Università
Ca'Foscari
Venezia

Master's Degree in

Languages, Economics and Institutions of

Asia and North Africa

Second Cycle (D.M. 270/2004)

Final Thesis

China and Big Data Management

An analysis from individuals' to
foreign enterprises' perspective

Supervisor
Ch. Prof. Renzo Riccardo Cavalieri

Assistant supervisor
Ch. Prof. Diego Todaro

Graduand
Silvia Formusa
858451

Academic Year
2019/2020

Acknowledgements

With the writing of this thesis, the educational path I chose 5 years ago is coming to an end. From the very beginning, I have always been grateful for having the opportunity to study, to come into contact with great students and professors and to approach Chinese culture and society. This path presented different challenges, many joys and some sorrows; in some cases, my family and I had to renounce to something in order to obtain greater satisfactions lately. Even if they are aware of how much I appreciate their help, this is the occasion to finally write their names on paper.

First of all, I would like to thank Professor R.R. Cavalieri for his faith on my ideas and his helpfulness, and Professor D. Todaro for his patience and his precious advices, that guided me throughout the writing of this research.

And now, dear friends and family, this paper is dedicated to you.

It is for my entire family, that have encouraged my ambitions since I was very young. Thank you all for believing in me.

It is for my mother, the person who supported me the most in every second of this journey. Without her love, every difficulty would have appeared insurmountable.

It is for Gaia, Irene, Kejti and Miriam, the best roommates, friends and soulmates I could ever met in the world, that fill my days with happiness and support me in every moment. I love you.

It is for Petra and Gaia: one friend who has been next to me for years, and another one who managed to steal my heart in just six months. Thank you.

Last, but not least, this thesis is for Andrei. The person with the biggest patience in the world, that completes me, supports me and loves me more than I deserve. I am grateful for having you in my life.

Table of contents

前言

从一开始，大数据行业就是全球资源和激烈国际辩论的来源。事实上，许多国家最近几年来都实施新的政策是为了保护消费者的敏感信息和当地企业的知识产权。

最近，中国和别的国家一样开始进行现代化的过程和大数据保护的过程。根据中国政府的观点，大数据具有双重性: 它们一边有经济的重要性，一边有政治的重要性。首先，因为互联网的普及率增长了，所以网络犯罪率也提升了。实际上，大部分中国消费者至少经历过信息盗窃一次，并且他们也不太了解保护隐私法律的存在。

为了避免这些问题，政府正在努力保护中国消费者和他们的个人信息。然后，政府不仅以建立完整的立法权制定了《网络安全法》和《个人信息安全规范》， 而且打算把大数据与人工智能结合在一起。这样做，它的目标是在全球推动中国技术而构建有中国特色的数字经济。

通过《网络安全法》，中国在个人信息保护的方面成为了全亚洲的典范。除了美国规定与《欧盟数据保护通用条例》（GDPR）以外，还提出了第三个选择。

第二章与大数据的政治重要性有关。首先，值得注意的是几十年前政府通过单位、居委会和派出所开始管理工人、市民的个人信息和生活。这些例子说明在中国最重要的不是每个人的私生活，而是全社会的福祉。目前，这个想法还是中国人的特色。政府仍然使用居委会和爬出所是为了收集人们的个人信息，监视有犯罪记录的人，并且管理像疫情一样的困难时期。

2013 年以后，爱德华·斯诺登事件使中国政府担忧。事实上，斯诺登透露了美国和英国的特务机关秘密地监视许多外国人、外国公司和外国政府， 比如说安格拉 · 默克尔，巴西政府和中国企业。

2018 年，习近平主席宣布：《没有网络安全就没有国家安全，没有信息化就没有现代化》。句子的意思是国家安全、经济稳定性和社会公共利益都取决于网络和关键信息的安全。因此，数据本地化和数据转输等重要原则都放在《网络安全法》与《公安机关互联网安全监督检查规定》里。

另外，根据新的规定警察现在能够检查任何网络运营者， 审问经理，要求顾客、供应商与员工的文件和信息。这样做他们可以确定数据泄露对国家安全有多大的威胁。

最后，第三章的目的是详细地讲外国企业对中国数据本地化、跨境数据转输的原则有什么样的反应。一部分与中国合作伙伴成立了合资企业，另一部分依赖在中国拥有云计算数据库的中国第三方。所有的行业，所有的供应商、顾客和投资者都受这些法律的影响。

一方面，跨国公司可以通过许多可用的资源来改变它们的产业。另一方面，由于建立新云计算的成本特别高，有比较少资源的中小型企业受到处罚。并且，美国政府对中国政府获得公司信息和知识产权的机会非常担忧。

尽管目前大数据具有经济和政治的重要性，但是我们应该继续支持技术和人工智能的进步，促进关于数据的国际合而保持信息的自由周转。就是因为它们的财富，所有的国家与行业应该始终保证人们的敏感和私人信息。

最后，中小型企业为中国经济增长做出了贡献，并且在意大利它们占大部分的国家经济。国家应该经济上支持这种公司，是为了让它们克服政治和法律的变化，让它们继续在中国活动，而且避免它们去别的地方做生意。

Introduction

From the very start, the Big Data industry has been a precious resource and the cause of heated international debate worldwide. In a very brief period of time, they have silently changed the world, the society and habits around us. As their deployment continues to increase, many countries in recent years have contributed in implementing policies aimed at protecting consumers' sensitive information, as well as intellectual property rights of local enterprises. China as well has started a process of modernization and protection of Big Data.

This research finds its own origins from the necessity to answer some questions about the dichotomy the Chinese government has showed several times when dealing with Big Data and adopting related regulations: how can China promote customers data protection and, at the same time, justify the access of officials to sensitive data of both citizens, private and public enterprises? How can this dichotomy find an explanation? Can Big Data protection and cyber-sovereignty coexist? And how can foreign enterprises and foreign network operators collaborate with Chinese partners and security officials?

In order to answer these and many other questions, I decided to divide the thesis into three different chapters. The first one dealing with Big Data as an economic power, the second chapter introducing Big Data as a political power were useful to understand the essence of data and personal information. Lastly, the third chapter through the analysis of the relations between foreign companies and Big Data management in China, aimed at providing a practical and concrete point of view.

First and foremost, with the rise of the Internet, cybercrimes have increased exponentially. As a matter of fact, most Chinese consumers have experienced information theft at least once, and they do not have a good understanding of privacy laws. In order to address these problems, the government is working to protect Chinese consumers and their personal

information: not only did it formulate the Cyber Security Law and the Personal Information Security Specification, creating a complete legislative framework, but it also plans to combine Big Data with artificial intelligence. By doing so, it aspires to globally promote Chinese technology and build a digital economy with Chinese characteristics.

Thank to the comprehensiveness of the Cyber Security Law, China has been classified a model in the protection of personal information all over Asia. Additionally, it has created an alternative to the American sectorial system and to the GDPR adopted by the European Union.

The second chapter tackles the political importance of Big Data. Firstly, it is worth noting that several decades ago, the government already began to manage personal information and life of workers and citizens through work units, neighborhood committees and local police stations. These examples clearly show that in China, the individual's private life is perceived as less important than the well-being of the whole community. To this day, this mentality still prevails among the Chinese, and the government still uses neighborhood committees and police stations to collect people's personal information, monitor individuals with criminal records and manage complex emergencies like the pandemic.

After 2013, the Snowden case deeply impacted and worried the Chinese authorities. The scandal revealed that the American and British secret services were secretly spying on many foreign enterprises, governments and people, with examples ranging from Angela Merkel to the Brazilian government and Chinese enterprises. In 2019, President Xi Jinping stated that ''without cyber security, there is no national security and without informatization, there is no modernization''; thus, national security, economic stability and social and public interests all depend on cybersecurity and on the correct management of critical information. For this reason, the crucial principles of data localization and data transfer are both present in the Cyber Security Law and in the Regulation on the Internet Security Supervision and Inspection. In addition, according to the new rules, the police are allowed to inspect any network operator, interrogate

managers and request documents and information from clients, suppliers and employees, all to determine the actual threat that a data leak could pose to national security.

The purpose of the third and last chapter is to describe in detail how foreign enterprises respond to the principles of data localization and cross-border data transfer in China. Some have established joint ventures with Chinese partners, while others rely on Chinese third parties with local cloud computing databases. Overall, all industries, suppliers, customers and investors are affected by these laws. On one hand, multinational corporations can change their business models thanks to their several available resources, while on the other, due to the high cost of building new cloud computing, small and medium-sized enterprises with less resources are at a disadvantage.

CHAPTER 1

Big Data as an economic value

1.1 Big Data, AI and cybersecurity.

During the 21st century or the so-called "century of data", through the progress achieved in IoT technologies, artificial intelligence (AI) and the use of Internet worldwide, the availability and complexity of sources of data[1] increased exponentially. As a consequence, the concern over people's privacy and over information security on a national and business level increased as well.

Definition and examples of Big Data

Big Data is commonly defined with the following three main attributes, known also as the 3 "Vs": first, it consists of "high-volume" sets of data since generated from a large scale of sources like transactions, social media, television, sensors, texts, user clicks and many others. Secondly, it is "high-velocity" information because they need to be collected, stored and analyzed instantaneously. The third characteristic is "high-variety": data can be divided into structured and unstructured forms. Structured data are information stored in traditional databases like numeric data, whereas unstructured formats are e-mails, documents, videos and different types of media[2]. The scope of data analytics embraces a huge variety of sectors from expanding market knowledge about costumers' insights to improving healthcare and educational systems and securing financial services by tracking frauds or monitoring assets. Looking in deeper details, specific sources of data have gained relative importance and more and more enterprises are interested in mastering them and gaining a competitive position in

[1] https://www.ibm.com/analytics/hadoop/big-data-analytics (2020-03-10).

[2] Nir KSHETRI, Big data's impact on privacy, security and consumer welfare, *Telecommunications Policy*, 38(11), 1134-1145, 2014.

their respective industry. For instance, in recent years, the role of transaction data[3] has become fundamental in data analytics, since they trace almost every aspect of the business process and combined with the click stream, they both create massive volumes of information[4]. Other elements strictly related to the rise of transaction data are the emergence of e-commerce platforms, the usage of mobile devices and new online financial trading providers. The analysis of this typology of information and its integration with other real-time data will help companies enrich services, gain costumers' loyalty and satisfaction and reduce risks[5].

In this century, also social media data or social data has developed rapidly and has grown into an incredibly valuable source for businesses, sociologists and governments. This is due to the fact that billions of people have access to social network websites every day. In 2018, major platforms such as Facebook, Instagram and Wechat registered respectively more than 2 billion and one billion users each, and TikTok, a Chinese social media app sharing short videos, from 2016 to 2018 recorded almost 20 million new registrations per month[6]. Such a big participation of the population in leisure activities online provides a precious occasion to analyze people's behavior, preferences, and other social phenomena, that are useful to enterprises in strategic advertising or marketing research but also in the enhancement of sectors like education and national security. Moreover, social media data are modifying even the development of data storage infrastructure, which have to be sufficiently spacious, as in the case of Facebook data centers in Sweden, whose dimension is equivalent to 11 football fields, or in the efficiency of algorithms in the processing phase, in order to forecast a potential

[3] *Transaction data* are that information related to the registered transactions of a company. They concern the type of product sold or bought, its quantity, details about payments, suppliers and clients. They can be linked even with the financial and logistic sphere.
[4] Mike FERGUSON, Big Data – Why Transaction Data is Mission Critical to Success, Intelligent Business Strategies, 2014, p. 6.
[5] Mike FERGUSON, Big Data – Why Transaction Data is Mission Critical to Success…, Cit., p. 10.
[6] Esteban ORTIZ-OSPINA, The rise of social media, Our World in Data, 2019. Available at: https://ourworldindata.org/rise-of-social-media (2020-03-15)

behavior or threat[7]. The concentration of citizens' personal information into social media apps has raised concerns and critics at an international level, especially in the US government. For this reason, in recent years, the Committee on Foreign Investment in the United States (CFIUS) investigated the acquisition plans, that according to the White House, could harm national security and the safety of data. Some examples, that could have been further deteriorated by the long-lasting disputes between China and the US, are the intervention of CFIUS in Alibaba Ant Financial project of purchasing MoneyGram International or the national security review of TikTok platform and its owner Beijing ByteDance Technology started in 2019, due to the US government suspicion that almost 110 million American users' information held by the social media could be stored and used by Chinese intelligence[8].

Big Data-driven economy

Except for representing an instrument for the development of society, the Big Data industry has taken on a valuable role, particularly in the market economy: studies have found that its collection and usage can make organizations more efficient, optimizing resources allocation, facilitating adaptability and helping them become more competent in directing promotions to customers[9]. For instance, McKinsey Global Institute in 2013 stated that annually big data provide an estimated economic gain of $610 billion in productivity and cost savings worldwide[10]. Also, governments all over the world such as the United States, the European Union and others recognized the importance of a data-driven economy and more and more countries have expressed interest in developing this industry to gain national competitiveness[11].

[7] Vikas DHAWAN, Nadir ZANINI, Big data and social media analytics, Research matter: A Cambridge Assessment Publication, 2014, p. 39.
[8] US investigating TikTok owner ByteDance over US$1 billion acquisition of social media app Musical.ly, South China Morning Post, 2019. Available at: https://www.scmp.com/news/china/article/3036012/ (2020-03-15).
[9] Nir KSHETRI, Big data's impact on privacy, security and consumer welfare, cit., pp. 6-7.
[10] Nir KSHETRI, Big data's impact on privacy, security and consumer welfare, cit., p. 2.
[11] Tao FU, China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent; *Global Media and Communication*; 2019, Vol. 15(2) 195-213.

As an example, the Data Driven Marketing Institute published a report showing that in 2014 the Data-Driven Marketing Economy (DDME) created almost 1 million jobs in the US and the country's economy registered an increase in revenue of 202 billion dollars[12]. Furthermore, in the same year, the European Union promoted the Big Data Public Private Forum that is aimed at encouraging scholars, firms and stakeholders to study and invest on big data[13]. Once the relevance of this area of interest has been highlighted, much effort has to be spent in order to implement data science programs in universities and create enough data analytics professionals to meet the high demand of the industry, which is in particular shortage in recent years. Additionally, some companies like Cisco Systems have established data education programs inside the company itself with the collaboration of professors coming from Washington and North Carolina State University to develop employees' skills and compensate the lack of talents[14].

Integration of Big Data with AI technology

The progress of Big Data analytics is also strictly related to the frontier technology of artificial intelligence 人工智能 *rengong zhineng*. It can be conceived as a system of integrated technologies, that is able to collect and analyze larger amount of information, has self-correction abilities and uses statistics and algorithms to improve performances and follow principles of logical reasoning.[15] As a consequence, governments are starting to rely on AI not only to increase countries' wealth and employment or to provide benefits in a variety of industries, but also to develop more capable control instruments. As we will see in deeper

[12] John DEIGHTON, A. J. PETER, The value of data: Consequences for insight, innovation & efficiency in the US economy. The Data Driven Marketing Institute, 2013.
[13] Vikas DHAWAN, Nadir ZANINI, Big data and social media analytics…, cit., p. 37.
[14] Big Data, Big Problem: Coping with Shortage of Talent in Data Analytics, business.com, 2016. Available at: https://www.business.com/articles/big-data-big-problem-coping-with-shortage-of-talent-in-data-analysis/#:~:text=Big%20Data%2C%20Big%20Problem%3A%20Coping,of%20Talent%20in%20Data%20Analysis&text=Big%20data%20is%20a%20big%20deal.&text=According%20to%20a%202015%20MIT,starting%20to%20look%20even%20bleaker. / (2020-03-15).
[15] Steven FELDSTEIN, The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 2019, p. 6.

details, according to Feldstein, 43% of nations in the world are actively deploying these technologies, including three main tools such as smart cities, smart policing and facial recognition (人脸识别 *Renlian shibie*)[16]. The former implies the transmission of real-time data to ease authorities in safeguarding the population and facilitate the management of the city. Smart policing is the result of a broader concept, which mixes together biometric data[17], previous illegal acts, geographic location and social media information in order to predict future behavior and react promptly. The latter is a biometric technology that collects past or live images and videos and associates them to those stored in the database[18]. Electoral autocratic and closed autocratic countries, as well as democracies adopted that kind of surveillance apparatus, but in the case of the last category, the balance between the need of security and civil privacy protection urges and must be respected. Except for this specific usage, artificial intelligence contributes to many other applications in the automotive, entertainment, logistics, healthcare, luxury and retail, through self-driving technologies, predictive capacities, emotional intelligence and natural language processing with speech recognition, etc.[19] In recent days, particular interest has grown towards the deployment of AI in healthcare, and especially in the tackle of Coronavirus or COVID-19. Algorithms have been already contributing in administrative processes or in diagnosing illnesses, but robots have been gradually collaborating with human staff. For instance, in order to fight the present global emergence, Tampa General Hospital in Florida developed an AI system that analyzes visitors' conditions with facial scan, Brigham and Women's Hospital and Massachusetts General Hospital are considering to use robots to reduce human contact, following the model of Wuhan Wuchang

[16] Steven FELDSTEIN, The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 2019, p. 6.
[17] According to the European Commission, biometric data comprehends all the information linked to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, DNA or dactyloscopy. Available at: https://ec.europa.eu/.
[18] Steven FELDSTEIN. The Global Expansion of AI Surveillance…, cit., pp. 16-21.
[19] Robert ADAMS, 10 Powerful examples of Artificial Intelligence in Use Today, 2017, Available at: https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificial-intelligence-in-use-today/ (2020-03-17)

Hospital that uses robotic personnel to deliver food and medicine, disinfect and measure temperature and install smart bracelets to patients in order to monitor their health[20].

Data breaches and personal information privacy rights

Along with the increasing amount of collected information, concerns over individual privacy violations and breaches in security systems are growing as well. Evidences show an increase of data theft in the United States from 2005 with 157 million cases to 1.47 billion in 2019, some of the biggest violations comprehend the 2018 security breach of a sales intelligence firm called Apollo involving almost 9 billion data points and the notification of Yahoo, a web service provider, which in 2014 and in 2013 reported two cyber-attacks that affected 500 million and 1 billion users respectively[21]. As a consequence of the exposure of people's information online, several studies in Australia, in the US and in the UK proved that people's highest levels of concern were caused by the fear of crimes like identity theft and fraudulent activities with consequent feelings of impotence, threat of reputational damage, loss of privacy and other ethical issues[22]. In his research, Professor Kshetri confirmed that the inappropriate use of data from institutions and companies may cause serious consequences like psychological, social and economic harm. As a result, consumers are becoming more and more aware and resistant to some organizations' data collection methods like GPS trackers and cookies[23].

Generally speaking, personal information privacy should always be guaranteed and safeguarded as a fundamental human right; however, the association of these two rights is relatively recent

[20] Kelley A. WITTBOLD, Colleen CARROLL, Marco IANSITI, Haipeng M. ZHANG, Adam B. LANDMAN, How Hospitals Are Using AI to Battle Covid-19, *Harvard Business Review*, 2020, Available at: https://hbr.org/2020/04/how-hospitals-are-using-ai-to-battle-covid-19 (2020-04-04).
[21] J. CLEMENT, Cyber crime: biggest online data breaches as of 2020, 2020. Available at: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/#:~:text=The%20biggest%20data%20breach%20as,companies%20and%20organizations%20were%20revealed. (2020-03-17).
[22] Lynne D. ROBERTS, David INDERMAUR, Caroline SPIRANOVIC Fear of Cyber-Identity Theft and Related Fraudulent Activity, Psychiatry, Psychology and Law, Vol. 20, 2013, pp. 315-328.
[23] Nir KSHETRI, Big data's impact on privacy, security and consumer welfare, cit., p.11.

and is still subject to several elaborations[24]. At the same time, it represents a commodity for both governments and businesses. For this reason, each government has to find a balance between protecting individuals and building a strong economy[25]. In order to achieve this goal, inadequate regulations should be improved and regularly updated since the big data industry is extremely wide and in continuous development. Many organizations tried to contribute in this field by elaborating general guidelines concerning data protection and privacy issues. The most active role was played by the Organization for Economic Cooperation and Development (OECD), which published the Guidelines on the Protection of Privacy and Transborder Flow of Personal Data in 1980. Nowadays, these documents provide the basic principles from which each country can create or renovate national regulations and enforce international cooperation[26]. In 2004, 21 member economies of the Asia Pacific Economic Cooperation (APEC) developed a Framework for Information Privacy Protection and in 2010 a group of privacy enforcement agencies called Global Privacy Enforcement Network (GPEN) was established in order to facilitate privacy enforcement authorities worldwide[27].

[24] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China, Policy Department C, Citizens' Rights and Constitutional Affairs, European Parliament, 2015, p. 7.
[25] Tao FU, China's personal information protection in a data-driven economy…, cit., p. 2.
[26] Hanhua ZHOU, *Consumer Data Protection in Brazil, China and Germany: a comparative study*, Göttingen University Press, 2016, pp.135-136.
[27] Hanhua ZHOU, *Consumer Data Protection in Brazil, China and Germany…*, cit., pp.141-147.

1.2 China and Big Data.

Internet in China

In 1994, the Institute of High Energy Physics at China's Academy of Sciences built its first cable connected to the World Wide Web and created an e-mail communication with Europe and the US[28]. Therefore, China became the 77th country to access the Internet. In more than 20 years, China's overall number of netizens hit 854 million and 99.1% of them are mobile phone users[29]. In 2016, 110 million people were able to receive secondary and tertiary education online, 152 million benefited from online medical services[30] and statistics show that in 2018 around 73.6% of netizens shopped online[31]. As it was previously stated in the example of the United States, the digitalization had great impact on the economies of the world and it rapidly reached developing countries such as China. In 2018, the digital economy in the nation incremented its size of nearly 21%, constituting the 34.8% of total GDP, and hopefully it will provide opportunities for Internet-based innovations in the entire world[32].

The massive impact Internet has on the Chinese and the development of new technologies both represent a strategic tool for the government, which strives to play the part of protector of the people, as well as the inspector of their behavior. In order to carry out this dual role, it built a complex cyber internal security surveillance system, whose main target are Chinese citizens, workers and the members of the Chinese Communist Party (CCP)[33]. President Xi Jinping himself delivered a speech during the National Meeting in Cybersecurity and Informatization in 2016, where he stated that cybersecurity is made for people and relies on the

[28] Ning ZHANG, 1994 China access to the Internet, CCTV.com, 2019, available at: http://www.cctv.com/english/special/60anni/20090907/110334.shtml (2020-03-18).
[29] Xia XIAO, China has 854 mln internet users: report; 新华网 *Xinhuawang*, 2019, available at: http://www.xinhuanet.com/, 2020-03-18.
[30] http://www.chinadaily.com.cn/china/2016even/index.html
[31] Agne BLAZYTE, Penetration rate of online shopping in China 2008-2018, 2019. Available at: https://www.statista.com/ (2020-03-18).
[32] Rising Innovation in China, *China Innovation Ecosystem Development Report 2019*, Deloitte China, 2019, p. 4.
[33] Greg AUSTIN, *Cybersecurity in China. The next wave*, Springer Briefs in Cybersecurity, 2018, p. 2.

responsibility of the entire society, from the government and organizations to Internet users[34]. The profound bond between information security and national security emerged several times in official statements and it was further confirmed by the establishment of the Central Leading Group for Internet Security and Informatization headed by President Xi Jinping, whose aim is to manage the entire online sector of the whole country[35]. This decision highlights the Chinese government's awareness that data constitutes the tool for creating a strong and secure environment[36].

AI and Big Data in contemporary China

In China, both the continuous innovation of technologies such as artificial intelligence (AI) and their implementation with Big Data (大数据 *dashuju*) in the everyday life, significantly improved services and several aspects of the society. In 2012, among the 22 Chinese provinces, Guizhou in particular was appointed as the "data valley" region, thanks to its mild climate, adequate power supply and network infrastructure like big data transaction and cloud service centers. It has hosted China International Big Data Industry Expo for five years, which has seen the participation of many national and international Big Data firms, contributing to the improvement of Guizhou's economic and social conditions[37]. Also the AI industry is attracting many foreign investors and it is developing at a very fast pace in some of the most prosperous regions of the country. In fact, the tier-one cities Beijing, Shanghai, Shenzhen (Guangdong province) and Hangzhou (Zhejiang province) house not only the majority of the top 100 Chinese internet companies, but also the 80% of the total amount of unicorn

[34] Greg AUSTIN, *Cybersecurity in China. The next wave*…, cit., p. 6.
[35] Rogier CREEMERS, Central Leading Group for Internet Security and Informatization Established, *China Copyright and Media*, 2014. Available at: https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/ (2020-04-03).
[36] Emilio IASIELLO, China's Cyber Initiatives Counter International Pressure, Journal of Strategic Security 10, no. 1, 2016, p. 2.
[37] Xia LI, Big Data prospering in southwest China's Guizhou, *Xinhua News*, 2019. Available at: http://www.xinhuanet.com/english/2019-08/09/c_138297001.htm /, (2020-04-04).

companies[38] of the entire nation, most of them received Tencent and Alibaba's investments[39]. The extent of resources deployed by these cities permitted the attraction and retaining of more than a half of the overall artificial intelligence talents in China, which are extremely rare and precious, especially considering the current global shortage[40]. As a result, AI technologies together with Big Data provide enormous advantages since they enable to collect and analyze larger volumes of information, the more data is integrated and the more these instruments will be predictive[41].

The most impressive example of the integration of Big Data with AI technologies, cloud computing and information systems can be found in Chinese smart cities. Due to the 20th century urbanization and technological innovation, smart city (智慧城市 *zhihui chengshi*) campaigns took place in many parts of China, including metropolis like Beijing, Shanghai, Hangzhou, Shenzhen, Wuhan (Hubei province), Guiyang (Guizhou province), Chongqing and Chengdu (Sichuan province), that count between 6 million and 20 million inhabitants. According to Yang and Xu (2018), the development of smart cities started in 1998, when nearly 300 cities, called "digital cities", introduced the digitalization of geo-location information[42]. In 2005, with the implementation of Internet infrastructure and wireless technologies, they were replaced by "Internet cities" or "wireless cities". Finally, in 2018, "sensor-networked smart cities" begun to use sensors and artificial intelligence in transports, healthcare, commercial services etc. The huge amount of data collected in smart cities is originated from the interaction citizens have with sensors, Wi-Fi and other technologies and it is useful to analyze geo-location, improve government control and create economic value[43]. Many other experiments and projects

[38] *Unicorn companies* are namely those extremely successful businesses valued at over 1 billion dollars.
[39] Rising Innovation in China, China Innovation Ecosystem Development Report…, cit., p. 20.
[40] Rising Innovation in China, China Innovation Ecosystem Development Report…, cit., p. 24.
[41] China Advances in AI with Big Data Development, *Global Times*, 2019, available at: https://www.globaltimes.cn/content/1140825.shtml#:~:text=According%20to%20the%20development%20plan, by%202030%2C%20People's%20Daily%20Overseas (2020-04-04).
[42] Fan YANG, Jian XU, Privacy concerns in China's smart city campaign: the deficit of China's Cybersecurity Law, *Asia Pacific Policy Stud*., 2018, p. 535.
[43] Fan YANG, Jian XU, Privacy concerns in China's smart city campaign: the deficit…, cit., pp. 536-537.

have been tested in different smart cities, which are aimed at tackling social and environmental issues[44]. Moreover, the relevance of smart city campaigns was further highlighted in 2011, when their development was strongly encouraged in the 12th Five Year Plan (2011-2015) 《国民经济和社会发展第十二个五年规划》（"十二五"规划"）*"Guomin jingji he shehui fazhan dishi'er ge wunian guihua" (shi'er wu guihua).* However, the government is aware that such a huge exchange and collection of information determines also big threats both for individuals and institutions[45].

Nevertheless, one of the benefits obtained through the innovation of Big Data industry undertaken by smart cities is how authorities managed to cope with the spread of COVID-19 in China. In order to contain the diffusion of the virus, technicians installed thermal scanners at train stations in major cities and transport authorities tracked every traveler's information and seat in the wagon. Using collected personal data was extremely useful in rapidly alerting passengers who were travelling with an infected person. Moreover, nearly 200 million security cameras all over the country constitute an expansive surveillance system, which is further reinforced by the "real-name" system[46]. It requires Chinese citizens and foreigners living in the country to use ID cards or passports, when using social media or purchasing any kind of goods, from plane tickets to medicines. According to a draft published on the 10th of February 2020 by the supervisor of the State Administration of Market Regulation 国家市场监督管理总局主管 *Guojia shichang jiandu guanli zongju zhuguan*, pharmacies in the city of Shenzhen have to send personal information and mobile number of every customer who buys cough or fever

[44] Max PARASOL, The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams, Computer Law & Security Review, Vol. 34, 2018, pp. 68-70.
[45] *Ibid*.
[46] Shawn YUAN, How China is using big data to fight coronavirus, *Aljazeera News*, 2020. Available at: https://www.aljazeera.com/news/2020/03/01/how-china-is-using-ai-and-big-data-to-fight-the-coronavirus/#:~:text=Other%20ways%20in%20which%20China,with%20a%20confirmed%20coronavirus%20carrier. (2020-04-06).

drugs[47] to authorities. Another way big data is used by local jurisdictions to know if quarantine has been respected is mobile phones' geo-localization. Telecommunication companies like China Mobile can provide doctors, police and employers a very detailed "travel history" of the patient's movements in the last 14 days. A text message will be sent to the user's phone and, according to the cities visited, a quarantine time will be recommended[48].

As both the success and economic value of Big Data increase, AI technologies are also growing and accelerating worldwide. The vast availability of information in China allows data-intensive instruments like AI tools and infrastructures to develop faster and more efficiently. Actually, these instruments have already been integrated to a large variety of industries and businesses in the country and registered an investment size of more than RMB130 billion[49]. A study published by Deloitte Research shows that higher education institutions like academies and universities as well as big internet companies are home of R&D laboratories of AI technology: in Beijing, major firms like Baidu, Xiaomi, Meituan, JD.com, Jinri Toutiao established their own laboratories and had been investing large amount of capitals. In Shanghai, the research is mainly led by institutions like Shanghai Jiao Tong University, Fudan University and Shanghai Tongji University, even if many private players are also active in the region[50]. Similarly, Tencent, ZTE and Huawei are massively investing in AI science in Shenzhen, but the government has intervened as well by building Shenzhen Academy of Robotics and Shenzhen Institute of Artificial Intelligence and Big Data. On the contrary, Alibaba, one of the leading technology companies chose Hangzhou to establish its research laboratories.

[47] 国家市场监督管理总局主管, "Tongzhi! Zai Shenzhen yaodian mai fare kesou yao, xu shimingzhi bing ce tiwen" 通知！在深圳药店买发热咳嗽药，须实名制并测体温 (Notice! Pharmacies in the city of Shenzhen that sell fever or cough medicines must deploy the real-name system and measure people's temperature.) *Zhongguo zhiliang xinwenwang*, 2020, Available at: http://www.cqn.com.cn/zj/content/2020-02/10/content_8168365.htm (2020-04-05).
[48] Shawn YUAN, How China is using big data to fight coronavirus…, cit.
[49] Rising Innovation in China, China Innovation Ecosystem Development Report…, cit., p. 31.
[50] Rising Innovation in China, China Innovation Ecosystem Development Report…, cit., p. 36.

The industry of airlines started using big data through the creation of passengers' information system and the introduction of AI tools in regular services in 2016. The construction of a massive information database let China Eastern Airlines win the China's first Civil Aviation Internet Security Protection Skill Competition and the China Southern Airlines' implementation of facial recognition facilitated the access to flights, ID control procedures, real-time surveillance and the process of tracking citizens by security agencies[51]. Furthermore, particular attention should be payed to SenseTime company, a Chinese technology giant, which managed to enter with its products sectors like retailing by improving marketing precision and costumers' experience, smartphones industry with facial unlocking, smart beauty and filters, healthcare with medical image recognition, automotive etc[52]. However, the concentration of such a huge amount of information in few companies and laboratories arises concerns about the efficiency of customers' privacy security systems in case of breaches of costumers' information and biometric data.

Privacy infringements, causes and remedies

Despite all the innovations and investments China is making in the Big Data industry, which improved many services towards society, citizens are still subjected to regular violations of personal privacy. According to a report made by a Chinese internet security company called Qihoo 360, in 2016, 14 million malware attacks were registered in Android platforms, 74% of which used victims' funds, users received 17.35 billion spam messages, of which 4.2% were "illegal" and 2.8% were scams, 20,000 users all over the country reported monetary losses of 195 million RMB, accounting for 9471 yuan per person and lastly, unlawful use of smart cameras increased[53].

[51] Greg AUSTIN, *Cybersecurity in China. The next wave*…, cit., p. 73.
[52] Rising Innovation in China, China Innovation Ecosystem Development Report…, cit., p. 35.
[53] Greg AUSTIN, Cybersecurity in China. The next wave…, cit., p. 83.

Frequent breaches of information in a country like China, that aims to excel in IT and the Big Data sector globally, represent a big threat for the government and its population and international customers as well. The actual situation could be a consequence of the fact that before the beginning of the informatization process at the end of the 20th century, concepts like consumer's right protection and personal information were almost unknown in China[54]. Nowadays, the country presents a meaningful fragmentation in terms of citizens' internet security awareness, but many netizens are progressively getting conscious of the risks they are exposed to. Austin G. (2018) mentioned a study made by China Ceprei Laboratories[55], which tried to explain how the need for cyber security is perceived differently according to the type of users' group (government, corporations and individuals) and the city where they are located. In megacities like Shanghai and Beijing, was reported a lower extent of individual cybersecurity precaution and as a result, more attempts of financial frauds. On the contrary, citizens of Lhasa, in the Autonomous Region of Tibet, seem to have a higher cybersecurity awareness, since many users registered lower level of vulnerabilities by using PC and mobile Trojan kill and defense mechanisms against phishing[56]. Moreover, prompted by the increasing anxiety of its consumers, Alipay, one of the biggest payment apps in China, had to publicly assure that the images collected by its facial recognition system couldn't in any case be used by criminals for online frauds[57].

The previously mentioned massive surveillance system used by the government to contain the epidemy and the application of facial recognition in every-day occasions like payment methods in supermarkets, together with the great amount of violations to which Chinese population is subjected, are raising concerns about privacy infringements, the typology

[54] Hanhua ZHOU, Consumer Data Protection in Brazil, China and Germany…, cit., p. 40.
[55] National Engineering Laboratory of Big Data Collaborative Security Technology, National Engineering Laboratory of Big Data Application Technology to Improve Governance, China Ceprei Laboratories, Key Laboratory of Big Data Strategy.
[56] Greg AUSTIN, *Cybersecurity in China. The next wave*…, cit., p.82.
[57] Chinese netizens get privacy-conscious, About Face, *The Economist*, 2019. Available at: https://www.economist.com/business/2019/09/07/chinese-netizens-get-privacy-conscious (2020-04-10).

and amount of data collected and how efficiently jurisdictions are safeguarding people's information. The government has entitled itself to collect and control citizens' information but simultaneously protect them from private actors. For this reason, the China Cybersecurity Center have recently denounced 100 apps belonging to companies coming from different industries like e-commerce or banking, which were not respecting data collection rules or lacked agreements on privacy issues[58]. Despite this significant intervention in support of the population, the actual main obstacle is the Chinese highly decentralized administration structure of personal information protection. Due to its nature, it presents some difficulties in identifying accountability and deteriorates communication among departments that supervise and enforce information protection related only to their sector[59]. The vagueness of liability and scarcity of people's information security were demonstrated to be the principal impediments to online business from 1999 to 2002, thus influencing nearly 30% of enterprises and business users[60].

Social Credit System

One last surveillance mechanism concerning Big Data and AI innovation in China, called Social Credit System (SCS) 社会信用体系 *shehui xinyong tixi*, is raising debates on privacy protection right among its citizens and international players. In ancient China, the word "credit" was associated to virtues linked to individual morality and ethics, which have been inherited from the Mandate of Heaven (天命 *tian ming*) and consequently, from the Confucian tradition. Lately, in modern society this term has assumed financial and economic significance, relating to an agreement where the borrower receives a good immediately and pays it in a later date[61]. Credit rating systems were created all over the world to measure the financial creditworthiness

[58] Celia CHEN, China Punishes 100 Apps Breaches of Personal Information as Consumer Anxiety Rises Over Privacy, South China Morning Post, 2019. Available at: https://www.scmp.com/tech/apps-social/article/3041217/china-punishes-100-apps-breaches-personal-information-consumer (2020-04-11.)
[59] Hanhua ZHOU, Consumer Data Protection in Brazil, China and Germany…, cit., p. 68.
[60] Greg AUSTIN, *Cybersecurity in China. The next wave*…, cit., p.120.
[61] https://www.investopedia.com/terms/c/credit.asp (2020-03-26).

of players. In the 21st century, the implementation of the Social Credit System in China goes further the economic concept developed for instance in the United States, comprehending also government and judicial affairs, social activities and the commercial sphere[62]. It aims at monitoring the trustworthiness of organizations, firms, citizens and even government members through the centralization of huge amounts of data and the construction of a countrywide surveillance infrastructure[63]. The Planning Outline for the Construction of a Social Credit System (2014) sets by the end of 2020 the fulfillment of SCS and the creation of a blacklist-system program. Its final objectives are developing the market economy, stimulating citizens' integrity and sincere behaviors and getting rid of political scandals in the highest ranks of society. These goals will be achieved through the assignment of rewards and punishments, such as the impossibility to travel on high-speed trains or first-class flights, get visas or make luxury purchases online, according to the score obtained or whether an individual belongs to a blacklist[64]. Few information is given about the methods of people's evaluation, but as R. Creemers (2018) states in his study, private agencies like Ant Financial Group, which developed Sesame Credit, base data scores according to traditional financial credit scoring systems, behavioral trends online, trustworthiness in agreements, willingness to share verifiable personal information and manners in which people create social relationships on the platform[65]. Nowadays, the SCS can't be defined as an integrated program, because it is still fragmented, communication among government departments is scarce and it partially depends on collaborations with credit scoring systems of private businesses like Alibaba or Baidu[66]. Furthermore, the SCS fragmentation could be related also to significant differences in wealth

[62] Fan LIANG, Vishnupriya DAS, Nadiya KOSTYUK, and Muzammil M. HUSSAIN, Constructing a data-driven society: china's social credit system as a state surveillance infrastructure, Policy and Internet, Vol. 10, n. 4, 2018, p. 431.
[63] *Ibid*.
[64] Rogier CREEMERS, *China's Social Credit System: An Evolving Practice of Control*, University of Leiden, Van Vollenhoven Institute, 2018, p. 7.
[65] Rogier CREEMERS, *China's Social Credit System: An Evolving Practice of Control*…, cit., p. 22.
[66] Rogier CREEMERS, *China's Social Credit System: An Evolving Practice of Control*…, cit., p. 27.

and technological development between local jurisdictions, which are doing their best to be in compliance with newly announced official plans. In the near future, the Social Credit System and broader surveillance plans announced by the government, could meet some resistance of a large portion of the population and criticism by international media and institutions like Human Right Watch, which already denounced how the SCS is likely to prevent people to express their political[67] or religious beliefs.

[67] Rogier CREEMERS, *China's Social Credit System: An Evolving Practice of Control* …, cit., p. 19.

1.3 Relevant regulations

The increase of the relevance and exploitation of Big Data industry, has raised concerns about which is the most complete and adequate set of regulations adopt in order to better protect people's information. Worldwide, the first national data protection law was enacted in 1973 in Sweden, shortly thereafter, in the 1970s, the U.S. published some principles regarding this topic, but due to the fragmented structure of the American government, a comprehensive regulation was never developed. During the Council of Europe Convention 108 in 1981, the first European legally binding paper, concerning the protection of individuals' personal data, was approved internationally and its aim was to safeguard people's freedom and rights to privacy[68].

Compared to western countries, China started developing regulations for the protection of personal information much later. This delay could be relatable to the nature of Chinese culture itself, which is categorized as a highly collectivist country according to the Hofstede model of cultural dimensions[69]. It explains that, in order to reach a good for the entire population, collectivist societies are more likely to permit the sharing of personal information and not to feel threatened by the government scrutiny. Thus, it could be possible that at first, Chinese netizens didn't feel the necessity to protect their information online, whereas more individualistic nations like the members of the European Union, started this process earlier[70]. Despite this explanation, other collectivist countries, that were highly influenced by Chinese traditions in the past, such as Taiwan and Hong Kong present extremely advanced data protection sets of laws. For this reason, some scholars believe that the development of privacy protection undertaken by EU and US in 1970s was precluded to China due to the particular

[68] Personal data protection, Fact Sheets on the European Union, 2020, available at: https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection

[69] For further information about Hofstede's Cultural Dimensions: Hofstede, G., & Bond, M. H., Hofstede's Culture Dimensions: An Independent Validation Using Rokeach's Value Survey, Journal of Cross-Cultural Psychology, 15(4), 1984, pp.417–433.

[70] Patrick E. SHARBAUGH, Phan Thi Le TRANG, What's Mine Is Yours: An Exploratory Study of Online Personal Privacy in the Socialist Republic of Vietnam, 2013, p. 4.

political conditions of those years[71], characterized by the uncertainty and disorder created after the Cultural Revolution, Mao Zedong regime and the accession to power of Deng Xiaoping's government after Mao's death.

At the beginning of data privacy development in China, the government approach, called also "cumulative effect", was similar to the one adopted by the US, opting for a sector-specific legal framework rather than a comprehensive regulation like the one offered by the European Union[72]. Taking this direction brought some negative consequences to the overall management system of the country such as protection limited just to specific regions and departments, dispersive provisions concentrated in many laws and complications of accountability between different ministries and administrations. At the same time, its framework distinguished from the other existent models and was built so as to preserve some "Chinese characteristics": first, it refers mainly to consumers and not to citizens; second, it draws a distinction between privacy from private players, who are subjected to strict controls and punishments by competent authorities, and privacy from the central government, in order to be in compliance with the fundamental principle of cyber-sovereignty of the State[73]. However, in recent years, it seems that the country is moving closer to the EU model, that is providing a general data protection law embodied by the Cybersecurity Law of 2017 and two correlated non-binding documents[74].

Constitution of 1982

A basic concept of privacy and personal dignity first appeared in the Chinese Constitution of 1982, more specifically in Article 38 and 40. The former states that human dignity must be respected and every kind of defamation is forbidden, the latter provides formal

[71] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way between the U.S and the EU?, *Penn State Journal of Law and International Affairs*, vol.8.1, 2020, p. 15.
[72] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China, Policy Department C, Citizens' Rights and Constitutional Affairs, European Parliament, 2015, p 14.
[73] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 4.
[74] The Guideline for Internet Personal Information Security Protection (2019) and the Information Technology – Personal Information Security Specification (2018).

protection to the freedom and privacy of correspondence and the intervention of authorities in case of illegal behaviors[75].

《第三十八条　中华人民共和国公民的人格尊严不受侵犯。禁止用任何方法对公民进行侮辱、诽谤和诬告陷害。

[…]

第四十条　中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密[76] [77]。》

However, Western standards always provide a constitutional mechanism - the Supreme Court or an independent body – that acts as a guarantor of constitutional rights. On the contrary, these provisions in China represent a mere formality in legal terms in case of judicial proceedings, since in the country does not exist a separate and independent constitutional organ, which is embodied by the National People's Congress (Art. 62). According to Zhang Q. (2010), one of the biggest weaknesses of the Chinese Constitution, as it happens in many authoritarian countries, is the lack of a judicial review. Laws are not enforced by the NPC, which tied to the political power, and they represent a formal "façade" for the population[78].

Civil laws and criminal laws

Civil and criminal laws both provide protection of people's personal information. To what concerns the civil law branch, only two regulations mention concepts linked to privacy

[75] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China…, cit., p. 16.

[76] 中华人民共和国中央人民政府，中华人民共和国宪法 *Zhonghua renmin gongheguo xianfa* (Constitution of People's Republic of China), 2018, available at: http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm

[77] "*Article 38*: The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false charge or frame-up directed against citizens by any means is prohibited.
Article 40: The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or of investigation into criminal offences, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law."
Constitution of the People's Republic of China 1982, USC US-China Institute, University of Southern Carolina, 2014, available at: https://china.usc.edu/constitution-peoples-republic-china-1982, (2020-04-20).

[78] Qianfan ZHANG, A constitution without constitutionalism? The paths of constitutional development in China, Oxford University Press and New York University School of Law, 2010, pp. 951-953.

and data security rights. The first one, the General Principles of Civil Law 中华人民共和国民法通则 (*Zhonghua renmin gongheguo minfa tongze*), was enacted in 1986 and provided a basis for privacy by preserving the "right of reputation" in Article 101[79]. Further Articles defend specifically the personal name, personal image and honor (articles 99, 100 and 102)[80]. In 2017, the law was renovated in order to include more specific rules for the security of data and the fundamental role that private actors play in their collection and safeguarding[81]. The second law is the Tort Liability Law 侵权责任法 *Qinquan zeren fa* (2009), in which the right to privacy is added to the listed civil rights. Moreover, it covers torts made by network users and providers and protects patients' medical history information[82]. When talking about the criminal law branch, Article 253 (A)[83] of the Amendment VII of the Criminal Law 刑法修正案七 *Xingfa xiuzhengan qi* (2009) establishes punishments like imprisonment or fines to citizens or members of specific sectors such as telecommunications, education, transportation, medical care etc. that illegally sell, steal or provide people's personal information. Furthermore, two more paragraphs are added in Article 285[84], which mention some computer information system

[79] 《第一百零一条 公民、法人享有名誉权，公民的人格尊严受法律保护，禁止用侮辱、诽谤等方式损害公民、法人的名誉。》
"Article 101 Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited." Available at: http://en.pkulaw.cn/.
[80] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China…, cit., p. 18.
[81] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 16.
[82] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China…, cit., p. 18.
[83] "*Article 253 (A)* Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined.
Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph.
Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph."
The Supreme People's Court of the People's Republic of China, Available at: http://english.court.gov.cn/, (2020-04-16).
[84] "*Paragraphs 2 and 3 of Article 285* Whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to fixed-term

crimes like illegal breaches and control of the systems or illegal collection of data. De Hert and Papakonstantinou (2015) in their study reported two judicial cases concerning online shaming and illegal purchasing of information. In the first dispute, the litigant Wang Fei was the subject of a harassment campaign on the internet made by an old friend of his wife, who committed suicide due to his infidelity. According to the General Principles of Civil Law, the court sentenced both the defendant and the network provider, which failed in removing Wang Fei's information, to pay hefty fines. The second case refers to an international company that established a subsidiary in China and was accused of illegally buying 150 million Chinese consumers' data. On the basis of Article 253 (A) of the Criminal Law, the conviction was a heavy fine and the imprisonment of four executives of the firm[85].

Sector-specific regulations

One of the most influential legislation that deals with data matters is the Decision on Strengthening Information Protection on Networks 关于加强网络信息保护的决定 *Guanyu jiaqiang wangluo xinxi baohu de jueding*, which was promulgated by the Standing Committee of the National People's Congress in 2012 and counts a total of 12 articles. It addresses to Internet service providers, companies and institutions that hold and use personal data. They have to respect specific criteria of legality, necessity and legitimacy, which means that is required to obtain the agreement of the consumer first and then guarantee confidentiality and protection, since all service providers have to collect real identity information. Netizens, who discover the violation of privacy norms, have the right to inform the controlling authorities and

imprisonment not more than three years or criminal detention, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to fixed-term imprisonment not less than three years but not more than seven years, and be fined.
Whoever provides special programs or tools specially used for intruding into or illegally controlling computer information systems, or whoever knows that any other person is committing the criminal act of intruding into or illegally controlling a computer information system and still provides programs or tools for such a person shall, if the circumstances are serious, be punished under the preceding paragraph."
The Supreme People's Court of the People's Republic of China, Available at: http://english.court.gov.cn/, (2020-04-16).

[85] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China…, cit., p. 23.

ask for the removal of the information[8687]. Even if the Decision on Strengthening Information Protection on Networks presents considerable gaps in comparison with the European model, it surely presents basic elements of personal data protection and for this reason, was used as a model for the enactment of other regulations such as the MIIT Regulation of 2013 and the modification of China's Consumer Law[88].

Other examples of sector-specific regulations following the US framework, are the Measures for the Administration of Internet E-mail Services (2006), the Medical Records Administration Measures of Medical Institutions, Several Regulations on Standardizing Market Order for the Internet Information Services (2012), the Telecommunications and Internet Personal User Data Protection Regulation, approved by the Ministry of Industry and Information Technology (MIIT) in 2013, the Administrative Measures for Online Transactions[89] etc. Even though the above-mentioned regulations present strong data protection rules, their range of action is limited to their distinct departments and problems of administration and accountability may arise.

Cyber Security Law

The Cyber Security Law became effective on June 1, 2017, it is composed by 7 chapters divided into 79 articles and could be conceived as the closest example of a national data protection law. Its adoption is considered a turning point in the development of privacy protection for private enterprises and individuals in China, and an important step forward towards consumers' right to be safeguarded[90]. On the contrary, other articles of the same law show the already mentioned data-approach with "Chinese characteristics", which implies a

[86] Decision on Strengthening Information Protection on Networks; Art. 1, Art. 2, Art. 3, Art. 4, Art. 6, Art. 8, Art. 9.
[87] Paul DE HERT, Vagelis PAPAKONSTANTINOU, The data protection regime in China…, cit., p. 19.
[88] *Ibid*.
[89] Hanhua ZHOU, Consumer Data Protection in Brazil, China and Germany…, cit., p. 37.
[90] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., pp. 51-52.

dichotomy between consumers' rights and citizens' rights and allows the government to have access to an always increasing amount of information[91]. The law can be divided into five topics: personal information and privacy protection, security obligations for network providers (included large financial institutions), definition of critical information infrastructure and the protection measures they have to follow, data localization, according to which sensitive information must be stored locally and penalties which imply fines, revocation of licenses or suspension of every activity[92]. Network operators and personal information are defined for the first time in Article 76[93], the former refers to owners, providers and administrators of networks, telecommunication operators and firms having websites, the latter is described as all types of electronically stored information that let others identify a "natural person" such as date of birth, name, identification number, address etc.[94] Furthermore, except for competent authorities, consent of citizens is a legal requirement for companies and institutions in order to collect and process information, but it isn't clearly stated whether also implicit consent is allowed.

Non-binding regulations

Generally speaking, the Chinese legal literature is composed by many regulations, whose vague and flexible content and lack of precision could potentially provoke legal uncertainty. For this reason, non-binding texts, which are richer in details and present clearer meanings, are often conceived as law's implementations[95]. This is the case also for the Cyber Security Law and the Information Technology – Personal Information Security Specification

[91] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., pp. 51-52.
[92] KPMG China IT Advisory, KPMG International Cooperative, 2017, p. 7.
[93] 《第七十六条　本法下列用语的含义: […]
（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。
[…]
（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。》 Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (2020-04-20).
[94] KPMG China IT Advisory, KPMG International Cooperative, 2017, p. 7.
[95] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 22.

个人信息安全规范 *Geren xinxi anquan guifan*, which is a non-binding provision introduced by the Standardization Administration of China in 2018. The Specification is mainly based on domestic and international rules, in order to take advantage of the experience of foreign countries. It enforces the CSL by outlining more precisely principles and requirements for enterprises like transparency, lawfulness and sensitivity, which means the distinction between sensitive information 敏感信息 *Mingan xinxi* and other information (6.3)[96]. However, contrarily to the GDPR, consumers' consent has not to be explicit. This could be a consequence of the necessity to facilitate domestic AI firms like Baidu, who need large amount of data[97]. Finally, it is the first official text that introduces the limitation of automated decision-making like user profiling 用户画像 *Yonghu huaxiang* (3.7), that consists in collecting and analyzing personal information in order to predict specific features of an individual like education, financial credit, behavior etc.[98]. It implies the possibility for data subjects to formally complain when automated wrong information are associated to them.

Lastly, after a previous draft in 2013, a final version of the Guideline for Internet Personal Information Security Protection 互联网个人信息安全保护指南 *Hulianwang geren anquan baohu zhinan* was released by the China's Ministry of Public Security in April 2019. As the Specification, it is a non-binding document whose aim is to protect individuals' interests and information from cybercrimes by providing more requirements for companies, organizations and other entities using Internet security systems. First, it classifies those systems

[96] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 25.
[97] Michael GENTLE, China's data-privacy law vs. GDPR, The Balance of Privacy, 2018. Available at: https://medium.com/the-balanceof-privacy/chinas-data-privacy-law-vs-gdpr-566fde8c213c (2020-08-30).
[98] 《3.7 用户画像
通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人特征模型的过程。》
Mingli SHI, Samm SACKS, Qiheng CHEN, Graham WEBSTER, Translation: China's Personal Information Security Specification, 2019, Available at: https://www.newamerica.org/cybersecurityinitiative/digichina/blog/translation-chinas-personal-information-securityspecification/ (2020-04-20).

located in China according to the Multi-level Protection Scheme (MPS), thus rating from one to five points the impact they could have on national security, economic stability and social order in case of cyberattack[99]. Then, it cites a new notion of "personal information holders", which comprehends data collectors, data processors and data controllers, and gives detailed instructions on how to properly hold data. Specific technical and organizational tools and measures are defined in order to protect the overall information life cycle, from the collection and retention to the usage and disclosure, and reiterates data localization requirements already stated in the Cyber Security Law[100].

Through the overview of China's privacy and personal information development, it is possible to affirm that many recent regulations present more and more similarities to the European model, conceived as one of the most complete sets of laws worldwide. Despite this, other core elements in the EU standards are still not promoted in the Chinese legal literature concerning people's data. For instance, information quality criteria, such as accuracy or update, are not clearly delineated in Article 42 of the Cyber Security Law and the same law does not define a unique controlling authority of data protection[101]. In order to tackle this problem, the government established the Cyberspace Administration of China 国家互联网信息办公室 *Guojia hulianwang xinxi bangongshi* (CAC) on 27 February 2014 as an attempt to reduce the multiple authorities which were previously regulating the Internet sphere. Its main duties are educating and building awareness about Internet risks and chances in Chinese netizens, promoting informatization and collaborations with other actors in the world, for example the

[99] Yan LUO, Zhijing YU, Nicholas SHEPHERD, China's Ministry of Public Security Issues New Personal Information Protection Guideline, *Inside Privacy Covington*, 2019.
[100] China Privacy Developments in 2018, Covington, 2019.
[101] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 32.

China-EU Digital Cooperation Roundtable or the China-ASEAN Internet Forum and finally, supervise the overall content online[102].

Despite this, Article 8[103] of CSL does not present a precise definition of the organs that administer data issues. In the text is stated that, except for the Cyberspace Administration of China, which has had a central role in coordinating and planning cybersecurity measures, "other pertinent organs", which could be the MIIT or the Ministry of Public Security, are also responsible for the process of enforcement, management and supervision of personal information in their respective departments[104].

A further law, called Personal Information Protection Law 个人信息保护法 *Geren xinxi baohu fa*, has been listed in the 13th NPC Standing Committee Legislative Plan (from 2018 to March 2023), since the features of its draft are almost mature and it is waiting for deliberation[105]. It is possible that this law will help China get closer to developed nations in terms of improvement of privacy rights and obtain more competitiveness in the global market[106].

---

[102] Weishan MIAO, Policy Review: The Cyberspace Administration of China, *Global Media Communication*, Vol. 12(3), 2016, pp. 337-340

[103] 《第八条　国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。》

"Article 8: State cybersecurity and informatization departments are responsible for comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations."

中共中央网络安全和信息化委员会办公室 (Office of the Central Cyberspace Affairs Commission), Zhonghua renmin gongheguo wangluo anquanfa 中华人民共和国网络安全法 (Cybersecurity Law of People's Republic of China), 2016. Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (2020-04-20).

[104] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 36.

[105] Changhao WEI, Translation: 13th NPC Standing Committee Five-Year Legislative Plan, NPC Observer, 2018. Available at: https://npcobserver.com/2018/09/07/translation-13th-npc-standing-committee-five-year-legislative-plan/ (2020-04-20).

[106] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way…, cit., p. 59.

1.4 Chinese influence over Asian countries.

Regarding data protection laws, two events have had great impact in Asia. First, China, one of the most influential countries in the area, started in the 21th century to focus on cybersecurity and personal data protection rights more carefully. In addition, in 2017 the adoption of the Cyber Security Law 网络安全法 *wangluo anquan fa* represented an important innovation in the overall Asian legislative system, since this comprehensive regulation introduced new concepts, including more specific data management rules and data localization, meaning that all the relevant information and personal information must be stored inside the country. For instance, Viet Nam Cyber Security Law (2019) was highly influenced by the Chinese law because it requires offshore service providers to settle a subsidiary inside the country, to respect data localization conditions and then, it allows the Vietnamese government to conduct census of online content. India's draft called Data Protection Bill took another direction with respect to other data protection laws in Asia, since it aims to combine different principles of the American, European and Chinese models[107]. The introduction of data localization restriction suggests the Indian alignment with the Chinese Cyber Security Law, but at the same time, it raised concerns of foreign companies operating in the country. Second, in 2016, the European Union adopted the General Data Protection Regulation (GDPR), which went into effect on May 25th 2018. This comprehensive law influenced heavily Asia Pacific and South-East Asian nations. Countries like Thailand, Sri Lanka and Malaysia, modelled their personal data protection laws after GDPR principles[108], whereas Japan became the only nation in Asia to adopt an Adequacy Decision with the European Union, that implies trading agreements and the free flow of data between the jurisdictions' borders[109]. Consequently, also

[107] Asia Pacific Data Protection and Cyber Security Guide, *Hogan Lovells*, 2019.
[108] Sarah PEARCE, Data Privacy in Asia Pacific: a Fragmented Landscape, 2019, available at: https://www.regulationasia.com/data-privacy-in-asia-pacific-a-fragmented-landscape/#:~:text=Asia's%20data%20privacy%20frameworks%20remain%20highly%20fragmented.&text=This%20has%20been%20driven%20in,Decision%20by%20the%20European%20Commission. (2020-04-21).
[109] *Ibid*.

in Cambodia, Lao PDR, Myanmar and Timor-Leste authorities and lawmakers are starting to study existing models and develop similar regulations.

As in the regulatory sphere both Chinese and European laws have deeply influenced Asian countries' data protection systems, also the commercial sector has been deeply influenced by Beijing's Big Data project, infrastructures and technologies. For many decades, the US has always excelled in the Big Data industry and AI development globally. At the same time, China is expected to overcome the United States by 2030 and become the world leader in these businesses[110]. Moreover, the "Made in China 2025" initiative, launched in 2015 by the Prime Minister Li Keqiang, aims at becoming one of the major powers of the world in high-tech industries with the aid of cloud computing, Big Data and IoT, like new energy transportation, aviation and robotics. It is going to shift from "made in China" to "designed in China" within a period of 10 years. This is due to the fact that in recent years the country has been surpassed by Viet Nam, Cambodia and other developing countries as low-cost labor market[111]. The main objective of the plan consists in innovating and relying more on domestic smart manufacturing companies, thus including the deployment of Big Data in the creation of robots and sensors, rather than import technologies from abroad[112]. The goal will be achieved by a process of standardization of cyber security regulations and practices like encryption and domestic IP, financial support of state-owned banks and the internationalization of Chinese companies. However, the race towards the dominance of Big Data and artificial intelligence technology does not only involve the U.S. and China, but concerns many other countries, from the European Union like France and Germany to the UK, from Canada and Israel to Asian countries

[110] Louise LUCAS, Richard WATERS, China and US Compete to Dominate Big Data, 2018, available at: https://www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd (2020-04-21).
[111] Ling LI, China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0", *Technological Forecasting and Social Change*, Vol. 135, 2018, pp. 66-74.
[112] Made in China 2025, Institute for Security & Development Policy, 2018, P. 2

such as Japan and South Korea[113]. Among the European nations mentioned above, the German government first announced the "Industry 4.0" plan in 2013 and confirmed its global leading role in the manufacturing and industrial world. Chinese and German programs are both directed at fulfilling the digitalization of industries, the development of robotics. In addition, China aims also to improve the quality of its products and create more cross-borders R&D collaborations and new patents[114].

Several branches of Artificial Intelligence like machine learning and Big Data analytics are leading the new market economy and have become meaningful strategic tools in the national and private field. Their international recognition was further confirmed in 2017 by the Russian president Vladimir Putin's statement, in which he said: "Artificial Intelligence is the future, not only for Russia but for all of humankind. Whichever country becomes the leader in this sphere will become the ruler of the world". However, even though in 2019 the Russian government approved a National Strategy for the Development of Artificial Intelligence (NSDAI), primarily implementing new technologies in the military sector, its investments in the R&D in other categories of AI, data mining and analytics are still relatively low[115].

In the Asia-Pacific region, besides China, also Japan and South Korea have been already facing the competition for AI dominance. Despite the well-known Japanese advancement in robotics and technology in general, many national companies did not react promptly to new AI opportunities, which were limited especially to the financial and manufacturing sector. For this reason, the government set the Artificial Technology Strategy in 2017, which is divided into 3 steps that will be completed by the end of 2030 and implies the collaboration between the government, universities and enterprises, in order to intensify the research and improve

[113] Kathleen WALCH, Why the Race for AI Dominance Is More Global Than You Think, 2020, available at: https://www.forbes.com/sites/cognitiveworld/2020/02/09/why-the-race-for-ai-dominance-is-more-global-than-you-think/#754a2809121f (2020-04-19).
[114] Ling LI, China's manufacturing locus in 2025…, cit., pp. 66-74.
[115] Kathleen WALCH, Why the race for AI dominance is more global…, cit.

country's welfare and transportation [116]. The development of these sectors and their implementation in more industries is fundamental for Japan in order to achieve a bigger project called Society 5.0, a future "technology-based, human-centered" society where big data, AI and robotics are interconnected with the "physical space"[117].

On the contrary, South Korea is the third country in the world in filing AI patents and the government is planning to invest massively on Big Data and AI R&D by 2022. For instance, it is actively implementing new developed technology in smart cities and companies' management, health care services, national defense and drones, in order to achieve the government's Fourth Industrial Revolution Plan[118]. This project has been conceived to let the country be in compliance with the fourth and currently the last of all the industrialization processes: the first wave dates back to 1700s and mid-1800s and involved the usage of coal, water and steam power to mechanize the manufacturing. The second, which broke out between the 19th and 20th century, implied the introduction of the assembly line and the exploitation of electricity to achieve mass production. The third took place in the 1950s and its scope was to deploy computers and the Internet in order to take advantage of automation. Finally, the 4IR is going to fuse together the physical, biological and digital world[119]. According to the Korean International Patent Office, the principal technologies needed in order to conform with this global plan and get on par with developed countries like Japan, Germany or the US, are artificial intelligence, Big Data, Internet of Things, 3D printing, autonomous driving, robotics, and Cloud computing[120].

---

[116] Kathleen WALCH, Why the race for AI dominance is more global…, cit.
[117] Government of Japan, Cabinet Office. Available at: https://www8.cao.go.jp/cstp/english/society5_0/index.html (2020-04-19).
[118] Olaf J. GROTH, Mark NITZBERG, Dan ZEHR, Tobias STRAUBE, Toni KAATZ-DUBBERKE, Comparison of National Strategies to Promote Artificial Intelligence; Part 1; Konrad-Adenauer-Stiftung, Berlin, 2019.

[119] Prosper FUNWIE, The 4th Industrial Revolution: International Relations and Policy: Case of S. Korea and China, Department of International Relations, GSIAS Hankuk University of Foreign Studies, Seoul, 2019, p. 5.
[120] Prosper FUNWIE, The 4th Industrial Revolution: International Relations and Policy…, cit., p. 10.

Thanks to the acceleration of the process of globalization in recent years, Internet of Things and Big Data have had such a great impact worldwide that even governments, that initially underestimated the sector, started constructing their own infrastructures and signing agreements with tech companies of foreign nations. Even ASEAN countries are becoming more and more aware of the relevance of digital economy in the 21st century and are willing to exploit it. The entire region shows a great capability since Internet and mobile phones penetration is among the highest in the world, thus many South-East Asian countries are individually designing new technological implementations[121]. Furthermore, in order to take advantage of this rising potential, some of them decided to rely on Chinese Big Data industry and AI infrastructures, rather than on American technology. For instance, at the beginning of the 21th century, Malaysia created a special economic zone called Multimedia Super Corridor and the "intelligent" city of Cyberjaya, following the model of Chinese SEZs. Both projects included the construction of new information and communication infrastructures and their scope was to promote a digital economy in the country and attract foreign investors[122]. In 2018, the government started a collaboration with a Chinese startup called Yitu, which aims to expand in the Southeast Asian region, to facilitate authorities' control and urban management through facial recognition. In 2014, also Singapore declared its willingness to create a Smart Nation through the strengthening of digital technologies with the interconnection of its 6th "Research, Innovation and Enterprise 2020 Plan" to develop smart manufacturing, healthcare and many other industries[123]. Moreover, it signed agreements with foreign tech companies, such as the Irish Accenture and the Chinese Huawei, in order to create smart cities[124]. Huawei found fertile

[121] Tse Gan THIO, Data and privacy protection in ASEAN – what does it mean for businesses in the region?, *Deloitte Southeast Asia,* 2018.
[122] Current Status on Science and Technology in ASEAN Countries, *Center for Research and Development Strategy*, Japan Science and Technology Agency, 2015, p. 47.
[123] RIE 2020 Plan, National Research Foundation, Prime Minister's Office Singapore, Government of Singapore, 2019. Available at: https://www.nrf.gov.sg/rie2020 (2020-05-04).
[124] Steven FELDSTEIN. The Global Expansion of AI Surveillance, Carnegie Endowment for International Peace, 2019, p. 18.

ground in South-East Asia, both for 5G technology and security systems deals. According to the South China Morning Post, the Philippines, a country that for long time had relied on US technology, recently chose the Chinese company to build a surveillance system in the area of Bonifacio Global City, which counts nearly 200 security cameras, and plans to extend it to other cities[125]. In 2018, Lao President Bounnhang Vorachit discussed with the president of Huawei South East department about starting some collaborations, to develop ICT industry, welfare programs and infrastructures in the nation[126].

Actually, more than sixty-three countries in the world receive supplies of AI surveillance technology by Chinese firms like Huawei, ZTE, Dahua, Hikvision etc. In the following table, provided by the Carnegie Endowment for International Peace Organization, are shown different types of surveillance instruments considered in the study, such as smart cities technology, facial recognition and smart policing, the type of regime of each country mentioned and finally, the collaborations started between giant tech companies and some China's neighboring states, members of ASEAN countries, Japan, Hong Kong and South Korea. Among the several Chinese enterprises cited before in the research, Huawei is standing out as the principal supplier of 13 countries out of 17[127] [128].

[125] How Philippines' embrace of Huawei reflects China's growing influence and failure of US pressure tactics, South China Morning Post, 2019, Available at: https://www.scmp.com/news/asia/southeast-asia/article/3013948/how-philippines-embrace-huawei-reflects-chinas-growing (2020-05-05).
[126] Laos and Huawei enhance nation ICT development, 2018, Available at: https://www.huawei.com/ch-en/news/2018/5/lao-president-huawei-ict (2020-05-05).
[127] Steven FELDSTEIN. The Global Expansion of AI Surveillance…, cit., pp. 25-28.
[128] CA = Closed Autocracy; EA = Electoral Autocracy/Competitive Autocracy; ED = Electoral Democracy/Illiberal Democracy; LD = Liberal Democracy.

COUNTRY	REGIME TYPE	SMART CITIES	FACIAL RECOGNITION	SMART POLICING	CHINA TECH	US TECH	KEY COMPANIES
HONG KONG	ED		X		X		Huawei, Bosch
INDIA	ED	X	X	X	X	X	Hikvision, IBM, Microsoft
INDONESIA	ED	X	X	X	X	X	Huawei, NEC
JAPAN	LD	X	X	X	X		Hikvision, NEC
KAZAKHSTAN	EA	X	X	X	X		Analytical Business Solutions,Huawei
KYRGYZSTAN	EA	X	X	X	X		Huawei
LAO PDR	CA	X		X	X		Huawei
MALAYSIA	ED	X	X	X	X		Huawei, Yitu
MONGOLIA	ED		X		X		Dahua, Sensetime
MYANMAR	EA	X	X		X		Hikvision, Huawei
PAKISTAN	EA	X	X	X	X		Huawei
PHILIPPINES	ED	X	X	X	X	X	Boeing, IBM, Huawei
RUSSIA	EA	X	X	X	X	X	Cisco, Huawei
SINGAPORE	ED	X	X	X	X	X	Accenture, Huawei
SOUTH KOREA	ED	X	X	X		X	IBM, Korea Telecom
TAJIKISTAN	CA	X	X		X		Huawei
THAILAND	EA	X	X		X		Huawei, ZTE

Despite the expansion of AI surveillance worldwide, citizens are starting to reject these tools, especially facial recognition technology. An astonishing example is linked to Hong Kong riots in the summer 2019, in which protesters covered their faces and removed the facial recognition login of their phones in order not to let police have access to their personal information. Furthermore, they managed to discover some officers' identity, who didn't wear identification badges, by taking and analyzing their pictures and later, published them on a famous instant messaging platform[129].

In conclusion, it is possible to affirm that Big Data and their implementation in AI technologies have assumed a particularly strong economic value in China, as well as in the rest of the world. Since they are the first driver of Chinese digital economy, the first challenge was

[129] Steven FELDSTEIN. The Global Expansion of AI Surveillance…, cit., p. 19.

creating a set of regulations, which was able to protect people's information from cyber-crimes. As a consequence, both the normative and commercial spheres have registered a great influence on other Asian countries, in some cases, like the Philippines, even ousting the U.S. as the main tech partner. However, the Chinese government's main objectives are not only safeguarding Chinese consumers and maintain domestic companies' competitive advantage, but also having the complete control of Big Data, as a political power, in order to preserve the stability of the regime and society.

1.5 Glossary of terms

- Amendment VII of the Criminal Law 刑法修正案七
- Artificial Intelligence 人工智能
- Big Data 大数据
- Constitution of People's Republic of China 中华人民共和国宪法
- Cyber security 网络安全
- Cyber Security Law 网络安全法
- Cyberspace Administration of China 国家互联网信息办公室
- Decision on Strengthening Information Protection on Networks 关于加强网络信息保护的决定
- Facial Recognition 人脸识别
- General Principles of Civil Law 中华人民共和国民法通则
- Guideline for Internet Personal Information Security Protection 互联网个人子女子安全保护指南
- Mandate of Heaven 天命
- Personal data 个人信息
- Personal Information Protection Law 个人信息保护法
- Personal Information Security Specification 个人信息安全规范
- Sensitive information 敏感信息
- Smart city 智慧城市
- Social Credit System 社会信用体系

▪ Supervisor of the State Administration of Market Regulation	国家市场监督管理总局主管
▪ Tort Liability Law	侵权责任法
▪ User Profiling	用户画像
▪ 12th Five Year Plan	国民经济和社会发展第十二个五年规划

CHAPTER 2

Big Data as a political value

This second chapter is going to describe the other function of Big Data in the Chinese society, that is its political value. First it aims at introducing the first community systems, whose objective was organizing people's lives and monitoring their activities and personal information. Then, it shows how Big Data and cyber sovereignty are vital for the national security of China as well as of other foreign countries, especially after the Snowden's scandal. At the end, the chapter provides a wider perspective of the new set of regulations, whose objectives are allowing authorities' broader access to businesses and citizens' information and enhancing the social, economic and political stability.

2.1 Earlier instruments of managing information in society

Traditionally, the relations Chinese have established with the government and the ways they perceive different sources of control towards the population have been deeply influenced by Confucianism. The Confucian philosophy aimed at providing social and ethical norms of behavior, that had to be respected by families, governors and friends. Contrarily to the legalist theories, which supported the prevalence of order and regulations, Confucius and Mencius rejected the formality of the law and highlighted the effectiveness of informal control for the prevention of crimes and the maintenance of social order[1]. According to Mencius (372-289 BC or 385-303 BC), humans are good by nature, they have a sense of morality and throughout their life, they will have to cultivate the innate four positive sprouts 四端 *siduan* that reside in every individual. In light of this, education and re-education are more influential in the creation of a good, honest individual rather than official rules and the judiciary system. Despite the

[1] Shanhe JIANG, Jin WANG, Eric LAMBERT, Correlates of informal social control in Guangzhou, China neighborhoods, *Journal of Criminal Justice*, Vol. 38(4), 2010, p.460.

Communist Party's absolute rejection of ancient philosophies and theories, when it came to power in 1949, it implicitly embraced the above-mentioned Confucian principles and created its own system of informal social control[2]. In fact, after the Civil War, communists felt the necessity to establish social and political stability in the country, but, at the time, with such a fast-growing population, it was financially and practically impossible to monitor almost 6 hundred million people[3]. For this reason, they opted to create vigilant neighborhood committees and work units' collectives to implement public security and form one of the first surveillance instruments of citizens in China.

Work Units

Work organizations or *danwei* 单位 were workplaces where employees' task was to fulfill the socialist state plan. They automatically became people's residence and through their neighborhood system, individuals could feel part of a community. A work unit was composed by an all-inclusive controlled mechanism that monitored not only employees' job and their behavior at work, but also their private sphere and the overall local order. These organizations planned housing, marriage and divorce, family planning, education and a certain number of arranged activities during the spare time[4]. From an administrative point of view, the public security office had to safeguard the unit from outsiders as well as manage the internal social order, whereas the armed forces department's objective was to protect the members of the work unit and organize militias. Furthermore, the closeness of the workplace with the employees' house, together with the sharing of communal spaces within the community, gave less

[2] Formal social control tools are conceived as those official and legal controls imposed by the government. On the contrary, informal social control tools are accomplished by controlling groups or individuals according to morality.
[3] Allen F. ANDERSON, Vincent E. GIL, China's Modernization and the Decline of Communitarism: The control of sex crimes and implications for the fate of informal social control, *Journal of Contemporary Criminal Justice*, Vol. 14(3), 1998, p. 250.
[4] Victor N. SHAW, *Social Control in China: a study of Chinese Work Units*, Praeger, London, 1996.

possibility to unauthorized lateness or absence[5]. The *danwei* was placed under the supervision of both the CCP and the government, their institutions were able to confer a larger extent of responsibilities or reduce people's freedom, plan and collect quotas and deploy several control methods[6]. After the liberalization of the country's economy and the increasing role of private enterprises, work units started to lose their power. Within 2000, many *danwei* were removed and their norms and customs, like requests for marriage or divorce, were loosened.

According to Shaw (1996), the *danwei* system was just one of many examples in the history of Chinese society that tends to gather together people into social units. Actually, before socialism, a similar type of organization was already represented by clan networks called "cells" and by the imperial 保甲 *baojia* system, created in the Song dynasty by Wang Anshi and lately developed also by the Nationalist Party[7]. It was between 1920s and 1930s that this mechanism was implemented in territories previously held by the communists as a local control tool and then, as a self-government instrument to locally develop fields like education, self-defense, census taking and the creation of a harmonious society. It basically grouped ten households or *hu*, forming a *jia*, and ten *jia* creating a *bao.* These units were positioned at the lowest level of governmental hierarchy and took orders from the central authority, but, at the same time, they had the possibility to handle businesses of the community with a certain degree of independence[8]. This type of network was abolished after the victory of the CCP since it was conceived as an imperialist tool, but with the dismantlement of *baojia*, a new local institution was formed: the residents' committee[9].

[5] E.M. BJORKLUND, The danwei: socio-spatial characteristics of work units in China's urban society, *Economic Geography*, Vol. 62(1), 1986, pp. 24-28.
[6] Victor N. SHAW, *Social Control in China: a study of Chinese Work Units*…, cit., pp. 11-15.
[7] Victor N. SHAW, *Social Control in China: a study of Chinese Work Units*…, cit., p. 1.
[8] Lane J. HARRIS, From Democracy to Bureaucracy: the Baojia in Nationalist Thought and Practice, 1927-1949, Front. Hist. China, Vol. 8(4), 2013, pp. 519-542.
[9] Ngeow Chow BING, *The Residents' Committee in China's Political System: Democracy, Stability, Mobilization*, 2012, p. 74.

Residents' Committees

Accordingly, the second tool used to guarantee informal social control are both the neighborhood committee 居委会 *juweihui* and neighborhood police station 派出所 *paichusuo*. The *juweihui* can be considered as a semi-public institution since it cooperates with local government offices and all the activities receive their approval first. At the same time, it counts on residents' participation and mobilization in order to inform the competent authorities about small crimes or immoral behaviors. Moreover, inhabitants work closely with the municipal police, who is the official representative that most of the time comes into contact with ordinary people and the community residing within its administration. Since 派出所 *Paichusuo* are closely tied to the population, among their tasks, they have to provide re-education programs to former offenders, as well as convince residents of the decisiveness of their help inside the district. Furthermore, their actions should be carefully observed in order to understand the Party's strategies of prevention of criminal behavior and terrorism[10]. In Wang's research is reported a concrete example of the combination of both the institutions' forces, in which residents of the Jingtai neighborhood collaborated in observing and reporting to the committee and local authorities some unusual reunions that took place in an apartment of Building 12. Driven by their assigned role of protectors of the well-being of the community, they carefully monitored the number of visitors, the time those meetings took place, the physical appearance of attendees etc., but after some investigation, police found out that gatherings were organized just for business reasons and not for political indoctrination[11].

Nowadays, committees' primary objectives are: embodying official ideology and civility, assuring public security at a local level, take care of environment and health issues and

[10] Elmer H. JOHNSON, Neighborhood Police in the People's Republic of China, *Police Studies*, Southern Illinois University, New York, Vol. 6(4), 1983.
[11] Jianfeng WANG, *The Politics of Neighborhood Governance: Understanding China's State-Society Relations Through an Examination of the Residents Committee*, Western Michigan University, Michigan, 2005, p. 138.

providing party-building encouragement. As a result, studies reported that these type of mass-interaction and control committees were the major reason why crime rates were particularly low in urban areas[12]. The first residents' committee was established in Hangzhou in 1950 and its task was to divide inhabitants into "good" and "evil" categories, depending on their engagement and activism in the communist cause, on their religious beliefs, criminal record and previous collaboration with the Kuomintang[13]. During the Cultural Revolution (1966-1976), neighborhood committees became highly politicized and militarized due to the strong connection they had with inhabitants, and this relation was further exploited by the Party as a political control instrument. Even if nowadays this organization's functions have changed, social control keeps being an historic priority and committees still monitor previous protesters and criminals[14]. In fact, when SARS broke out in 2003, the surveillance networks exerted by these institutions played a decisive role in the epidemy containment and control. The crucial reaction of *juweihui* was repeated during the breakout of COVID-19, that together with new technologies and AI promptly transferred critical information to health authorities and enacted an active scrutiny of quarantined people[15].

The relevance neighborhoods had reached in the achievement of public security is further expressed in the Organic Law of the Urban Residents' Committees of the People's Republic of China 中华人民共和国城市居民委员会组织法 *Zhonghua renmin gongheguo chengshi jumin weiyuanhui zuzhifa* of 1989, which was lately amended in 2018. Generally speaking, this regulation establishes the legitimation of the above-mentioned type of organization and its activities on behalf of residents. Furthermore, in the third Article are listed

[12] Lening ZHANG, Steven F. MESSNER, Sheldon ZHANG, Neighborhood Social Control and Perceptions of Crime and Disorder in Contemporary Urban China, *American Society of Criminology*, Vol. 55(3), 2017, pp. 632-637.
[13] Ngeow Chow BING, *The Residents' Committee in China's Political System: Democracy…,* cit., p. 96.
[14] Jianfeng WANG, *The Politics of Neighborhood Governance: Understanding China's State-Society Relations…*, cit., p.95.
[15] Ngeow Chow BING, *The Residents' Committee in China's Political System: Democracy*…, cit., p. 106.

several tasks a committee must respect and achieve. Among them, the fourth and fifth commas highlight the deeply rooted connection between the community and social surveillance, as well as the explicit participation of the government through these informal tools of control in more private issues like family, job, education etc[16].

At first, in order to fight criminality, this system was widened not only to neighborhood committees and work units, but also to schools and national security companies, in order to develop a more comprehensive surveillance network. In 1985, public and private security service enterprises 保安服务公司 *bao'an fuwu gongsi* entered Chinese urban market and met urban communities' unsatisfied need of public order with the aid of new technologies[17].

As can be seen, the intervention of the Chinese government into citizens' life, family and environment, is nothing new. It has survived more than 2.000 years and is deeply rooted in the country's traditions of the Confucian philosophy[18]. This concept developed through the above-mentioned informal instruments of social control, such as work units and residents' committees, and reached the highest level of concreteness with the deployment of Big Data and AI technologies for cyber security. The State was able to penetrate into communities and pursue a "total society strategy" 综合治理 *zonghe zhili*, that is the mobilization of the overall forces a society can display, from political, judicial, economic ones to media, culture and education,

[16] 《*第三条* 居民委员会的任务：
（一）宣传宪法、法律、法规和国家的政策，维护居民的合法权益，教育居民履行依法应尽的义务，爱护公共财产，开展多种形式的社会主义精神文明建设活动；
（二）办理本居住地区居民的公共事务和公益事业；
（三）调解民间纠纷；
（四）协助维护社会治安；
（五）协助人民政府或者它的派出机关做好与居民利益有关的公共卫生、计划生育、优抚救济、青少年教育等项工作；
（六）向人民政府或者它的派出机关反映居民的意见、要求和提出建议。》
Available at: http://www.npc.gov.cn/wxzl/gongbao/1989-12/26/content_1481131.htm, 2020-06-24.
[17] Lening ZHANG, Steven F. MESSNER, Sheldon ZHANG, Neighborhood Social Control and Perceptions of Crime and Disorder…, cit., p. 638.
[18] Xiaoming CHEN, Social and Legal Control in China, *International Journal of Offender Therapy and Comparative Criminology*, Vol. 48(5), 2004, p. 533.

because of entrenched principles of exemplary conduct, sincerity and prevalence of social duty over privacy[19]. Compared to the welfare of the community, the individual fades into the background, since China is a relationship-based country and tend to preserve collectivism. According to Chen (2004), Chinese citizens are educated in order to prefer community commitment to their own interests; moreover, a crime is considered a problem of the entire family group or residence committee rather than just an individual mistake[20]. There isn't a clear distinction between public and private life and authorities' intrusion in the population's personal sphere and the government management of sensitive information are conceived as necessary for public security, because of the assumption that society is both a victim and an oppressor, causing criminal behaviors and suffering at the same time[21]. In the end, it must be kept in mind that the government's objective is implicitly to control both behavior and thoughts of its population; thus, social control in China presents a dual meaning: it refers both to the right behavior a citizen must have in compliance with the law and to the conduct suggested by morality and standards imparted by the community and the Party[22].

[19] Shanhe JIANG, Jin WANG, Eric LAMBERT, Correlates of informal social control in Guangzhou…, cit., p. 460.
[20] Xiaoming CHEN, Social and Legal Control in China…, cit., p. 525.
[21] Xiaoming CHEN, Social and Legal Control in China…, cit., p. 525.
[22] Xiaoming CHEN, Social and Legal Control in China…, cit., p. 526.

2.2 "There's no national security without cybersecurity"

Cyber-Sovereignty

The first chapter of this thesis discussed China's Internet development from 1994 to recent years, the penetration of this instrument in almost every aspect of daily life by the population and the efforts of authorities in protecting Chinese consumers from domestic and foreign cyber crimes 网络犯罪 *Wangluo fanzui*. Then, Section 2.1 presented the main informal practices of social control in order to understand to what extent the government used to participate in its population's daily lives and monitor their personal information before the advent of modern technologies. Soon enough, however, telecommunications, their information and infrastructures and the whole cyberspace, also became object of strict surveillance and censorship by the Chinese government. This is due to the regime far-reaching idea of sovereignty, that is not just limited to a territorial and administrative sphere, but it expands to the digital world, coining the term of "cyber-sovereignty" 网络主权 *Wangluo zhuquan*[23]. This term is based on the principle that a nation has the right and duty to regulate, censor and control online information of its citizens within its borders without other countries' intervention.

Recently, both the US and China have been running cyber sovereignty plans, but the methods through which they aim to reach their goals seem to differ: the American strategy is focused on creating a hegemonic cyber power, enlarging national Internet supremacy in the global cyberspace. In 2015, the US Defense Department declared the "right of self-defense" in the cyberspace, that is the right to attack foreign sources which are suspected of being threats for the country[24]. According to the White House, American Cyber Security Strategy is based firstly on protecting domestic infrastructures and systems with the aid of allies and commercial

[23] Aynne KOKAS, Platform Patrol: China, the United States and the Global Battle for Data Security, *The Journal of Asian Studies*, Vol. 77(4), 2018, p. 923.
[24] Yi SHEN, Cyber Sovereignty and the Governance of Global Cyberspace, *Chinese Political Science Review*, Fudan University, 2016, pp. 81-93.

partners. Second, it aims at promoting data transfers, investing on the tech and Big Data market and enhancing its digital economy. Lastly, it suggests to create a Cyber Deterrence Initiative, involving international players, in order to prevent future cyber-attacks and promote an open and secure environment on the Internet[25].

On the contrary, the Chinese cyber sovereignty seems to be more defensive and mainly oriented its policies inside the country. Furthermore, it accuses the U.S. of establishing an Internet hegemony, where the majority of basic Internet instruments like routers, software and IP knowledge mainly depend on American companies. Actually, the protection of China's Internet supremacy is expressed as the principal goal in many national laws like the National Security Law and the Cyber security Law[26].

However, both American and Chinese cyber experts like James Lewis and Amy Chang state that a cooperative approach between the two countries in the field of cyberspace, seems to be far from reaching and national influences and mistrust still represent important obstacles for establishing bilateral collaboration[27]. For instance, Beijing has been accused several times of intellectual property and sensitive information theft. In 2011, the U.S. Office of the National Counterintelligence Executive classified China as the country that most persistently undertake cyber intrusions in North America[28]. Relations between the two countries declined when, three years later, five officers of the People's Liberation Army have been accused of hacking activities and as a consequence, China interrupted the Cyber Working Group agreements[29]. According to the U.S. Department of Justice, in 2018, two individuals related with the Chinese Ministry of State Security's Tianjin State Security Bureau have been accused of illegally

[25] The White House, National Cyber Strategy of the United States of America, Washington DC, 2018, pp. 1-40.
[26] Yi SHEN, Cyber Sovereignty and the Governance of Global Cyberspace…, cit., 2016, p. 91.
[27] Harold S. WARREN, Martin C. LIBICKI, and Astrid Stuth CEVALLOS, The "Cyber Problem" in U.S.-China Relations, In *Getting to Yes with China in Cyberspace*, Santa Monica, Calif.: RAND Corporation, 2016, pp.3-4.
[28] Kenneth LIEBERTHAL, Peter W. SINGER, Cybersecurity and U.S.-China Relations, China Center-Brookings, 2012, pp. 1-52.
[29] Harold S. WARREN, Martin C. LIBICKI, and Astrid Stuth CEVALLOS, The "Cyber Problem" in U.S.-China Relations…, cit., p. 7.

intercepting more than 100.000 navy staff's information[30]. More recently, Chinese hackers have been charged by the U.S. with trying to illegally obtain American healthcare data about COVID-19 vaccine and possible treatments[31].

Except for cyber espionage, the second biggest concern is the threat of a cyberwarfare, which could damage all the infrastructures dealing with critical information both in the U.S. and in China. Statistics from the Business Information Industry Association show that cyber-attacks increased by 440% between within 9 years (between 2009 and 2018)[32].

Impact of Snowden's scandal on cybersecurity

> "For now, know that every border you cross, every purchase you make, every call you dial, every cellphone tower you pass, friend you keep, site you visit and subject line you type is in the hands of a system whose reach is unlimited, but whose safeguards are not."
>
> Edward Snowden's email to Laura Poitras, 2013[33].

Before the scandal that made him famous in 2013, Edward J. Snowden worked in the American Central Intelligence Agency (CIA) and lately, was hired both by Dell and as a sub-contractor by the National Security Agency (NSA) as system administrator, infrastructure analyst and cybersecurity expert. Throughout his career, he came into contact with different countries' information systems, including those of China, North Korea and some European nations, and all the amount of data and documents he was exposed to set up inside him ethical and constitutional conflicts and concerns[34], that at the end, brought him to resign in 2013 and

[30] The U.S. Department of Justice, Office of Public Affairs, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, 2018. Available at: https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion 2020-09-25).
[31] Nicole PERLROTH, David. E. SANGER, U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks, *The New York Times*, 2020. Available at: https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html (2020-09-25).
[32] Joachim BARTELS, Cyber Security Statistics: 440% Increase in Global Documented Attacks from 2009 to 2018, Business Information Industry Association, 2019. Available at: https://www.biia.com/cyber-security-statistics-440-increase-in-global-documented-attacks-from-2009-to-2018 (2020-09-25).
[33] David LYON, *Surveillance After Snowden*, Polity Press, Cambridge, 2015.
[34] Profile: Edward Snowden, *BBC News*, 2013, available at: https://www.bbc.com/news/world-us-canada-22837100, 2020-07-11.

to denounce publicly the US and UK intelligence's violations of people's privacy all over the world by releasing at least 58.000 secret documents. As a consequence of his revelations, the US government sentenced him to prison on charges of State secrets theft and transfer and communication of national intelligence information. At first, in May 2013, he travelled to Hong Kong, where he had his first interactions with journalists like Laura Poitras and Glenn Greenwald and his identity was consensually revealed by the UK's Guardian. Subsequently, he fled to Russia, in Moscow, where he still living now. In many countries, Snowden is considered a whistleblower, since he explained to journalists that he previously presented several complaints to higher rank officials when working for the NSA, thus, according to the Whistleblower Protection Act (1989), he should enjoy protection from the government. He even received the Whistleblower Award in Germany and the Swedish Right Livelihood Honorary Award in 2014[35]. However, the United States reject this classification, since authorities did not find any evidence of his former reports to his superiors.[36]

Snowden's revelations have represented both a global scandal and a decisive turning point for many nations' cyber security projects, since they found themselves and their citizens being the target of a mass surveillance plan of the United States. The documents, made available to the public, showed several espionage activities of the NSA together with the UK's Government Communications Headquarters (GCHQ), not only towards terrorist or criminal suspects, but also towards America and other foreign countries' population. For instance, mobile phones of the German Chancellor Angela Merkel and the former Brazilian President Dilma Rousseff were carefully controlled. The French-Dutch Gemalto company, a SIM card manufacturer, was also hacked by the NSA, who further stole encryption keys, obtaining the automatic access to phone calls and information. The impact of this breach has immeasurable

[35] David LYON, *Surveillance After Snowden*, Polity Press, Cambridge, 2015.
[36] U.S. House of Representatives, (U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, 2016.

consequences on the global population's right to privacy, since this company provides nearly 2 billion SIM cards every year[37]. Moreover, the NSA's Prism, a data mining program, became the subject of an investigation, since it seems to have entered servers of private US companies like Apple, Microsoft, Skype, Yahoo! and YouTube and collected information without the permission of users. Stolen data comprised emails, posts, voice calls, login and IDs, photos and videos, etc.[38]. With the accusations of Snowden, emerged the seriousness of a reality in which the espionage of citizens and politicians and the intrusion of the government in private information hold in mobile phones and industries' servers are tolerated and extensively used. In addition, some enterprises are willing to share the sets of data collected from their customers with the nation they operate in, so as to receive preferential treatments. Nowadays, surveillance technologies are not only limited to security cameras on the streets or in the airport, but they concern every movement, purchase, interaction on social media and online apps of ordinary people with no distinctions[39]. It became evident that the concept of "national security", especially the idea of foreseeing potential criminal or violence acts, has led intelligence agencies to a misuse of Big Data and security technologies in such a way that collides with citizens' right to information protection of the United States and many other democratic nations all over the world[40]. Furthermore, trust among intelligence services of different countries have almost disappeared and new measures have been taken since then, in order to tackle information leaks from national cyberspace. As an example of the changing of national approach, from then on, the Brazilian government modified its policies in order to produce domestically online services like email or social media in order to reduce the threat of data breaches[41].

[37] David LYON, Surveillance After Snowden, Polity Press, Cambridge, 2015.
[38] Sygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON, R.B.J. WALKER, After Snowden: Rethinking the Impact of Surveillance, *International Political Sociology*, Vol. 8, 2014, p. 122.
[39] Sygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON, R.B.J. WALKER, After Snowden: Rethinking the Impact of Surveillance…, cit., p. 137.
[40] David LYON, Surveillance After Snowden, Polity Press, Cambridge, 2015.
[41] Sygmunt BAUMAN, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON, R.B.J. WALKER, After Snowden: Rethinking the Impact of Surveillance…, cit., p. 130.

Besides European and Latin American countries, also China became the object of secret documents showing the scrutiny of the U.S. According to Jiang Tianfa, Professor of cybersecurity in the South-Central University for Nationalities, Snowden had and still has great influence both on his students, who started to actively attend his lessons, and on authorities dealing with national security matters. Soon after the scandal, the Chinese government requested The China Computer Federation Database Technical Committee to supervise and find out all the weak spots of communication and financial networks and provide all the hardware and software upgrades needed[42]. As for the case of Brazil, the regime explicitly highlighted the importance of the usage of domestic products and asked telecommunication companies to take foreign technologies and components away and substitute them with locally produced ones. China Unicom, for instance, removed Cisco routers because of new network security measures. Actually, Cisco was targeted directly from Snowden for being one of those companies who were wiretapped by the NSA, entering covertly in the Chinese territory.[43] However, the rejection of foreign technologies and foreign enterprises' participation in the Chinese market in the name of national security, implies a lack of competitiveness, expertise and intellectual property that will lead to a stalemate of innovation and inventiveness in the Chinese territory[44]. At the same time, successful domestic e-commerce companies like Alibaba, Baidu and Tencent are gaining competitive advantage and expanding their presence in an almost uncompetitive market thanks to the backing of the government itself [45]. The protectionist behavior and policies of the State towards national industries is causing more and more alarm amongst other countries and the WTO (World Trade Organization).

[42] Stephen CHEN, Kristine KWOK, Snowden effect changes US-China dynamic on cybersecurity, *The South China Morning Post,* 2014, available at: https://www.scmp.com/news/china/article/1532984/snowden-effect-changes-us-china-dynamic-cybersecurity, 2020-07-11.
[43] *Ibid*.
[44] Samson YUEN, Becoming a Cyber Power: China's Cybersecurity Upgrade and its Consequences, *China perspectives*, 2015, pp. 56-58.
[45] Sonali CHANDEL, Jingji ZANG, Yunnan YU, Jingyao SUN, Zhipeng ZHANG, The Golden Shield Project of China…, cit., p. 115.

It was in the light of this new threat that the concepts of cyber sovereignty and cyber security found breeding ground and the need of thickening national digital borders became essential. From 2013, China adopted several regulations and policies that aimed at concentrating the control over cyberspace at a central level, cyberspace authorities' powers increased, new cybersecurity committees were established in some metropolis, local leading groups were created in ten provinces and new restrictions for imported technologies, components and chips were set[46]. One of the industries that was mostly subjected to commercial reforms was the banking sector, in which new requirements asked suppliers to provide secret source codes, accept Chinese authorities' inspections and build software backdoors 软件后门 *Ruanjian houmen*[47]. These decisions were taken because experts recently discovered nearly 57.000 backdoors attacks from the United States in more than 1.700 Chinese websites, thus, sensitive data of strategic industries, like the financial world, must be protected.

Link between national security and Big Data

As it was previously said, from 2013, the President Xi Jinping emphasized in different speeches the interconnected nature between cybersecurity, Big Data, national security and their fundamental role in every aspect of society. In 2014, Internet security officially became a political priority and part of the national strategy through the President's statement: "There's no national security without cyber security […]" (没有网络安全就没有国家安全 *Meiyou wangluo anquan, jiu meiyou guojia anquan*). He explained that there won't be any modernization without informatization and, in order to become a world leader country in terms of Big Data and AI technologies, and to build a data-driven economy, high-tech, local infrastructures, as well as efficient network services and population's increased awareness, will

[46] Samson YUEN, Becoming a Cyber Power: China's Cybersecurity Upgrade…, cit., pp. 54-56.
[47] A *backdoor* in the hardware or software is an undocumented portal that permits an administrator to enter the system, but at the same time, could be used as a covert tool for the remote access of intelligence agencies into the computer in order to obtain and manage information. Available at: https://en.wikipedia.org/wiki/Backdoor_(computing), 2020-07-14.

be needed and even inserted in national development objectives.[48] When the first draft of the Cybersecurity Law was released in 2016, some supplemental explanations were shared in the governmental website. The concept of cyber sovereignty is now considered of the same fundamentality as the geographical and political sovereignty, and cyber-attacks or the destruction of China's networks are put at the same level of a bombardment, thus the State is obliged to intervene and protect its citizens. Moreover, with the adoption of the National Security Law 中华人民共和国国家安全法 *Zhonghua renmin gonghueguo guojia anquan fa*, this principle started having legal foundations, thus foreign nations have to respect its territorial and digital borders, and China will commit itself to observe its own regulation as well.

《当打击一国的网络所产生的破坏力不亚于对其领土领空进行轰炸时，国家有权利也有其义务对网络空间进行保护和规范，捍卫本国的网络主权和安全。[…] 因此，网络空间主权应该受到尊重，我国也同样尊重其他国家在网络空间的主权[49]》。

Subsequently, in the General Secretary's speech, emerged another relevant principle, that is the maintenance and protection of ideological security 意识形态安全 *Yishi xingtai anquan*. Internet is a place where people can exchange opinions and information, they easily create groups and influence each other, but it is important to keep in mind that it is also a space where the law must always be respected. For this reason, another role of the government cyber sovereignty is to prevent that the dominant values and ideology are questioned, ensuring stability and prosperity of the country and Chinese society[50]. Authorities are concerned that

[48] 《没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济 […]。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。》习近平：没有网络安全就没有国家安全， 2018 年，Available at: http://www.cac.gov.cn/2018-12/27/c_1123907720.htm, 2020-07-14.

[49] Office of the Central Cyberspace Commission, 维护网络主权对意识形态安全的作用 (The functions of maintaining cyber sovereignty for ideological security), 2017. Available at: http://www.cac.gov.cn/2017-03/20/c_1120657215.htm, 2020-07-14.

[50] *Ibid*.

through the possibility to talk and express oneself anonymously in the online communication process, the web could become the origin of temptations and immoral behaviors that would lead groups of people, who in the daily life wouldn't dare to act outside the law, to misbehave. Furthermore, they affirm that the influence of some foreign social media, videos and games is creating hostility among people and government, endangering the country's unity. Thus, not only cyber-attacks, but also the penetration of foreign theories, as potential threats, must be blocked through the monitoring of netizens' data.

> 《保证意识形态安全即是保证国家占主导地位的思想、政治意识形态不受侵害，使其稳定存在和健康发展。因此，能否维护和巩固意识形态安全直接关系到国家的繁荣稳定与社会长治久安。[…] 一些境外敌对势力通过发布影像、游戏等数字文化产品对网民进行意识形态的渗透，甚至利用各种社交平台煽动和宣扬民族仇恨、文化仇恨，给国家的安定团结带来隐患[51]。》

However, in order to ensure cyber security's activities and maintain sensitive information inside the country, the government insists in developing modern technologies and Big Data infrastructures locally, overthrowing foreign tech companies that were threatening China's Internet development plan[52].

During the National Cybersecurity and Informatization Work Conference in 2018, Xi made a discourse in which he reiterated the above-mentioned priorities of the cyberspace management, the necessity to link together data infrastructures and security mechanisms, coordinating them efficiently and stressed once again the acceleration of domestic development in the cybersecurity sector. In addition, for the first time, the military sphere was officially combined with civil issues like the digital world and Internet, extending the authority of the army in the cyberspace. According to Xi, achieving this fundamental goal will be possible thanks to the participation of the whole society. Users will discipline their behavior; the CCP

[51] Office of the Central Cyberspace Commission, 维护网络主权对意识形态安全的作用 *Weihu wangluo zhuquan dui yishi xingtai anquan de zuoyong* (The functions of maintaining cyber sovereignty for ideological security), 2017. Available at: http://www.cac.gov.cn/2017-03/20/c_1120657215.htm, 2020-07-14.
[52] Pengfei ZHANG, Xi stresses cybersecurity, Positive Internet Environment, *Xinhua News*, 2016. Available at: http://english.cctv.com/2016/04/26/ARTIytu6SlRGHWfOikb18ntG160426.shtml, 2020-07-14.

will supervise activities together with security societies, the government will manage the industry's development and companies will perform their duties and be accountant of leakages[53].

An example of the concrete use of Big Data and its policies to safeguard national interests is the safeguarding of the Belt and Road Initiative. From both maritime and terrestrial perspectives, this plan links together many countries with different backgrounds; thus, it is possible that unexpected events like social and political unrest could threaten international agreements. Deploying specific Big Data storage policies, could help governments understand, foresee and prevent dangerous risks and preserve national stability[54]. In Zhang, Xiao and Liu's research, data were extremely useful in identifying more than 10 million assaults, protests, fights and other violent events, through which they identified the level of unrest in BRI partners. In addition, the complete perspective Big Data are able to provide, can be useful to multinational companies to decide whether to invest or not in a specific nation's project and to the Chinese government to monitor internal and external turmoil and political instability[55].

Central Leading Group and CAC

Small leading groups have been powerful decision-making components of the Chinese political and administrative system since 1958, but they were fully developed under Deng Xiaoping and Hu Jintao's leaderships. These bodies managed very sensitive information and their decisions have always been able to influence the CCP Politburo, for this reason in the past, mass media rarely mentioned them. In 1980, relevant leading groups such as the Central Committee's (CC) Finance and Economy Leading Group and the CC Taiwan Affairs Leading

[53] Rogier CREEMERS, Paul TRIOLO, Graham WEBSTER, Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference, 2018, Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/, 2020-07-15.
[54] Chuchu ZHANG, Chaowei XIAO, Helin LIU, Spatial Big Data Analysis of Political Risks along the Belt and Road, *Sustainability*, Vol. 11 (2216), 2019, pp.1-16.
[55] Chuchu ZHANG, Chaowei XIAO, Helin LIU, Spatial Big Data Analysis of Political Risks along the Belt and Road, cit., p. 12.

Group were established, and in 1981, the CC Foreign Affairs Leading Group was created as well, in order to deal with the new market-economy reforms and the opening-up of the country[56]. Even if many characteristics about the functioning of this system continue to be unknown, during the Hu Jintao and Xi Jinping era, more information was shared with the population, due to the government's commitment to be more transparent. Moreover, from 2013, many others have been formed according to the society's new needs, like the Comprehensive Deepening Reform Leading Group and the Cyber Affairs Leading Group, and most of them are directly controlled by the President himself. All those examples, are classified as Permanent Small Groups, which means that they are operative for a long-lasting period, since they deal with topics and policies considered both strategic and of high priority for the nation[57].

Following Snowden's revelations and the exposed weaknesses in the Chinese cyber security system, the government felt the urgency to increase the operative and decision-making power of competent authorities. Hence, on February 2014, the Central Cyber Security and Informatization Leading Group 中央网络安全和信息化领导小组 *Zhongyang wangluo anquan he xinxihua lingdao xiaozu* was established. Its objectives were mainly based on the protection of national interests, Big Data and networks, the drafting of major development policies and strategies and the reduction of threats coming from the West[58]. In order to achieve these goals, the team must be composed by members with political, professional and strategical qualities, among them Li Keqiang and Liu Yunshan, who at the time were also representatives of the Standing Committee of the Political Bureau of the CCP Central Committee[59]. To actively and efficiently carry out such a supervision and many other tasks, the group formed the already

[56] Alice MILLER, More Already on the Central Committee's Leading Small Groups, *China Leadership Monitor*, n. 44, 2013, p. 4.
[57] Alice MILLER, More Already on the Central Committee's Leading Small Groups…, cit., p. 2.
[58] Samson YUEN, Becoming a Cyber Power: China's Cybersecurity Upgrade…, cit., p. 54.
[59] People's Republic of China State Council, 中央网络安全和信息化领导小组第一次会议召开 *Zhongyang wangluo anquan he xinxihua lingdao xiaozu diyici huiyi zhaokai* (The first meeting of the Central Cyber Security and Informatization Leading Group), 2014. Available at: http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm, 2020-07-15.

mentioned Cyberspace Administration of China, substituting the State Internet Information Office (SIIO) led by the State Council Information Office[60].

In 2018, due to a major effort of centralization of the cyberspace department's power and to the government's desire of relaxation of bureaucratic procedures, the Central Leading Group of Cyber Affairs was enhanced CCP Central Commission for Cybersecurity and Informatization Office 中央网络安全和信息化委员会办公室 *Zhongyang wangluo anquan he xinxihua weiyuanhui bangongshi*, highlighting the immediate dependence to the Party's internal mechanisms[61]. This move aimed at concentrating several cybersecurity departments of different ministries and offices in a unique comprehensive body, in order to quicken the policy-making process and easily individuate accountability. The first office dealing with cyberspace issues, that was incorporated in the Commission, was the one of the Ministry of Industry and Information Technology 工业和信息化部 *Gongye he xinxihua bu* (MIIT), whose responsibilities are now reduced to the management of the telecommunication networks and its inner managerial activities[62].

[60] Samson YUEN, Becoming a Cyber Power: China's Cybersecurity Upgrade…, cit., p. 54.
[61] People's Republic of China State Council, 国务院关于机构设置的通知 *Guowuyuan guanyu jigou shezhi de tongzhi* (State Council's notice about the institutional setting), 2018. Available at: http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm, 2020-07-20.
[62] People's Republic of China State Council, 中共中央印发《深化党和国家机构改革方案》*Zhonggong zhongyang yinfa "shenhua dang he guojia jigou gaige fang'an"* (The Party's Central Committee published the "Deepening the Party and State's Institutional Reform Plan"), 16th section, 2018. Available at: http://www.gov.cn/zhengce/2018-03/21/content_5276191.htm#1, 2020-07-20.

2.3 Relevant regulations

National Security Law

As it was previously explained, the information security sphere and Big Data started to be conceived as relevant actors of protection of the country from the beginning of the 21st century, but their integration became consistent only after the promulgation of the National Security Law in 2015. Generally speaking, before the enactment of this law in China, the concept of national security had always been interpreted with a conventional meaning, implying mostly the safeguarding of terrestrial, marine and air space borders. Moreover, in the national security law of 1993, the significance of the word was further developed with the introduction of foreign espionage threats and the necessity to protect the country and individuate in advance these illegal activities[63]. Lately in 2014, in order to abrogate the existing regulation and prepare a more comprehensive one, an independent law, the People's Republic of China Counter Espionage Law, was specifically devoted to the theme of espionage. It was with the new regulation that the idea of national security reached its maximum extent, which includes several societal and governmental aspects like economy, politics, culture, cyber and territorial security, religious beliefs and ideology, etc.[64]. In addition, in Articles 2 and 3 is provided a general clarification that defines the country security status as a condition of absence of dangers or threats from the external environment, foreign nations, as well as from internal forces. The government's sovereignty and unity, the overall borders, social welfare and economic, political and military development are guaranteed and safeguarded by the law, together with the regime commitment to promote internationally the evolution of national security with Chinese characteristics[65]. To what concern data protection and cyber security, the regulation demands

[63] Kurt TIAM, Sherry GONG, Andy HUANG, Andrew MCGINTY, Mark PARSONS, China's New National Security Law Creates More Insecurity For Foreign Businesses, *Hogan Lovells*, 2015, p. 1
[64] *Ibid.*
[65] 《*第二条* 国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。》

to store locally all the infrastructures, network systems and databases and to allow authorities' recurring monitoring and intervention. This last requirement, in particular, is fundamental for the Chinese government to continue preserving Internet supervision and the regime sovereignty. For instance, according to Articles 24 and 25, providing locally manufactured high-tech machinery and components, R&D and innovation is strongly encouraged by the State as a matter of national security. This decision is both a strategic choice that creates entry barriers for foreign enterprises and facilitates domestic tech companies, but it also represents a way in which the Party can introduce itself inside the sector and have access to every kind of information, dismantling those which can threat Chinese interests in the cyberspace (Art. 25)[66].

"Art. 2 "National security" means a status in which the regime, sovereignty, unity, territorial integrity, welfare of the people, sustainable economic and social development, and other major interests of the state are relatively not faced with any danger and not threatened internally or externally and the capability to maintain a sustained security status."

《第三条 国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。》

"Art. 3 All national security work shall adhere to the overall national security view, regard people's security as the tenet, regard political security as the fundamental, regard economic security as the basis, regard military, cultural, and social security as the safeguard, and by promoting international security, maintain national security in all fields, build a national security system, and walk a path of national security with Chinese characteristics." Available at: http://en.pkulaw.cn/display.aspx?id=93dad838890b8468bdfb&lib=law, 2020-07-20.

[66] 《*第二十四条* 国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术，[...]。》

"Article 24 The state shall strengthen the building of capability of indigenous innovation, accelerate the development of indigenous and controllable strategic new and high technologies and core technologies in important fields, […]."

《第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。》

"Article 25 The state shall build a network and information security guarantee system, improve network and information security protection capability, strengthen the innovation research, development, and application of network and information technologies, realize the controllable security of the core technologies and crucial infrastructure of network and information and the information systems and data in important fields; strengthen network management, prevent, frustrate, and legally punish network attack, network invasion, network information theft, dissemination of illegal and harmful information, and other network-related infractions of law and crimes, and maintain the state's sovereignty, security, and development interests in the cyberspace." Available at: http://en.pkulaw.cn/display.aspx?id=93dad838890b8468bdfb&lib=law, 2020-07-20.

Cyber Security Law

In the first chapter, it was discussed the decisive impact the Cyber Security Law (2017) had on the administration of the cyberspace and the protection of Chinese consumers' data. Moreover, it established a third model of privacy regulation between the European Union and the United States, as well as let China classify as one of the leader countries in Asia in terms of consumers' safeguarding rights. However, an incongruence emerged between the regime's effort to better protect private actors in society from cyber-crimes or foreign threats and its contemporary intent to exploit citizens' sensitive and non-sensitive data, without considering or respecting any privacy rights or the previously mentioned set of laws the State itself have recently established. This ambivalence is evident even in the Cyber Security Law, where many articles are pioneers of Chinese personal information protection and others allow the government and competent authorities to control and have access to data, limiting this defense in the name of national security issues[67].

In the first section, called General Provisions, many articles clearly present the role the State plays in the monitoring process of people's life. First, Article 1 immediately describes the primary objective of the regulation, that is maintaining cyber security and protecting the government's sovereignty of the cyberspace[68]. Then, Article 5 provides to the regime the legal authorization to control critical information databases and prevent cyber-crimes and threats, that could damage national security, both inside and outside the country. According to Article 9, among the several duties and responsibilities network operators have to face, if they want to work in China, create websites, apps or deal with every kind of personal information, are requested to accept the government and public organs' surveillance:

[67] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law: a third way between the U.S. and the EU?, *Penn State Journal of Law and International Affairs*, Vol. 8 (1), 2020, pp. 49-51.
[68] *《第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。》* Cyberspace Administration of China, 2016, Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm, 2020-07-21.

《 网络运营者开展经营和服务活动，必须遵守法律、[…]，接受政府和社会的监督，承担社会责任[69]。》

Furthermore, they are also required to grant Chinese authorities all the assistance needed in order to let them freely investigate potential illegal acts and safeguard the country's cyberspace from criminals (Art. 28)[70].

A characteristic that is reiterated in many articles throughout this law is the importance attributed to the social morality 社会公德 *Shehui gongde* that each individual should have while using instruments like the Internet. China's sovereignty must always be guaranteed and, through the supervision and limitations of contents and information flows, the government's aim is to suggest the best possible style of behavior. Thus, people are active participants and represent a watchful eye for the overall social well-being and harmony. Article 12, for instance, clarifies that every individual or organization that uses or possesses networks must in any case be in compliance with the Chinese Constitution and regulations, must not put at risk cyber security, public order 公共秩序 *Gonggong zhixu*, national security, interests and honor 国家荣誉 *Guojia rongyu*[71].

In the third Chapter of CSL, entitled Network Operations Security, Article 35 states that operators with services or networks that are suspected to be dangerous for national security, are mandatorily subjected to security inspections or reviews[72]. Article 37 introduces the concept of data localization, which was previously explained in Chapter 1 of this thesis. It is based on the requirement that all critical information operators are obliged to store locally those sensitive

[69] Cyberspace Administration of China, 中华人民共和国网络安全法 *Zhonghua renmin gongheguo wangluo anquanfa* (Cyber Security Law of People's Republic of China), 2016. Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm, 2020-07-21.
[70] *Ibid*.
[71] *Ibid.*
[72] Yan LUO, Zhijing YU, China Issues New Measures on Cybersecurity Review of Network Products and Services, *Covington – Inside Privacy*, 2020. Available at: https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/, 2020-07-25.

data obtained from Chinese citizens[73]. Not only it is one of the fundamental elements of this law, but is also an exception among every other data protection and data management systems in the world.

In addition, on 27 April 2020, CAC officially published the Measures on Cybersecurity Review 网络安全审查办法 *Wangluo anquan shencha banfa*, whose was to clarify criteria and details about the conditions, time periods and procedures of security reviews[74]. Some of the most relevant characteristics, that were added by this law to the overall set of cybersecurity regulations and specifications, are the creation of an Interagency Review Body and some concrete examples of the type of network or operator that will be inspected, like high-performance infrastructures, significantly big databases, cloud services, principal network apparatus etc. However, this definition still remains flexible enough to allow authorities to introduce potential new cases. On the contrary, operators should try to foresee the risks that a determined service or product would cause and inform the competent Office[75]. To what concern the new comprehensive body, it will be composed by eleven statal agencies (MIIT, Ministry of Public Security, Ministry of National Security, Ministry of Commerce, Ministry of Finance, the People's Bank of China, the State Administration for Market Regulation, the National Radio and Television Administration, the National Administration of State Secrets Protection and the State Cryptography Administration), called also "members", who will separately take charge of different aspects of a security investigation, depending to the extent of their departments' responsibilities[76].

[73] Emmanuel PERNOT-LEPLAY, China's approach on data privacy law…, cit., p. 49.
[74] Yan LUO, Zhijing YU, China Issues New Measures on Cybersecurity Review of Network Products…, cit. Available at: https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/, 2020-07-25.
[75] *Ibid*.
[76] Yan LUO, Zhijing YU, China Issues New Measures on Cybersecurity Review of Network Products…, cit. Available at: https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/, 2020-07-25.

Regulation on the Internet Security Supervision and Inspection

At the end of 2018, another document, the Regulation on the Internet Security Supervision and Inspection 公安机关互联网安全监督检查规定 *Gong'an jiguan hulianwang anquan jiandu jiancha guiding* was adopted by the Chinese government. It specifically addresses to the extent of authorities' freedom of intervention and supervision, determining their range of different approaches, conditions and procedures. It is relatively concise, since it presents twenty-nine articles altogether, divided into five chapters. To what concern the lexicon of several Chinese sets of laws, which was criticized for being unclear and open to misinterpretations, the general meaning of "network operators" which was amply used in the CSL, is substituted in this law from the expression of "Internet network providers"[77]. Due to the vagueness of the definition of "network operators", Article 9 seeks to clarify which categories are included in the new regulation, that are Internet access suppliers, Internet services providers, companies that hold databases or furnish domain name services, entities that provide Internet to the public like Internet cafes and, lastly, " providers of other Internet services"[78]. Instead, the authorities who are appointed to fulfill the State's objective, work in Public Security Bureaus (PSB) and are usually local and county-level police officers. Since the adoption of the Regulation, PSBs have gained much power in their inspection practices, differentiating two different ways of intervention. The first method is based on physical surveillance, police are

[77] Yan LUO, Ashden FEIN, Huanhuan ZHANG, Moriah DAUGHERTY, China Releases New Regulation on Cybersecurity Inspection, *Covington Inside Privacy*, 2018. Available at: https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/, 2020-07-25.

[78] 《*第九条* 公安机关应当根据网络安全防范需要和网络安全风险隐患的具体情况，对下列互联网服务提供者和联网使用单位开展监督检查：
（一）提供互联网接入、互联网数据中心、内容分发、域名服务的；
（二）提供互联网信息服务的；
（三）提供公共上网服务的；
（四）提供其他互联网服务的 [...]。》
People's Republic of China State Council, 中华人民共和国公安部令: 公安机关互联网安全监督检查规定 *Zhonghua renmin gongheguo gong'an buling: gong'an jiguan hulianwang anquan jiandu jiancha guiding* (Order of the Ministry of Public Security of RPC: Regulation on the Internet Security Supervision and Inspection), 2018. Available at: http://www.gov.cn/gongbao/content/2018/content_5343745.htm, 2020-07-26.

authorized to access the company's documents, copy them and in case of necessity, talk directly with the chief executive without previous notice. In Article 15 is stated that they can enter companies' databases, work places and computer rooms, ask for immediate demonstrations and explanations, obtain relevant data for security matters and control all the other technical aspects[79]. The second one (Art. 16) consists in remotely testing and supervising the company networks and files, however the firm must be warned before the PSB's intervention and must know the reasons why and when the inspection will take place. In addition to that, in case of specific consultations with the police, it is possible that even a third party with suitable knowledge would have access to companies' information[80]. Nevertheless, all the private information, State or commercial secrets, that could be revealed during the inspection, must in any case be kept confidential (Art.17)[81]. At the end of the monitoring process, authorities will write up a final report that must be necessarily signed by the Internet network provider. If he disagrees with the judgement of the police, he has the right to provide explanations, however refusing to sign it will be automatically reported inside the document (Art.18)[82]. The Regulation relies on national laws like the CSL and the Counterterrorism Law in order to establish

[79] 《*第十五条* 公安机关开展互联网安全现场监督检查可以根据需要采取以下措施:
（一）进入营业场所、机房、工作场所;
（二）要求监督检查对象的负责人或者网络安全管理人员对监督检查事项作出说明;
（三）查阅、复制与互联网安全监督检查事项相关的信息;
（四）查看网络与信息安全保护技术措施运行情况。》
People's Republic of China State Council, 中华人民共和国公安部令: 公安机关互联网安全监督检查规定 *Zhonghua renmin gongheguo gong'an buling: gong'an jiguan hulianwang anquan jiandu jiancha guiding* (Order of the Ministry of Public Security of RPC: Regulation on the Internet Security Supervision and Inspection), 2018. Available at: http://www.gov.cn/gongbao/content/2018/content_5343745.htm, 2020-07-26.

[80] Yan LUO, Zhijing YU, China Issues New Measures on Cybersecurity Review of Network Products…, cit. Available at: https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/, 2020-07-26.

[81] 《*第十六条* 公安机关对互联网服务提供者和联网使用单位是否存在网络安全漏洞，可以开展远程检测。公安机关开展远程检测，应当事先告知监督检查对象检查时间、检查范围等事项或者公开相关检查事项，不得干扰、破坏监督检查对象网络的正常运行。
第十七条 [...]。网络安全服务机构及其工作人员对工作中知悉的个人信息、隐私、商业秘密和国家秘密，应当严格保密，不得泄露、出售或者非法向他人提供。[...]》
People's Republic of China State Council, 中华人民共和国公安部令: 公安机关互联网安全监督检查规定, 2018. Available at: http://www.gov.cn/gongbao/content/2018/content_5343745.htm, 2020-07-26.

[82] Yan LUO, Zhijing YU, China Issues New Measures on Cybersecurity Review of Network Products…, cit. Available at: https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/, 2020-07-26.

administrative penalties, since it was created by the Ministry of Public Security, at a departmental level, thus has no jurisdiction in independently setting new penalizing provisions. For instance, the refusal to collaborate and assist public security officers during their inspections, will be punished in accordance with Article 69 of the CSL (Art.21)[83]. Accordingly, Article 69 of the Cybersecurity Law states that in case of minor violations, the company will be required to immediately intervene and make corrections, but if the executive refuses to cooperate, impedes authorities' job, fails in improving critical mistakes and the violation is serious, the company and managers will be both fined between RMB 50.000 and 500.000[84].

The Counterterrorism Law

The Counter Terrorism Law (CTL) of the People's Republic of China 中华人民共和国反恐主义法 *Zhonghua renmin gongheguo fankong zhuyi fa*, was adopted in 2015 and was lately amended in 2018. Its main objective is preventing terrorism in the country, punishing extremists and granting national, public and people's protection and, for this reason, is introduced in the country's security strategy. By the enactment of this regulation, the Chinese government expects its citizens, domestic and foreign companies to collaborate and assist authorities, rising concerns of international actors and investors.

Article 3 defines the word "terrorism" as

> "Any proposition or activity that, by means of violence, sabotage or threat, generates social panic, undermines public security, infringes upon personal and property rights, or menaces state

[83] 《*第二十一条*（六）拒不为公安机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助的，依照《中华人民共和国网络安全法》第六十九条第三项的规定予以处罚。》
People's Republic of China State Council, 中华人民共和国公安部令: 公安机关互联网安全监督检查规定, 2018. Available at: http://www.gov.cn/gongbao/content/2018/content_5343745.htm, 2020-07-26.

[84] 《*第六十九条* 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款 [...]。》
Cyberspace Administration of China, 中华人民共和国网络安全法, 2016. Available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm, 2020-07-27.

authorities and international organizations, with the aim to realize political, ideological and other purposes."[85]

After the attack of September 11 in the US and other following terrorist threats to Chinese citizens in the Xinjiang region and in foreign countries, China started setting new police units and a central leading small group, as well as implementing new regulations and amendments, in which it clearly defined basic concepts like terrorism and terrorist organizations[86]. This is a comprehensive law, that unifies together institutions such as security authorities, police, courts and the government, and in addition, it monitors different areas of interest like media, ethnicity and ideology, education, financial and information systems etc. For instance, in Article 17, the government requires different departments to collaborate in people's anti-terrorism education and publicity, expecting the participation of entities like press, broadcasting instruments and Internet network operators[87].

As cyber security is considered a national security matter and its related crimes can cause social and ideological instability, this field has been integrated in the Counterterrorism Law with the introduction of some provisions and obligations about Internet services and operators. According to Articles 18 and 19, Internet service providers have the responsibility to supervise their networks and immediately block or delete any terrorist content. Subsequently, they have to strengthen their filtering systems or close their websites, keep relevant information and deliver them to the police. Even foreign Internet websites are subjected to the control and censorship of Chinese public and private actors. Moreover, Internet operators are legally

[85] Peking University, Counterterrorism Law of the People's Republic of China (2018 Amendment), 2018. Available at: http://en.pkulaw.cn/display.aspx?id=92bb5d4a2bc3fdd3bdfb&lib=law&SearchKeyword=counterterrorism&SearchCKeyword=, 2020-07-28.

[86] Murray Scot TANNER, James BELLACQUA, China's Response to Terrorism, CNA Analysis & Solutions, 2016, p. 38.

[87] 《*第十七条* […] 新闻、广播、电视、文化、宗教、互联网等有关单位，应当有针对性地面向社会进行反恐怖主义宣传教育。》
Peking University, Counterterrorism Law of the People's Republic of China…, cit., 2018. Available at: http://en.pkulaw.cn/display.aspx?id=92bb5d4a2bc3fdd3bdfb&lib=law&SearchKeyword=counterterrorism&SearchCKeyword=, 2020-07-28.

obliged to handle information, decrypt messages and offer all the technical support to competent authorities during an investigation, before and after an extremist activity takes place[88]. This concept is further highlighted in Article 46 were it is stated:

> "The relevant departments shall, according to the requirements of the national counterterrorism intelligence center, provide the information obtained in security protection as provided for in Chapter III of this Law in a timely manner."[89]

Besides Internet providers, also financial and rental services, hospitality, transportation and many other sectors, have to register and supervise the identity of their customers and refuse to let clients have access to their services if they do not accept to provide their personal information[90].

As it was previously analyzed in this work, the government intervention isn't just limited to setting new regulations concerning cyber security or inspections of people's online activities, but it involves also other forms of supervision integrated together. For instance, Article 29 of the CTL recalls the above-mentioned relevance of the role of informal surveillance organizations in society. When an individual is involved in illegal actions, that do not punished with imprisonment, neighborhood committees, workplaces, schools and families are requested to keep an eye on him, re-educate him properly, thus correcting his behavior[91]. Nevertheless,

---

[88] 《*第十八条*　电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。

第十九条　电信业务经营者、互联网服务提供者应当依照法律、行政法规规定，落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播；发现含有恐怖主义、极端主义内容的信息的，应当立即停止传输，保存相关记录，删除相关信息，并向公安机关或者有关部门报告。》
Peking University, Counterterrorism Law of the People's Republic of China…, cit., 2018. Available at: http://en.pkulaw.cn/display.aspx?id=92bb5d4a2bc3fdd3bdfb&lib=law&SearchKeyword=counterterrorism&SearchCKeyword=, 2020-07-28.

[89] *Ibid*.

[90] Eric CARLSON, Ashwin KAJA, Yan LUO, China Enacts New Counter-Terrorism Law, *Inside Privacy – Covington*, 2016. Available at: https://www.insideprivacy.com/international/china-enacts-new-counter-terrorism-law/, 2020-07-29.

[91] 《第二十九条　对被教唆、胁迫、引诱参与恐怖活动、极端主义活动，或者参与恐怖活动、极端主义活动情节轻微，尚不构成犯罪的人员，公安机关应当组织有关部门、村民委员会、居民委员会、所在单位、就读学校、家庭和监护人对其进行帮教。[…]》

the language and some definitions inside the regulation are still unclear and can be interpreted with broader meanings, allowing the government and each department to widen or constrict the limits of the law according to the specific need[92].

In the light of the set of cybersecurity regulations approved in recent years by China, which allow police units to have access to a broader extent of information, foreign companies who want to have an opportunity in the Chinese market have been implicitly forced to comply with the new conditions and change their business and operating model on the Internet.

Peking University, Counterterrorism Law of the People's Republic of China…, cit., 2018. Available at: http://en.pkulaw.cn/display.aspx?id=92bb5d4a2bc3fdd3bdfb&lib=law&SearchKeyword=counterterrorism&SearchCKeyword=, 2020-07-29.

[92] Eric CARLSON, Ashwin KAJA, Yan LUO, China Enacts New Counter-Terrorism Law, Inside Privacy – Covington, 2016. Available at: https://www.insideprivacy.com/international/china-enacts-new-counter-terrorism-law/, 2020-07-29.

2.4 Glossary of terms

▪ Administrative System of Baojia	保甲
▪ Backbone Network	骨干网络
▪ Central Commission for Cybersecurity and Informatization Office	中央网络安全和信息化委员会办公室
▪ Central Leading Group for Cyberspace Affairs	中央网络安全和信息化领导小组
▪ Counter Terrorism Law	中华人民共和国反恐主义法
▪ Cyber Crime	网络犯罪
▪ Cyber Sovereignty	网络主权
▪ Four Sprouts	四端
▪ Golden Shield Project	金盾工程
▪ Great Firewall of China	防火长城
▪ Ideological Security	意识形态安全
▪ Local Police Station	派出所
▪ Measures on Cybersecurity Review	网络安全审查办法
▪ Ministry of Industry and Information Technology	工业和信息化部
▪ National Honor	国家荣誉
▪ National Security Law	中华人民共和国国家安全法
▪ Neighborhood Committee	居委会
▪ Organic Law of the Urban Residents'	中华人民共和国城市居民委员

Committees of the RPC	会组织法
▪ Public Order	公共秩序
▪ Regulation on the Internet Security Supervision and Inspection	公安机关互联网安全监督检查规定
▪ Security Service Firm	保安服务公司
▪ Social Morality	社会公德
▪ Software Backdoor	软件后门
▪ Total Society Strategy	综合治理
▪ Work Unit	单位

CHAPTER 3

Foreign enterprises dealing with Big Data in China

From the moment Big Data successfully appeared in the global society, they have been placed at the center of several international cooperation, agreements among private and public companies and even disputes between governments. Chapter 1 and 2 of this thesis discussed the value of Big Data as both an economic and political source of power and the dichotomy of the Chinese State's role as a protector of sensitive information and primary user of citizens' data.

Generally speaking, countries who understood the relevance of the data-driven economy, are increasingly eager to develop new AI technologies, databases, and data analytics systems, which could allow them to gain competitive advantage. At the same time, they are also starting to intensify the protection of local consumers with the establishment of new regulations and the amendment of already existing ones. In recent years, the Chinese government and the Chinese Consumers Association have seen national netizens being victim of personal information violations and data breaches. In order to tackle this problem, they provided comprehensive laws and non-binding documents, such as the Cyber Security Law and the Information Technology – Personal Information Security Specification[1]. By classifying itself as guardian of people's data and privacy, the government aims at supervising data transfer and storage from the misuse of private and foreign players and further, broadening Chinese consumers' personal information rights.

[1] Huw ROBERTS, Josh COWLS, Jessica MORLEY, Mariarosaria TADDEO, Vincent WANG, Luciano FLORIDI, The Chinese Approach to Artificial Intelligence: an Analysis of Policy, Ethics, and Regulation, AI & Society, 2019, pp. 1-20.

The second chapter explained how associating the Big Data industry to a matter of national security, allows the Chinese leadership to become the first user and collector of people's information. Storing domestically large amount of data contributes to the operation of surveillance systems, whose aim is to maintain the country's internal stability. These systems imply the Social Credit System for the financial field, Skynet for the personal security or tracking technologies for tackling COVID-19 pandemic in the case of public health. Furthermore, the operations of newly established monitoring bodies, such as the CCP Central Commission for Cybersecurity and Informatization Office, are fundamental to protect government's sovereignty in the cyberspace. In fact, cyber-sovereignty and the domestic management of Big Data are synonym of lack of cyber threats and political stability. Especially after Snowden's scandal, citizens, companies and foreign nations' flows of data are subjected to the strict control of governmental authorities, who can now access vast amount of information for investigation purposes.

Based on this analysis, Chapter 3 is going to present recent international disputes about Big Data, concerning the Chinese and American tech decoupling, U.S. and Chinese protectionism and measures of data localization, and the consequent Chinese local transformations and reactions. It aims at representing some changes and challenges foreign enterprises have to face when operating in the country or collaborating with Chinese firms and dealing at the same time with critical information.

3.1 US-China decoupling

When talking about Big Data, one of the main drivers of Chinese reforms can be directly related to the uncertain Sino-American relations. Since the ascent of Xi Jinping, some researchers already suggested the possible beginning of a new Cold War between the two countries, but it was with the Trump administration that the US-China decoupling started being a concrete threat[2]. The word "decoupling" is generally defined as the situation in which two or more systems or entities, which used to operate together, are now separating, or are not developing in the same way anymore[3]. In the case of the two global powers, the economic separation is embracing two different spheres: the trade one and the technological one.

First, trade decoupling 贸易脱钩 *Maoyi tuogou* focuses on decreasing the dependence on each other's imports and exports through the reduction of their volumes, together with the imposition of tariffs on Chinese and American goods[4]. For instance, Trump declared taxes on more than $268 billion of Chinese products, whereas the Chinese government charged nearly $110 billion on US commodities. Moreover, due to this trade war, ASEAN (Association of Southeast Asian Nations) have replaced the U.S. as China's second trading partner[5][6].

Second, technological decoupling 技术脱钩 *Jishu tuogou* refers to the contraction of technological cooperation between the two largest economies, between the know-how of respective companies and the overall trade and investment volume[7]. In recent years, both China

[2] Michael A. WITT, Prepare for the U.S. and China to Decouple, *Harvard Business Review*, 2020. Available at: https://hbr.org/2020/06/prepare-for-the-u-s-and-china-to-decouple (2020-08-22).
[3] Cambridge Dictionary, available at: https://dictionary.cambridge.org/dictionary/english/decoupling (2020-08-22).
[4] Li WEI, Towards Economic Decoupling? Mapping Chinese Discourse on the China–US Trade War, *The Chinese Journal of International Politics*, Vol. 12(4), 2019, pp. 519–556.

[5] Behind China's first trading partner, that is the European Union.
[6] Li WEI, Towards Economic Decoupling? Mapping Chinese Discourse on the China–US Trade War…, cit.
[7] *Ibid*.

and the U.S. have undertaken extreme measures in order to keep domestic data within their countries' borders and protect national security.

American measures towards Chinese companies

Reportedly, the main commercial objectives of Trump administration are protecting intellectual property of American companies from the Chinese government's scrutiny, reducing unfair competition and monitoring the flow of information.[8] Actually, China has been accused of perpetrating industrial espionage by foreign nations for decades. For example, in 2013, an American cybersecurity agency, called Mandiant, published a report in which it showed the theft of sensitive data from more than 140 institutions operating in different sectors. The Advanced Persistent Threat group, that had connections with the Chinese People's Liberation Army, was considered accountable for the crime[9]. From an international legal perspective, each country has the right to exercise sovereignty within its borders and industries as long as does not prevent other nations to exercise this right as well. It means that China can manage domestic business by setting specific obligations, but at the same time, foreign countries are also legally free to block Chinese goods or services, if they consider them as national security threats[10]:

"Article XXI: Security Exceptions: Nothing in this Agreement shall be construed (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests[11]."

Among the above-mentioned measures, in 2018, the American government stopped providing electronic components to the Chinese tech company Zhongxing Telecommunication Equipment

[8] Ewan SUTHERLAND, The strange case of US v. ZTE: a prosecution, a ban, a fine and a presidential intervention, Digital Policy, Regulation and Governance, Emerald Publishing Limited, Vol. 21 (6), 2019, pp. 550-573.
[9] Kadri KASKA, Henrik BECKVARD, Tomáš MINARIK, Huawei, 5G and China as a Security Threat, CCDCOE (Nato Cooperative Cyber Defence Centre of Excellence), 2019, p. 10.
[10] Kadri KASKA, Henrik BECKVARD, Tomáš MINARIK, Huawei, 5G and China as a Security Threat…, cit., p. 13.
[11] The General Agreement on Tariffs and Trade, *World Trade Organization (WTO)*, 1947, Article XXI. Available at: https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI (2020-08-28).

(ZTE) Corporation 中兴通讯股份有限公司 *Zhongxing tongxun gufen youxian gongsi,* after the firm was accused of having commercial ties and selling surveillance systems like interception tools, hardware and software to North Korea and Iran.[12] After a five-year inspection, undertaken by the Bureau of Industry and Security, the U.S. charged the corporation with a $1billion fine and included the company in the "national threat" blacklist[13]. Soon after the ban, the smartphone producer was forced to stop its manufacturing because of a lack of semiconductors. This move clearly confirmed the dependence many Chinese tech firms have on American products and components[14]. Then, in 2019, another tech giant, Huawei 华为技术有限公司, was also subject to American charges, since investigations showed the company had collaborated with sanctioned countries. This is a decision that derives from even deeper concerns, that are more specifically tied to the company's 5G technologies. International institutions fear that the Chinese government has gained the power to monitor databases and valuable information through Huawei, an approach that is now legal in the country[15]. Actually, through the Chinese Cybersecurity Law and the Regulation on the Internet Security Supervision and Inspection by Public Security Agencies, and according to the National Intelligence Law 中华人民共和国国家情报法 *Zhonghua renmin gongheguo guojia qingbao fa* (2018)*,* private actors as well as individuals are required to provide assistance and support to Public Security

[12] Relations between Iran and the U.S. have been troubled for decades. From 2018, conflicts became more severe due to nuclear threats, American sanctions got higher and imposed more tariffs on those companies who worked together with Iranian firms or Iranian government. Lastly, in 2020, Qasem Soleimani is killed by an American drone, forcing Iran to exit the nuclear treaty.
Available at: https://www.bbc.com/news/world-middle-east-24316661, (2020-08-26).
North Korea has been experiencing a similar treatment from the U.S since 2017. The nuclear tests raised concern over the American government and caused the imposition of commercial taxes and limitation from the world largest economy.
[13] Antonio VILLAS-BOAS, Huawei has been blacklisted by the US government. Here's what happened to the last Chinese tech company that got the 'death penalty.', *Business Insider*, 2019. Available at: https://www.businessinsider.com/huawei-us-ban-similar-to-zte-us-ban-2019-5?IR=T (2020-08-26).
[14] Ewan SUTHERLAND, The strange case of US v. ZTE: a prosecution, a ban, a fine and a presidential intervention…, cit., p. 555.
[15] Kadri KASKA, Henrik BECKVARD, Tomáš MINARIK, Huawei, 5G and China as a Security Threat…, cit., pp. 1-26.

authorities and intelligence organizations (Art. 7) [16]. However, their extent of cooperation and support towards the government is not clearly defined. Huawei had been accused many times of espionage and intellectual property theft and, in the past, two executives have been imprisoned in Canada and Poland. On the other side, the firm has always affirmed the absolute absence of the Chinese regime in its business and denies to have provided consumers' information to any institution or government [17]. At last, on 30th June 2020, the Federal Communications Commission (FCC) of the U.S. released a document (the Order), which states the removal of Huawei Company and ZTE Corporation from the list of enterprises that receive federal subsidy funds to keep, modify and administer technological infrastructures and services in the U.S.[18]. This is due to the fact that both companies are officially defined by the American institution as national security threats. According to the Order, the participation of the Chinese government in commercial entities' matters could imply the use or transfer of customers and networks' data for surveillance purposes[19]. This fear is further confirmed by the Opinion on Strengthening the United Front Work of the Private Economy in the New Era 关于加强新时代民营经济统战工作的意见 *Guanyu jiaqiang xinshidai minying jingjizhan gongzuo de yijian*, a document approved by the CCP Central Committee General Office on September 2020, whose purpose is connecting private entities to a CCP department called the United Front Work Department. According to the Chinese State, linking the CCP to the private sphere is another

[16] "Article 7: Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The State protects individuals and organizations that support, assist and cooperate with national intelligence work." National Intelligence Law of the People's Republic, 2017. Available at: https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (2020-09-30).
[17] Kadri KASKA, Henrik BECKVARD, Tomáš MINARIK, Huawei, 5G and China as a Security Threat…, cit., p. 8.
[18] Chief of Public Safety and Homeland Security Bureau, Order DA 20-690, *Federal Communications Commission*, Washington, 2020.
[19] *Ibid*.

step towards the enhancement of the socialist system with Chinese characteristics and broadening the Party's control to another aspect of society[20].

On the contrary, the debate about data management between the President of the United States, Donald Trump, and ByteDance Ltd., the owner of the popular app TikTok, is still open and particularly intense. The company, as previously said in this thesis, have faced the American authorities' diffidence, especially concerning the data collection and transfer process. Furthermore, in recent days, the Chinese app has been at the center of other critics concerning the methods of recording costumers' tracking information through MAC addresses. MAC addresses are unique identifier encoded in smartphones, that can't be modified by consumers' choice. In the past, companies used to take advantage of this tool for advertising reasons, since these data allow them to identify more precisely individuals and their habits. Despite the ban of this tool by Google and Apple[21], their functioning on TikTok was hidden in a second layer of encryption and was exploited thanks to a bug in the system until November 2019[22]. In the light of these new revelations, on 6 August 2020, Trump ordered a halt to ByteDance's businesses with American enterprises within 45 days. At the same time, the Chinese company is considering selling US assets to a domestic company like Microsoft, Oracle or Walmart or temporary interrupt the business in the country[23].

Chinese measures toward foreign companies

As it was already mentioned, also China took radical decisions in order to secure the protection of data from foreign illegal access and improve the extent of surveillance within its territories.

[20] CPC Issues Guidelines for Strengthening United Front Work Involving Private Sector, China Daily, 2020. Available at: https://www.chinadaily.com.cn/a/202009/16/WS5f617e66a31024ad0ba79e09.html (2020-10-01).
[21] Apple forbid MAC addresses in 2013, whereas Google's Android system banned them in 2015.
[22] Kevin POULSEN, Robert MCMILLAN, TikTok Tracked User Data Using Tactic Banned by Google, The Wall Street Journal, 2020. Available at: https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738 (2020-08-28).
[23] China's ByteDance asks TikTok to prepare for US shutdown: report, *Aljazeera News*, 2020. Available at: https://www.aljazeera.com/ajimpact/china-bytedance-asks-tiktok-prepare-shutdown-report-200828023847793.html (2020-08-28).

In order to keep data inside the country's border, the government ordered specific state departments and sensitive industries to replace their foreign software and hardware with domestic ones within three years[24]. Two main objectives can be delineated from this measure: the first one implies a possible solution to the problems of data leaks and international cyber-espionage. It should prevent foreign access in government and Party's matters by using "secure and controllable" technological tools; the second one is showing a reaction to the policies undertaken by the U.S. in order to weaken Chinese tech enterprises. As a consequence of the Sino-American tech decoupling, Beijing aims at increasing the national reliance on domestic technologies, undermining at the same time companies such as HP, Dell and Microsoft. The official order, also called "China's 3-5-2 policy", is planned in order to remove 30% of foreign technologies in 2020, 50% in 2021 and the final 20% within 2022. Moreover, soon after the adoption of the Cyber Security Law, officials approved the Catalogue of Network Critical Equipment and Cybersecurity-Specific Products. This document provides a list of every technological product such as firewalls or routers that must obtain a permission in order to be sold in the country[25]. However, the transition into the adoption of fully domestic tech instruments will represent a challenge for the country, that, as many other nations, relies on components manufactured by foreign companies abroad[26]. As an example, even the majority of Smart Cities, urban centers that deploys advanced technologies, data analysis and storage, in order to enhance citizens' lives and governmental activities, are built in collaboration with American firms like IBM and Cisco, whose need to transfer data and know-how inside and outside China, would collide with Article 37 of the Cyber Security Law[27].

[24] Yuan YANG, Nian LIU, Beijing orders state offices to replace foreign PCs and software, *Financial Times*, 2019. Available at: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406 (2020-08-30).
[25] Samm SACKS, Manyi Kathy LI, How Chinese Cybersecurity Standards Impact Doing Business in China, *Center for Strategic & International Studies* (CSIS), 2018, p. 6.
[26] Yuan YANG, Nian LIU, Beijing orders state offices to replace foreign PCs and software, *Financial Times*, 2019. Available at: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406 (2020-08-30).
[27] Max PARASOL, The Impact of China's 2016 Cyber Security Law on foreign technology firms and on China's Big Data and Smart City dreams, Computer Law & Security Review, *Elsevier*, 2018, pp. 67-98.

Another example, that shows the government's willingness to develop advanced technologies independently, comes as a consequence of American sanctions towards Semiconductor Manufacturing International Corporation (SMIC). Recently, the US Department of Commerce has imposed export restrictions to the company, meaning that all American suppliers of SMIC should first obtain a license in order export products to the Chinese firm[28]. The Chinese largest semiconductor manufacturer was accused of providing services and products for military purposes and was targeted as a "national risk". This move heavily penalized SMIC and Huawei, its first customer, as well as international customers such as Qualcomm, an American chip designer, and provided more reasons for the Chinese government to speed up the process of technological self-sufficiency and replacement, especially in the semiconductor field[29].

The second significant decision undertaken by the Chinese government is the establishment of the Corporate SCS (Social Credit System) 企业信用体系 *Qiye xinyong tixi*. It is constituted by a complete system of data collection and analysis, that allows authorities to insert those local and international companies, which do not comply with new norms and standards, in blacklists. According to the European Chamber, this measure deeply influences businesses' operations, especially those of small and medium size enterprises, who lack sufficient resources to be up-to-date and respect the multitude of laws and scoring characteristics. In addition to the surveillance of the entire supply chain, the government requires also to keep record of employees and suppliers' behavior and information, which is not well accepted in Western countries, where the privacy of individuals is highly evaluated[30]. The rating mechanism concerns various aspects of a company, from tax paying and

[28] Yuan YANG, Kathrin HILLE, Qianer LIU, China's biggest chipmaker SMIC hit by US sanctions, *Financial Times*, 2020. Available at: https://www.ft.com/content/7325dcea-e327-4054-9b24-7a12a6a2cac6 (2020-10-02).
[29] *Ibid*.
[30] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions Market Actors, 2019, pp. 1-27.

environment safeguarding to pricing, data transfers or market monopoly issues. Authorities have already started to assign scores according to some of these factors, whereas others still have to be implemented in the next years[31]. According to the total amount of scores received, "severe distrusted" entities 严重违法失信主体 *Yanzhong weifa shixin zhuti* could face different types of sanctions like being subjected to more frequent investigations, receiving no State concession of the land or government's subventions and procurement. Other companies are precluded to operate in the Chinese market until they are able to improve their scores and exit blacklists. However, the report published by the European Chamber of Commerce denounces that the greatest obstacle for international enterprises is facing continuous surveillance and undefined demands, and less importance is attributed to meet Chinese information management requirements [32]. In 2019 and 2020, two more documents were respectively released by the State Administration for Market Regulation and the Ministry of Commerce of People's Republic of China (MOFCOM): the Guiding Opinion on Accelerating the Building of the Social Credit System and Building a Credit-based Monitoring System[33], and the MOFCOM Order No. 4 on Provisions on the Unreliable Entity List. Their aim is providing clarifications and more concrete instructions both for authorities and private actors, in order to reach as soon as possible the maximum level of enforcement. For instance, in Article 2 of the Order No. 4, are listed the criteria according to which foreign companies, institutions or individuals can be blacklisted in China and how they will be judged by officials in the security assessment (Art.7)[34].

[31] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions…, cit., p. 3.
[32] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions…, cit., p. 4.
[33] 国务院办公厅关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见, *Guowuyuan bangongting guanyu jiakuai tuijin shehui xinyong tixi jianshe yi xinyong wei jichu de xinxing jianguan jizhi de zhidao yijian*. Full text available at: http://www.gov.cn/zhengce/content/2019-07/16/content_5410120.htm
[34] "*Article 2* The State shall establish the Unreliable Entity List System, and adopt measures in response to the following actions taken by a foreign entity in international economic, trade and other relevant activities:
(1) endangering national sovereignty, security or development interests of China;
(2) suspending normal transactions with an enterprise, other organization, or individual of China or applying discriminatory measures against an enterprise, other organization, or individual of China, which violates normal

In order to achieve its surveillance goals towards enterprises and individuals, the government is going to deploy both Big Data and AI technologies, as it is officially stated in the previously-mentioned Guiding Opinion[35]. Accordingly, tech giants like Taiji Computer Corporation, Huawei, Alibaba, Tencent and VisionVera are participating in the creation of a comprehensive meta-database (the National Internet+ Monitoring' System 国家 "互联网+监管" 系统 *Guojia "Hulianwang+ jianguan" xitong*), to monitor in the most efficient way the overall amount of data collected from companies (Tab. 4).

Tab. 4 [36]

	Huawei	Alibaba	Tencent	Taiji Computer	VisionVera
Basic infrastructure					
	■				
Big Data centre					
Big Data analysis	■	■			
Databases		■	■	■	
Data integration				■	
Data application					
		■	■	■	
Risk and early-warning system (on basis of Corporate SCS ratings and records)					
Field-specific		■	■		
Overall performance		■	■		
Policy- and decision-making support					
		■	■		
Interface					
		■	■		
Video surveillance platform					

market transaction principles and causes serious damage to the legitimate rights and interests of the enterprise, other organization, or individual of China […]."
Ministry of Commerce People's Republic of China, MOFCOM Order No. 4 of 2020 on Provisions on the Unreliable Entity List, 2020. Available at: http://english.mofcom.gov.cn/article/policyrelease/questions/202009/20200903002580.shtml (2020-10-04).

[35] 《(十六) […] 依托国家"互联网+监管"等系统，有效整合公共信用信息、市场信用信息、投诉举报信息和互联网及第三方相关信息，充分运用大数据、人工智能等新一代信息技术，实现信用监管数据可比对、过程可追溯、问题可监测。[…]》
国务院办公厅关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见, 2019. Available at: http://www.gov.cn/zhengce/content/2019-07/16/content_5410120.htm (2020-09-01).

[36] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions…, cit., p. 29.

It should include information gathered by the government, media, e-commerce apps and even from surveillance materials. As a consequence, solving the lack of integration of data, its biggest complication[37]. Actually, the overall amount of data has already been collected from three main sources: first, firms have been contributing directly to the sharing of information to the State; second, government's concrete inspections collect and provide companies' relevant internal data and lastly, the final and biggest part comes from digital investigations[38]. Furthermore, many enterprises, who provide information to the regime, aren't completely aware about the security standards and methods through which it is managed and elaborated by Chinese authorities. Even domestic companies operating outside China in foreign markets continue to be rated by the Corporate SCS according to their behavior and could be inserted in the blacklists as well[39]

[37] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions…, cit., p. 5.
[38] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions…, cit., p. 14.
[39] European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions…, cit., p. 14.

3.2 Data transfer, localization and storage

*Cross-Border Data transfer (*跨境数据转输 *Kuajing shuju zhuanshu)*

According to the Peking University Internet Development Research Center, despite the difficult commercial relations between China and the U.S. and the overall measures that are driving to an economic and technological decoupling, the Chinese government had no intention to penalize foreign private and public enterprises with the reforms of cross-border data exchanges and storage. In fact, the expert of data protection, transfer and cybersecurity and leader of the National Information Security Standardization Technical Committee project for data safeguarding, states that the set of laws recently adopted by the Party is actually an attempt to find the right balance between avoiding national security threats, protecting domestic information and developing at the same time the Big Data industry[40]. In 2017, the Cyberspace Administration of China published the Measures on Security Assessment of Cross-Border Transfer of Personal Information and Important Data 个人信息和重要数据出境安全评估办法 （征求意见稿） *Geren xinxi he zhongyao shuju chujing anquan pinggu banfa (Zhengqiu yijiangao)*, whose aim was regulating the typology and amount of data leaving the country. Later, in 2019, a draft (the Draft Measures) was published by the same institution. Its objective was introducing both the use of contractual clauses to safeguard cross-border data and the possibility to request authorities' approval for data transfer outside China[41]. It also focused on clarify some vague principles written in the Cyber Security Law. Nevertheless, even in this document, there are some ambiguous requirements that still leave broad discretion to Chinese

[40] Yanqing HONG, The Cross-Border Data Flows Security Assessment: An important part of protecting China's basic strategic resources, Peking University Internet Development Research Center, 2017, pp. 1-13.
[41] Susan NING, Han WU, Yuanshan LI, Dan XUEZI, Development of PRC: Regulations on Cross-border Data Transfer, 2019. Available at: https://www.chinalawinsight.com/2019/06/articles/crossing-borders/development-of-prc-regulations-on-cross-border-data-transfer/ (2020-09-02).

authorities. For instance, is not clearly described what are the threats on national or social security that could impede information to be transferred abroad[42].

This first part of the Draft Measures implements in more details Article 37 of the Cyber Security Law, in which it was stated that only operators dealing with critical information had to go through the assessment process[43]. Nevertheless, from 2019, every network operator who wants to transfer sensitive information outside the country, has to make an explicit request to the provincial cyberspace administration where the business is located, in order to let officials and technicians start the security evaluations (Art.3)[44] [45]. After the evaluation, an application could be rejected when experts believe that the data shared could damage national security, the contracts are not respected or the firm has precedents of data breaches. In these cases, companies have the right to submit a complaint to the National Cybersecurity Administration, that will analyze directly the issue (Art.7)[46]. If the recipient of information is always the same, there's no need to sustain other security assessments every time the transfer occurs. However, if the typology, objective or recipient change, then the application needs to be updated. Lastly, it is necessary to keep the documents concerning every transfer, exact amount and relevance of cross-border data, and receiver's identity for at least five years[47].

---

[42] Samm SACKS, Manyi Kathy LI, How Chinese Cybersecurity Standards Impact Doing Business in China, *Center for Strategic & International Studies* (CSIS), 218, p.11.

[43] Yan LUO, Zhijing YU, Nicholas SHEPHERD, China Seeks Public Comments on Draft Measures related to the Cross-border Transfer of Personal Information, Covington – Inside Privacy, 2019. Available at: https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/ (2020-09-03).

[44] 《*第三条* 个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。向不同的接收者提供个人信息应当分别申报安全评估，向同一接收者多次或连续提供个人信息无需多次评估 […]。》Available at: http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html (2020-09-02).

[45] Susan NING, Han WU, Yuanshan LI, Dan XUEZI, Development of PRC: Regulations on Cross-border Data…, cit., Available at: https://www.chinalawinsight.com/2019/06/articles/crossing-borders/development-of-prc-regulations-on-cross-border-data-transfer/ (2020-09-02).

[46] Qiheng CHEN, Mingli SHI, Kevin NEVILLE, Cindy L, Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China, 2019.
Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/ (2020-09-02).

[47] Yan LUO, Zhijing YU, Nicholas SHEPHERD, China Seeks Public Comments on Draft Measures..., cit.., available at: https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/ (2020-09-03).

The second innovation inserted in the Draft Measures is the demand of including specific provisions in contracts between network operators and receivers. According to Article 13, a contract regulating cross-border data transfers should contain provisions concerning general characteristics of the information exchanged, instructions about the termination of the business relations, details describing data subjects' rights etc.

《*第十三条* 网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件，应当明确：

（一）个人信息出境的目的、类型、保存时限。

（二）个人信息主体是合同中涉及个人信息主体权益的条款的受益人。

（三）个人信息主体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。

（四）接收者所在国家法律环境发生变化导致合同难以履行时，应当终止合同，或者重新进行安全评估。

（五）合同的终止不能免除合同中涉及个人信息主体合法权益有关条款规定的网络运营者和接收者的责任和义务，除非接收者已经销毁了接收到的个人信息或作了匿名化处理。

（六）双方约定的其他内容。》[48] [49].

Then, Article 14 and 15 define both parties' obligations and liabilities. More specifically, network operators have to provide copies of the contract to the subjects of personal information who request it, inform them about the scope, period of the transfer and eventually, grant financial recompense to the harmed individual. Recipients have to allow individuals to have

[48] Ministry of Justice of the People's Republic of China, 个人信息出境安全评估办法（征求意见稿）, 2019. Available at: http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html (2020-09-02).

[49] "*Article 13***:** The contracts or other legally-binding instruments ("Contracts") signed by network operators and recipients of personal information shall specify:

1. The purposes, types, and retention period of the outbound transfer of the personal information;
2. The data subjects of the personal information are the beneficiary of the contractual provisions related to data subjects' rights and interests;
3. Where data subjects' legitimate rights and interests are harmed, they can, by themselves or through an authorized proxy, claim for damages against network operators, recipients, or both, who shall then compensate for the damages, unless they prove they were not responsible;
4. If the contract cannot be implemented due to changes to the legal environment of the country where the recipient is located, the contract shall be terminated or go through a new security assessment;
5. The termination of contracts cannot exempt contractual duties and obligations of network operators or recipients related to the legitimate rights and interests of data subjects, unless the recipients have already destroyed received personal information or carried out anonymization processing;
6. Any other content specified by the parties."

Avilable at: www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/ (2020-10-02).

access to their information and modify or delete them in case of inappropriateness[50] [51]. Lastly, Article 20 declares that also those companies that deal with Chinese personal data but do not operate directly in China, like subsidiaries, foreign network operators or suppliers, have to apply for the transfer of cross-border information and designate a legal representative in the country[52].

It should be also considered that many Articles of the Draft Measures present some similarities with European regulations like the GDPR and the European Union's Standard Contractual Clauses (SCCs)[53], which have been commonly deployed for years by companies all over the world. For instance, even Article 27 of the GDPR requires a written appointment of a delegate operating in the EU. Moreover, the attention the new regulation pays on individual's rights such as the possibility to correct and control their own personal information[54], receive compensation or obtain a copy of the contract between data exporter and importer,

[50] 《*第十四条* 合同应当明确网络运营者承担以下责任和义务：
（一）以电子邮件、即时通信、信函、传真等方式告知个人信息主体网络运营者和接收者的基本情况，以及向境外提供个人信息的目的、类型和保存时间。
（二）应个人信息主体的请求，提供本合同的副本。
（三）应请求向接收者转达个人信息主体诉求，包括向接收者索赔；个人信息主体不能从接收者获得赔偿时，先行赔付。
第十五条 合同应当明确接收者承担以下责任和义务：
（一）为个人信息主体提供访问其个人信息的途径，个人信息主体要求更正或者删除其个人信息时，应在合理的代价和时限内予以响应、更正或者删除。
（二）按照合同约定的目的使用个人信息，个人信息的境外保存期限不得超出合同约定的时限。
（三）确认签署合同及履行合同义务不会违背接收者所在国家的法律要求，当接收者所在国家和地区法律环境发生变化可能影响合同执行时，应当及时通知网络运营者，并通过网络运营者报告网络运营者所在地省级网信部门。》Ministry of Justice of the People's Republic of China, 个人信息出境安全评估办法（征求意见稿）, 2019. Available at: http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html (2020-09-02).

[51] Susan NING, Han WU, Yuanshan LI, Dan XUEZI, Development of PRC: Regulations on Cross-border Data…, cit., Available at: https://www.chinalawinsight.com/2019/06/articles/crossing-borders/development-of-prc-regulations-on-cross-border-data-transfer/ (2020-09-03).

[52] 《*第二十条* 境外机构经营活动中，通过互联网等收集境内用户个人信息，应当在境内通过法定代表人或者机构履行本办法中网络运营者的责任和义务。》Available at: http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html (2020-09-03).

[53] More details about SCCs available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_it.

[54] Art. 16 (Right to rectification) and 17 (right to erasure) of the GDPR.

recalls the SCCs' provisions, showing an illusory convergence of the basic principles that give foundation to privacy rights globally[55] [56].

In addition to the Draft Measures, in 2019, China also announced the deployment of the Blockchain-based Services Network (BSN) 区块链服务网络 *Qukuailian fuwu wangluo*, that is an infrastructure allowing individuals, firms and government departments to interconnect personal and sensitive information within national territories. Furthermore, it will be also used by those nations participating in the Digital Silk Road, in order to safely and efficiently share data around the world through cryptography and new privacy rules. The price of the protocol should even allow small and medium enterprises to participate in the Chinese digital market as well as in international trade[57].

*Data Localization (*数据本地化 *Shuju bendihua)*

According to R. D. Taylor, the concept of data localization is strictly connected with the one of data sovereignty, in which each country aims at regulating domestic information through their own sets of laws. Both data localization and data sovereignty present some challenges, especially with the advent of the cloud computing. In fact, the cloud deploys a central server to widespread elements in different locations, creating uncertainty about the right jurisdiction they are associated to[58]. Looking at the fields and measures included in the principle of data sovereignty, data localization seems to be the most restrictive and challenging, since it implies the storage of citizens' information in servers located inside the national borders. Additionally,

[55] Yan LUO, Zhijing YU, Nicholas SHEPHERD, China Seeks Public Comments on Draft Measures..., cit.., available at: https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/ (2020-09-03).
[56] Clause 5, Clause 6 and Clause 7 of the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council, 2010. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 (2020-09-03).
[57] Michael SUNG, China's National Blockchain will Change the World, *Coindesk*, 2020. Available at: https://www.coindesk.com/chinas-national-blockchain-will-change-the-world (2020-09-04).
[58] Richard D. TAYLOR, "Data Localization": The Internet in the Balance, *Elsevier – Telecommunication Policy*, Vol.44, 2020, pp. 1-15.

some researchers have expressed concerns about the risk to locate the totality of information in a unique place or country and not distributing data in different servers around the world. Their concentration in a single location could debilitate the infrastructure protection capabilities and attract the attention of criminals[59]. The second criticism finds its basis on the implicit consequence of data localization, that is favoring multinational firms, that through lots of resources are able to comply to governments' rules and invest on locally-based infrastructures. On the contrary, small and medium size enterprises are considered in disadvantage, since they lack big amount of resources, the necessary legal and financial advice etc. to modify their systems according to always changing regulations[60]. Lastly, limiting data flows around the world would inevitably impact and slow down AI technology development, because these instruments require a huge number of diverse information, through which machines can learn new patterns and analyze more and more algorithms to describe more precisely the reality[61].

Among the several countries interested in data localization, China, Russia and the U.S. have recently started developing new regulations and infrastructures to achieve their goal and enhance national security. First, Russia has developed internal servers and its own domain name system, due to a defensive attempt to be independent from a future possible disconnection from the World Wide Web. Second, the U.S. ordered the annulment of cooperation with the Chinese subsidiaries such as China Telecom Americas, China Unicom Americas, Pacific Networks etc. located in the country, in order to keep American sensitive information within its borders, since the government feared leaks of personal data[62].

As it was previously analyzed, China adopted many policies, which require the storage of data in the country, with the exception of those companies or institutions that manage to

[59] Richard D. TAYLOR, "Data Localization": The Internet in the Balance…, cit., p. 6.
[60] Richard D. TAYLOR, "Data Localization": The Internet in the Balance…, cit., pp. 6-8.
[61] *Ibid*.
[62] Richard D. TAYLOR, "Data Localization": The Internet in the Balance…, cit., p. 9.

receive the government's consent. At first, data localization was applied according to a sector-specific basis whereas lately, the focus moved to a general and comprehensive law, which includes all the network operators dealing with critical information. The first regulation was the Notice to Urge Banking Financial Institutions to Protect Personal Information 关于银行业金融机构做好个人金融信息保护工作的通知 *Guanyu yinhangye jinrong jigou zuohao geren jinrong xinxi baohu gongzuo de tongzhi* in 2011, which forbid the analysis and storing of Chinese personal and financial data outside the country's borders. Also, credit reports and health information have specific regulations (Administrative Regulation on Credit Information Industry 行业信用信息管理办法 *Yinhang xinyong xinxi guanli banfa*, 2013, Administrative Measures for Credit Agencies 征信业管理条例 *Zhengxinye guanli tiaoli*, 2013 and Population Health Information Management 人口健康信息管理办法 *Renkou jiankang xinxi guanli banfa*, 2014) that demand to locate the entire procedures of collection, processing and storage of information in China[63]. It was in 2016, that the Cyber Security Law clearly stated in Article 37:

"Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China […]."[64]

Liu's study explains that Article 37 derives from the fear of losing critical information control when data are transferred abroad, thus network operators would fail in reaching the security standards established by the government[65]. As it was previously described, localize data within a single country, would bring both advantages and disadvantages. In the case of China, in 2017

[63] AmCham China 中国美国商会, Protecting Data Flows in the US-China Bilateral Investment Treaty 保护《中美双边投资协定》中的 数据流通, 2015. Available at: https://www. amchamchina.org/policy-advocacy/policy-priorities/download/file/policy_spotlight/5/e242ff078dbfcd38cfd5d601318aaf6cfc5821aa.pdf (2020-09-04).

[64] Rogier CREEMERS, Paul TRIOLO, Graham WEBSTER, Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), 2018. Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/#:~:text=Article%2037%3A%20Critical%20information%20infrastructure,store%20it%20within%20mainland%20China (2020-09-04).

[65] Jinhe LIU, China's Data Localization, *Chinese Journal of Communication*, Vol. 13 (1), 2019, pp. 84-103.

it was registered an increase of the Big Data industry of 32.4% and, one year later, nearly 437 plans of data centers' constructions were provided to the Ministry of Industry and Information Technology. Moreover, the more data the country collects and the more they will contribute in developing the digital economy, which already constitutes 34.8% of GDP (2019)[66]. However, this choice would inevitably imply the limitation of free data flows and the creation of trade barriers around the world. It also requires foreign companies to build local data centers in each country they are operating. As a consequence, foreign direct investment and Chinese exports would be strongly penalized by the complete implementation of this policy[67].

In order to avoid the disappearance of international players in the country, the government encouraged transnational enterprises to create new joint ventures with Chinese businesses and exploit this union to store data internally without excessive expenses. For instance, Microsoft Azure, Amazon AWS and Apple started collaborations respectively with CenturyLink Internet, Sinnet Technology and the Guizhou-Cloud Big Data Industry[68].

Even Chinese companies like Alibaba, Baidu and Tencent were directly impacted by new regulations, since their businesses concerned AI technology R&D, imports and cloud computing 云计算 *Yun jisuan* in other nations[69].

Foreign response to data regulations

In the light of regulations such as the Cyber Security Law and the Draft Measures, transnational companies started feeling uncertain about their future businesses in China.

[66] Jinhe LIU, China's Data Localization, Chinese Journal of Communication…, cit., pp. 91-92.
[67] AmCham China 中国美国商会, Protecting Data Flows in the US-China Bilateral Investment Treaty 保护《中美双边投资协定》中的 数据流通, 2015. Available at: https://www. amchamchina.org/policy-advocacy/policy-priorities/download/file/policy_spotlight/5/e242ff078dbfcd38cfd5d601318aaf6cfc5821aa.pdf (2020-09-04).
[68] Jinhe LIU, China's Data Localization, Chinese Journal of Communication…, cit., pp. 97-98.
[69] Sam SACKS, Paul TRIOLO, Graham WEBSTER, Beyond the Worst-Case Assumptions on China's Cybersecurity Law, 2017. Available at: https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/ (2020-09-04).

Requests such as data localization and storage within the country's borders as well as limitations in personal information flows, seemed to prevent them from using cloud computing or regularly reporting any kind of data to the headquarters established in another country. Furthermore, the strict controls undertaken by cyber security authorities through the Corporate Social Credit System and the Multi-Level Protection Scheme (MLPS)[70] could significantly slow down foreign firms' entrance in the Chinese market[71].

Generally speaking, Chinese security requirements and network systems could impact negatively foreign businesses in three different ways: the first one is the invasive intrusion of the government and officials, asking for encryption codes, domain names and IP. The second one is based on the several costs firms will probably face in order to be updated and in compliance with always changing standards. The last risk is that all these steps firms have to go through could further deteriorate relations between the U.S. and China[72].

Despite all the possible obstacles, many foreign enterprises coming from a multitude of sectors have already found different solutions to continue their operations or keep their suppliers and customers in China. One possibility could be relying on local cloud service providers, for this reason, as it was previously mentioned, several cloud data centers have been rapidly established in the country since 2017[73]. Building a local infrastructure would imply the respect of government's data sovereignty, but at the same time it means higher costs and firms' great expenditure of resources. A concrete example is provided by Chindata Group Holding

[70] MLPS is a system that was first launched in 2004 and aims at grading companies with a 1-5 scale. Those enterprises rated with 3 or more points are more likely to endanger national security. Thus, they will be subjected to intensive investigations and more limitations in data transfer and storage.
[71] Antonio DOUGLAS, How Companies Are Reacting to China's New Data Security Scheme, *China Business Review – US-China Business Council*, 2020. Available at: https://www.chinabusinessreview.com/why-companies-are-still-reluctant-to-file-in-chinas-new-data-security-scheme/ (2020-09-10).
[72] Samm SACKS, Manyi Kathy LI, How Chinese Cybersecurity Standards Impact Doing Business in China, Center for Strategic & International Studies (CSIS), 2018, p. 3.
[73] Allan LEINWAND, Three things companies must know about data sovereignty when moving to the cloud, 2017. Available at: https://enterprisersproject.com/article/2017/1/three-things-companies-must-know-about-data-sovereignty-when-moving-cloud (2020-09-06).

Ltd. 秦淮数据集团 *Qinhuai shuju jituan*. This company acts as a third-party operator both in China and Malaysia, providing data storage services for foreign enterprises, who aren't allowed to run their own data centers. During the current year, it reported an overall revenue of more than 118 million dollars, moreover it plans to build six new centers in India and China[74]. Furthermore, according to Caixin report, not only overseas network operators but also foreign investors have been deeply influenced by data localization requirements and cyber security laws. The several efforts of opening up of the Chinese financial market to foreign capitals are not equally paired to a smooth execution, since there is vagueness and confusion about the language and provisions of the new regulations[75]. Some fund managers interviewed confirmed to have found some obstacles in sharing relevant information with the HQs. Thus, the Asset Management Association of China and the China Securities Regulatory Commission (CSRC) agreed to let investors undertake risk controls and store data in their home-country. However, they have to comply Chinese institutions' request to transmit immediately transaction and investments information to Chinese servers.[76]

Except for the financial sector and the reliance on local database services of cloud computing companies, also tech giants had to establish new joint ventures with Chinese players and make some adjustments, which allow them to be in compliance with the government's cyber security regulations. This is the case of the American firm Apple, that removed some applications from the Store like VPNs, which were accused of violating the law and endangering the Great Firewall[77]. Moreover, in 2018, the firm confirmed the transfer of data

[74] Yang GE, Wall Street Abuzz Over Chinese Data Center Operator's IPO, Business & Tech, 2020. Available at: https://www.caixinglobal.com/2020-09-09/wall-street-abuzz-over-chinese-data-center-operators-ipo-101603268.html (2020-08-09).
[75] Caiping LIU, Timmy SHEN, In Depth: Progress and Pitfalls for Foreign Investors in China's Capital Markets, Caixin, 2020. Available at: https://www.caixinglobal.com/2020-06-18/in-depth-progress-and-pitfalls-for-foreign-investors-in-chinas-capital-markets-101569516.html (2020-08-09).
[76] Caiping LIU, Timmy SHEN, In Depth: Progress and Pitfalls for Foreign Investors in China's Capital Markets, Caixin, 2020. Available at: https://www.caixinglobal.com/2020-06-18/in-depth-progress-and-pitfalls-for-foreign-investors-in-chinas-capital-markets-101569516.html (2020-08-09).
[77] Intensive censorship system implemented by the Chinese government in order to filter information, websites, apps, that could threaten the social, economic and political stability of the country.

collected in China to the state-owned Guizhou-Cloud Big Data (GCBD) 云上贵州大数据产业发展有限公司 *Yunshang Guizhou dashuju chanye fazhan youxian gongsi*. Every material, back up and information on iCloud will be automatically handled by GCBD with Apple's technical assistance[78]. Another example is Amazon Web Services, which lets Beijing Sinnet Technology, a local partner, manage the overall information and collect it directly in the country. Its service is principally based on leasing hardware and software in order to ease SMEs' work on apps and websites. Being associated with Sinnet, is useful to maintain relations with Chinese authorities, receive funds from the government and manage data storage[79].

Another step that companies have to go through is the Multi-Level Protection Scheme together with the Cyberspace Administration of China's (CAC) inspections. Businesses have the possibility to independently register and allow the government to have free access to information. This preventive measure could show their goodwill towards Chinese regulations and, at the same time, let them start in advance a self-analysis process of the security of their systems and the types of services offered. However, the fear of leakages of sensitive, personal data and intellectual property (知识产权 *Zhishi chanquan*) holds many companies back to operate in the market[80]. According to Sacks and Li (2018), the requirements imposed by the regime, might favor domestic companies both for the internal competition, since they can be more frequently chosen by the State because they are easier to control, and for the management

[78] Erchi ZHANG, Wei HAN, Apple Hands Off China iCloud Data Operations, *Caixin*, 2018. Available at: https://www.caixinglobal.com/2018-01-11/apple-hands-off-china-icloud-data-operations-101196242.html (2020-09-10)
[79] Paul MOZUR, Joining Apple, Amazon's China Cloud Service Bows to Censors, *The New York Times*, 2017. Available at: https://www.nytimes.com/2017/08/01/business/amazon-china-internet-censors-apple.html (2020-09-10).
[80] Antonio DOUGLAS, How Companies Are Reacting to China's New Data Security Scheme, *China Business Review – US-China Business Council*, 2020. Available at: https://www.chinabusinessreview.com/why-companies-are-still-reluctant-to-file-in-chinas-new-data-security-scheme/ (2020-09-10).

of critical information, which couldn't be influenced or hindered by foreign nations and institutions[81].

In conclusion, what is fundamental for foreign companies is being aware and always up-to-date about recent data regulating laws in China, so as to promptly modify their businesses and infrastructures when they have enough resources or rely on Chinese partners that could help understand such complex environment, or eventually, abandon that market and focus on other nations. International enterprises have to consider the advantages, disadvantages and risks they will face when operating in China, for instance the great discretion authorities have, due to the ambiguity of the language of official regulations. Actually, the publishment of the Position Paper 2020/2021 of the European Union Chamber of Commerce in China (EUCCC) clearly shows several concerns and challenges European entities face when deciding to operate in the Chinese market. It includes different sectors and themes such as finance, environmental projects, offline and online services, cybersecurity issues etc.[82]. Enterprises are calling for a comprehensive harmonization of the market as well as equal competitive basis compared to Chinese firms. In order to achieve these objectives, EUCCC members cite some obstacles that should be solved. First, laws should be more detailed and with a clearer language since requirements' vagueness impede institutions to be in compliance with the law. Second, data localization within the nation and cloud computing regulations prevent both multinational companies to integrate information globally and their customers to feel safeguarded[83]. In addition, the European Chamber recommends the Chinese government to discern national security from commercial security, allowing international firms to share data freely and letting foreign technologies participate in the market. These reforms would not only promote a fair

[81] Samm SACKS, Manyi Kathy LI, How Chinese Cybersecurity Standards Impact Doing Business in China, *Center for Strategic & International Studies* (CSIS), 2018, pp. 1-3.
[82] EUCCC, European Business in China – Position Paper 2020/2021, European Chamber Publications, 2020. Available at: https://europeanchamber.com.cn/en/publications-position-paper (2020-10-04).
[83] EUCCC, European Business in China – Position Paper 2020/2021, European Chamber Publications, 2020, p. 336. Available at: https://europeanchamber.com.cn/en/publications-position-paper (2020-10-04).

competition in the IT market worldwide, but through the integration of new advanced products manufactured abroad, it would also enhance Chinese security systems, which are now relying just on domestic instruments[84]. From the Chinese perspective, these measures and laws are needed in order to secure the State political, economic and social stability. However, requirements may exclude several small and medium-size enterprises as well as big multinational companies from having business, investing and building infrastructures in China, keeping out many precious opportunities for the country's development.

[84] EUCCC, European Business in China – Position Paper 2020/2021, European Chamber Publications, 2020, pp. 338-339.

3.3 Glossary of terms

▪ Administrative Measures for Credit Agencies	征信业管理条例
▪ Administrative Regulation on Credit Information Industry	行业信用信息管理办法
▪ Blockchain-based Services Network	区块链服务网络
▪ Chindata Group Holding Ltd.	秦淮数据集团
▪ Cloud computing	云计算
▪ Corporate Social Credit System	企业信用体系
▪ Cross-Border Data Transfer	跨境数据转输
▪ Data Localization	数据本地化
▪ Guizhou-Cloud Big Data	云上贵州大数据产业发展有限公司
▪ Heavy Distrusted Entity	严重违法失信主体
▪ Huawei Technologies Co., Ltd.	华为技术有限公司
▪ Intellectual Property	知识产权
▪ Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data	个人信息和重要数据出境安全评估办法
▪ National Internet+ Monitoring' System	国家“互联网+监管”系统
▪ National Intelligence Law	中华人民共和国国家情报法
▪ Notice to Urge Banking Financial Institutions	关于银行业金融机构做好

to Protect Personal Information	个人金融信息保护工作的通知
▪ Opinion on Strengthening the United From Work of the Private Economy in the New Era	关于加强新时代民营经济统战工作的意见
▪ Population Health Information Management	人口健康信息管理办法
▪ Technological decoupling	技术脱钩
▪ Trade decoupling	贸易脱钩
▪ Zhongxing Telecommunication Equipment Corporation	中兴通讯股份有限公司

Conclusions

The objectives of this thesis were to let the reader understand the essence of Big Data and how they are implemented in modern society and in the every-day life; a major focus was dedicated to China. It aimed at giving explanations of how the government perceives this extremely valuable source and what methods is using and is going to use in the future in order to preserve and exploit Big Data throughout the 21st century.

The question I asked to myself, that constitutes the basis of this research, was: how can China combine the increasing concern of customers towards the fate of their personal information and, at the same time, allow officials to access sensitive data of both citizens, private and public enterprises?

From the Chinese population's perspective, the awareness of the importance of privacy and the risks they could incur when inserting their information on websites or apps, is growing exponentially. This is also due to the fact that many people have experienced at least once in life cyber-crimes and identity theft. Thus, in China, as well as in the rest of the world, the government is required to provide sets of law that are able to safeguard data. At the same time, it also established several monitoring systems such as Skynet and the Social Credit System that, through the aid of AI instruments, smart cities and Big Data analytics, control every facets of citizens' behavior and manage various types of information.

Firstly, the analysis focused on individuating Big Data implementation in society, citing different examples, from the health system and AI technologies to payments and socializing, and eventually on the improvements and threats they brought inside every industry. Secondly, more attention was paid to the new regulations China recently approved, such as the Cyber Security Law, the Regulation on the Internet Security Supervision and Inspection by Public Security Agencies, IT – Personal Information Security Specification and many others

mentioned in the text. It emerged that Big Data are considered by the Chinese government as having two separate values that have to be handled distinctly. On one hand, the economic value of Big Data must be safeguarded in order to place the country in a competitive position in the global digital-economy. On the other hand, the social and political value, must be monitored by security agencies so as to preserve national stability and ensure cyber-security and cyber-sovereignty, thus promoting Chinese "tech-protectionism".

These characteristics, as two sides of the same coin, coexist and integrate each other, but, at the same time, are kept separate by the regime. In addition, the balance China has found between these two aspects of Big Data, as well as their implementation in AI infrastructures, have influenced several Asian countries like Viet Nam, the Philippines and India, but raised also new commercial obstacles and criticism, especially from the U.S.

In the light of these results, a second question raised naturally. How do foreign companies, operating in the country or with Chinese partners, perceive China's Big Data management requirements? The outcome of further analysis showed that the principal challenges international enterprises face are the following. First, the vagueness of written language in the newly adopted laws creates uncertainty and confusion. Even after the publishment of new non-binding documents, which should have been useful to better understand some Articles of the Cyber Security law, ambiguous terminology still leaves the Chinese government free to modify judicial decisions depending on specific circumstances. The second challenge is based on the requirement of data localization within Chinese borders and strict limits on cross-border data transfers. Theses decisions prevent multinational firms to share information collected in the country to other subsidiaries and headquarters located around the world. It also blocks them from building their own independently managed databases, except for joint ventures established with local players. Thus, new data management rules will

impact significantly foreign investments, infrastructures and business operations, damaging at the same time the competitive environment.

Lastly, it emerged that foreign companies dealing with Chinese personal information feel penalized and discriminated in both innovative and competitive spheres. Nevertheless, the lack of market competition and international influences in IT R&D will actually put China at a disadvantage as well[85].

In conclusion, promoting global harmonization in different countries, societies and industries should imply the opening up of borders, from terrestrial and maritime to cyber ones. Governments all over the world should encourage collaborations and integration in every aspect of society. In order to ensure a fair competition, actual innovation and a safe environment for the global population, Big Data free flows and comprehensive regulations should be encouraged and not hindered

[85] EUCCC, European Business in China – Position Paper 2020/2021, European Chamber Publications, 2020, pp. 338-339.

Bibliography

ANDERSON, Allen F., GIL, Vincent E., China's Modernization and the Decline of Communitarism: the control of sex crimes and implications for the fate of informal social control, *Journal of Contemporary Criminal Justice*, Vol. 14(3), 1998, pp. 248-261.

Asia Pacific Data Protection and Cyber Security Guide, *Hogan Lovells*, 2019, pp. 1-30.

AUSTIN, Greg, *Cybersecurity in China. The next wave*, Springer Briefs in Cybersecurity, Stuttgart, 2018, pp. 1-130.

BAUMAN Sygmunt, BIGO Didier, ESTEVES Paulo, GUILD Elspeth, JABRI Vivienne, LYON David, WALKER R.B.J., After Snowden: Rethinking the Impact of Surveillance, *International Political Sociology*, Vol. 8, 2014, p. 122.

BING Ngeow Chow, *The Residents' Committee in China's Political System: Democracy, Stability, Mobilization*, 2012, p. 74.

BJORKLUND E. M., The danwei: socio-spatial characteristics of work units in China's urban society, *Economic Geography*, Vol. 62(1), 1986, pp. 24-28.

CHANDEL Sonali, ZANG Jingji, YU Yunnan, SUN Jingyao, ZHANG Zhipeng, *The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall*, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2019, p. 111.

CHEN Xiaoming, Social and Legal Control in China, *International Journal of Offender Therapy and Comparative Criminology*, Vol. 48(5), p. 533.

Chief of Public Safety and Homeland Security Bureau, Order DA 20-690, *Federal Communications Commission*, Washington, 2020.

CREEMERS, Rogier, *China's Social Credit System: An Evolving Practice of Control*, University of Leiden, Van Vollenhoven Institute, 2018, pp. 1-32.

DE HERT, Paul, PAPAKONSTANTINOU, Vagelis, The data protection regime in China, Policy Department C, *Citizens' Rights and Constitutional Affairs*, European Parliament, 2015, pp. 1-32.

DEIGHTON, John, PETER, A.J., The value of data: Consequences for insight, innovation & efficiency in the US economy, *The Data Driven Marketing Institute*, 2013.

Deloitte China, Rising Innovation in China, *China Innovation Ecosystem Development Report 2019*, 2019, pp. 1-68.

DHAWAN, Vikas, ZANINI, Nadir, Big data and social media analytics, *Research matter: A Cambridge Assessment Publication*, 2014, pp. 36-41.

European Chamber – The Digital Hand, How China's Corporate Social Credit System Conditions Market Actors, 2019, pp. 1-27.

EUCCC, European Business in China – Position Paper 2020/2021, European Chamber Publications, 2020.

FELDSTEIN, Steven, The Global Expansion of AI Surveillance, *Carnegie Endowment for International Peace*, 2019, pp. 1-42.

FERGUSON, Mike, Big Data – Why Transaction Data is Mission Critical to Success, *Intelligent Business Strategies*, 2014, pp. 1-13.

For further information about Hofstede's Cultural Dimensions: HOFSTEDE, Geert, BOND, Michael H., Hofstede's Culture Dimensions: An Independent Validation Using Rokeach's Value Survey, Journal of Cross-Cultural Psychology, 15(4), 1984, pp.417–433.

FU, Tao, China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent; *Global Media and Communication*; 2019, Vol. 15(2) 195-213.

FUNWIE, Prosper, The 4th Industrial Revolution: International Relations and Policy: Case of S. Korea and China, Department of International Relations, GSIAS Hankuk University of Foreign Studies, Seoul, 2019, pp. 1-24.

GROTH, Olaf J., NITZBERG, Mark, ZEHR, Dan, STRAUBE, Tobias, KAATZ-DUBBERKE, Toni, *Comparison of National Strategies to Promote Artificial Intelligence*, Part 1, Konrad-Adenauer-Stiftung, Berlin, 2019, pp.1-70.

HARRIS, Lane J., From Democracy to Bureaucracy: the Baojia in Nationalist Thought and Practice, 1927-1949, *Front. Hist. China*, Vol. 8(4), 2013, pp. 517-557.

HONG Yanqing, The Cross-Border Data Flows Security Assessment: An important part of protecting China's basic strategic resources, Peking University Internet Development Research Center, 2017, pp. 1-13.

IASIELLO, Emilio, China's Cyber Initiatives Counter International Pressure, Journal of Strategic Security, Vol. 10, no. 1, 2016, pp. 1-16.

JIANG, Shanhe, WANG, Jin, LAMBERT, Eric, Correlates of informal social control in Guangzhou China neighborhoods, *Journal of Criminal Justice*, Vol. 38(4), 2010, pp. 460-469.

JOHNSON Elmer H. Neighborhood Police in the People's Republic of China, *Police Studies*, Southern Illinois University, New York, Vol. 6(4), 1983.

KASKA Kadri, BECKVARD Henrik, MINARIK Tomáš, Huawei, 5G and China as a Security Threat*, CCDCOE (Nato Cooperative Cyber Defence Centre of Excellence)*, 2019, p. 10.

KOKAS Aynne, Platform Patrol: China, the United States and the Global Battle for Data Security, *The Journal of Asian Studies*, Vol. 77(4), 2018, p. 923.

KPMG China IT Advisory, KPMG International Cooperative, 2017, pp. 1-16.

KSHETRI, Nir, Big data's impact on privacy, security and consumer welfare, *Telecommunications Policy*, Vol. 38(11), 2014, 1134-1145.

LI, Ling, China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0", Technological Forecasting and Social Change, Vol. 135, 2018, pp. 66-74.

LIANG Bin, LU Hong, Internet Development, Censorship and Cyber Crimes in China, *Journal of Contemporary Criminal Justice*, Vol. 26(1), 2010, p. 106.

LIANG, Fan, DAS, Vishnupriya, KOSTYUK, Nadiya, HUSSAIN, Muzammil M., Constructing a data-driven society: china's social credit system as a state surveillance infrastructure, *Policy and Internet*, Vol. 10, n. 4, 2018, pp. 415.453.

LIU Jinhe, China's Data Localization, *Chinese Journal of Communication*, Vol. 13 (1), 2019, pp. 84-103.

LYON David, *Surveillance After Snowden*, Polity Press, Cambridge, 2015.

Made in China 2025, *Institute for Security & Development Policy*, 2018, www.isdp.eu, pp. 1-9.

MIAO, Weishan, Policy Review: The Cyberspace Administration of China, Global Media Communication, Vol. 12(3), 2016, pp. 337-340.

MILLER Alice, More Already on the Central Committee's Leading Small Groups, *China Leadership Monitor*, n. 44, 2013, p. 4.

Murray Scot TANNER, James BELLACQUA, China's Response to Terrorism, CNA Analysis & Solutions, 2016, p. 38.

PARASOL Max, The Impact of China's 2016 Cyber Security Law on foreign technology firms and on China's Big Data and Smart City dreams, Computer Law & Security Review, *Elsevier*, 2018, pp. 67-98.

PERNOT-LEPLAY Emmanuel, China's approach on data privacy law: a third way between the U.S. and the EU?, *Penn State Journal of Law and International Affairs*, Vol. 8 (1), 2020, pp. 49-51.

PERNOT-LEPLAY, Emmanuel, China's approach on data privacy law: a third way between the U.S and the EU?, *Penn State Journal of Law and International Affairs*, Vol.8.1, 2020, pp. 1-60.

ROBERTS Huw, COWLS Josh, MORLEY Jessica, TADDEO Mariarosaria, WANG Vincent, FLORIDI Luciano, The Chinese Approach to Artificial Intelligence: an Analysis of Policy, Ethics, and Regulation, *AI & Society*, 2019, pp. 1-20.

ROBERTS, Lynne D., INDERMAUR, David, SPIRANOVIC Caroline, Fear of Cyber-Identity Theft and Related Fraudulent Activity, *Psychiatry, Psychology and Law*, Vol. 20, 2013, pp. 315-328.

SACKS Sam, LI Manyi Kathy, How Chinese Cybersecurity Standards Impact Doing Business in China, *Center for Strategic & International Studies* (CSIS), 2018, pp. 1-16.

SHARBAUGH, Patrick E., TRANG, Phan Thi Le, What's Mine Is Yours: An Exploratory Study of Online Personal Privacy in the Socialist Republic of Vietnam, 2013, pp. 1-11.

SHAW Victor N., *Social Control in China: a study of Chinese Work Units*, Praeger, London, 1996.

SHEN Yi, Cyber Sovereignty and the Governance of Global Cyberspace, *Chinese Political Science Review*, Fudan University, 2016, pp. 81-93.

SUTHERLAND Ewan, The strange case of US v. ZTE: a prosecution, a ban, a fine and a presidential intervention, Digital Policy, Regulation and Governance, *Emerald Publishing Limited*, Vol. 21 (6), 2019, pp. 550-573.

TAYLOR Richard D., “Data Localization”: The Internet in the Balance, *Elsevier – Telecommunication Policy*, Vol.44, 2020, pp. 1-15.

THIO, Tse Gan, Data and privacy protection in ASEAN – what does it mean for businesses in the region?, *Deloitte Southeast Asia*, 2018, pp. 1-8.

TIAM Kurt, GONG Sherry, HUANG Andy, MCGINTY Andrew, PARSONS Mark, China’s New National Security Law Creates More Insecurity For Foreign Businesses, *Hogan Lovells*, 2015, p. 1

U.S. House of Representatives, (U) Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, 2016.

WANG Jianfeng, *The Politics of Neighborhood Governance: Understanding China’s State-Society Relations Through an Examination of the Residents Committee*, Western Michigan University, Michigan, 2005, p. 138.

WEI Li, Towards Economic Decoupling? Mapping Chinese Discourse on the China–US Trade War, *The Chinese Journal of International Politics*, Vol. 12(4), 2019, pp. 519–556.

YANG, Fan, XU, Jian, Privacy concerns in China’s smart city campaign: the deficit of China’s Cybersecurity Law, *Asia Pacific Policy Studies*, 2018, pp. 333-343.

YUEN Samson, Becoming a Cyber Power: China’s Cybersecurity Upgrade and its Consequences, *China perspectives*, 2015, pp. 54-58.

ZHANG Lening, MESSNER Steven F., ZHANG Sheldon, Neighborhood Social Control and Perceptions of Crime and Disorder in Contemporary Urban China, *American Society of Criminology*, Vol. 55(3), 2017, pp. 632-637.

ZHANG, Qianfan, A constitution without constitutionalism? The paths of constitutional development in China, Oxford University Press and New York University School of Law, Vol. 8 No. 4, 2010, pp. 950–976.

ZHOU, Hanhua, *Consumer Data Protection in Brazil, China and Germany: a comparative study*, Göttingen, Göttingen University Press, 2016, pp.1-222.

ZITTRAIN Jonathan, EDELMAN Benjamin, *Internet Filtering in China*, Harvard Law School, Research paper n. 62, 2003, p. 74.

Website citations

ADAMS, Robert, 10 Powerful examples of Artificial Intelligence in Use Today, 2017, in www.forbes.com, 2020-03-17.

AmCham China 中国美国商会, Protecting Data Flows in the US-China Bilateral Investment Treaty 保护《中美双边投资协定》中的 数据流通, 2015. Available at: https://www.amchamchina.org/policy-advocacy/policy-priorities/download/file/policy_spotlight/5/e242ff078dbfcd38cfd5d601318aaf6cfc5821aa.pdf (2020-09-04).

BLAZYTE, Agne, Penetration rate of online shopping in China 2008-2018, 2019, www.statista.com, 2020-03-18.

Cambridge Dictionary, available at: https://dictionary.cambridge.org/dictionary/ljazee/decoupling (2020-08-22).

CARLSON Eric, KAJA Ashwin, LUO Yan, China Enacts New Counter-Terrorism Law, *Inside Privacy – Covington*, 2016. Available at: https://www.insideprivacy.com/international/china-enacts-new-counter-terrorism-law/, 2020-07-29.

CHEN Qiheng, SHI Mingli, NEVILLE Kevin, L Cindy, Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China, 2019. Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/ (2020-09-02).

CHEN Stephen, KWOK Kristine, Snowden effect changes US-China dynamic on cybersecurity, *The South China Morning Post,* 2014. Available at: https://www.scmp.com/news/china/article/1532984/snowden-effect-changes-us-china-dynamic-cybersecurity, 2020-07-11.

CHEN, Celia, China Punishes 100 apps breaches of personal information as consumer anxiety rises over privacy, *South China Morning Post*, 2019, www.scmp.com, 2020-04-11.

China's ByteDance asks TikTok to prepare for US shutdown: report, *Aljazeera News,* 2020. Available at: https://www.aljazeera.com/ajimpact/china-bytedance-asks-tiktok-prepare-shutdown-report-200828023847793.html (2020-08-28).

Chinese netizens get privacy-conscious, About Face, *The Economist*, 2019, www.economist.com, 2020-04-10.

CLEMENT, J., Cyber crime: biggest online data breaches as of 2020, 2020, www.statista.com, 2020-04-01.

CREEMERS Rogier, TRIOLO Paul, WEBSTER Graham, Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), 2018. Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/#:~:text=Article%2037%3A%20Critical%20information%20infrastructure,store%20it%20within%20mainland%20China (2020-09-04).

CREEMERS Rogier, TRIOLO Paul, WEBSTER Graham, Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference, 2018, Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/, 2020-07-15.

CREEMERS, Rogier, Central Leading Group for Internet Security and Informatization Established, in *China Copyright and Media*, 2014, www.chinacopyrightandmedia.wordpress.com, 2020-04-03.

DOUGLAS Antonio, How Companies Are Reacting to China's New Data Security Scheme, *China Business Review – US-China Business Council*, 2020. Available at: https://www.chinabusinessreview.com/why-companies-are-still-reluctant-to-file-in-chinas-new-data-security-scheme/ (2020-09-10).

GE Yang, Wall Street Abuzz Over Chinese Data Center Operator's IPO, *Business & Tech*, 2020. Available at: https://www.caixinglobal.com/2020-09-09/wall-street-abuzz-over-chinese-data-center-operators-ipo-101603268.html (2020-08-09).

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 (2020-08-03).

https://www.bbc.com/news/world-middle-east-24316661, (2020-08-26).

LI Xia, Big Data prospering in southwest China's Guizhou, in *Xinhua News*, 2019, www.xinhuanet.com, 2020-04-04.

LIU Caiping, SHEN Timmy, In Depth: Progress and Pitfalls for Foreign Investors in China's Capital Markets, *Caixin*, 2020. Available at: https://www.caixinglobal.com/2020-06-18/in-depth-progress-and-pitfalls-for-foreign-investors-in-chinas-capital-markets-101569516.html (2020-08-09).

LUCAS, Louise, WATERS, Richard, China and US compete to dominate big data, 2018, www.ft.com, 2020-04-14.

LUO Yan, FEIN Ashden, ZHANG Huanhuan, DAUGHERTY Moriah, China Releases New Regulation on Cybersecurity Inspection, *Covington - Inside Privacy*, 2018. Available at: https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/, 2020-07-25.

LUO Yan, YU Zhijing, China Issues New Measures on Cybersecurity Review of Network Products and Services, *Covington – Inside Privacy*, 2020. Available at:

https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/, 2020-07-25.

LUO Yan, YU Zhijing, SHEPHERD Nicholas, China Seeks Public Comments on Draft Measures related to the Cross-border Transfer of Personal Information, *Covington – Inside Privacy*, 2019. Available at: https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/ (2020-09-03).

LUO, Yan, YU, Zhijing, SHEPHERD, Nicholas, China's Ministry of Public Security Issues New Personal Information Protection Guideline, *Inside Privacy Covington*, 2019, www.insideprivacy.com, 2020-03-05.

Ministry of Justice of the People's Republic of China, 个人信息出境安全评估办法（征求意见稿）, 2019. Available at: http://www.moj.gov.cn/news/content/2019-06/13/zlk_3225812.html (2020-09-02).

MOZUR Paul, Joining Apple, Amazon's China Cloud Service Bows to Censors, *The New York Times*, 2017. Available at: https://www.nytimes.com/2017/08/01/business/amazon-china-internet-censors-apple.html (2020-09-10).

NING Susan, WU Han, LI Yuanshan, XUEZI Dan, Development of PRC: Regulations on Cross-border Data Transfer, 2019. Available at: https://www.chinalawinsight.com/2019/06/articles/crossing-borders/development-of-prc-regulations-on-cross-border-data-transfer/ (2020-09-02).

ORTIZ-OSPINA, Esteban, The rise of social media, in *Our World in Data*, 2019, www.ourworldindata.org, 2020-03-15.

PEARCE, Sarah, Data Privacy in Asia Pacific: a fragmented landscape, 2019, www.regulationasia.com, 2020-04-16.

Personal Data Protection, Fact Sheets on the European Union, 2020, www.europarl.europa.eu, 2020-04-16.

POULSEN Kevin, MCMILLAN Robert, TikTok Tracked User Data Using Tactic Banned by Google, *The Wall Street Journal*, 2020. Available at: https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738 (2020-08-28).

SACKS Sam, TRIOLO Paul, WEBSTER Graham, Beyond the Worst-Case Assumptions on China's Cybersecurity Law, 2017. Available at: https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/ (2020-09-04).

Society 5.0, Government of Japan, *Cabinet Office*, www8.cao.go.jp/cstp/english/society5_0/index.html, 2020-04-02.

SUNG Michael, China's National Blockchain will Change the World, *Coindesk*, 2020. Available at: https://www.coindesk.com/chinas-national-blockchain-will-change-the-world (2020-09-04).

Supervisor of the State Administration of Market Regulation 国家市场监督管理总局主管, "Tongzhi! Zai Shenzhen yaodian mai fare kesou yao, xu shimingzhi bing ce tiwen" 通知！在深圳药店买发热咳嗽药，须实名制并测体温 (Notice! Pharmacies in the city of Shenzhen that sell fever or cough medicines must deploy the real-name system and measure people's temperature.), *Zhongguo zhiliang xinwenwang*, 2020, www.cqn.com.cn, 2020-04-05.

The General Agreement on Tariffs and Trade, *World Trade Organization (WTO)*, 1947, Article XXI. Available at: https://www.wto.org/ljazee/docs_e/legal_e/gatt47_02_e.htm#articleXXI (2020-08-28).

VILLAS-BOAS Antonio, Huawei has been blacklisted by the US government. Here's what happened to the last Chinese tech company that got the 'death penalty.', *Business Insider*, 2019. Available at: https://www.businessinsider.com/ ljaze-us-ban-similar-to-zte-us-ban-2019-5?IR=T (2020-08-26).

WEI, Changhao, Translation: 13th NPC Standing Committee Five-Year Legislative Plan, *NPC Observer*, 2018, www.npcobserver.com, 2020-04-20.

WITT Michael A. Prepare for the U.S. and China to Decouple, *Harvard Business Review*, 2020. Available at: https://hbr.org/2020/06/prepare-for-the-u-s-and-china-to-decouple (2020-08-22).

WITTBOLD, Kelley A., CARROLL Colleen, IANSITI Marco, ZHANG Haipeng M., LANDMAN Adam B., How Hospitals Are Using AI to Battle Covid-19, in *Harvard Business Review*, 2020, www.hbr.org, 2020-04-01.

www.bbc.com

www.cac.gov.cn

www.en.pkulaw.cn

www.encyclopedia.com

www.english.court.gov.cn

www.npc.gov.cn

XIAO, Xia, China has 854 million internet users: report, in 新华网 *Xinhuawang*, 2019, www.xinhuanet.com, 2020-03-18.

YANG Yuan, LIU Nian, Beijing orders state offices to replace foreign PCs and software, *Financial Times*, 2019. Available at: https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406 (2020-08-30).

YUAN, Shawn, How China is using big data to fight coronavirus, in *Aljazeera News*, 2020, www.aljazeera.com, 2020-04-06.

ZHANG Erchi, HAN Wei, Apple Hands Off China iCloud Data Operations, *Caixin*, 2018. Available at: https://www.caixinglobal.com/2018-01-11/apple-hands-off-china-icloud-data-operations-101196242.html (2020-09-10)

ZHANG Pengfei, Xi stresses cybersecurity, Positive Internet Environment, Xinhua News, 2016. Available at: http://english.cctv.com/2016/04/26/ARTIytu6SlRGHWfOikb18ntG160426.shtml, 2020-07-14.

ZHANG, Ning, 1994 China access to the Internet, in *CCTV*, 2019, www.cctv.com, 2020-03-18.

国务院办公厅关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见，*Guowuyuan bangongting guanyu jiakuai tuijin shehui xinyong tixi jianshe yi xinyong wei jichu de xinxing jianguan jizhi de zhidao yijian*. Full text available at: http://www.gov.cn/zhengce/content/2019-07/16/content_5410120.htm

More details about SCCs available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_it.