip of the iceberg of the sporadic organized mass movements that have developed in the recent years and did not happen so often before. Stronger position and support of the opposition are also examples of the people's demand and desire to participate in deciding how their country is managed. Therefore, because of a broader support of the non-governmental actors by the population, the former is gaining small but improved momentum in their struggle to weaken the ruling elite's monopoly on power.

Consequently, it can be stated that Singapore is a non-democratic state where traditional ruling elites have a strong domination over the political life of the country. Government, legislature and court work in one direction to maintain the created status quo, building fences for the non-governing elites and organization to contest and diverging public opinions to have any impact in the public sphere. In the Dahl's world, Singapore would be somewhere close to the non-democratic model of the inclusive hegemony, where with unrestricted possibilities to vote and have access to information, very limited and high-cost possibilities exist to actually contest and influence the way the state is ruled.

But the interesting case of Singapore is that it resembles a closed bottle with water. The latter is shapeless and formless, but in the former water takes ideal shape of the container. However, with time, where there is more water than the bottle can actually keep hold of, a decision should be made - either you open up the bottle and let the water go loose, so to say, or you create the mechanism to lower the pressure inside the bottle, leaving it as it is. In any case, the problem is real - as with metaphorical water, citizen's demand for mechanisms of participation and inclusiveness in the political environment of Singapore is growing, giving the first impressions of an alternative political system to the non-democratic dictatorship of the ruling party. Because of this long discussion of the political regime in Singapore, the perspective on e-government and ICT integration into the governmental structure of the state has received some new

colors - what is the purpose that the ruling elites of Singapore are trying to achieve? Offering the instrument that empowers civil society and opposition is clearly not the case Singaporean government is trying to achieve. Hence, before diving into the practical part of our research, our investigation should understand the role e-government plays as a political framework and as a concept in the evolution of modern governmental practices.



## 5 The concept of e-government: theoretical perspective

### 5.1. E-government and society of control

Along the centuries diverse societies have gone through a myriad of social, economic, political changes, and with the rise of global interconnectivity, those underlying trends became common for the most part of the world. The modern trend of government digitalization is another trend that many countries are trying to follow. According to the UN e-Government Knowledge Database, more than 100 governments in the world today provide online public service delivery and open governmental data, comparing to just 40 in 2003 (UN E-Government Survey, 2016). The first reason for that is that technologies became faster, more affordable, and efficiently better at dealing with routine tasks of storing and working with data than papers and people. The second reason is that with the rise of new modes of communication and style of life in the virtual sphere in the society, governments are also adapting to the new state with ICT innovations to reach and interact with these people.

Hence, the reform of the public services became an imminent task for the governments in the modern world whose citizens were more and more exposed to the new modes of communication that were beyond the scope of the accessible power range of the bureaucratic state. E-government emerged as a perfect solution to this problem - by using ICTs to provide faster, easier and more efficient access to the delivery of information and services to the public, businesses, other agencies, and governmental entities (Reddick, 2010: 5), state has obtained a new digital instrument of exercising its power.

Webster and Robins (1999) have identified two main functions that ICTs fulfill in modern societies: “on the one hand, they have been the mechanism for social management, planning, and administration; and, on the other, they have been at the heart of surveillance and control strategies” (p. 90). They follow Foucault’s idea that surveillance coexists with administration, so that «power, even when faced with ruling a municipality of men, could be as efficacious as if it were being exercised over a single one» (Foucault, 1980: 152). This idea is very powerful, coinciding with the true nature of administrative power of the state - to manage and control society. Looking back at the political regime of Singapore, it is highly possible that it is what Singaporean political elites are trying to achieve - to build the country with the highest standards of living, but where the rule of the government as an administrator is undeniable, and where surveillance plays an important role to guarantee that the established state of affairs remains.

Before the emergence of massive market ICTs, this system worked perfectly well in the form of state’s institutions like factories, hospitals, and schools which created a closed societal system with three main techniques of control applied to it by the powerholders: hierarchical observation, normalizing judgement, and the examination (Foucault, 1978). What this form of power achieved is that it guaranteed obedience and ‘right’ behavior of the society’s members through legitimized practices and common values. Singaporean citizen would go through the ladder of these institutions and fit perfectly well in the stable political system, whose legitimacy is based on the values of stability, prosperity, and economic growth.

However, as valid as it seemed for the time of Foucault’s writing, the model of state as a disciplinary prison only partly applies to the today’s societies influenced by ICTs and strong winds of globalization and glocalization. In the Foucault’s world, surveillance was ‘the most efficient form of power, the most totalitarian and the hardest to resist’ (Allmer, 2015: 82), but the rise of multiple channels of information and decentralized social interactions made surveillance as

as instrument of the political institutions not so effective, as it was for common model of 'disciplinary' society of the 19th-20th century.

Deleuze was one of the philosophers who was cornered by this dilemma, and he argued that all disciplinary institutions are in crisis, with administration trying unsuccessfully to perform reforms just to keep those institutions afloat (Deleuze, 1992: 4). Hence, philosopher pointed out that new shape of society is appearing: society of control. According to Deleuze, the main difference between the two is that disciplinary societies have two poles: individual pole with signature as the main 'identifier', from the one point, and a collection of administrative numeration that indicates his or her position within a mass, from the other. In the societies of control there is no poles, as a continuous integration of all spectrums of life made individual 'dividuals' - codes, or containers of data, that are constantly in the process of establishing themselves, interacting with other containers, and never 'being finished with anything' (Deleuze, 1992: 5). Citizen's obedience became immanent in the flexible, fluid, and fluctuating networks of existence itself (Cheney-Lippold, 2001: 168).

Returning to the real world, what Deleuze is saying is that modern states are building the systems of control where citizens are not just human beings with a passport, some documents, occupation and official duties that make them formally citizens of the country, but they are also digital data containers that are always active in the social world - data about movement, messaging, registration for a doctor's visit, phone calls, moving in and out of the country, voting - all these pieces of information is data that can be theoretically stored and retrieved by the user ID, as in any database. Moreover, with a modern style of life where people do not usually live and work in the same place for a long time, it is essential for administration to understand the status of this or that person in the society to make the right administrative decisions and choices.

So, a common person has the freedom to do whatever he or she desires, but this freedom is constrained in the form of data that can be gathered, stored,

retrieved, analyzed, and then used by other actor or organization. This the way business world is working today, and this is how the control as power of the government in the 21st century is built. ICTs have a become a working solution for the bureaucratic political institutions to expand their authority through the digital realm. By making the Internet infrastructure more inclusive and opened to the masses, motivating people to use public online services with online IDs, the state is able to gather information about country's citizens much more efficiently, overcoming the barriers of apparent surveillance mechanisms common for the previous centuries.

It is pretty impressive that Deleuze was able to conduct a socio-technological study of the mechanisms of control with computer as the main machine behind this process decades before the first real examples of successful e-governments, the rise of smart homes and smart cars, and the popular trend of programming as the trending competence of the 21st century (Haaromo, 2014). Even though Deleuze was one of the pioneers in investigating the nature of power with the spread of ICT, he was not the first one in outlining the shape of the societies of control. Information society (Beniger, 1989), post-industrial society (Bell, 1973), network society (Castells, 2010) are all related concepts that are dealing with the digitalization of communication, but without the political power perspective. In order to understand how ICT as a mechanism of control power can influence a common citizen, the model of the modern society in terms of digitalization should be critically looked at and projected on the Singaporean realities.

Therefore, in next chapter of our research, in order of not losing focus among diverse descriptions of the same thing, this research will stop its attention on the network society, as far as the scope of discussion lies in the structure of the society, means of political management of that society, and the technology as the main instrument of the state's power. Network society is the concept that concentrates primarily on these parameters, so it will be also easier for us to

connect it to the theory of the society of control, building bridges between the sociological and political understanding of the society itself.

## 5.2. E-government and network society

A huge step from the industrial age to the information age brought a drastic change to way societies exist and communicate - faster, much more decentralized, interconnected, and global. Hence, ICT as an asset have not proposed new gadgets and digital services that are part of every person's life, but also developed a new way of how society functions - via networks. There are two different camps of defining what is network society. The more radical side claims that network society is a social structure founded on networks operated by ICTs based in microelectronics and digital computer networks that generate, process, and distribute information on the basis of the knowledge accumulated in the nodes of the networks (Castells & Cardozo, 2006: 7). In other words, the basic unity of such society is a computer, or a code that defines the nature and form of social interaction of its members. A more moderate approach advocates that the basic unit of the network society still consists of the individuals who are linked by networks (van Dijk, 2012: 35). The difference is that the latter approach puts online communication as a parallel mode to already existing traditional ones, whereas the former defines microelectronics in the hierarchical order as the dominant force in all forms of possible interactions. The contrast has a more of a philosophical question opened for discussion, because both approaches describe how technology changes the form and context of the societal dwellings. So, despite those differences, they share a lot in common.

Firstly, networks are flat and polycentric with a number of centers cooperating and competing with each other (van Dijk, 2012: 36). In contrast to the mass society with the disciplinary power where relations inside of it are

centralized and vertical integrated modes of organization prevail (van Dijk, 2012: 33), network society possesses the quality of a self-organized system that constantly fluctuates and adapts according to the needs and interests of the main centers inside of it. For example, in the Singaporean society there is an evident shift towards horizontal non-centralized cooperation between different civil society actors that have interest in the same political issue: in 2008 the Animal Concerns Research & Education Society created an alliance with six other NGOs to launch an online petition against the import of whale sharks into Singapore. The year after the governmental plan to exhibit white sharks was abandoned because of the pressure from the above-mentioned organizations and different society representatives (Ow Yeong Wai Kit, 2016). For Singapore as a country with a very centralized hierarchical structure, example of decentralized voluntary civic engagement shows how those networks work in practice.

Secondly, mass media as an actor of the public sphere has a form of a customized and fragmented multimedia system, whose audiences are increasingly segmented. As a result, the social system is increasingly inclusive of every message sent in the network society (Castells & Cardozo, 2006: 14), resulting in a graduate merging of telecommunications in the society (van Dijk, 2012: 7) and deeper integration of all elements of the society into one context. In terms of the power of control, this form of integration is the main reason why new form of power has appeared, because without the traditional division of information channels government loses the ability either to administer or to conduct surveillance, because it does not know how to transfer message to the right receiver. Beforehand, Singaporean government has solely depended on the TV and traditional media, but nowadays, with the development of ICT and implementation of e-government initiatives, the presence of the government is noticeable in every realm of social media - starting from Prime Minister and finishing with a minister - every one of them have their own active and often updated Facebook, Twitter, Instagram accounts (Sagar, 2015). Consequently, such

trends in the telecommunication services make the hierarchical division between private and public spheres less obvious, and old mechanisms of disciplinary power ineffective.

Continuing the topic of media, domination of the multimedia system with the abundance of information forms the state where absence of a message in a media space becomes a non-entity that eventually cannot reach members of the society (Castells & Cardozo, 2006: 17). In spite of the fact that absence of message in the public space of the traditional societies had the same outcome, the continuous presence of the information in the overcrowded decentralized public space of the network society holds a fundamental role in shaping public opinion of the whole population and its groups. With the information abundance, constant presence of one message can make a difference in shaping public opinion. Hence, state's dominance over the media channels in Singapore allow powerholders to build the dominant discourse that is overpowering other decentralized centers in the network. Because information flows from node to node, control of the majority of channels is one of the main priorities for modern governments to survive. That is why Singaporean political elites had put the development of e-government into their top priority, before it was too late and other actors like opposition parties, opinion leaders have overtaken major centers of influence inside network.

Thirdly, increasing complexity of the social interaction and its potential insecurity due to the publicity of communication in the online spectrum has led to the emergence of code and programmed control as means of managing communication in the network society. As relations in the network society are in fact programmed and coded more and more (van Dijk, 2012: 40), the code itself becomes an instrument of power together with such instruments as word, symbol, gesture etc. Eventually, those groups and stakeholders that manage or 'own' the code of the application, product, system, have the ability to influence or control people's opinions and behavior. This idea is very powerful and crucial for the

understanding of the role e-government plays in the evolution of power. Before, when relation between powerholders and citizens was confined with such instruments as law and order, personal interaction, for example, with a police officer, document like passport, or intrinsic social values, in the age of e-government code as a language of digital existence offers a new, higher level of power abstraction. Now every bit of communication and interaction between citizens, or between citizen and representative of the public sphere is coded, and the owner of the code is the actual powerholder. In other words, it means that when citizen agrees to use or starts using digital technologies in the public sphere, he agrees to follow the rules of the code owner - and this is a game changer for the political institution as an administrator.

Fourthly, technical foundation of the network society lies in the 'store and forward' principle that is implemented through the usage of electronic memories and storage in databases of all types to manage information (van Dijk, 2012: 44). For a common citizen this foundation does not have a big impact on his everyday life, because he is the user of the service, not his owner. In contrast, for the government, similarly to the business outlet, control and management of the technical basis is one of the most important tasks: code is a strong instrument, but without the data storage infrastructure, as well as capacity to save and hold those great amounts of information, it is useless. Therefore, to develop a successful e-government, a lot of background work must be done to support the tip of the iceberg which is the actual services and operations political institutions provide electronically. Singaporean politicians clearly understood that years ago, and today country's data center industry accounts for over 60% of the Southeast Asia market, with putting much emphasis on constant uptime power, high bandwidth capacity, and efficient space usage (Goh, 2015). With infrastructure in place, Singapore has also directed its intellectual forces towards what is called 'Smart Nation Big on Big Data', creating the analytical centers that are experts in



collecting and interpreting right information correctly (Infocomm Media Development Authority, 2016), getting rid of meaningless junk.

Lastly, states are reshaping themselves to become less structured systems to the point of getting the form of infrastructures that are able to orchestrate complex self-organized systems of the society (Castells & Cardozo, 2006: 237). Through the ICT that are being absorbed into governmental institutions, bureaucratic state is adapting to the changes the modern times are leading to. Hence, the hierarchical order of the state is giving space to a network of political institutions and private parties that share sovereignty and policy dimensions of power (Castells, 2006, p. 16). In the next chapter I will analyze how political institutions of Singapore are reshaping themselves according to functions they play in the network, but there is one thing that should be emphasized: as power of control is hidden inside the societal network, it is impossible to define it in terms traditional, charismatic or legal authority. Surely, they are also present in the political system, but to hold the authority over the decentralized societal network a different approach is needed - and this approach lies in managing the network flows of the society: flow of production, flow of information, flow of services etc.

Consequently, the structure of political institutions is shifting towards both the needs of the society and the possibilities of today's technologies. Contradictory to expectations, even though traditional hierarchical and bureaucratic procedures are declining, central control inside and over organizations is increasing (van Dijk, 2012: 109), because, from the one point, ICT allows to automatize a lot of routine processes inside the governmental operations, taking away uncertainties and influence of a human factor. From the other point, the functional orientation of the political institutions makes the process of management more result-oriented and, thus, more centralized.

Therefore, e-government in the network society is not just a new website of a Ministry, or innovation in the medical sphere online services. It is a much more complex phenomenon that describes the new way of managing society that

is dynamic, flexible, fluid, and that is highly dependent on the technological side of the communication. Normalizing disciplinary practices are extending well outside the structured sites of social institutions (family, school, hospital) through fluctuating and self-organized networks (Hardt & Negri, 2000: 23), and ICT offered state a new way of practicing its power to govern its population with code as the new language of power. By developing data management infrastructure, as well as services that are based on the former, government goes jumps from the era of disciplinary power to the age of the power of control over the decentralized networks that largely constitute modern societies.

## 6 How the nation of Singapore is E-Governed

### 6.1. Ministry of Communications and Information: structure and goals

The problem I find with analytical reports on the establishment of e-government is that they tend to generalize the way how political structure of the state is changing due to the digitalization by referencing raw facts and numbers without any contextual analysis of the actual changes in a given context. To close this gap, in this part of our research I am going to take a good look at the practical side of how e-government is implemented in the Singaporean political environment.

Leaving behind philosophical perspective on e-government, in practice the terms refers to the facilitation of government-to-government (G2G), government-to-citizen, government-to-business processes (information, communication, transactions) by the means of ICT (Rahman, 2010: 302). To achieve this goal, e-government as a model has four main functional layers: network layer (information infrastructure, servers, Internet), integration layer (database development, e-mail, network-enabled systems), management layer, and user application layer (G2G, G2C, etc.) (Reddick, 2010: 45). The diversity of functional levels means that the e-government reform cannot be achieved without the centralized body inside the Singapore government that is managing all those different parts to get the fully functional e-government network.

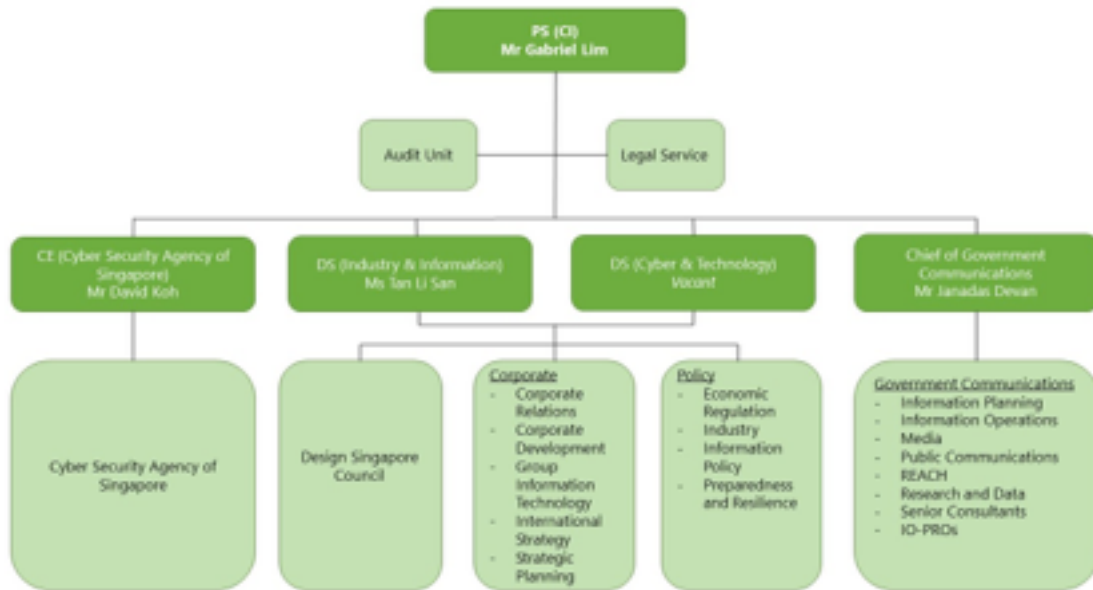
The executive branch of power in Singapore consists of the President and the Cabinet of Singapore headed by the Prime Minister - the head of the government. The Cabinet's Ministries are formed according to the public policy directions and national interests of the state. One of Ministry's name is the Ministry of Communication and Information (MCI) that is responsible for the ICT

policies implementation in Singapore. Even though it is stated on the main website that the mission of the MCI is to ‘connect our [Singaporean] people to community, government and opportunity’ (Ministry of Communication and Information), those words should be taken with a grain of salt, because none of these priorities can be traced in the structure of the organization, and the structure of the political structure always corresponds to the goals organization has. Therefore, by looking at the structure (Figure 4) of MCI, three main directions in which the Ministry is working can be seen: it manages cyber security, coordinates media and design sectors, oversees government’s information and public communication policies, as well as manages ICT policies in the country. Overall, MCI is the main actor in terms of e-government initiatives development, being only accountable to the Prime Minister.

Moreover, the goals of the Ministry aligns closely with the national interests of Singapore in the sphere of e-government that are outlined in a set of public policy plans: Intelligent Nation 2015, Intelligent Government 2010, and former e-Government Action Plans (2000 - 2003, 2003 - 2006), Civil Service Computerization Programme etc. All named plans circulate around the same ideology, and that is to create an environment with the ‘enviable synthesis of technology, infrastructure, enterprise and manpower’ (GovTech, 2016). The journey of the e-government started in Singapore in the early 80s, but during the last decade the process received a huge boost in terms of built infrastructure and knowledge during the past years, and now the process of ICT integration into public life is outlined in terms of practical planning for the span of 4-10 years with the main strategic goals etc., that makes this body the most important stakeholder in digitalization of the Singapore’s public service. Thus, our research should look more closely at the directions in which the Ministry is working.

The first (cyber security) direction is the field that has has an important safe-guarding role of the state’s security and stability of the e-government online environment. The central national agency that works under the supervision of the

Figure 4. Organizational structure of the Ministry of Communications and Information *Source: Ministry of Communications and Information Website*



Minister is the Cyber Security Agency of Singapore (CSA) that oversees cybersecurity strategy and operations. Having replaced the InfoComm Technology Security Authority, the body was created in 2015 to manage the cyber risks across interconnected networks on the national level like banking, telecommunications, transportation etc (Jacqueline, 2015).

The second direction entitles the public policy itself in the fields of ICT economic regulation, information policy, and public communications. There are three main agencies that execute those tasks - DesignSingapore Council, Government Technology Agency of Singapore (GovTech), and Infocomm Media Development Authority (IMDA). While the former is promoting an economic growth in Singapore that does not lie in the focus of our research, the other two hold our interest, as they are the center of e-government initiatives implementation and management in Singapore.

GovTech is tasked with ‘harnessing ICT and related engineering for public sector transformation by deploying a wide range of ICT solutions within the public sector, and developing the Smart Nation infrastructure and applications’ (GovTech). In other words, GovTech holds keys to the practical side

of building a network society in Singapore and is of a strategic importance in the executive network. By visiting section 'Programmes & Partnerships' at the GovTech's website, it becomes instantly evident how broad and advanced is the e-government development in Singapore, and how much the GovTech is important as a body - there are 43 active initiatives that are in progress or are already implemented in the spheres of G2C and G2B. By analyzing the content and main goals of the programs, I have found the following tendencies:

- programs are centered on digitalizing the identities of social actors in the public field - CorpPass (digital identity for businesses), SingPass (digital identity for citizens), GovTech CloudStore - online storage for governmental agencies, CitizenConnect - municipal centers providing people with no Internet connection to transact with the governmental services online etc. It is evident that Singaporean state objective is to cover the whole population with the ability to communicate with the government in virtual space, and this goal corresponds to the idea of individuals - social actors as containers of data in the societal network. Government massively uses code to datify the identities of the social actors, and this process confirms our idea that the power of control is overshadowing the disciplinary power, putting more effort at coordinating and directing the network society via code and computer.
- apart from building the service-oriented applications, Singapore also develops systems that are capable of supporting them from the technological point of view - the National Authentication Framework, Government IT Security Incident Response, Smart Nation Sensor Platform among others. To guarantee the security and stability of the created infrastructure, government takes measures in developing basis for the effective management of the society in the virtual realm. This trend is also very closely aligned with the previously discussed 'store and forward' principle of the network society, developing infrastructure and main back-end capacities to guarantee electronic services are capable to withstand the dynamic nature and size of the network.

Consequently, GovTech as an institution is the executive of the e-government reform in Singapore, its main coordinator and 'implementator'. The other Ministry - IMDA - is mainly concerned with the regulatory function. It oversees media and telecommunications sector, and also regulates data protection in Singapore via the Personal Data Protection Commission in order to 'ensure that public confidence in the private sector's use of personal data is safeguarded' (Infocomm Media Development Authority, 2016). In other words, IMDA, in comparison to the GovTech, is an agency that manages the health of the public sphere, overlooking all information channels that are active in the national discourse. This includes also taking actions against those activists and that content that goes against the established political regime. When I discussed in the first chapter different cases of opposition representatives and independent opinion leaders being persecuted, IMDA was one of the main political institutions that coordinated those actions. Moreover, in terms of the network society, IMDA plays crucial role in controlling the information streams in the society, bearing in mind the dominant role of state in the media control in Singapore. This is a very dangerous position for the person's privacy matters, because when government that implements the digitalization of the public service also has keys to the information management in the society, including all the content and data flowing on the surface of the public sphere, a normal citizen automatically gets under the surveillance umbrella of the authority.

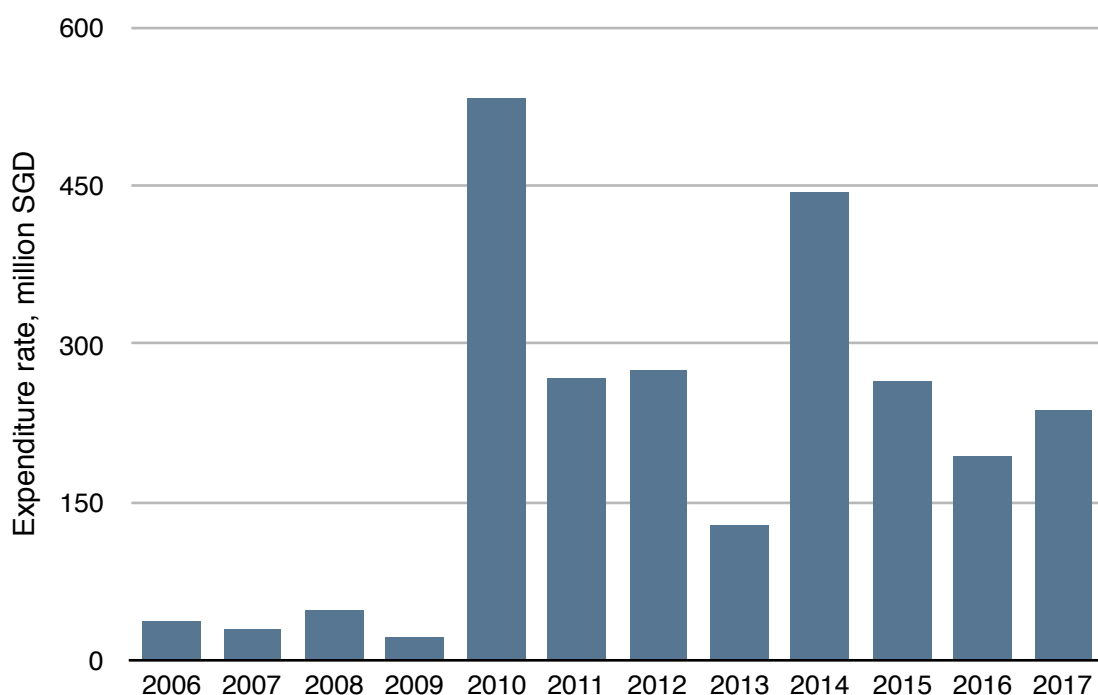
To sum up, e-government reform in Singapore is managed dominantly by the MCI. All four functional layers of the e-government are maintained and executed by the Ministry's agencies that are responsible for covering information security issues, ICT integration into the public service, and management of media and telecommunication. The structure is sophisticated, but relates to the goals the Ministry puts - to build a smart nation in Singapore that is highly digitalized, and where every possible public service operation could be done online. In the next chapter I am going to look at the evolution of the Ministry in terms of budget

expenses through the years on the e-government initiatives, so the scale of those digital changes in the society can be better understood.

## 6.2. E-Government in Singapore from the state's budget viewpoint

The budget expenses of the Ministry are very representative of the above-described process - just by looking at the data of expenditures by the Ministry in the last 10 years, evident progression of the amount of expenses the political institution has on e-government reform can be seen. If we look at the chart (Figure 5), there is a six times difference between Development expenditures in 2006 and in 2017, and the latter are equal to 237 million Singaporean dollars. However, 2017 is not the highest peak of development expenses of the Ministry. For example, the state's investments on projects development has received an astonishing 24 times increase in 2010 comparing to 2009 because of the development of the Next Generation National Broadband Network - a nationwide all-fibre broadband access of 1Gbps and more, offering high-speed Internet connection to app physical addresses across Singapore, including homes, schools, government buildings, businesses and hospitals (MyRepublic, 2015). Expenses of

Figure 5. Development Expenditures of the Ministry of Communications and Information, 2006 – 2017

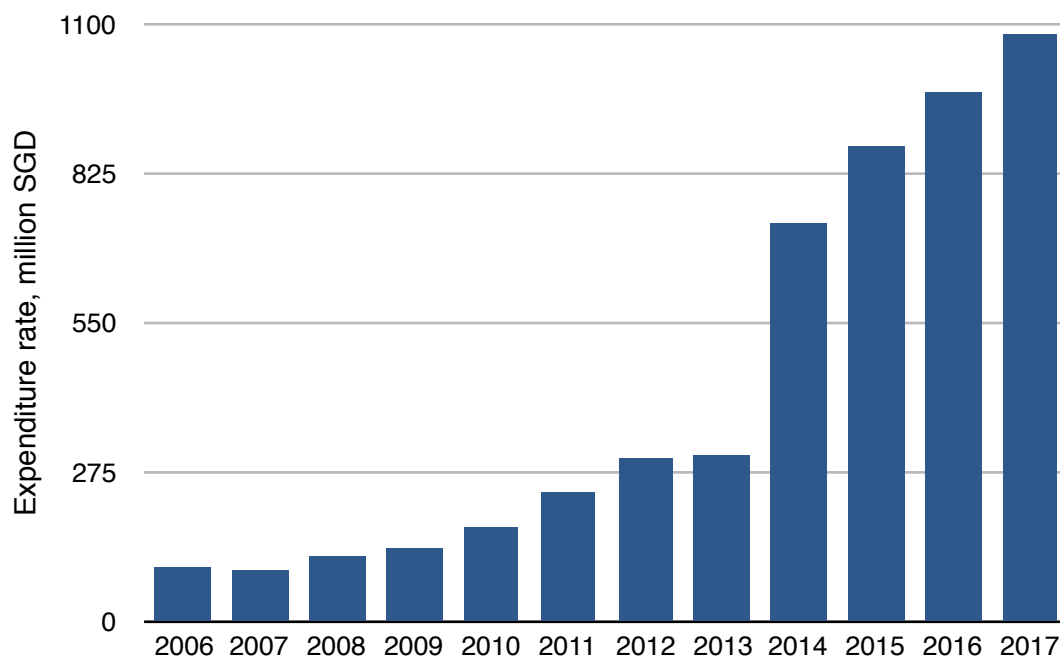




the period of 2010-2014 were mostly connected to the infrastructure implementation, and with new more efficient upgrade, a range of programs connected to the Intelligent Nation 2015 plans and some background operations (engineering preparations, databases establishment), that were mentioned in the previous chapter, have also started to be actively worked on.

However, fluctuating expenditures between 2010-2017 may be disturbing and the question may be risen: «Perhaps, Singaporean government is not so much engaged into the development of the e-government?» Logical expectation is to see the ideal rising trend of expenses on the projects development in the sphere of e-

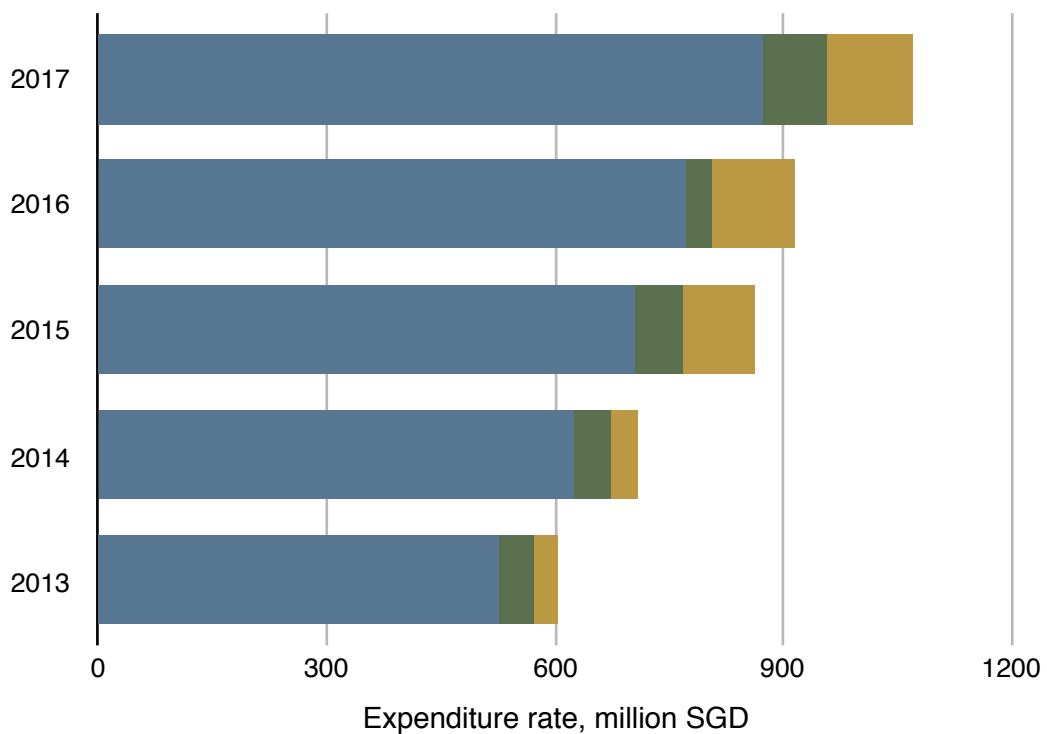
Figure 6. Operating Expenditures of the Ministry of Communications and Information, 2006 – 2017



government, not the strange ups and downs of the Ministry's expenditures. However, next chart of Operating Expenditures - working expenses of the organization (Figure 6) - sheds the light and shows us an expected progression: comparing to 2006, when the total operation expenses of the Departments that were connected to ICT development equaled \$101 million, the same type of expenses now for the independent Ministry, whose responsibility is only concerned with e-government management and development, now is are more

than 1 billion Singaporean dollars. Hence, operating expenditures have increased 10 times, and that shows how much the support machinery of the e-government management has increased during this timespan. Inside the Ministry's operating

Figure 7. Divided operating Expenditures of the Ministry of Communications and Information by purpose, 2013 - 2017



expenses are 1) manpower 2) grants, subventions and capital injections to organizations 3) other operating expenditures.

By breaking down the total expenses on the above-mentioned directions, the following picture will become evident (Figure 7): most of those expenses are going as subventions and injections to Statutory Boards (GovTech, IMDA) and other organizations that have some agreement with the Ministry concerning e-government implementation. The reason why this kind of expenditure exists in the first place is straight-forward: implementation of the technical side of the e-government reform may become either an unreal task for the governmental officials with no technical knowledge, or a genuine burden for the government at large to spend financial, time, human resources to implement digitalization steps

entirely from the beginning inside the bureaucratic setting of the governmental political structure. Therefore, the common way of integrating e-governmental functionality into the executive operations is to go through the process of technology integration from the outside. In other words, political bodies outsource the electronic functional component to private IT companies and expert organization, because it is not only easier for decision-makers to outsource operations than to change the political structure of the institutions in question (Castells & Cardozo, 2006: 161), but also is less expensive and more efficient in a short-term. Thus, political outsourcing is an IT system management mode for government departments where electronic software and services, including system construction, day-to-day operation and maintenance, are totally or partly executed by professional IT vendors (Tjoa, 2008: 1191). For example, the US state governments has spent around 11.4 billion dollars alone in 2012 on outsourcing, while the estimated market size for ICT services in UK costs around 16-18 billion dollars (Mutiangpili, 2010: 3).

In case of Singapore, those expanses are more modest, but if we take into account the size and population of the city-state, the numbers are significant. Returning to operation expenditures, grants & capital injections hold roughly 88-90% of the total expenses - meaning that for the management of the e-government programs Singaporean government outsources the technical side of such operations to other businesses and corporations. This conclusion supports the idea of the technocratic side of the e-government development where infrastructure and data operations cannot be build without the investment of expert manpower, knowledge and funds.

What those numbers mean for us in terms of our research? E-government in Singapore is not a fiction or a policy bubble, but a genuine process of the political evolution of the public service in Singapore to the point where it is the reality that has an impact on the life of every citizen. If the non-democratic political regime of Singapore and the changing nature of power are connected to

the rise of ICT in the political setting of the country, fast development of e-government may indeed be the first step towards the digital autocracies, if there are no barriers in the country to limit the surveillance procedures of the governmental institutions. Consequently, this research has reached the stage when our research question can be given answer to:

*Does the establishment of e-government by the state make citizens' privacy more vulnerable to the government's interference under the non-democratic regime, and, if so, to what extent?*

In the next chapter I will study what the establishment of e-government in Singapore means to a usual Singaporean citizen, and to what extent, if any at all, his or her privacy becomes more or less threatened because of this political reform advancement.

## 7 State of citizen's privacy in Singapore

### 7.1 Legal background of personal data protection in Singapore

Today to be considered a modern and developed country that is included in the international relations as a full-fledged political and economical actor, a state has to build a system of power that corresponds to the international norms and practices. Singapore, being one of the most developed financial hubs in the world and inheritor of the common law, is a country that is orientated towards the Western world of capitalist and democratic values, so the legal correspondence and health of the judicial system play a vital role in terms of the international reputation of the country.

However, the image and the general correspondence to the international norms does not suggest that the law itself does not hide the mechanisms that obliterate the rights and privacy of state's citizens. The ability of a citizen to protect his privacy from the government or other organization lies in the legal perspective - if there are check and balances in the political system, where judicial branch interprets and protects the law from the authoritative abuse, or if there are possibilities for a person to legally defend his right for privacy, then even with the most advanced e-government and surveillance mechanisms political elites have their hand tight in terms of the freedom of what they can actually do with all technologies in hand. But what about the rule of law in the non-democratic setting? For the sake of a proper political analysis of the privacy matters, I am going to look in this chapter at the state of the legal system in Singapore in terms of personal data management and the possibilities government has to gather and use private data against its owners.

Apart from the Constitution of the Republic of Singapore, there also a number of ordinary statutes called Acts that are enacted by the Parliament of Singapore which complement the supreme law of the country, regulating a variety of spheres, including those spheres that are connected with the ICT management. The first document is a Computer Misuse and Cybersecurity Act (2007), that was originally enacted in 1993. Basically, it describes provisions for securing computer material against unauthorized access or modification from the third parties, and authorizing measures to ensure cybersecurity in the country. Listing a diverse types of offenses in terms of unauthorized access to private computer data, it does a very vague description of the actor that is forbidden to conduct such offense by calling actor a 'person', never actually defining legally whether 'person' also covers governmental institutions, apart from natural and juridical persons. This doubt becomes more evident when the document tries to explain difference between a person and the Minister or The Commissioner of Police, who represents the state in the matter of cybersecurity and acts as its executive mechanism. In the section 'Cybersecurity measures and requirements' it is stated that Minister for the purpose of 'preventing, detecting, or countering' any kind threat to national security or essential services (communications infrastructure, banking and finance, shipping etc.) of Singapore may gain an almost almighty range of possibilities to acquire without limitation all personal data of the convicted person, or a person under suspicion (Computer Misuse and Cybersecurity Act, 2007: 15a).

In other words, representative of the political institution has an unrestricted power of getting the information of a private nature, if there is a suspicion of an unauthorized or dangerous activity. That leads us to the question - what are the prescriptions to control what is considered a threat? Document does not give us such answer. Instead, the Act underscores that the Commissioner of Police, acting under the supervision of the Minister of the specific Department, is responsible for collecting data and prescribing the offences that may be

compounded (Computer Misuse and Cybersecurity Act, 2007: 12a), whereas the Court plays only the role of imposing the punishment and hearing the cases without mentioning any judicial monitoring of the process of data collection. Moreover, the Minister of Home Affairs can give direct permission to collect private data from any device, even in real time, when it is 'necessary for the purposes of preventing, detecting or countering any threat to the national security, essential services or defense of Singapore or foreign relations of Singapore' (Computer Misuse and Cybersecurity Act, 2007: 12).

The question of the role judicial branch plays in all this matter brings us to the Criminal Procedure Code (2012) in the section of regulating the situation when governmental representative is able to use its power to obtain private information. In the legal document it is not stated in any way that a judicial authorization is needed for the Executive to obtain the private data of the person. In other words, any person can be monitored for the sake of national security, and no legal boundaries for the data that could be investigated exist. In this situation, person would have no chance to prove that state institutions are monitoring him illegally, because the monitoring itself is a choice the Executive could voluntarily make. Hence, judicial power acts as the state's political instrument, rather than an independent body in the political structure. This statement is further supported by the Constitution of Singapore, because President is solely responsible for appointing The Chief Justice, the Judges of Appeal and the Judges of the High Court (Constitution of Singapore, 1985: part 8), so it means that the judicial system is not able to work as a fully independent institution in the state's political structure, because the Executive is solely responsible for appointing main judges of the Court, giving way to the domination of interest of powerholders over the postulates of the human rights and justice.

Another question is the criminal punishment for posing cyber danger for the state's security that is mentioned in the Act. What cases are included in the list of dangers for the national security of Singapore, especially if the perceived

dangers that are managed and reacted upon by the corresponding political bodies are taken into account? Lack of any legal certainty brings into shape the suggestion that the Executive may use its power of surveillance and enforcement any time it wants to, without any prescriptions or judicial permission.

Another document that holds our interest is Personal Data Protection Act published in 2012. The Act, by defining personal data as data about an individual who can be identified from that data other information that the actor has or is likely to have access to, outlines its main purpose: to govern the collection, use and disclosure of such information according to the rights of individuals and the need of organizations (individual, company or association resided in Singapore) to have access to this data according to the expectations and reasonability of such action.

However, when the Act is analyzed more closely, its purpose may become not so liberal. Firstly, Act states that IMDA - the Statutory Board of the MCI - has been formed as the Personal Data Protection Commission, functions of which have both educational and instrumental sides. But, following the statement of the Section 58 of the Telecommunication Act, document argues straightforwardly that the Minister on the grounds of public interest and national security can give directions to the executive institution like IMDA or to the telecommunication provider concerning the usage and taking control of telecommunication system and equipment, as well as stopping, delaying and censoring of messages in public sphere as deemed necessary by the Minister (Privacy International, 2015: 5). Consequently, the will of the Act whose purpose is to protect personal data is at the same time the will of the executive whose main concern is political elites interests, that in the non-democratic setting in Singapore exist in contrast to the liberal approach of private data protection.

Secondly, the Act, following the logic of the previous documents, also describes when the collection of personal data may be conducted without the



consent or awareness of the individual. There a couple of statements that should be pointed out in terms of our research:

- *the collection is necessary for any purpose that is clearly in the interest of the individual.* What is the interest of the individual? The document does not point that out, and so by collecting person's information about his movement, emails, family, history of payments, the responsible governmental actor may declare that he is doing it for the person's interests that were defined by the actor himself.
- *the collection is necessary in the national interest.* This statement supports our previous points of the ambiguity of such concepts as national interests and threats to the state. The main purpose of the executive body lies in the fact that it implements the policies for the sake of and protects the national interests of the state. Consequently, if it is responsible for the state's interests, executive bodies have the legal background to collect private data to serve the purpose they exist in the first place. It is an eternal circle that is centered around the executive body, rather than around society whose representatives want to be included in the process of political governance.
- In the Third Schedule of the Act it is stated that all the terms of the collection of the data should not apply unless it is «impracticable for the organization to seek the consent of the individual for the use» (Personal Data Protection Act, 2012). Putting into context, it becomes evident that organization should not seek the consent of the individual, if it finds it to be irrelevant. Indeed, it is logical from the point of the organization that collects data not to ask for consent. So, if organization is a political body with the omnipotent power of data collection, should it also not seek consent because of the impracticality of such action?

All these statements highlight the idea that the law exists for those who govern, but not for those that are governed. In the end, the final word and the final right will have the state, not a common citizen. This situation could also be highlighted by the fact that Singapore has not ratified the International Covenant

on Civil and Political Rights (ICCPR) that was adopted and put into force by the General Assembly of the United Nations back in 1976. Document covers the civic rights of individuals, so countries that have signed the document are responsible to act according to its statements in order of not creating a precedent of non-compliance, both domestically and internationally. As mentioned by Privacy International, Article 17 of the ICCPR provides that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.” (Privacy International, 2015: 5). So, if country does not agree to follow such norm, significant concerns are rising in the legal framework that regulates interception of communication, as well as judicial authorization and democratic oversight in Singapore (Privacy International, 2015: 11).

Only a bunch of countries like Malaysia, Qatar, Saudi Arabia, Myanmar have also not signed this multilateral treaty, and those are also countries that are not examples of the democratic regimes. Following the above-described legal background of the privacy regulation of Singapore, it becomes understandable why the ICCPR was not signed - Executive of Singapore has the possibility and legal authority to collect any type of private of data it wants, without restrictions and preliminary regulations - an example of a very undemocratic practice of managing privacy matters of country’s citizens.

## 7.2. Practice of using surveillance technologies by the state

Apart from the legal factors, there are also evidences that Singaporean government direct its policy regarding private data collection in a harmful way for a common citizen. Firstly, on the institutional level, there are examples of how Singaporean government has used the services of foreign agencies that specialize in cybersecurity and network management, especially in the field of monitoring Internet traffic and getting possession of the user’s data while he is online. For

example, Citizen Lab has conducted an investigation of the Blue Coat Systems Inc. devices that propose ways to filter, censor and conduct surveillance of the targets by the owners of such devices (Citizen Lab, 2013). What is interesting is that the customers of the corporation were mostly found to be non-democratic countries like Russia, China, Venezuela, Qatar, and, eventually, Singapore, that integrated Blue Coat Systems technologies on public or government networks. Singaporean government was found to be using technology named PacketShaper - real-time network intelligence service that is able to filter application traffic by content category. Keeping in mind the existing law enforcement offers broad power for the government to access data and encrypted material when approaching private information of a usual citizen (Privacy International, 2015), government has found the right instruments to enforce this surveillance power. The research found that the PacketShaper services in Singapore were applied by the political institutions to filter content that has divisive racial, political, or religious side that could be harmful to the national stability of the country (Citizen Lab, 2013), which means also 'harmful' messages for the monopoly of power in the public sphere that were discussed in the first chapter.

But Blue Coat devices are only a tip of the iceberg. There are a number of services that have been found to be used by the government of Singapore for the personal data collection. One of them is FinFisher - remote intrusion and surveillance software that is able to capture information from an infected device (Citizen Lab, 2013). According to WikiLeaks, the customer of the FinFisher technologies in Singapore was PCS Security Pte Ltd corporation that delivers 'value-added systems in Homeland Security and InfoComm Security' and has spent almost 4 million euros on the licenses for the malware products (Online Citizen, 2014) - meaning that at some point of a time Ministry of Home Affairs or MCI had access to this technology in return for grants and investments that were mentioned when describing budget expenditures of the executive institutions of Singapore.

Another one is Hacking Team - an Italian company that sells surveillance and intrusion tools to government and law enforcement agencies in the world, enabling them access private data on target's computers - has been found to have an active contract among other countries with IMDA (Online Citizen, 2015), and Singaporean government has paid almost 1,5 million USD for the company's services, taking a top 10 position in the list of customers (Berthelsen, 2015). Being connected to a number of repressive regimes in the world like Bahrain, Uzbekistan, Ethiopia, Sudan (Hen, 2015), the inclusion of Singapore is not a coincidence, but rather an implication about the way government is shaping its policy towards privacy nationwide.

Lastly, the other one is Kai Square cyber surveillance startup that has been bought by the SingTel - Singapore's largest telecommunications operator - to 'better serve customer needs' (Singtel, 2014). Kai Square offers a technology that is able to identify a person by scanning his or her facial features through a camera, and analyze accumulated patterns of the behavior of the same targets across a specific amount of time (Lee, 2014). If to put everything mentioned above together, it becomes possible for the investigator or an executive body to get not only private information, but also person's location, phone calls, places he or she visits, video tape of the person in a public place etc. just by analyzing accumulated data gathered by smart devices and services, and that is done directly or indirectly by governmental institutions on a national level.

On the macro level, all the diversity of such apps are used systematically in the scope of the governmental programs whose aims are to predict, manage, and eliminate the dangers to the national security of the state. One of those that is publicly known is Risk Assessment and Horizon Scanning (RAHZ) that is used to plan procurement cycles and budgets, study housing markets, or even getting the idea of 'nation's mood' about government social programs or potential civil unrest by analyzing Facebook posts, Twitter messages etc (Harris, 2014). Hence, the main concern of the Singaporean government is not to take hold of the random

citizen's private data, just for the sake for it, but rather to put this data into the context of managing the country by understanding the population that is governed and predicting the possible directions of the public policy.

Thus, Singapore has established a wide and legal framework of surveillance mechanisms that work as an asset for the powerholders to control citizens behavior, mood, expectation by applying desired or expected public policies and measures that strengthen the established status quo. This situation closely corresponds to the society of control, where powerholder does not need to use punishment or any direct action to practice its power. Instead, by gathering all kind of data 'legally' and by integrating public services into the digital context, Singaporean state creates the society of individuals that are encoded and influenced by code and - universal instrument of power in the 21st century.

### 7.3. SingPass - an instrument of the power of control

Among the myriad of political initiatives in the sphere of e-government there is one initiative that connects all the dots between the ideas that were studied in this thesis - e-government in the non-democratic settings and citizens as containers of data that lose their hold on privacy. The name of the e-government initiative is Singapore Personal Access (SingPass) - a unique digital identity that serves as a gateway to «hundreds of e-services provided by more than 60 government agencies» in Singapore (Singapore Personal Access, 2013). Having started in 2003, currently SingPass has close to 3.3 million users in Singapore (Ministry of Communications and Information, 2017), whereas the total number of citizens and permanent residents of the country in 2016 was 3.9 million people (Department of Statistics Singapore, 2016). Thus, 84% of Singaporean population has a SingPass in their private possession. However, by bringing comfort to citizens as users of digital technologies, this innovation also brings this user into

the bright light of the state's control, empowering the latter, and taking power from the former.

The process of receiving SingPass is easy. By entering the website of the SingPass - [www.singpass.gov.sg](http://www.singpass.gov.sg) - the first visual effect that strikes you is the amount of red color, which is the dominant color on the Singaporean flag. In the right bottom of the screen the user will see a chatbot with a nice, young, friendly, and smiling face of a Singaporean woman named Jamie - a standard bot for the e-governmental services in Singapore. Being a new user, I am interested how can I sign up and what do I need for that. Going to the 'Register Now' link, the user is informed that the registration takes only three minutes with a hassle-free process of getting the actual ID. In order of not reading the other instructions, I can opt for watching a two and a half minutes introduction to what SingPass is and in what ways I can get it. Then I just follow simple steps to register to receive digital identity that will make my life much more easier as a citizen.

The above description may have sounded like a marketing analysis rather than a political investigation, but it is not - SingPass plays an important role in the e-government implementation in Singapore, and the way it is proposed to the citizen makes a difference for the success of such procedure. Even though the choice of getting digital ID is by default voluntary, in reality without the SingPass Singaporean citizen is deprived of the ability of getting any online public services from the governmental institutions at all. From the perspective of a citizen, the cost of getting SingPass on the surface is much lower than the cost of losing the comfortable and way of paying taxes, getting medical reports, registering personal commodities etc. Serving both as a tool of transacting with the government and a tool of authenticating citizens, SingPass is an example of a healthy e-governmental initiative that brings citizens closer to the modern public services through the ICT channels.

However, behind this comfortable opportunity a bigger danger is hidden. For example, to receive SingPass, apart from passport, user should also put down

his mobile number, email address, and a home address. Meanwhile, pre-paid SIM card regulatory regime exists in the country that undermines the possibility for the citizen to communicate anonymously. According to the Privacy International, such state of affairs facilitates the establishment of extensive databases of user information, enabling location-tracking, and simplifying communications surveillance and data interception (Privacy International, 2015: 6). Therefore, such innovation as SingPass in reality serves as an instrument of identification of the citizen digitally. Hence, all information about his transaction with the government, his private data, as well information about his movement is connected to one simple ID that is stored in the databases owned by the governmental institutions.

Example of such e-governmental service in the end of our thesis was not random - only after our research went a long road of understanding that Singaporean regime is non-democratic and puts the position of powerholders above other interest groups and civil society representatives, after it was presented what role e-government plays in the establishment of the new form of power realized via code and digital networks - power of control, after I have been exposed as a researcher to how broad in scope e-government reform is in Singapore, and, lastly, when it became obvious how privacy matters of Singaporean citizens are overshadowed by legal dictatorship of the executives and diverse mechanisms of retrieving personal data of citizens, SingPass does not longer seem to be solely an effective instrument of better governance and higher inclusiveness of country's citizens. In the context of Singapore, the main priority of SingPass is to connect people to the digital network, where government would have the ability to propose him comfortably not only the public service he needs, but also receive data about the person this service is supplied to. It is an effective solution for the country that wants to have better information for decision-making, but a rather harmful state of affairs for a common citizen who has no guarantee that his personal information is not in the possession of the state's institutions.

## 8 Conclusion

The aim of this thesis was to investigate whether introduction and establishment of e-government in the non-democratic regime poses a higher danger to the security of citizens' privacy. The main reason behind that was the problem of e-government in terms of a political reform: by offering innovative technology that drastically changes the way public service is provided to the citizens and organizations as end users, it does not guarantee that it will be used against the latter for the sake of the ruling elites' interests in the political regime with autocratic tendencies.

To answer this question, I undertook a case study research with Singapore as my only case of the non-democratic regime that has successfully established the e-government on a massive scale. To understand the prerogatives of the concepts I was looking at, I divided the research question into independent (political regime) and dependent (e-government reform, citizen's privacy) variables to understand how they can be defined and in what way they relate to each other.

The findings suggest that the establishment of e-government in the non-democratic regime plays an important role in the evolution of political power of a state from the disciplinary power to the power of control that is realized via code and computer. A strong correlation was found between the political regime, from the one hand, and e-government initiatives implementation and citizens' privacy, from the other. With more effective and result-oriented political management that state receives as an outcome of the e-government introduction, ruling elites also obtain a mechanism of unrestricted data gathering that in the non-democratic setting strongly empowers the public administration's hold on power. Singapore case has shown that with the state that is actively pushing the development of ICT infrastructure and integration of the expert knowledge into the political system,



government's surveillance as a process of monitoring information flows poses a serious danger to the privacy and safety of citizens that are actively involved in using and receiving digital public services. If they are identified as dangerous elements in the political system by being opposition leaders or civic society activists, government has an easy access to their personal data that can help powerholders to take a better informed and more effective disciplinary action. This denotes the power dynamics where non-democratic governments become more efficient in managing and controlling society, and where the citizen's right to privacy in the digital environment is neglected.

## 8.1. Further research

The results are encouraging, as they show that consequences of the establishment of the e-government has a different tone in the non-democratic regime, serving first and foremost the interests of the powerholders in securing the dominance of their political power in the country. However, this research only shed some light on one of the cases of the non-democratic country where e-government was successfully established. One of the suggestions for further research would be to investigate more similar cases to understand whether there are common patterns in the way e-government is developed and used in the autocratic regime.

Moreover, a closer study should be conducted on the matter of e-government establishment in the democratic country from the perspective of the society of control and surveillance mechanisms that the respected government uses in its daily operations. It is possible that the same surveillance and political control tendencies exist in the democratic countries where e-government is being developed, but its consequences are less noticeable and evident. Thus, with broader research, a more coherent and universal view on the problem of the e-government development will be constructed.

## References

- Allmer, T. (2015). *Critical Theory and Social Media: Between. Emancipation and Commodification*. New York, NY: Routledge. 214 p.
- Alois, P. (2014). Through Liquid Democracy to Sustainable Non-Bureaucratic Government. *Ejournal Of Edemocracy & Open Government*, Vol 6, Iss 2, Pp 216-230 (2014), (2), 216.
- Amnesty International (2017). Singapore: Authorities given broad new powers to police protests. [Electronic Resource] Retrieved from <https://www.amnesty.org/en/latest/news/2017/04/singapore-authorities-given-broad-new-powers-to-police-protests/> (Accessed on Aug 12, 2017)
- Åström, J., Karlsson, M., Linde, J., & Pirannejad, A. (2012). Understanding the rise of e-participation in non-democracies: Domestic and international factors. *Government Information Quarterly*, 29142-150.
- Baller et al. (2016). *The Global Information Technology Report 2016: Innovating in the Digital Economy*. Geneva: .World Economic Reform and INSEAD. 62 p.
- Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity: The International Journal Of Government & Democracy In The Information Age*, 10(1/2), 65-78.
- Baquero-Hernandez, R. (2012). Characterizing E-Government in China. *Desafios*, 24(2), 233-257.
- BBC News (2013). Rare mass rally over Singapore immigration plans. [Electronic Resource] Retrieved from <http://www.bbc.com/news/world-asia-21485729>
- Beniger, J. R. (1986). *The control revolution : technological and economic origins of the information society*. Cambridge, Mass. : Harvard Univ. Press, 1986.
- Bell, D. (1973). *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York, NY.

- Berthelsen, J. (2015). How Asia's Governments Spy on Their Citizens. Asia Sentinel [Electronic resource] Retrieved from <http://www.asiasentinel.com/society/asia-governments-spy-citizens/> (Accessed on Aug 12, 2017)
- Bennett, Andrew & Jeffrey T. Checkel (2014) Process tracing: from philosophical roots to best practices, in Bennett, Andrew; & Jeffrey T. Checkel, eds, Process Tracing: from Metaphor to Analytic Tool. Cambridge: Cambridge University Press (3–37).
- Bozbeyoğlu, A. Ç. (2011). Citizenship rights in a surveillance society: The case of the electronic ID card in Turkey. *Surveillance & Society*, 9(1/2), 65-79.
- Castells, M., & Cardoso, G. (2006). *The network society : from knowledge to policy*. Washington, D.C. : Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University cop. 2006.
- Castells, M. (2010). *The rise of the network society*. Chichester, West Sussex ; Malden, MA : Wiley-Blackwell, 2010.
- Citizen Lab (2013). Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. [Electronic resource] Retrieved from <https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/> (Accessed on Aug 12, 2017)
- Citizen Lab (2013). You only click twice: FinFisher's Global Proliferation [Electronic resource] Retrieved from <https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/> (Accessed on Aug 12, 2017)
- Chartlene (2015). This Is What Happens If You Don't Vote In Singapore. Vulcan Post. [Electronic Resource]: Retrieved from <https://vulcanpost.com/364781/what-happens-when-you-dont-vote/> (Accessed on 12 Aug 2017)
- Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, 164-181.
- Collier, D. (2011). Understanding Process Tracing. *PS: Political Science and Politics*, 44, No. 4: 823-830 pp.
- Computer Misuse and Cybersecurity Act (2007 Rev. Ed.)

- Constitution of the Republic of Singapore (1985 Rev. Ed.)
- Criminal Procedure Code (2012 Rev. Ed.)
- Dahl, R. A. (1971). *Polyarchy: participation and opposition*. New Haven, Conn.: Yale University Press, cop. 1971.
- Deleuze, G. (1992). *Postscript on the Societies of Control*. MIT Press, Cambridge, MA, 3-7.
- Department of Statistics Singapore (2016) Latest Data. [Electronic resource] Retrieved from <http://www.singstat.gov.sg/statistics/latest-data#16> (Accessed on Aug 12, 2017)
- Dijk, J. v. (2012). *The network society*. Thousand Oaks, CA : Sage Publications, 2012.
- Eisenhardt, Kathleen M., 1989. "Building Theories from Case Study Research". *The Academy of Management Review*, pp. vol. 14, no. 4, pp. 532-550.
- Foucault, M. (1978). *The History of Sexuality*. Paris: Editions Gallimard.
- Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*
- Freedom House (2006). *Freedom in the World 2006: Singapore*. Washington, D.C.: Freedom House.
- Freedom House (2007). *Freedom in the World 2007: Singapore*. Washington, D.C.: Freedom House.
- Freedom House (2008). *Freedom in the World 2008: Singapore*. Washington, D.C.: Freedom House.
- Freedom House (2009). *Freedom in the World 2009: Singapore*. Washington, D.C.: Freedom House.
- Freedom House (2010). *Freedom in the World 2010: Singapore*. Washington, D.C.: Freedom House.
- Freedom House (2011). *Freedom in the World 2011: Singapore*. Washington, D.C.: Freedom House.

- Freedom House (2012). *Freedom in the World 2012*: Singapore. Washington, D.C.: Freedom House.
- Freedom House (2013). *Freedom in the World 2013*: Singapore. Washington, D.C.: Freedom House.
- Freedom House (2014). *Freedom in the World 2014*: Singapore. Washington, D.C.: Freedom House.
- Freedom House (2015). *Freedom in the World 2015*; Singapore. Washington, D.C.: Freedom House.
- Freedom House (2016). *Freedom in the World 2016*: Singapore. Washington, D.C.: Freedom House.
- Freeman, R. E. (2010). *Strategic management: a stakeholder approach*. Cambridge: Cambridge University Press, 2010.
- Fukuyama, Francis (1989). "The End of History?". *The National Interest* (16): 3–18.
- George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge, Mass. ; London : MIT, cop. 2005.
- Goh, C. (2015). The secret behind Singapore's data center success. *Enterprise Innovation*. [Electronic Resource] Retrieved from <https://www.enterpriseinnovation.net/article/secret-behind-singapores-data-center-success-1926059439> (Accessed on Aug 12, 2017)
- Government Technology Agency of Singapore (2017). [Electronic resource] Retrieved from <https://www.tech.gov.sg> (Accessed on Aug 12, 2017)
- Grönlund, Å. (2002). Introduction. In Å Grönlund (Ed), *Electronic Government: Design, Applications and Management* (pp. 1 – 22), London: Idea Group Publishing
- Harris, S. (2014). The Social Laborator. *Foreign Policy*. [Electronic resource] Retrieved from <http://foreignpolicy.com/2014/07/29/the-social-laboratory/> (Accessed on Aug 12, 2017)

- Hern, A. (2015). Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. Guardian. [Electronic Resource] Retrieved from <https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim> (Accessed on Aug 12, 2017)
- Huxley, A. (2007). Brave new world. Toronto: Vintage Canada.
- Infocomm Media Development Authority (2016). Personal Data Protection [Electronic Resource] Retrieved from <https://www.imda.gov.sg/community/consumer-education/personal-data-protection> (Accessed on Aug 12, 2017)
- Infocomm Media Development Authority (2016). Smart Nation Big on Big Data. [Electronic Resource] Retrieved from <https://www.imda.gov.sg/infocomm-and-media-news/buzz-central/2016/6/smart-nation-big-on-big-data> (Accessed on Aug 12, 2017)
- Jacqueline, Ng. (2015). New Cyber Security Agency set to lead the way in combating emerging cyber threats. [Electronic resource] Retrieved from [https://www.hometeam.sg/article.aspx?news\\_sid=201501282Uakllrzrg7S](https://www.hometeam.sg/article.aspx?news_sid=201501282Uakllrzrg7S) (Accessed on Aug 12, 2017)
- Johnson, E. & Kolko, B. (2010). E-government and transparency in authoritarian regimes: Comparison of national- and city-level e-government web sites in Central Asia. *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, (3), 15–48.
- Mutiangpili, J. (2010). Government Sector Outsourcing: Transforming Public Service with Outsourced IT Services, NY: Tholons.
- Lee, C., Chang, K., & Berry, F. S. (2011). Testing the Development and Diffusion of E-Government and E-Democracy: A Global Perspective. *Public Administration Review*, 71(3), 444-454. doi:10.1111/j.1540-6210.2011.02228.x
- Lee, T. (2014). Foxconn, SingTel invest \$3.2M in smart video surveillance by Singapore startup. TechInAsia [Electronic resource] Retrieved from <https://>

[www.techinasia.com/singapore-startup-32m-foxconn-singtel-cctvs-smart](http://www.techinasia.com/singapore-startup-32m-foxconn-singtel-cctvs-smart)

(Accessed on Aug 12, 2017)

Kardan, A. & Sadeghiani, A. (2011). Is e-government a way to e-democracy? *Government Information Quarterly*, 28(4), 466–473.

Kirsten, H. (2013). Singapore: Regulation or censorship? Journalists and bloggers criticise country's new media law. Al Jazeera [Electronic Resource] Retrieved from <http://stream.aljazeera.com/story/201305302216-0022797> (Accessed on Aug 12, 2017)

Kneuer, M., & Harnisch, S. (2016). Diffusion of e-government and e-participation in Democracies and Autocracies. *Global Policy*, 7(4), 548.

Kollár, V., Gasperová, J., & Poliak, P. (2016). View of Electronic Participation and its Application in the Present Conditions of Democracy. *Studia Commercialia Bratislavensia*, Vol 9, Iss 33, Pp 58-64 (2016), (33), 58. doi:10.1515/stcb-2016-0006

Kok, L. (2015). GE2015: Voter turnout at 93.56 per cent, improves slightly from 2011 record low. *The Straits Times*. Electronic Resource: <https://web.archive.org/web/20150913025400/http://www.straitstimes.com/politics/ge2015-voter-turnout-at-9356-per-cent-improves-slightly-from-2011-record-low> (Accessed on Aug 12, 2017)

Kukovic, S., & Brezovsek, M. (2015). E-Democracy and E-Participation in Slovenian Local Self-Government. *Croatian And Comparative Public Administration*, (2), 451.

Lyon, David and Colin J. Bennett (2008). Playing the ID Card: Understanding the Significance of Identity Card Systems. In *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, edited by Colin J. Bennett and David Lyon, 3-20, New York: Routledge.

Maerz, S. F. (2016). The electronic face of authoritarianism: E-government as a tool for gaining legitimacy in competitive and non-competitive regimes. *Government Information Quarterly*, 33(7), 727-735.

Makarava, Y. (2011). FRIENDS WITHOUT BENEFITS: Critical Assessment of the Relationship between E-governance and Democracy. *Master of Arts Thesis*, Mid Sweden University. 79 p.

Ministry of Communications and Information (2017). TODAY Online - SingPass introduces 2-step verification. [Electronic Resource] Retrieved from <https://www.gov.sg/news/content/singpass-introduces-2step-verification> (Accessed on Aug 12, 2017)

MyRepublic (2015). What is the Singapore Next Generation Nationwide Broadband Network? [Electronic Resource] Retrieved from <https://support.myrepublic.com.sg/hc/en-us/articles/202898734-What-is-the-Singapore-Next-Generation-Nationwide-Broadband-Network-> (Accessed on Aug 12, 2017)

Online Citizen (2017). Activists protest on MRT to show solidarity for ISA detainees [Electronic Resource] Retrieved from <https://www.theonlinecitizen.com/2017/06/04/activists-protest-on-mrt-to-show-solidarity-for-isa-detainees/> (Accessed on Aug 12, 2017)

Online Citizen (2014). “Weaponised German surveillance malware” purchased by S’pore company: Wikileaks [Electronic resource] Retrieved from <https://www.theonlinecitizen.com/2014/09/15/weaponised-german-surveillance-malware-purchased-by-spore-company-wikileaks/> (Accessed on Aug 12, 2017)

Online Citizen (2015). Singapore’s IDA reported to have dealings with spyware firm [Electronic resource] Retrieved from <https://www.theonlinecitizen.com/2015/07/07/singapores-ida-reported-to-have-dealings-with-spyware-firm/> (Accessed on Aug 12, 2017)

Ow Yeong Wai Kit (2016). The rise of S’pore’s civil society. Today Online [Electronic resource] Retrieved from <http://www.todayonline.com/singapore/rise-spores-civil-society> (Accessed on Aug 12, 2017)

Personal Data Protection Act (2012 Rev. Ed.)

Privacy International (2015). The Right to Privacy in Singapore: Stakeholder Report Universal Periodic Review 24th Session - Singapore. 10 p.



- Rahman, H. (2010). Local e-government management: A wider window of e-governance. *In Handbook of research on e-government readiness for information and service exchange: Utilizing progressive information communication technologies (pp. 295-323)*. Hershey, PA: Information Science Reference
- Reddick, C. G. (2010). *Comparative E-Government*. [Elektronisk resurs]. New York, NY : Springer New York, 2010.
- Reporters Without Borders (2016). *Qatar*. [Electronic Resource] Retrieved from <https://rsf.org/en/qatar> (Accessed on Aug 12, 2017)
- Reporters Without Borders (2017). *World Press Freedom Index*. [Electronic Resource]: Retrieved from <https://rsf.org/en/ranking> (Accessed on Aug 12, 2017)
- Robins, F., et Webster., F. (1999). *Times of the Techno-Culture: From the Information Society to the Virtual Life*, New York, Routledge
- Sagar, M. (2015). Singapore champions social media: Singapore government uses social media to engage with citizens daily. OpenGov. [Electronic Resource] Retrieved from <http://www.opengovasia.com/blogs/5-opengov-expert-opinion/post/6618-singapore-champions-social-media> (Accessed on Aug 12, 2017)
- Shroff, M., & Fordham, A. (2010). "Do you know who I am?" Exploring identity and privacy. *Information Polity: The International Journal Of Government & Democracy In The Information Age*, 15(4), 299-307. doi:10.3233/IP20100162
- SingTel (2014). Singtel launches cloud-based video analytics solution for the retail industry. [Electronic resource] Retrieved from <https://www.singtel.com/about-us/news-releases/singtel-launches-cloud-based-video-analytics-solution-retail-industry> (Accessed on Aug 12, 2017)
- Singapore Budget 2006: Budget Book Revenue and Expenditure (2006)
- Singapore Budget 2007: Budget Book Revenue and Expenditure (2007)
- Singapore Budget 2008: Budget Book Revenue and Expenditure (2008)
- Singapore Budget 2009: Budget Book Revenue and Expenditure (2009)
- Singapore Budget 2010: Budget Book Revenue and Expenditure (2010)
- Singapore Budget 2011: Budget Book Revenue and Expenditure (2011)

- Singapore Budget 2012: Budget Book Revenue and Expenditure (2012)
- Singapore Budget 2013: Budget Book Revenue and Expenditure (2013)
- Singapore Budget 2014: Budget Book Revenue and Expenditure (2014)
- Singapore Budget 2015: Budget Book Revenue and Expenditure (2015)
- Singapore Budget 2016: Budget Book Revenue and Expenditure (2016)
- Singapore Elections Department (2017). Who can vote? [Electronic Resource] Retrieved from <http://www.eld.gov.sg/voters.html> (Accessed on 12 Aug, 2017)
- Singapore Personal Access (2015). About Us. [Electronic Resource] Retrieved from <https://www.singpass.gov.sg/singpass/common/about> (Accessed on Aug 12, 2017)
- Southeast Asian Press Alliance (2013). Shaking off the fear of state censorship in Singapore - youth hold out hope. IFEX 25. [Electronic Resource] Retrieved from [https://www.ifex.org/singapore/2013/09/25/state\\_censorship/](https://www.ifex.org/singapore/2013/09/25/state_censorship/) (Accessed on Aug 12, 2017)
- Stanley, J., & Steinhardt, B. (2014). *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*. New York: American Civil Liberties Union
- Mossberger, Karen, Tolbert, Caroline J. and Ramona S. McNeal. 2008. *Digital Citizenship: The Internet, Society and Participation*. Cambridge, Massachusetts and London: The Massachusetts Institute of Technology Press.
- Stake, Robert E. (1995). *The Art of Case Study Research*. California: SAGE Publications.
- Stier, S. (2015). Political determinants of e-government performance revisited: Comparing democracies and autocracies. *Government Information Quarterly*, 32270-278.
- Taylor, N. (2002). State Surveillance and the Right to Privacy. *Surveillance & Society* (1):66-85
- Tharoor, I. (2016). The man who declared the 'end of history' fears for democracy's future, *Washington Post*, [Electronic Resource]: Retrieved from <https://www.washingtonpost.com/news/worldviews/wp/2017/02/09/the-man-who->

[declared-the-end-of-history-fears-for-democracys-future/?utm\\_term=.8e9b4aa73321](http://www.economist.com/news/leaders/21711904-worrying-experiments-new-form-social-control-chinas-digital-dictatorship) (Accessed on Aug 12, 2017)

The Economist (2016). Big data and government: China's digital dictatorship. [Electronic Resource] Retrieved from <http://www.economist.com/news/leaders/21711904-worrying-experiments-new-form-social-control-chinas-digital-dictatorship> (Accessed on Aug 12, 2017)

The Economist (2015). The Singapore Exception. [Electronic resource] Retrieved from <https://www.economist.com/news/special-report/21657606-continue-flourish-its-second-half-century-south-east-asias-miracle-city-state>

The Economist Intelligence Unit (2006). Economist Intelligence Unit democracy index 2006, 3 p.

The Economist Intelligence Unit (2007). The Economist Intelligence Unit's index of democracy, 11 p.

The Economist Intelligence Unit (2008). The Economist Intelligence Unit's Index of Democracy 2008, 31 p.

The Economist Intelligence Unit (2010). Democracy index 2010: Democracy in retreat, 46 p.

The Economist Intelligence Unit (2011). Democracy index 2011: Democracy under stress, 48 p.

The Economist Intelligence Unit (2012). Democracy index 2012: Democracy at a standstill, 45 p.

The Economist Intelligence Unit (2013). Democracy index 2013: Democracy in limbo, 67 p.

The Economist Intelligence Unit (2015). Democracy Index 2014: Democracy and its discontents, 58 p.

The Economist Intelligence Unit (2016). Democracy Index 2015: Democracy in an age of anxiety, 67 p.

The Economist Intelligence Unit (2017). Democracy Index 2016: Revenge of the "deplorables", 75 p.

- Ungku, F. (2017). Water price hike sparks rare public protest in Singapore. Reuters. [Electronic Resource] Retrieved from <http://www.reuters.com/article/us-singapore-protest-idUSKBN16I0H8> (Accessed on 12 Aug, 2017)
- Ungku, F. (2017). Singapore protest calls for inquiry over PM's alleged abuse of power. Reuters. [Electronic Resource] Retrieved from <http://www.reuters.com/article/us-singapore-politics-protests-idUSKBN1A00CO> (Accessed on 12 Aug, 2017)
- United Nations E-Government Survey 2016 (2016). E-Government in Support of Sustainable Development, New York: United Nations, 2016.
- Verplanke J., Martinez J., Miscione G., Georgiadou Y., Coleman D., Hassan A.A. (2010) Citizen Surveillance of the State: A Mirror for eGovernment?. In: Berleur J., Hercheui M.D., Hilty L.M. (eds) What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience. IFIP Advances in Information and Communication Technology, vol 328. Springer, Berlin, Heidelberg
- Waseda University (2017). Waseda-IAC International e-Government Rankings [online] Available at: <https://www.waseda.jp/top/en-news/53182> [Accessed 12 Aug. 2017].
- Webster, C. R. (2012). Surveillance as X-ray. *Information Polity: The International Journal Of Government & Democracy In The Information Age*, 17(3/4), 251-265.
- Wiebe, E., Mills, A. J., Durepos, G., & Albert, M. (2009). *Encyclopedia of Case Study Research*. [Elektronisk resurs]. Sage Publications 2009.
- Xu, L. D., Tjoa, A. M., Chaudhry, S. S., Bo, Y., Qian, L., & Meiyun, Z. (2008). Analysis of E-Government Outsourcing. In , *Research & Practical Issues of Enterprise Information Systems II* (p. 1191). doi:10.1007/978-0-387-76312-5\_44
- Yang, Kaifeng (2014). Qualitative Analysis. In: Mark Bovens, Robert E. Goodin and Thomas Schillemans (eds.) *The Oxford Handbook of Public Accountability*. Oxford: Oxford University Press.

Yin, Robert K. (2014). *Case Study Research – Design and Method*. Los Angeles: Sage Publications.