Bachelor's thesis

Information and Communications Technology

2019

Jani Tuominen

COMPARISON BETWEEN GDPR, PEOPLE'S REPUBLIC OF CHINA CYBERSECURITY LAW, AND PIPA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2019 | 25 pages

Jani Tuominen

COMPARISON BETWEEN GDPR, PEOPLE'S REPUBLIC OF CHINA CYBERSECURITY LAW, AND PIPA

The General Data Protection Regulation, the People's Republic of China Cybersecurity Law, and the Personal Information Protection Act are sets of regulations, some of which, are accompanied by other legislation and practices. They respectively affect the regions of the EU and its Member States, China, and South Korea. Each of them has brought changes to corresponding average citizens, companies, and states. However, while there are some articles which make comparisons between some of them, for example, the GDPR and the PIPA, there are only a few if any, which would make a comparison between all of them.

The thesis aims to give an insight on the inner workings of the three regulations mentioned above, the main focus is on how different rights and obligations along with security measures are expressed in respective regulations, as well as, how the regulations have been implemented.

The thesis is divided into two parts. The first part of the thesis examines each set of regulations at a time, what the legislation dictates; how it is implemented, and what effects the implementation has caused. In addition, the first part describes the benefits, drawbacks, and concerns. The second part of the thesis compiles and compares all three of the regulations and similarly goes through them as the first part did.

The objective of the thesis was achieved. The thesis concludes that while the regulations and practices involved are different in certain aspects, there are also many similarities. The thesis also mentions some useful information which the average citizen or a company should take note of, if they are planning to enter, for example, the South Korean internet ecosystem.

KEYWORDS:

GPRD, PRC Cybersecurity Law, PIPA, personal information, information security

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2019 | 25 sivua

Jani Tuominen

VERTAILU GDPR:N, KIINAN KYBERTURVALLISUUS LAIN JA PIPA:N VÄLILLÄ

Yleinen tietosuoja-asetus (GDPR, General Data Protection Regulation), Kiinan Kyberturvallisuus Laki (PRC Cybersecurity Law) ja Henkilötieto tietosuoja-säädös (PIPA, Personal Information Protection Act) ovat säädöksiä, joista osa omaa lisäsäädöksiä ja käytänteitä. Ne vastaavasti koskevat, EU:n ja sen jäsenmaiden alueita, Kiinan aluetta ja Etelä-Korean aluetta. Säädökset ovat tuoneet paljon uudistuksia kansalaisille, yrityksille ja valtioille. Ja vaikka on olemassa artikkeleita, jotka käyvät vertailevasti läpi näitä säädöksiä esimerkiksi GDPR:n ja PIPA:n välillä, ei kuitenkaan ole olemassa juurikaan artikkeleita, jotka käsittelisivät niitä kaikkia.

Opinnäytetyö on kirjoitettu siten, että se pyrkii antamaan alustavan käsityksen yllä mainittuihin säädöksiin. Erityisen huomion kohteena on ollut säädösten tapa käsitellä erilaisia oikeuksia ja velvollisuuksia tietoturvaratkaisuiden ohella, sekä miten näitä säädöksiä ollaan varsinaisesti toteutettu.

Opinnäytetyö on kirjoitettu kahdessa osassa. Ensimmäinen osa käsittelee säädöksiä erikseen. Siinä käydään läpi mitä eri säädökset ja käytänteet määrävät, miten niitä toteutetaan ja mitä vaikutuksia näillä toteutuksilla on. Sen lisäksi kuvaillaan niiden hyviä ja huonoja puolia mahdollisten pelkokuvien lisäksi. Toisessa osassa opinnäytetyötä käsitellään säädöksiä toisiinsa vertaillen pitkälti samalla tavalla kuin ensimmäisessäkin osassa.

Opinnäytetyön tavoite saavutettiin. Opinnäytetyön lopuksi todetaan, että vaikka säädöksissä onkin jonkin verran eroavaisuuksia, niin niissä on myös paljon samankaltaisuuksia. Opinnäytetyössä mainitaan myös mitä tavallisen kansalaisen tai yrityksen tulisi ottaa muun muassa huomioon, mikäli he olisivat aikeissa siirtyä esimerkiksi Etelä-Korean verkon alle.

ASIASANAT:

GDPR, Kiinan Kyberturvallisuus Laki, PIPA, henkilötieto, tietoturva

CONTENTS

1 INTRODUCTION

1.1 Background

The author of this thesis has personally dealt with various laws and practices related to information protection in both China and South Korea before for 5 years due to using or trying to use websites, services, and platforms in those countries. After the advent of the GDPR in the EU region and its Member States on May 2018, the author has had many conversations comparing all of the three sets of regulations to each other and came to realize that there are few if any direct comparisons of the three published, which is why the author chose this topic for the thesis.

The GDPR, as is commonly known, is the EU's regulation related to personal information protection, which was enacted in 2016, but came into effect as of May 25th, 2018. The PRC Cybersecurity Law, on the other hand, is a set of regulation in the People's Republic of China, which is equivalent to the GDPR and it was enacted in 2016, but came into effect as of June 1st, 2017. The PIPA is to South Korea what the GDPR is for EU and it was enacted in March 2011, but came into effect as of September 30th, 2011.

1.2 The objective of the thesis

The main objective of the thesis was to compile, describe, and compare the three sets of regulations and possible additional practices within each of the regions they affect namely; European Union and the Member States, China and South Korea. The regulations for the regions respectively are the GDPR, the PRC Cybersecurity Law, and the PIPA. Practices and regulations were examined from the perspective of legislation; practical implementation; and pros, cons, and fears. The point of the examination was also narrowed down to examining mostly what rights and obligations separate entities such as the average citizen, companies, and the state hold respectively in regards to personal information protection.

2 GENERAL DATA PROTECTION REGULATION

General Data Protection Regulation or what is commonly known as the GDPR is the European Union's (EU) data protection regulation, which aims to improve individual control of one's data further. The regulation itself is quite specific on the types of data that it affects, the various types of entities it affects and the way it affects them, as well as how information about the used procedures between the entities needs to be presented. The regulation was set in motion on 25.5.2018

The data mainly affected by the GDPR is personal data, and the GDPR's main aim is to achieve a more private internet environment which is especially reinforced by articles of the GDPR such as Art. 15 also known as "Right of access by the data subject" and Art. 17 respectively known as "Right to erasure ('right to be forgotten')." (Intersoft Consulting 2019) (EUR-Lex 2019)

2.1 Private internet ecosystem

Article 15 of the GDPR is an article, which mainly describes various rights and reasonable expectations that a data subject can have, in regards to what data controllers and processors should grant them in terms of legislation. Article 15 decrees that the data subject has:

- The right to obtain a confirmation from a controller as to whether or not his or her data is being processed, and, if so, what is the purpose of the processing;
- The right to know the categories of data used, and to which individual(s) and organization(s) the data has been or will be disclosed to;
- The right to know, where possible, the predicted time for which the personal data will be stored or at least the criteria used to determine such period if it has not been determined as is;
- The right to request that the controller rectifies or erases the personal data or restricts its processing or right out object to it;
- The right to complain to an authority;
- The right to obtain all available information on data sources of personal data not directly collected from the data subject;

- The right to know about the existence of automated decision-making, including profiling, and in some cases, meaningful information about the logic involved, as well as the aim and possible effects of such processing of the data subject. (Intersoft Consulting 2019) (EUR-Lex 2019)

Article 15 described mostly various rights and expectations which a data subject should expect to receive from data controllers and processors according to the GDPR, Article 17, however, describes more what obligations data controllers and processors have, and how those obligations should be acted on. Article 17 Paragraph 1 decrees that the data subject has the right to obtain from the controller the erasure of their data without undue delay and the controller should do so where one of the following conditions applies:

- If the personal data are no longer necessary for the purposes they were initially collected or processed for;
- If the data subject withdraws their consent on the processing of information they initially allowed it on, and where there is no other legal ground for the processing;
- If the data subject objects to the processing pursuant on the processing of personal data be it for direct marketing or otherwise, unless the controller can provide legal grounds for dismissing the objection.;
- If the data has been illegally processed;
- The personal data have to be erased due to a legal obligation in Union or Member State law to which the controller is situated and thus subject to;
- The personal data have been collected concerning the offer of information society services to children above the age of 16 or in some Member States above the age of 13. (Intersoft Consulting 2019) (EUR-Lex 2019)

Paragraph 2 decrees that the controller which has made the personal data public, and is obligated pursuant by a data subject to erase personal data, is to take reasonable steps, according to technology and the cost of implementation, including technical measures, to inform controllers which are processing the personal data that has been requested for erasure. (Intersoft Consulting 2019) (EUR-Lex 2019)

Paragraph 3 decrees that Paragraph 1 and 2 do not apply to the extent that processing is necessary:

- If it infringes on exercising the right to freedom of expression and information;

- If there is a legal obligation which requires processing by Union or Member State law to which the controller is subjected to or if the task being carried out serves the public interest or is in the exercise of official authority vested in the controller;
- For reasons concerning public health;
- For archiving purposes in the public interest or for significant research purposes or statistical purposes while aiming to minimize the amount of used personal data or using 'pseudonymization' as long as the right for erasure referred to in Paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- Alternatively, for the establishment, exercise or defense of legal claims. (Intersoft Consulting 2019) (EUR-Lex 2019)

Article 22 states that the data subject has the right not to have decisions made regarding themselves based solely on automated processing, such as profiling, which would have either legal effects or which would have other significant effects towards them. The right, however, does not apply, if the automated processing is necessary for a contract between the data subject and a data controller. It also does not apply, if the automated processing is authorized by Union or Member State law to which the controller is subject and which also describes all the required measures to safeguard the subject's rights, freedoms, and so on. (Intersoft Consulting 2019) (EUR-Lex 2019)

Article 23 describes various scenarios in, which the data controllers and processors are allowed to restrict rights, obligations, and freedoms of the data subject, as long as such restrictions respect the essence of the fundamental rights and freedoms and are necessary for a democratic society to safeguard. National security and defense are considered to be causes serious enough to disregard some of the rights a data subject would have. Public security and criminal investigation, prevention, detection, and prosecution are also considered to be legitimate areas in which it is not necessary to follow through all of the data subjects wishes according to their rights. Monitoring and inspecting various sectors, including governmental and judicial, are also considered to be legal in the event, where it would serve the public interest. (Intersoft Consulting 2019)

(EUR-Lex 2019)

2.2 Rights of an individual

The GDPR legislation, in other words, seeks to give the power for individual people to choose whether or not to give out specific details about themselves to the various organization(s), companies and in extension any possible third-parties involved. The legislation also gives one the right to request the parties mentioned above to give out the explanation for why they are asking for specific information as well as how that information is used in all intents and purposes. The organization(s) and companies are also obligated to tell the individual if they so request, whom they are giving their data for storage purposes and processing purposes. In most cases, it is illegal to collect personal data of children under the age of 16 except for some Member State laws that allow the collection for children older than 13. There are some exceptions though, such as if the personal data is used to serve the public interest, for example, the public health.

The legislation also gives individuals the right to withdraw the consent they have given for the organization(s) and companies. The aforementioned entities are obligated to stop collecting and processing such data, and if one wishes they can request the erasure of personal data, which the entities are obligated to follow through with some exceptions, for example, public interests or legal claims that require further collecting, storing and/or processing of personal data from the individual.

The entities involved are also required, unless there are legal claims not to do so, to inform any third-parties and ask them to follow through with the erasure of one's data or any other request the individual might have based on the rights granted to them by the legislation described in the GDPR.

In regards to automated processing, including profiling, in practice, the average citizen has the right to opt out of such processing, unless there is a legal reason to do otherwise, for example, if one has signed a contract which can only come to fruition if the automated processing is used. Companies also should avoid causing harm to a person with automated processing, and in many cases, should notify the person concerned what kind of effects this processing could cause.

Many of the legal reasons, which could be used to circumvent some of the rights of the average citizen, include, but are not limited to, public security; criminal investigation, prevention, and detection; national security; defense; and public interests. The average citizen, who does not commit any or notable criminal offenses, is likely only to be

subjected to a few situations where their rights could be bypassed. The most common reason for bypassing these rights include contracts they have signed, public health, other public interests, and research of significance where a person's information is considered crucial.

2.3 Results, Consequences, and Fears

Some of the rather glaring results of the GDPR are: making a more secure ecosystem, especially for children. Due to making it illegal to collect personal data and use it, for example, for direct marketing, GDPR has curbed some of the more invasive data collecting by various software and media platforms. The strictness of GDPR has also enforced companies to be more careful and precise, when they are operating any services within the Union or its Member States, as far as personal data collection goes. It can also be said that to an extent the GDPR promotes freedom of speech on the internet by allowing an even higher level of anonymity.

Some of the consequences of the GDPR have much do with how the Union and its Member States as a whole are in a situation, that for specific platforms a small portion of their customers and users and thus some websites, platforms, and services et cetera. Such as Allrecipes.com have decided not to go through with the GDPR audit and have instead chosen not to provide their services to the GDPR subject countries. There have also been many cases where some forms of websites, platforms, and services have delayed their launch or had it delayed due to causes pertaining to the GDPR legislation and audits, such as the game "Ring of Elysium" by a Chinese company Tencent, which had its EU launch delayed by almost 3 months due to ongoing GDPR audits.

The heightened privacy and anonymity that has resulted from the GDPR has also brought up some fear-inducing scenarios, mainly focusing on how the increased anonymity could be used for criminal activities or otherwise morally unethical activities such as bullying. The fears are mostly fuelled by the fact, that one could use and manipulate the types of data which they wish to reveal, to the extent that they could still use a service or platform etc., to commit acts mentioned above without actually having to fear being caught. Thus, there is a fear that the GDPR could increase specific problems in society while fixing or positively affecting other aspects of society.

3 PEOPLE'S REPUBLIC OF CHINA CYBERSECURITY LAW

There is no single comprehensive data protection law in China. Instead, there are various often provincial rules relating to personal data protection and data security as a part of their framework, and they are found across various laws and regulations.

On June 1, 2017, the PRC (People's Republic of China) Cybersecurity Law, became the first enacted national-level law to address cybersecurity and personal data privacy protection. There is still quite a bit of uncertainty as to how the legislation will be administered; however, as well as, what practical steps need to be taken to achieve compliance. After the law was set in motion, there have been various Draft guidelines released, at times, even weekly, it is suspected that the standards and guidelines will be finalized soon. (DLA PIPER 2019)

The Chinese government has also released and passed many other new laws and regulations to accompany the PRC Cybersecurity Law such as:

- The Decision on Strengthening Online Information Protection, set in motion on December 28, 2012
- National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services, set in motion on February 1, 2013
- National Standard of Information Security Technology – Personal Information Security Specification, set in motion on May 1, 2018

The Decision aims to protect the online information security, safeguard the rights and interests of citizens, various organizations, and ensure national security and public interests. The Decision is legally binding. While the Guideline and PIS Specification are not legally binding, they are highly persuasive. (DLA PIPER 2019)

3.1 Personal information and a notice of rights.

Among the various laws related to personal data in China, the PRC Criminal Law states that selling of personal information, illegal provision of, or illegal access (such as theft)

to citizens' personal information are all illegal activities. The PRC Consumer Rights Protection Law, on the other hand, contains data protection obligations which concern most types of businesses that deal with consumers. (DLA PIPER 2019)

There is no clear definition of personal data or 'personal information' as it is referred to in China among the many laws. Generally speaking; however, it often means that all kinds of information, sensitive or otherwise, that is recorded by electronic means or via any other method that can be used to identify individuals or combined with other information to identify a natural person's information. The PIS Specification, however, while not legally binding, does describe how to differentiate general and sensitive personal information. It is described that any information which, if disclosed or abused, could lead to negative results is considered to be sensitive information. Individual's phone number, personal identification number, credit information, and health information are few of the types of information that are classified as sensitive personal information. It is also worth noting that the collection of data from children under the age of 14 is prohibited unless explicit consent is obtained from their legal guardians. (DLA PIPER 2019)

In general, for any form of data to be collected from a data subject by a controller, it first needs to express consent from the subject. There are few types of information such as overseas data transfers and direct marketing, which need specific consent from the data subject. Besides, a data controller or in other words the organization should provide consumers or the data subjects with a privacy policy or term of service or something similar that informs them of the scope and ways in which the data is collected, processed and disclosed. The notice should also describe, who/which entity is the data controller and specific details on where it operates, the name of the operated place and telephone number and e-mail address etc. There also needs to be a mention of how the data controller is going to keep the data collected securely as well as whether or not the data subjects have rights to the data collected and how those rights function as well as potential risks of providing the data and the risks of not providing the data. Also if there are any changes to the policy, the data subject should be notified and if needed ask for further consent. (DLA PIPER 2019)

If the data controller wishes to share, disclose or in any form transfer an individual's personal information to a third party: they are not allowed to share or transfer any personal biometric or sensitive information if it has been prohibited under relevant laws or regulations. They also need to perform an impact assessment and take measures to

protect the data subject according to the assessment results. They must also inform the subject of the reasons for the sharing, disclosure or transfer of information and inform them of the types of data recipients along with prior express consent from the data subject; as well as record all significant details of the sharing, disclosure or transfer of personal information in detail. (DLA PIPER 2019)

For sharing, disclosing or transferring of the personal information to a third party abroad additional rules are applied. The core rules for the transfer involve informing the data subject, making a copy of the data to remain within the PRC and conducting a security assessment on the data to be transferred. There are also certain types of personal information that at the moment are not allowed to leave China, such as, banking and online mapping. (DLA PIPER 2019)

Organizations, network operators and to an extent some websites in China are required under the PRC Cybersecurity Law to implement technical and other necessary measures to make sure that security of personal information is maintained and to prevent the data from being accidentally disclosed, tampered with or destroyed. Affected organizations have seen that CIIOs (Critical Information Infrastructure Operator) must apply additional security safeguards. (DLA PIPER 2019)

Organizations with information systems are also expected to self-evaluate the type of information they are dealing with, which is categorized into five tiers with 5th being the highest one and then deal accordingly to various laws and regulations to ensure that necessary level of information security is being applied. (DLA PIPER 2019)

The PRC Cybersecurity Law states that the data subject should be notified of methods to use to restrict any automated decision making, as well as, be notified of any information collected that could significantly affect the data subject. It is, however, essential to remember that even, if one desired to restrict automated decision making, they would be unable to do so, if that process would be required to serve the public interest or have any other kinds of legal justifications for it. (DLA PIPER 2019)

The PRC Cybersecurity Law hints at various restrictions that could apply to a data subject, or a data controller, or the state. While a legitimate legal reason, for example, a criminal investigation is something that can be used to bypass some rights, there are also some guidelines that are used to restrict activities and rights. Most of the relevant articles in the PRC Cybersecurity Law indicate that the main restriction to any activities, rights, obligation, and freedoms for data subjects, controllers, and the state is the lawful

and proper use of the internet. The proper usage of the internet includes that one does not spread or create information which would damage anyone's reputation, privacy, intellectual property or other lawful rights. (Privacypedia 2019)

3.2 Business opportunities

For the average citizen, the PRC Cybersecurity Law has given them control over their personal information due to the many rights stated. The average Chinese citizen does not have much they can do to limit how automated decision taking and profiling is taking place, at least as far as the law states explicitly. It is important to note, however, that in various parts of the law, it is described, what kind of information can be used, and what are the limits for specific types of information in terms of usage.

For the Chinese citizen and companies, the PRC Cybersecurity Law gives restrictions on internet and information used in a rather straightforward manner. One could say that, as long as the person, or the company follows the law and the values which are regarded highly in the Chinese culture, such as, privacy, respect, and modesty they are allowed to use the internet freely. All of the above values were in regards to proper mannerism used in the internet and social media and did not include many other highly regarded values in the Chinese culture.

The newly enacted laws have brought great changes to progress the level of security of personal information for the people of China, and, while they have certainly brought changes for the average citizen, the laws have had a much more significant impact on the various companies situated in China or dealing with the new Chinese laws. (Bell R. & Liu Y. 2018)

The laws have affected various companies in enforcing their security measures and making them as transparent as possible, with all possible customers as well as possible third parties. Part of the reason is due to many of the new regulations enforcing average citizens' rights to query from the companies (also knows as data controllers in most cases), how their information is used and who the information is being shared with.

Insurance and law companies are one of the two main types of companies that have boomed even more due to the enacted laws continuously. The main reason for this is that there are more and more companies and people in general, requesting help from the insurance firms and other law firms for that matter as well, on how to deal with the

new laws and what rights and obligations each party involved have. The insurance and law companies, however, do not enjoy smooth sailing in the unclear waters, which are the continually changing draft guidelines for the newly enacted personal information security laws set by the Chinese government.

The other type of business that has boomed due to the increasing requirements of cybersecurity is the hardware manufacturing companies, the main reason being that the increased requirements have also increased the required minimum amount of hardware needed, to achieve sufficient levels of security. The need for hardware is even more substantial for the higher tiered companies that are enforced to have even more rigorous safeguards ready for any attempts of theft or intentional leaks and so on.

3.3 Future, Past, and Fears

The future of China's general data protection rules seem like a bright one, while the current regulations are still to a degree, yet to be fleshed out, they are moving forward to ensure the privacy and security for their citizens. In many ways, the laws being enacted are very similar at least in the scope of personal data to many other modern countries. Some of the best examples of this are the ways they require consent for collecting data and in-depth detail of the way the data will be used and collected as well as shared.

The past of China's data protection could be considered to be quite bleak, which is clearly evidenced by the fact that the government is driving with great vigor to elect and pass new laws and regulations to fill the hole that was there, and, thus secure their public interests along with the interests of the Chinese people.

As for the fears related to the yet to be fleshed out regulations and laws, many of them have to do with the fact that many of the details have yet to be standardized and are thus somewhat ambiguous. There is also some fear caused by the reason mentioned above that specific rules could be slightly different at different places for example during travel.

4 PERSONAL INFORMATION PROTECTION ACT

Personal Information Protection Act (PIPA) is a set of regulations enacted by the South Korean government and set in motion on 30.9.2011. The PIPA is known to be one of the strictest set of regulations in the entire world. It is known to be extremely comprehensive and affecting various levels of organizations, even some government entities. The PIPA is also vigorously enforced, and its penalties go all the way from various forms of fines to imprisonment depending on the actual crime committed. (IAPP 2019)

South Korea, in general, has various other data protection laws besides the PIPA and most South Korean websites and especially internet using services require the usage of valid RRN or Resident Registration Number to even register on them or at least to adequately use such services. It is also possible for most foreigners besides those affiliated with the U.S. military to apply for ARN or Alien Registration Number, which allows them to use some websites and services during their stay.

4.1 Security by all levels of state

The PIPA decrees that any personal information which is being collected by the PIC (personal information processor) is required to make the processing as transparent as possible and specified to the point that only the bare minimum information is collected lawfully and fairly for the purposes they are intended for. It is also decreed in the PIPA that PIC is not allowed to use the information they collect for one purpose for any other purpose if it was not mentioned beforehand and required to attain the original aim of the processing mentioned. The PIC is also expected to maintain bare minimum standards required for the processing purpose as far as accuracy and “freshness” of information are concerned.

The PIPA also enforces that the PIC maintains required processing, collecting and storing standards to make sure that the data subject’s rights would not be infringed upon or subjected to other similar kinds of risks. PIC is also required to have a public privacy policy, and a notice that makes transparent their processing methods and they are expected to guarantee data subject’s rights to access their information.

The processing done by the PIC is also expected to be done in a way that would have the least chance of infringing on the privacy of the data subject, and, if possible in a manner that would allow them to process the information in anonymity. The PIPA also enforces the PIC to follow through the various regulations set to obtain the trust of data subjects. (Korean LII 2019)

The rights of data subjects, on the other hand, are merely made more apparent in their section in the PIPA. First and perhaps the most apparent right is, the right to be told of any processing related to their personal information. One of the more essential rights mentioned is, the right to consent or not and choose the scope of that consent concerning the information about to be processed. In the PIPA there is also decreed that the data subject has the right to confirm processing of their information and to demand access to the collected information as well as a token of sorts to guarantee their access in future as well. Data subjects are also given the right to demand the suspension of any processing activities pertaining to their information as well as to make correction, deletion and destruction of any personal information, as well as ,demand reparations in prompt and fair procedure in the event that the processed information ends up causing damage to the data subject. (Korean LII 2019)

The state and government are also expected to devise and maintain policies that would aim to prevent any unnecessary harmful impacts. The policies are aimed primarily to beyond-purpose collection and processing of personal information, and to limit the extent of possible abuse or misuse of personal information et cetera, and to make policies that would maintain and improve the dignity of human beings and individual privacy. The PIPA also decrees that policy measures and legislation should be designed to a high enough degree to protect the various rights of the data subject. It is also expected that various governmental agencies should respect, promote and support data protection activities designed by PIC to improve on the irrational social practices relating to the processing of personal information. It is also enforced that state and local governments should support and follow through any enactments or amendments of laws, regulations or ordinances in regards to the processing of personal information as long as they follow the purposes described in the PIPA. (Korean LII 2019)

The PIC is according to the PIPA allowed to restrict or deny access of a data subject to their information after notifying them of the reason under particular circumstances. If the PIC is operating under a zone where access by non-personnel is prohibited or restricted by law. If granting access could endanger the life of others, or bring harm to their

properties or benefits. If the access could hinder collection or repayment of taxes, or if the access could cause problems regarding testing and evaluating academic competence. Last reason to deny access is if there are an ongoing audit and examination under other laws. (Korean LII 2019)

4.2 Rigorous, effective and at times fraudulent

In practice, the PIPA is a rigorous set of regulations, which makes it nearly impossible for a foreigner who is not staying in South Korea and has not already applied for the ARN to access most South Korean sites and services, and their functions assuming that registration is required on them. For South Korean citizens, however, the PIPA signifies a type of support structure. As it is likely to give a sense of relief and security due to the transparency, it enforces the various organizations to strive for, as well as, how under normal circumstances one can be sure that no single entity is legally allowed to infringe on the many rights granted to them. The PIPA and the South Korean law itself does indeed not include the highly valued property of near absolute anonymity, which is due to the requirement of using the equivalent of social security number to register on most South Korean hosted websites. The infrastructure has, however, been designed to reinforce the other aspects relating to information security and the laws and legislation are enforced to follow suit.

Additionally, as long as one wishes so, it is possible to request access to one's information, there are, however, few restrictions in regards to the location and use of the information, where one is likely not allowed access or can gain only restricted access. Most of these locations are public, or state institutions, which are considered to be "for personnel only," and thus gaining access on any information stored within is quite unlikely. In terms of use, the most common cause for not gaining full access is, that there is a legal reason, usually another law, which denies access to the information.

The lack of anonymity is of extreme importance, however, for the PIPA and the various other laws enacted in South Korea. The main reason for this is the fact that it makes it much easier for companies, the state and for the average citizen to vie for their rights and make sure that people will be prosecuted and punished accordingly in the event of any crimes being committed. It also makes it much easier to investigate any potentially illegal activities as there is no need to track a person's internet account name (or Alias, in general) to the actual person behind it. Beyond the usage of criminal investigation and

prevention, throughout usage of the RRN is also something that makes many different services, primarily monetary and governmental ones much faster and simpler to use. Mainly because in South Korea many services, banks included are often attached to one's mobile number along with the RRN so many day-to-day tasks can be done on the go quite smoothly.

The nearly universal use of the RRN, however, has brought along with it some complications, mainly with foreign users whom would like to use different South Korean services, mainly in the gaming scene, which South Korea is quite famous for. The problem lies with many services willing to sell South Korean game platform accounts, and, while it is not possible to know for sure whether or not the accounts are stolen or sold by their actual owner, the practice is still nevertheless highly illegal. The unlawfulness of this practice is of course caused by the fact that the accounts are tied to their own respective RRN. In other words, a foreigner using a South Korean account which is bound to someone else's RRN is more often than not guilty of identity theft, and, depending on the platform or organization that the illegally used RRN is used on it might not stop there. Identity theft alone is a severe crime in South Korea just like in most other modern countries.

4.3 Hopes, Losses, and Fears

From a global point of view, the South Korean the PIPA and other legislation could serve as a predecessor to future global legislation regarding personal information protection. Systems similar to RRN could be also be used or invented in other countries as well to make keeping order easier and faster as well as making many other day-to-day tasks smoother.

The PIPA and throughout usage of the RRN have admittedly isolated the South Korean internet community partially from the rest of the world which does not follow similar kind of regulation at the moment. The leading cause being that the South Korean internet community is highly exclusive due to the use of what is essentially a social number to access websites and platforms and that number is not possible to be gained by foreigners. The only "saving grace" is that foreigners do have the option to apply for ARN if they are staying in South Korea, which does grant at least some level of access to many websites and platforms.

There are involved with the PIPA and even more so with RRN. The main fear that people have of the system and similar systems is the lack of anonymity, and along with it the fear of being vulnerable, especially if a data center gets infiltrated one's RNN number along with the bound account and other personal details would be at risk. The other fear, more so, from the perspective of public interest is, the fear of uncertainty, especially as South Korean website and platform accounts et cetera are quite sought after. It also does not help that many do not realize that RRN, which is bound to the account(s) is the same as a social security number. The combination of the two has resulted in some fear in people that the person they are interacting with or have interacted with in the past could be someone other than who they claim to be or should be. From a legal standpoint, the selling of online accounts to the unknown foreign user(s) has caused quite a bit of extra work than before. The cumbersome task has been partially alleviated by both South Korean citizen of native or foreign origin that have chosen to report all mostly obvious cases of identity theft to the police or other similar authorities.

5 SIMILARITIES AND DIFFERENCES

While the culture and political environments of EU; China and South Korea are quite different from each other, the data protection regulations enacted by each are quite similar in many ways, while still having some differences between them as well.

5.1 Differences in legislation

In terms of legislation, the GDPR, the PIPA, and the PRC Cybersecurity Law hold some similarities between them. While the PRC Cybersecurity Law is somewhat obscure about their exact definition for what counts as personal information and data, in general, all three systems do regard the matter overall in a similar light. The basic definition holds that personal information is a type of information that could be used to identify an individual on the information alone or from a derivation of that information.

The treatment of data processors and controllers is only separated in the GDPR, while both the PIPA and the PRC Cybersecurity Law consider both of the roles to be included in legislation concerning data controllers. The GDPR treats data controllers as legal entities, legal persons and organizations et cetera that hold the collected information and decide how it is being processed. Data processors according to the GDPR are legal entities, legal persons and organizations et cetera that process the information. The PIPA and the PRC Cybersecurity Law combine the two and do not differentiate the description much at all from what the GDPR has used as well.

The data subject(s) are treated similarly in all three regulations as natural people, from whom the information is being collected from, and, who have quite a vast array of different rights granted by their legislation. All three regulations grant the data subject(s) the right to access all collected and processed information, as well as right for erasure. Right for erasure in all three regulations is comprehensive, from the erasure of the information from the controller and the controller should pass the message on to all the third parties involved who should act accordingly. Consent is also treated alike in all three regulations as something that needs to be given beforehand before any processing takes place and in all three the withdrawal of consent exists as well.

Automated processing, including profiling, is explicitly mentioned, only in the GDPR. In the GDPR it is explicitly stated that a data subject has the right to be exempted of having decisions with significant effects take place when they are solely based on automated processing. In the PIPA and the PRC Cybersecurity Law, the right to be safe from the decisions solely made by automated decision making is mentioned implicitly by other various rights described.

Restrictions for the rights of a data subject are described differently in all three of the laws, but they are very similar in the end. The similarity comes mainly from the fact that all three regulations restrict the rights of their data subjects by relying on the other articles in the legislation and other laws. A common similarity is that all three restrict or deny access to confidential information, which could potentially harm, for example, another person or the institution in question. The other similarity, which is more implicitly mentioned in the PIPA and especially in the PRC Cybersecurity Law is proper manners, which means acting in a way that would respect highly regarded local values.

In terms of the respective regulations expecting that future legislation and laws would follow suit with the regulation, all three are quite similar as well. While the GDPR is a bit more complicated due to not being a set of regulations by a country but by a union of countries, it does still aim to have a similar spirit of handling enactment of new policies as the other two regulations. The PIPA and the PRC Cybersecurity Law both expect the government and local authorities to continue enacting laws and policies which would follow suit with the aims presented in their regulations. Out of the three, the PIPA is the one that expects the most and to a degree even enforce all levels of state to follow suit in terms of making future laws and policies to support an even more secure internet ecosystem for those living in it, or in the PIPA’s case for South Korean citizens.

5.2 Differences in practice

In practice, all three regulations allow citizens to view their rights as well as what information is collected and how it is processed from respective privacy policies or similar notices. Also according to each set of regulation, it is possible to demand access to one’s information and withdraw consent from collecting and processing any information, as well as, demand erasure of any stored, collected or processed information.

In terms of how old a person has to be for their information to be collected and processed by just their consent, the PRC Cybersecurity Law has the lowest age needed on average with the age of 14 being the limit after which one does not need explicit consent from their legal guardian(s). The GDPR has the age set to the age of 16. Some Member States, however, have the age set to as low as the age of 13 which in turn would make those Member States have even lower age limit after which one would not need explicit consent from any legal guardian(s) than in China. The PIPA, on the other hand, could be said to have the limit set as the highest as the RRN, which is needed to register on most site and platforms can only be gained at the month one turns to the age of 17 in South Korea.

All three regulations, also agree that on an event where there is a legal reason to do so, any request for erasure; or access; or lack of consent for collecting, storing and processing of data can be disregarded, if it would compromise the legal need for which they are needed for. The legal reasons are also described quite similarly in all three regulations. Most common reasons are if the legal cause has something to do with public interest or with significant research, it is possible, to an extent, ignore the rights of the average citizen, in regards to, their information.

In terms of exclusivity, assuming that language barrier is not an issue, the PRC Cybersecurity Law can be thought of as the most inclusive, due to a lack of extremely rigorous auditing process, or of practices that would cause most region(s) to be locked out. the GDPR is the second most exclusive of the three mainly due to the rigorous auditing process, which has turned many sites and platforms away from entering the EU “market.” The PIPA and South Korean legislation are the most exclusive, mainly due to throughout usage of the RRN which makes that most foreigners do not have any proper access to various websites and services hosted in South Korea.

5.3 Pros, Cons, and Fears

In terms of pros, the GDPR has increased the level of anonymity and information security within its area of effect. The PRC Cybersecurity Law, on the other hand, has finally formed and given some level of security for the Chinese citizen. The PIPA’s main achievement after a higher level of security lies in keeping order even more so than before. The PIPA and the PRC Cybersecurity Law along with some other laws and practices have also allowed for day-to-day life activities to be done even smoother.

In terms of cons, the GDPR and the PIPA both share the fact that they have resulted in somewhat exclusive internet ecosystems for their respective areas of effect. The PRC Cybersecurity Law, on the other hand, suffers mainly from the fact that many details have yet to be completely fleshed out, thus resulting in some additional hassle over what would be considered future best practices in the Chinese internet ecosystem.

In terms of fears, the GDPR's increased anonymity has caused some fears on whether or not it could be abused for criminal activities in a way where one could hide some critical information of themselves and thus partially or entirely be impossible to catch or trace at least through tracking their internet usage et cetera. The PRC Cybersecurity Law mainly shares their fears with the cons related to the entire set of regulation. The law is shrouded in quite a bit of obscurity, and many details are vague, and many practices are brand new and to some degree not standardized. The PIPA's lack of anonymity and the extensive use of RRN, on the other hand, have caused some people to fear what would happen if a data center, for example, got breached. Would all of the information inside be in risk of being leaked, and, thus a sizeable portion of South Korean citizens' information (possibly private) being out in public completely vulnerable.

6 CONCLUSION

The main objective of the thesis was to compile, describe, and compare personal information protection regulations and practices in European Union and its Member States, China, and South Korea. These regulations and practices were mainly examined from the perspective of legislation; implementation; and pros, cons, and fears.

During the research and writing process of the thesis, it became apparent that while there are some differences in both legislation and implementation of personal information protection regulations and practices in EU and its Member States, China, and South Korea, there are far more similarities between the regulations and practices of the mentioned regions. The main differences come from exclusivity and rigorous standards. While exclusivity is more apparent in the systems affecting the EU and its Member States and South Korea, the rigorous standardization for the level of personal information security is relevant in all three regions but has mostly been implemented differently.

A foreign citizen should take note of how their access could be partially or mostly limited in the particular system they are trying to access or are accessing from. EU citizens should be aware that there are many sites and services they are no longer capable of using due to the respective sites and services not willing or capable of passing the GDPR audits. Non-South Korean citizens should be aware that their access unless staying in South Korea and having applied for an alien registration number, is likely to be extremely limited. Non-Chinese citizens should be aware that their information, will likely need to be legally stored (with consent) to Chinese data centers, in the event, that the information would leave the Chinese internet due to their rigorous standards regarding international data transfers.

It is important to note that the thesis has not touched all the aspects regarding the respective regulations and related practices and was mostly limited to personal information security. It is also important to note that some of the possible ways the regulations and practices have been implemented are not present in the thesis due to unavailability caused by the lack of broad real-life experience living within the respective regions to gain an even deeper understanding.

REFERENCES

DLAPIPER 2019, Jan 4, (updated)-last update. Available: https://www.dlapiperdataprotection.com/index.html?t=law&c=CN [2019, April 9,].

*EUR-Lex, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*2016, -05-04-last update. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [2019, May 28,].

IAPP; GDPR matchup: South Korea's Personal Information Protection Act, . Available: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/ [2019, Apr 9,].

Intersoft Consulting; General Data Protection Regulation (GDPR) – Final text neatly arranged, . Available: https://gdpr-info.eu/ [2019, Apr 9,].

Korean LII; Personal Information Protection Act, . Available: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf [2019, April 9.].

Bell R. & Liu Y. 2018, Jan 12,-last update*, The PRC Cybersecurity Law and its impact on the insurance sector;* Available: https://www.clydeco.com/insight/article/prc-cybersecurity-law-and-its-impact-on-the-insurance-sector [2019, April 9,].

Privacypedia; Cybersecurity Law of the People's Republic of China (CSL) | PrivacyPedia. Available: https://privacypedia.org/laws/china-cybersecurity-law/ [2019, May 4th,].