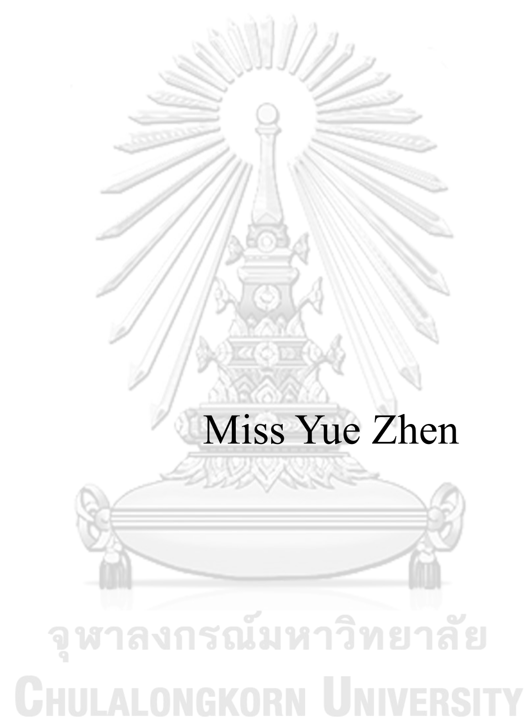
Existence and Enforcement of a Right to be Forgotten in China


จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Miss Yue Zhen

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Laws in Business Law
FACULTY OF LAW
Chulalongkorn University
Academic Year 2022
Copyright of Chulalongkorn University

การรับรองและบังคับใช้สิทธิที่จะถูกลืมในสาธารณรัฐประชาชนจีน

น.ส.เย่ เจิน

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สาขาวิชากฎหมายธุรกิจ ไม่สังกัดภาควิชา/เทียบเท่า

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2565

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Thesis Title	Existence and Enforcement of a Right to be Forgotten in China
By	Miss Yue Zhen
Field of Study	Business Law
Thesis Advisor	Piti Elamchamroonlarp, Ph.D.

Accepted by the FACULTY OF LAW, Chulalongkorn University in Partial Fulfillment of the Requirement for the Master of Laws

.... Dean of the FACULTY OF LAW
()

THESIS COMMITTEE

.... Chairman
(Associate Professor Kanathip Thongraweewong)

.... Thesis Advisor
(Piti Elamchamroonlarp, Ph.D.)

.... Examiner
(Assistant Professor TIDARAT SINLAPAPIROMSUK, Ph.D.)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เย่ เจิน : การรับรองและบังคับใช้สิทธิที่จะถูกลืมในสาธารณรัฐประชาชนจีน. (Existence and Enforcement of a Right to be Forgotten in China) อ.ที่ปรึกษาหลัก : ปิติ เอี่ยมจำรูญลาภ

งานวิจัยนี้ตรวจสอบถึงการที่ระบบกฎหมายของสาธารณรัฐประชาชนจีนรับรอง และคุ้มครองสิทธิที่จะถูกลืม โดยมีขอบเขตของการศึกษาที่ครอบคลุมถึงการ เกิด ขนึ้ และลกัษณะของ "สิทธิที่จะถูกลืม" ตลอดจนกฎระเบียบเกี่ยวกับการ "ลบ" ผลการศึกษาแสดงให้เห็นถึงความท้าทายในการคุ้มครองสิทธิที่จะถูกลืมอันเนื่อง มากจากการที่ข้อมูลส่วนบุคคลของผู้ทรงสิทธิที่จะถูกลืมนั้นถูกเผยแพร่และ สามารถถูกเข้าถึงได้ในทางออนไลน์ นอกจากนี้ การคุ้มครองสิทธิที่จะถูกลืมใน แตล่ ะประเทศซงึ่ เชือ่ มตอ่ กนั ผา่ นอนิ เทอร์เน็ตนนั้ มีความแตกตา่ งกนั งานวจิยันี้ พบว่าการกรอบทางกฎหมายในระดับรัฐบัญญัติเพื่อคุ้มครองสิทธิที่จะถูกลืมของ สาธารณรัฐประชาชนจีนนั้นยังขาดศักยภาพในการคุ้มครองสิทธิที่จะถูกลืม หากเปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) กฎหมายของสาธารณรัฐประชาชนจีนนั้นยังขาดกลไกในการสั่งและตอบสนองต่อ การลืมข้อมูลที่ถูกเผยแพร่ต่อสาธารณชนโดยผู้ให้บริการสืบค้นข้อมูลออนไลน์ นอกจากนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐประชาชนจีนมี ความแตกต่างจากมาตรา 17 ของ GDPR เนื่องจากไม่มีบทบัญญัติรับรองถึง "สิทธิที่จะถูกลืม" เอาไว้อย่างชัดแจ้ง ในขณะที่กฎหมายอื่น ๆ ได้แก่ กฎหมาย แพ่งและกฎหมายว่าด้วยความปลอดภัยทางไซเบอร์ก็ไม่อาจให้ความคุ้มครอง สิทธิที่จะถูกลืมได้ในอย่างเพียงพอในทางปฏิบัติ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สาขาวิชา	กฎหมายธุรกิจ	ลายมือชื่อนิสิต	....
ปีการศึกษา	2565	ลายมือชื่อ อ.ที่ปรึกษาหลัก	....

6384010034 : MAJOR BUSINESS LAW
KEYWORD: RIGHT TO BE FORGOTTEN, PERSONAL DATA, SEARCH ENGINE COMPANY

Yue Zhen : Existence and Enforcement of a Right to be Forgotten in China. Advisor: Piti Elamchamroonlarp, Ph.D.

This research examines establishment and enforcement of the right to be forgotten under the Chinese legal system, including the origin and characteristics of the "right to be forgotten", as well as the regulations on "erasure" in China. It finds that protection challenges stem from the fact that personal data can be publicly accessible online. In addition, different countries, which are electronically connected through the internet, may have different legal protection measures for a right to be forgotten. In China, a legislative protection on a right to be forgotten is relatively weak. Firstly, compared with the General Data Protection Regulation (GDPR), the Chinese legal system does not have mechanisms to call for and respond to deletion of personal data that must be forgotten made publicly accessible by a search engine company. Unlike Article 17 of the GDPR Personal Information protection law of China does not explicitly stipulate the right to be forgotten in the law; whereas, other areas of laws namely, civil law, cyber security law, are not sufficient to practically guarantee a right to be forgotten.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Field of Study:	Business Law	Student's Signature ....
Academic Year:	2022	Advisor's Signature ....

ACKNOWLEDGEMENTS

First of all, I would like to express my gratitude to Chulalongkorn University Law School, it is an honor to be a member of the Law School, although the covid-19 pandemic in 2020 and 2021 will have a bad impact on our study and life, making Classes have become mainly online courses. In the past two years of study and life, there have been many unimaginable difficulties, but we have successfully overcome them.

I would like to thank Asst. Prof. Dr.Piti Eiamchamroonlarp for his unconditional support from the beginning of the thesis proposal, and for his continuous and valuable advice throughout my research process. It is my great honor to study under his guidance, without him guidance, the dissertation could not be completed on time. Thanks to other research committee members for their suggestions. Besides, I had lots of help from other law faculty staff, such as Sirithida Ngeanthong.

Last but not least, Thanks to my family and friends for their support and love. And I would like to thank my classmates Liang Shuang, Xiang Yi Chen, Dora and Tanty for giving me some advice and encouragement when I encountered difficulties in writing the thesis.

Yue Zhen

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

TABLE OF CONTENTS

Page

ABSTRACT (THAI) iii

ABSTRACT (ENGLISH)...iv

ACKNOWLEDGEMENTS...v

TABLE OF CONTENTS vi

CHAPTER 1 Introduction...1

1.1 Background 1

1.2 Research Question 4

1.3 Hypothesis..4

1.4 Scope..4

1.5 Research Methodology 5

1.6 Significance and Contributions..5

CHAPTER 2 Basic concept of “Right to be Forgotten”......................................7

2.1 Background and definition 9

2.2 Core features of the “right to be forgotten”..12

2.3 Contents of the “Right to be forgotten”...14

2.4 The legal nature of the right to be forgotten 16

2.4.1 Right to personality...17

2.4.2 Basic human rights..19

2.4.3 Right to be forgotten and right to erasure 21

2.4.4 Right to be forgotten and privacy 24

2.4.5 Right to be forgotten and right of reputation 27

CHAPTER 3 Challenges of protecting a “right to be forgotten” in a digital era.........29

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.1 Theoretical challenges 29
3.1.1 Publicly accessible personal data published on the internet 29
3.1.2 Unequal protection in different jurisdictions 30
3.2 Practical challenges...31
3.2.1 Personal data electronically published by a search engine on the internet 31
3.2.2 Determination on the period of time 33
3.2.3 Insufficient legal text 36
3.2.4 The complexity of social media users...41
CHAPTER 4 The protection of the right to be forgotten..43
4.1 Legislative basis for the protection of the right to be forgotten in China......43
4.1.1 Civil Law 43
4.1.2 Economic law..46
4.1.3 Cybersecurity Law 48
4.1.4 Personal Information Protection Law 49
4.2 China's first "right to be forgotten" case -Ren Jiayu V. Baidu 50
4.3 Foreign Legislation and Judicial Practice...54
4.3.1 GDPR legislative experience on protecting the "right to be forgotten" 54
4.3.1.1 Legislative history of the "right to be forgotten".....................54
4.3.1.2 Provision of "right to be forgotten" 57
4.3.2 The judicial practice of protecting the "right to be forgotten" in Japan 58
4.4 Comparison table of the Right to be Forgotten, existing restrictions and protection 59
CHAPTER 5 Conclusion and Recommendations...64
5.1 Conclusion 64

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

5.2 Recommendations....67
REFERENCES....69
VITA....77

CHAPTER 1 Introduction

1.1 Background

In February 2022, the 49th "Statistical Report on Internet Development in China" released by the China Internet Network Information Center (CNNIC) showed that by December 2021, the number of Internet users in China reached 1.032 billion, and the Internet penetration rate reached 73.0%[1]. Personal life is closely linked with the Internet, which comprehensively records our lives. While the development of the Internet has brought much convenience to our lives, it has also brought us many risks. In the process of information utilization and dissemination, due to the influence of other factors, the information subject may lose control over personal information, resulting in information becoming an alien force controlling individuals. This alienation of data has many negative effects. For example, by analyzing your browsing records, consumer APPs can push commodity advertisements in a targeted manner, and intrude into consumers' personal areas in all directions; the advancement of network technology has provided convenient conditions for cybercrime. One of the most worrying ones is the invasion of privacy caused by the permanence and sharing of data. Once the information exists publicly on the Internet, thanks to the rapidity of big data and network dissemination, while we can easily obtain the required information, personal information is also rapidly disseminated to the entire network in virtual space, and through the transmission of search engines, The privacy attribute of personal information is difficult to maintain. For example, with the technical support

[1]Available at: Statistical Report on Internet Development in China ,http://www.stdaily.com/index/kejixinwen/202202/a4d43a3e70714781bf692d63c3f56781.shtml

of cloud algorithms and cloud storage, information such as consumption, shopping, and travel in the network has become data stored in the cloud, and our lives are facing the dual perspective of digital space and time. When we browse information on the Internet, this fragmented information can restore a specific digital portrait of a person through algorithms, and when this information is combined with other behaviors, our privacy will be exposed. For example, the consumption information is integrated with the data of travel, communication, circle of friends and other data of the day, and your daily behavior will be seen in front of the public. The aggregation of personal information and the deeper integration of data can outline a person's daily life scene. This penetration of privacy is not only "1+1=2", but is often greater than 2.[2]

In the Internet era, data is information. Memory becomes the norm, forgetting becomes the exception. When many companies recruit employees, they will retrieve the relevant personal information of candidates on social networking sites as one of the basis for hiring.[3] When enrolling students, some schools also use the Internet to retrieve the personal information released by the students on the Internet, so as to judge the personality of the students, and use this as an important basis for whether to recruit students.[4] On the one hand, the Internet expands the scope of human memory by collecting, processing, and storing people's information. On the other hand, postings, comments, and pictures on the Internet will cause eternal "branding" to the main body of information[5]. A person's "digital history" can affect his reputation and development opportunities. Illegal records, criminal records and bad information recorded on the Internet will cause many people to receive various discriminatory

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[2] Zipei Tu. Big Data [M]. Guilin: Guangxi Normal University Press, 2012: 162.

[3] Brian Geremia, "Chapter 336: Protecting Minors' Online Reputations and Preventing Exposure to Harmful Advertising on the Internet", 45 McGeorge Law Review(2013), p.440.

[4] Brian Geremia, "Chapter 336: Protecting Minors' Online Reputations and Preventing Exposure to Harmful Advertising on the Internet", 45 McGeorge Law Review(2013), p.440.

[5] Erving Goffman, Stigma: Notes on the Management of Spoiled Identity (Touchstone Press,1986), pp.25-26.

treatment in terms of further education, employment, and participation in social and public life. According to the statistics of some scholars, there are at least more than 160 laws restricting the rights of citizens who have been criminally punished[6].

In China, a reporter from the Southern Metropolis Daily revealed that the whereabouts of colleagues can be purchased for only 700 yuan, including 11 records such as taking a plane, opening a house, and surfing the Internet. The location can even be accurate to longitude and latitude. JD.com 12G user data leaked And so on, all showing the destructive power of the Internet and big data. Every individual appears insignificant in the face of such a behemoth, so is there a way to free us from the fear of personal information and privacy security violations? It is the rapid expansion of big data and the various negative impacts that gave birth to the "right to be forgotten". As an emerging right, the right to be forgotten is mainly aimed at personal information that has been legally disclosed, and aims to return the disclosed personal information to the privacy field[7]. It attempts to reverse the network system with permanent memory, allowing data subjects to selectively "forget" data through special means. Relevant jurisprudences in other countries reveal potential capability of their legal systems to protect the right to be forgotten. In the *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, the European Court of Justice established the right to be forgotten judicially based on the provisions of Articles 12 and 14 of the 1995 EU Data Protection Directive, and clarified that Google Inc. Deletion obligations as a data controller[8]. It

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[6] Constructing a Juvenile Conviction Elimination System from the Perspective of the New Criminal Procedure Law, China Court Network, http://www.chinacourt.org/article/detail/ 2013/09/id/1083484.shtml

[7] Meg Leta Ambrose and Jef Ausloos, The Right to Be Forgotten Across the Pond, 3 Journal of Information Policy (2013), p.14.

[8] Michael L. Rustad , Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow", 28 Harvard Journal of Law, Technology (2015) 251, p.360.

can be seen that the right to be forgotten plays a very important role in safeguarding human dignity.

1.2 Research Question

In the era of big data, the permanence, openness, and sharing of digital memory have brought many troubles to human beings. Whether personal information that has been stored and publicly accessible can be forgotten has become an urgent problem that needs to be answered. The right to be forgotten is an emerging right in the Internet era, China's laws on the protection of personal information are scattered in many laws and regulations, including the Personal Information Protection Law that has come into effect in November 2021, only stipulates the right to erasure, and don't have the right to be forgotten. Therefore, Whether Chinese laws can adequately protect the "right to be forgotten" is the main question of this research. To answer this main question, the primary question that should be answered is whether China's law have right to be forgotten, and the second question that should be answered is enforcement of the right to be forgotten in China.

1.3 Hypothesis

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

The Chinese legal system is unable to adequately protect an individual's right to be forgotten especially in the digital era because an absence of explicit recognition of a right to be forgotten in the Personal Information Protection Law of China.

1.4 Scope

This research mainly focuses on the establishment and enforcement of the right to be forgotten under the Chinese legal system, including the origin and characteristics of the "right to be forgotten", as well as the regulations on "erasure" in China. It discusses challenges on enforcement of the right to be forgotten arising from the

current legislation. In addition, this research performs comparative analysis with foreign legislation and enforcement experience on the "right to be forgotten" under the EU GDPR, as well as selected case studies especially *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.*

1.5 Research Methodology

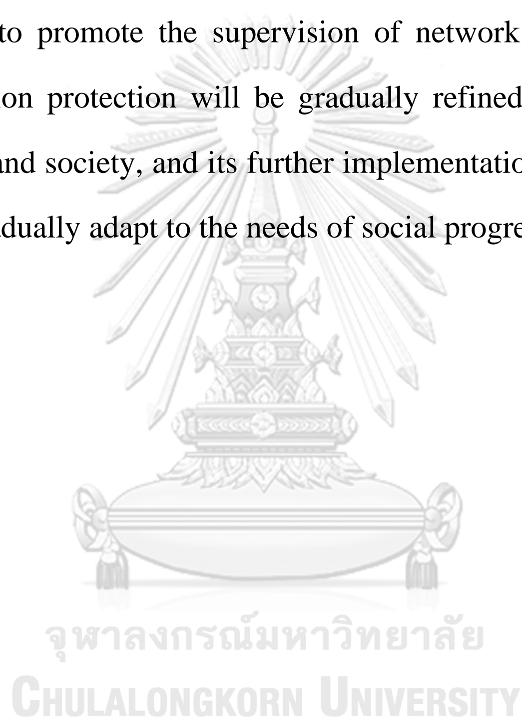
This research mainly searches and organizes various relevant domestic and foreign materials, including but not limited to laws and regulations, articles, journals, books and newspapers, and discusses the problems through theoretical analysis and qualitative research. In terms of basic attributes, this research also compares the relationship between the right to be forgotten and the right to personality and human rights, and compares the right to be forgotten and the right to delete through Google Case. In addition, based on different legislative, political and cultural backgrounds and traditions, using functional comparative analysis to compare the provisions and Judicial Practice of the "right to be forgotten" in EU Japan and China and the analysis of actual cases, and compare the judicial experience of the EU and Japan, and find out better experiences from China which explore and solve the problems of the existence and implementation of the "right to be forgotten" in China. In essence, China can refer to the legislative and judicial practice experience of the European Union or Japan and find its own legislative and judicial practice path suitable for the right to be forgotten based on different cultural traditions and economic and political backgrounds.

1.6 Significance and Contributions

This research explores theoretical as practical difficulties in implementing the "right to be forgotten" in more legislative blanks and practices in China. With the gradual development of network technology, the ever-growing search engine system has

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

created new threats to the personal information security of information subjects, and the original legal implementation methods and strengths can no longer meet the requirements of new legal relations. Introducing the concept of the right to be forgotten into China still has the problem of how to promote its implementation, and it will also raise new problems of integrating and linking relevant provisions in China's existing legal system. The demand for the implementation of personal information protection will further increase, especially in terms of the use of big data cloud computing to promote the supervision of network operators. Legislation on personal information protection will be gradually refined with the development of China's economy and society, and its further implementation will also prompt China's legal system to gradually adapt to the needs of social progress.



CHAPTER 2 Basic concept of “Right to be Forgotten”

With the rapid development of digital technology and network services, the pattern between memory and forgetting has been subverted, and the "right to be forgotten" as an "emerging" right has gradually become the focus of public attention. The purpose of the right to be forgotten is to make the data subject "forgotten" in the online society, so as to protect personal dignity and personal interests. In order to achieve this purpose, the content of the right to be forgotten is set to give the data subject the right to request deletion of personal data, so that the data subject is free from outdated, irrelevant and unnecessary personal data.

If the right to be forgotten is included in the list of dishonest people in China. The list of dishonest persons subject to execution published by the Supreme People's Court includes names and ID numbers. Based on the strict arrangement rules for ID card numbers, it exposes the province, city, district, date of birth and other information of the dishonest persons subject to execution. According to the "identifiability" standard currently generally adopted in China, the ID card number should belong to personal information. According to the regulations--Several Provisions of the Supreme Court on Publishing the List of Dishonest Persons Subject to Execution" (2017 Amendment), the people's court shall delete the information within three working days after the execution is completed or the execution is suspended[9]. Corresponding to the EU's "return to social expectations" standard, after being removed from the court list, the dishonest person subject to enforcement may request the search engine or other reprinting media to delete or obscure their personal information after a certain period

[9] "Several Provisions of the Supreme Court on Publishing the List of Dishonest Persons Subject to Execution" (2017 Amendment), Fa Shi [2013] No. 17, Article 10.

of time. It can be seen that the function of the right to be forgotten lies in conflict resolution[10] and effective avoidance of the outdated information stored on the network from continuing to intrude on the current living state of the information subject[11], and prevent others from violating privacy, second, the right to be forgotten also removes the unwanted impact of negative information on individual interests and development. From the perspective of legislative evolution, China's existing laws are similar to those of the EU to some extent, but there are also big differences. In the European Union, the right to protect personal information is considered a fundamental right, but in China, we can be traced back to the 2010 China tort liability law of notification and delete mechanism, "tort liability law" stipulated in article 2010, when the third party service implementation through the network tort, the victim shall have the right to inform the Internet service provider to delete, necessary measures such as shielding, disconnected[12]. It is worth noting that although this regulation requires the deletion of personal information, the precondition is the existence of an "infringement", which largely distinguishes between the Chinese version of the right to delete and the EU's right to be forgotten. Europe's right to be forgotten is an inherent right of the individual, However, China's legislation does not only construct its right to be forgotten on an individual basis. This was also reflected in the subsequent Chinese Cyber Security Law and Personal Information Protection Law.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

[10]Peiru Cai, Reflection and Reconstruction of the Right to Be Forgotten System, http://www.calaw.cn/article/default.asp?id=13355

[11] Wancheng Gao and Yiqing Cheng, “What exactly is the "right to be forgotten?", “Procuratorate Daily”, 2016.

[12] Article 36 of the PRC 2010 Tort law: “A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability.

Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user.” China has integrated Tort law into new civil code and this article does not change.

The different foundations of the right to be forgotten in China can be seen from the fact that the reasons for deletion are ascribe to existing laws, administrative regulations and mutual agreements in a conservative way. China's position is not individualistic in nature in enacting the right to be forgotten, as it does not treat personal information as personal property. As such, it does not give individuals an inherent right to apply for the deletion of personal information[13].

2.1 Background and definition

In Chinese academic literatures, a "right to be forgotten" means, “The data controller is required to delete or disconnect the information that has been legally disclosed on the Internet, but is inappropriate, irrelevant, beyond the original purpose of processing, and will lead to lower social evaluation. A right to the necessary measures such as linking[14].” In the age of traditional media, information dissemination has a certain life cycle. Because of the instant nature of radio and television, after the broadcast of the program, some information will gradually disappear at the audience level, which is equivalent to a drop of water that falls into the vast ocean and is difficult to find. Although the information disseminated by paper media will not be instantly annihilated at the audience level, due to the accumulation of paper media, it requires a large physical space to preserve it, and the audience capacity is limited, so it is difficult to preserve a large number of paper media. At the same time, the scale of information release in the age of traditional media also has certain particularities. Since traditional media resources are relatively scarce and the responsible party is relatively clear, legal means, public opinion and industry self-discipline can be comprehensively used to punish non-standard media, making the protection of

[13] Zhengyu Shi, The Right to Be Forgotten in China--A Third Way to Construct Public Sphere (April 3, 2021). Available at SSRN: https://ssrn.com/abstract=3832803 or http://dx.doi.org/10.2139/ssrn.3832803

[14] Lixin Yang and Xi Han: "The Chinese Localization of the Right to Be Forgotten and the Application of Laws", "Application of Law", No. 2, 2015, p. 24.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

personal information still within a controllable range. Therefore, in the age of traditional media, it is not easy to collect and organize information in disguised form. In the era of big data, with the popularization of the Internet and the generation and development of technologies such as cloud backup and data capture, people's words and deeds can be digitized, and once data is generated, it can be transmitted at low cost, extremely fast, and across regions. , copying and storage, people can extract information from massive data at any time through the keyword "one-click retrieval" and other methods. However, the whole network storage and high extractability of this information make everyone a "transparent" in a sense. people". Because anyone can understand and evaluate a person by retrieving relevant information, breaking the tranquility of people's lives. Because everyone can be the source of information generation, once an infringement incident occurs, it is more difficult to effectively grasp the determination of the responsible subject and the delineation of the scope of responsibility than in the traditional media era. Therefore, in the Internet age, "forgotten" has become an urgent need of the information society. In China, it is more emphasized that certain communication behaviors or more explicit information flow in the public domain violate existing rights and values, or it is more emphasized that the reasonable flow of information entrusts human rights, and China understands the reasonable flow of information and the expectations of individuals and communities as the embodiment of existing laws and regulations. China's legislation does not push China's right to be forgotten into another era without freedom of speech. The concept of the right to be forgotten is not deeply rooted in China's legal culture. For the legislation itself, it only protects the flow of information in line with the public interest and individual expectations, rather than the social atmosphere of complete freedom of speech. China's legal practice on this issue shows a different way of thinking from that of Europe and America. Chinese law refuses to distinguish between public and private in the digital age by considering only factors such as

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

control or public concern. The fact that relevant Chinese laws stipulate that the deletion of personal information is premised on the violation of laws and regulations or the agreement of the parties concerned shows that the right to be forgotten is not only an individual right in Chinese laws, but also a mechanism to coordinate various interests embedded in personal information, including the original idea to give individual a second chance and extensive public concern[15]. The right to be forgotten is not just about deletion, delinking, erasure, it also contains many other elements.

It is also in the context of this era that the European Union gave citizens the “right to erasure” in the 1995 Data Protection Directive (1995 Data Protection Directive 95/46/EC) to protect personal information. This can be considered the initial form of the "right to be forgotten". In 2012, the European Union published the General Data Protection Regulation (Draft) (hereinafter referred to as "GDPR"), which established the "Right to be Forgotten and to Erasure" clause, 3 It is stipulated that the information subject has the right to claim to the information controller to delete the relevant personal information, or to prevent the further dissemination of some personal information. The regulation was finally passed on April 14, 2016, and came into effect in May 2018, marking that the “right to be forgotten” has been recognized as a legal right. In May 2014, the Court of Justice of the European Union (“CJEU”) made a final decision in the Google Spain SL and Google Inc. v AEPD and Mario Costeja González case[16], upholding the Part of the plaintiff's "right to be forgotten" claim. Since this decision of the CJEU will apply to all EU member states, it also marks that the "right to be forgotten" has been reaffirmed within the EU through the highest judicial authority of the CJEU. In this case, CJEU considers that when the

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[15] Zhengyu Shi, The Right to Be Forgotten in China--A Third Way to Construct Public Sphere (April 3, 2021). Available at SSRN: https://ssrn.com/abstract=3832803 or http://dx.doi.org/10.2139/ssrn.3832803

[16] Google Spain SL and Google Inc. v. Agencia Esñpaola de Protección de Datos (AEPD) and Mario Costeja Gonzalez , C-131/12,2014.

personal information of the information subject becomes inadequate, irrelevant or no longer relevant, or excessive in the relation to the purpose of the processing due to the passage of time, The information subject may request the search engine service provider to delete the link to the index-related information.

2.2 Core features of the “right to be forgotten”

In the "Google Spain case", the website of the Spanish newspaper La Vanguardardia published the announcement that Mario Costeja González's house was auctioned due to debts, and the information was cataloged by the Google search engine. So Gonzalez sued the "Herald" website and Google Inc. to the court on the grounds that the relevant information is irrelevant, unnecessary and outdated. In the end, the court agreed to some of the plaintiff's petitions and asked Google to disconnect the search link for relevant information, but for reasons such as freedom of the press, it did not ask the Herald to delete the corresponding news reports. Throughout this case, combined with the basic concept of the "right to be forgotten", it can be roughly concluded that the "right to be forgotten" has the following five characteristics:

1. The first is that the object pointed to by "forgotten" is "legal circulation of network information"[17]. In the "Google Spain Case", the real estate auction information of the plaintiff Gonzalez was published on the website of "The Herald" because of the particularity of this type of information, that is, to deal with personal real estate by public auction to repay the arrears. , its dissemination method is not illegal. If there is an infringement in the use of the information, the information subject may claim that the right to privacy, right of reputation, right of name, etc. should be applied to protect their own

[17] Xiaying Mei: "On the Legal Positioning of the Right to Be Forgotten and the Limitation of the Scope of Protection", "Applicable Law", No. 16, 2017, p. 49

rights and interests from being infringed, rather than the protection of the "right to be forgotten".

2. The second is that the retention of relevant information may lead to a decrease in the social evaluation of the information subject. The era of big data, characterized by the vigorous development of digital retrieval technology, makes it easy for others to discover some old stories dormant on the Internet, and then reintegrate them to judge the "current me".
3. The third is that the relevant information can identify a specific individual. "Identifiability" is the fundamental feature of personal information. If the relevant information cannot identify a specific subject, it does not belong to "personal information" and can only be regarded as "data" or "information" in a broad sense. In addition, information or data that is not "identifiable" cannot be "targeted" to a specific individual, so it does not have the potential to damage the reputation of a specific subject.

4. The fourth is the "right to be forgotten" for "unnecessary, irrelevant, outdated" personal information. However, what exactly is "unnecessary, irrelevant and outdated" personal information, the relevant EU regulations and judicial decisions are still unclear. This kind of overly abstract expression is not only inefficient in practice, but also easily breeds "abusive lawsuits" in such a loose context. In addition, some scholars believe that the value of the "right to be forgotten" is actually to deal with "outdated, useless or decontextualized information"[18]. This kind of expression seems to be clearer than "unnecessary and irrelevant information", but what is "useless" and "outdated" information is still in the blind spot for judgment. What subject

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[18] Mónica Correia,Guilhermina Rêgo&Rui Nunes. Gender Transition: Is There a Right to Be Forgotten. Health Care Analysis, 2021,29(4):291.

makes the judgment? If a certain information has no value for the information subject, but the information will involve the interests of other subjects, or even social welfare, how to decide the retention or deletion of this information is still a question.

5. The fifth is to ensure freedom of speech and the public's right to know. The main way to exercise the "right to be forgotten" is to delete and block the links provided by search engines to retrieve relevant information, thereby cutting off access to relevant information in massive data, rather than Claim to the search engine service provider to delete the original information published by the third party. As stated by Viviane Reding, the former Vice-President of the European Commission, the "right to be forgotten" is not a complete deletion of the original information, but a "partial deletion"[19]. This feature is also reflected in the "Google Spain Case". The CJEU's final judgment only requires the search engine service provider to take measures to prevent the acquisition of corresponding information through "name" searches, but does not require prohibiting the behavior of extracting relevant information through other words[20]. Therefore, the "right to be forgotten" in the EU context does not allow the information subject to request the "total deletion" of the relevant information. Of course, it is not realistic to "completely delete" all information.

2.3 Contents of the "Right to be forgotten"

[19] Viviane Reding: The EU Data Protection Reform 2012:Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age

[20] Article 29 Data Protection Working Party.Guidelines on the implementation of the Court of Justice of the European Union Judgment on"Google Spain SL and Google Inc. v. Agencia Esñpaola de Protección de Datos (AEPD) and Mario Costeja Gonzalez "C-131/12,2014:2.

The content of the right to be forgotten refers to the relationship between rights and obligations between the subject of rights and the subject of obligations. In a nutshell, the data subject has a right to request the obligated subject to delete network information, and the obligated subject has the obligation to review the request and deal with it. Therefore, when constructing the right to be forgotten, it should also be carried out from these two aspects, as follows:

First, the subject of the right needs to apply to the subject of the obligation. What is the procedure for the information subject to apply to the obligated subject to delete the information? The EU mainly locks the obligated subject as the search engine, and the search engine conducts the application review and makes the final judgment, and the publisher is only informed of the processing result. But in fact, the act of disconnecting a search engine does not eliminate the existence of information on the Internet. Because in addition to obtaining information through search engines, network users can also obtain information through the publisher's official website and APP. Therefore, the right subject should be given the right to choose, and it should choose the obligatory subject to apply. The rights subject can also apply to the publisher and the search engine at the same time to facilitate the exercise of the right to be forgotten. After all, the publisher and the search engine are different subjects, will judge differently, and publishers remove the content itself, while search engines remove links. Or as Professor Luciano suggested: the right holder must first apply to the publisher, and if it fails, he can apply to the search engine[21]. That is to say, applying to the publisher is a precondition for applying to the search engine. However, this requires another obligation for search engines to really work, that is, search engines should remove links to information when publishers take action to remove

[21] LUCIANO FLORIDI. Right to be Forgotton: Who May Ex-ercise Power，over Which Kind of Information? (2014)，
https://www.theguardian.com/technology/2014/oct/21/right-to-be-forgotten-who-may-exercise-power-information

information and notify search engines. Secondly, the application should be in writing to indicate formality and facilitate future proof, and the content should include information links, reasons for deletion, and legal provisions on the object of the right to be forgotten, such as the subject of the requested deletion, inaccuracy, and damage to one's own rights and interests. To bear the burden of proof to prevent the abuse of the right to be forgotten, of course, when the right to be forgotten is incorporated into the legislation, the obligated subject should provide a formatted application.

Second, obligated subjects, including publishers and search engines, should fulfill their censorship and notification obligations. First of all, the obligated subject should review the request of the right subject as soon as possible after receiving the notice of application for deletion and deal with it. Professor Yang Lixin believes that in order to prevent damage to the right subject, the obligated subject should take action within 24 hours[22]. However, the author believes that 24 hours is too short, because it is not a simple matter for the judiciary, let alone publishing and search engines. In addition, the information has existed in the network for a long time, and it is not necessary to pursue the speed of information processing. Therefore, it is recommended to stipulate that the obligated subject should process it within 3 days. Secondly, in terms of the result of processing, the obligated subject can make three decisions: deletion, non-deletion and restriction of processing. Of course, the deletion and restriction measures taken by the subject of the rights to the subject of the obligation can seek judicial protection. Finally, after the obligated subject makes the deletion decision, it should also fulfill the obligation of notification.

2.4 The legal nature of the right to be forgotten

[22] Lixin Yang, Xu Han. The Chinese localization of the right to be forgotten and the application of the law. The application of the law, 2015(2).

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

2.4.1 Right to personality

According to the traditional dichotomy between personality rights and property rights, which attribute of the right to be forgotten belongs to is worth exploring. Some scholars put forward the viewpoint of “propertyization of personal information”[23],claiming that personal information can become the object of property rights, and the data subject enjoys the ownership of personal information and can protect personal information through tort law. However, some scholars hold objections, claiming that data subjects do not enjoy the property rights of personal information except for the intellectual property rights formed by the processing of information; in addition, they believe that the data subject is the source of personal information, but not necessarily the creator of personal information with property attributes, so the data subject does not enjoy the property rights of personal information. The EU pays attention to the protection of personal rights and rarely mentions property rights. The United States recognizes that personal data can be bought and sold, but does not make it a property right. However, Article 127 of the Civil Code of China clearly stipulates that if the law has provisions for the protection of data and network virtual property, such provisions shall be followed. In the draft of the Civil Code for comments, data information was included in the protection of intellectual property rights, but in the final bill, data information was taken out of the legal provisions of Article 123 "Intellectual Property Rights", and was used as a separate law. "Data" under Section 127. This adjustment undoubtedly means that data information is no longer regarded as the protection field of intellectual property rights, but is protected as a kind of property. It can be seen that personal information has property attributes, personal information property rights are expected to become a new type of property rights, and data processors should enjoy the economic benefits

[23] Arthur R. Miller, Personal Privacy in the Computer Age:The Challenge of New Technology in an Information-Oriented Society (Michigan Law Review Press,1969), p.35-40.

brought by information processing. This emerging right is different from real right, which is the right of the right holder to directly control and exclusively enjoy his interests, while personal information is non-exclusive, non-depleting and infinitely replicable. In fact, a lot of personal information has property attributes, such as trade secrets and databases.

Although personal information has property attributes as the object protected by the right to be forgotten, the right to be forgotten is not a property right. First, the right to be forgotten has a personal attachment and is closely related to human dignity. Although the right to be forgotten is subordinate to the personality right, it is not an independent specific personality right, it can only be attached to a specific personality right and cannot be regarded as a property right. Second, property rights correspond to personal rights, and are rights enjoyed by the subject of rights that can bring economic benefits. However, the right to be forgotten is to hide or delete outdated personal information with personality characteristics that has been disclosed, irrelevant or no longer relevant, and does not bring economic benefits to the data subject. Third, property rights are transferable and inheritable, and the right to be forgotten is only enjoyed by the right holder, is exclusive, and cannot be transferred or inherited[24]. Therefore, the right to be forgotten is not a property right.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

The Italian scholar Giorgio Pino advocates that the right to be forgotten is a right of personality[25],the Swiss scholar Franz Wero also believes that the right to be forgotten belongs to the protection scope of the personal right of data, rather than the right to

[24] Zejian Wang: The Law of Personality Rights: Legal Interpretation, Comparative Law, and Case Studies, Peking University Press, 2013, p. 46.

[25] Giorgio Pino, The Right to Personal Identity in Italian Private Law:Constitutional Interpretation and Judge-Made Rights, The Harmonization of Private Law In Europe，M.Van Hoecke and F.Ost，eds.，Hart Publishing，Oxford 2000，p.225-237.

property[26]. The "personality right" called in modern civil law has a legal status "inherent in the person"[27]. As for the right to be forgotten, it belongs to the right of personality because of the following two aspects: First, the right to be forgotten has personality attachment, closely related to human dignity, should belong to the category of personality rights. Second, personality rights are only enjoyed by the right holder, are exclusive and cannot be transferred or inherited; property rights are transferable and inheritable[28]. The right to be forgotten is only enjoyed by the data subject, and the right to correct, delete or withdraw consent shall not be transferred. Therefore, the right to be forgotten belongs to the protection of personality rights.

2.4.2 Basic human rights

Fundamental human rights are universal human rights due to being human, and everyone should have the right to forget their past and start over. When individuals choose to forget, they should not be disturbed by the outside world. Some scholars may think that establishing the right to be forgotten as a basic human right can better protect citizens' human dignity from being violated. The EU maintains that the right to personal information belongs to the protection scope of basic human rights, while some scholars advocate that the right to be forgotten belongs to the right to personal information[29]. Thinking that the right to be forgotten can be regarded as a specific type of the right to personal information is also an indirect recognition that the right to be forgotten belongs to basic human rights. Although the U.S. has not incorporated

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[26] Franz Wero, “The Right to Inform v.the Right to Be Forgoten: A Transatlantic Clash”, Georgetown Public Law Research Paper (2009)290, p.291.

[27] Junju Ma: Lectures on the Theory of Personality and Personality Rights, Law Press, 2009, p. 71.

[28] Zejian Wang: The Law of Personality Rights: Legal Interpretation, Comparative Law, and Case Studies, Peking University Press, 2013, p. 46.

[29] Zhifeng Zheng: "Research on the Right to Be Forgotten in the Network Society", Legal Business Research, No. 6, 2015, p. 59; Luo Liuhu: "The Right to Be Forgotten: Private Law Regulation of Outdated Personal Information on Search Engines", " Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), May 2016, p. 34.

the right to personal information into the Constitution, the U.S. right to privacy has a very rich connotation. The function of the U.S. law "Information Privacy" is equivalent to that of the German information protection law "Information Selbstbestimmungsrecht"[30]. It is also equivalent to the function of "personal information right" in my country. It can be seen that in the United States, the right to be forgotten originates from the protection of the right to privacy, which is a fundamental right of the Constitution, and the right to be forgotten in the United States may become a basic human right[31].

The primary consideration of the right to be forgotten as a basic human right is the protection of human dignity. First, the right to be forgotten is established as the domestic legal basis of basic human rights. Article 38 of the Chinese Constitution stipulates that the human dignity of citizens shall not be violated. Determining the legal status of human dignity is the legal basis for personal data protection. Second, incorporate the right to be forgotten into constitutional protection to prevent public power from infringing upon citizens' right to be forgotten. Here we can introduce the definitions of "positive freedom" and "negative freedom" in liberalism, analyze it from the perspective of government power, and protect citizens' right to be forgotten[32]. First, from the perspective of positive freedom, if the right to be forgotten is established as a basic human right, the government should provide protection for citizens' information autonomy, and can formulate relevant laws in the form of legislation to eliminate citizens' bad records. Second, from the perspective of negative freedom, if the right to be forgotten is established as a basic human right, the

---

[30] Zejian Wang: The Law of Personality Rights: Legal Interpretation, Comparative Law, and Case Studies, Peking University Press, 2013, pp. 207-209.

[31] Ioana Stupariu, "Defining the Right to be Forgotten. A Comparative Analysis between the EU and the US", LL.M. Short Thesis, Central European University, 2015, p.52-53.

[32] Yu Liang, On the Legal Protection of the Right to be Forgotten, Jilin university. China Academic Journal Electronic Publishing House.

government shall not interfere and hinder citizens' information autonomy. Excessive state intervention will weaken citizens' enthusiasm and violate citizens' human dignity.

2.4.3 Right to be forgotten and right to erasure

Many scholars have discussed the relationship between the right to erasure and the right to be forgotten, and there are differences among various views. Distinguishing the established relationship between the right to erasure and the right to be forgotten is not only conducive to the correct application and protection of the right to erasure, but also to paving the way for increasing the right to be forgotten.

(1) The same theory: the equivalence relationship between the right to erasure and the right to be forgotten.

Scholars who hold the same view believe that the right to erasure and the right to be forgotten are equivalent, and the connotation and extension of the two almost completely overlap. Specifically, in practice, the result of "forgetting" personal information is to let the information be forgotten by people or relevant institutions and platforms in the relevant environment, which is characterized as the purpose of exercising rights; "deleting" personal information The result is that the relevant information is physically deleted on the information network or information platform, which is represented as a means of realizing rights[33]. Some scholars also pointed out that the basic content of the construction of the right to be forgotten in the era of big data is deletion. The right to be forgotten and the right to data deletion have the same meaning, and the two expressions can be used each other[34], both reflect the issue of

33 Wenjie Liu: "Right to be Forgotten: Traditional Elements, New Context and Interest Measurement", Legal Research, No. 2, 2018.

34 Jianwen Zhang: "The Intention, Structure and Characteristics of the Legislation of the Right to Be Forgotten in Russia", Qiushi Journal, No. 5, 2016.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

individuals' control over their data[35]. By reviewing the formulation process of the EU ‘s GDPR , it can be seen that the distinction between the right to be forgotten and the right to erasure has been gradually weakened intentionally. In 2012, the European Parliament and the Council of the European Union published Draft No. 2012/72, 73 on the protection of individuals involving the processing of personal data and the free flow of such data, in which Article 17 provides for the "right to be forgotten and erasure", the specific content is that the information subject has the right to ask the information controller to permanently delete the relevant personal information, and has the right to be forgotten by the Internet, unless there are reasonable reasons for the retention of the information. In March 2014, after a vote by the European Parliament, the title of the original Article 17 was changed from "right to be forgotten and erasure" to "right to erasure", but the specific provisions still contain the expression of the connotation and extension of the right to be forgotten. In April 2016, the European Union adopted the General Data Protection Regulation, in which Article 17 was amended several times and finally expressed as the “right to erasure ‘right to be forgotten’” (right to erasure ‘right to be forgotten’). Judging from the legislative wording, the EU replaces the "right to be forgotten" with "the right to erasure", and at the same time, in order to straighten out the conceptual connection problem, the "right to be forgotten" is placed in the following quotation marks [36], which is similar to The alias of the right, its legal concept is the right to erasure, so the right to erasure and the right to be forgotten can be regarded as the same concept.

(2) Difference theory: the differential relationship between the right to erasure and the right to be forgotten.

[35] Weili Duan: "On the Legal Protection of the Right to Be Forgotten——Also on the Status of the Right to be Forgotten in the Lineage of Personality Rights", "Learning and Exploration", No. 4, 2016.

[36] Fang Wan: "The Right to Be Forgotten: Reflections on the Introduction of the Right to Be Forgotten in China", Law Review, No. 6, 2016.

Scholars who hold the dissent theory believe that there is an essential difference between the right to erasure and the right to be forgotten[37], and the two can be juxtaposed as two separate rights. Some scholars start from the content of the right to erasure and the right to be forgotten, and discuss the major differences between the two, including the subject of the right, the object of exercise and the conditions of application. As far as the subject of the right is concerned, the subject of the right of deletion is all unspecified individuals, and no special distinction is made in the scope. The subject of the right to be forgotten refers to a natural person who is accurately determined by name, ID number, location information, online identity identifier, or one or more physical, physiological, psychological, genetic, economic, cultural, social identity and other characteristics. Applicability to specific groups is specific.

(3) Inclusion: the embedded relationship between the right to erasure and the right to be forgotten

Scholars who hold the theory of inclusion believe that the right to erasure is subordinate to the right to be forgotten. Under the framework of inclusion theory, there are two different views on whether the right to erasure covers the right to be forgotten, or whether the right to be forgotten embraces the right to erasure. The first view holds that the right to be forgotten is only a part of the right to erasure, a special case of the right to erasure. The second view holds that the right to be forgotten is an extension of the right to erasure. The right to erasure has a “one-to-one” feature and is a request made by the data subject when the data controller collects and uses information illegally or in breach of contract. The right to be forgotten is "one-to-many", which not only includes the traditional right to erasure, but also

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

[37] Li Xue: "Research on the Establishment of China's Right to Be Forgotten in the Background of the Entry into Force of GDPR", Legal Forum, No. 2, 2019.

requires the data controller to take necessary measures to eliminate the personal data that has been diffused.

2.4.4 Right to be forgotten and privacy

The original intention of the establishment of the information processing system is to serve human beings. The system is based on the premise of conforming to the basic rights of natural persons, focusing on protecting the right to privacy of individuals, and promoting all-round economic and social development. It can be seen that the processing of personal information is closely related to privacy protection, and the relationship between the right to be forgotten and the right to privacy deserves in-depth consideration.

The legalization process of privacy rights in China: first, Article 12 of the 1984 Universal Declaration of Human Rights clearly states: “No one shall be subjected to arbitrary interference with his private life, family, home and correspondence, nor to attacks on his honor and reputation. Everyone has the right to the protection of the law against Such interference or attack." This is the most important source of international human rights law for the right to privacy. Although different countries have different definitions of the right to privacy, it is generally accepted that the right to privacy mainly protects the privacy of individuals from interference, and only the state can provide protection of privacy[38]. Second, before the right to privacy was explicitly stipulated in 's laws, it was protected by the concept of "reputation right" in judicial practice. The Supreme People's Court's "Answer to Several Issues Concerning the Trial of Original Names" and "Interpretation of Several Issues Concerning Determining Liability for Compensation for Spiritual Damage in Civil Torts" both

[38] Blanca R. Reitz: "Privacy Rights in Electronic Communications: A Comparative Perspective of European Law and American Law", translated by Lin Xifen et al., Shanghai Jiaotong University Press, 2017, p. 37.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

take the infringement of others' privacy interests as the scope of the court's acceptance, and regard the infringement of the right of reputation and the infringement of privacy interests. The separate provisions amount to an acknowledgment that the right to privacy can become a separate civil right. Third, Articles 38, 39, and 40 of the Chinese Constitution stipulate that citizens' human dignity, residence, freedom of communication, and privacy of correspondence shall not be violated. Although the Constitution does not directly state that the right to privacy shall not be violated, It provides a constitutional basis for the protection of the right to privacy, and also clarifies the legal status of the right to privacy as a basic constitutional right. Some scholars have proposed that in the absence of constitutional provisions, constitutional interpretation techniques can also be used through specific cases to complete the task of constitutional protection of the right to privacy. This process shows the effectiveness of the constitutional protection of the right to privacy[39]. Compared with the right to privacy, the right to be forgotten is the right to return the disclosed information to privacy, and to ensure that the data subject returns to a state of seclusion, quiet, and undisturbed. The right to be forgotten eventually reverts the protected object to the field of privacy, and both the right to be forgotten and the right to privacy aim to protect human dignity from being violated. It can be seen that there is a certain relationship between the two.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Although the right to privacy and the right to be forgotten are related, there is a big difference between the right to be forgotten and the right to privacy in my country. Specifically, it includes the following aspects:

[39] Xiuzhe Wang: "Research on Public Law Protection of Personal Privacy Rights in the Information Society", China Democracy and Legal System Press, 2017 edition, pp. 100-101.

First, the attributes of rights are different. The right to privacy is a passive defensive right. It requires exclusion of nuisance and compensation for damages only when it is violated. It is impossible to predict whether the use of personal information will have a negative impact on individuals. Even if individuals can foresee impacts, these impacts are abstract, unpredictable and uncertain[40]. The right to be forgotten is a proactive right. If the personal information related to the data subject is published by himself or others, and the information is outdated and irrelevant, the data subject has the right to request the data controller to change or delete it.

Second, there are differences in whether information disclosure is legal or not. The violation of privacy is caused by the illegal disclosure of personal private information by others. When the right to be forgotten is violated, the release of personal information is legal, and the purpose of the legislation is to reclassify legally released personal information into the privacy field.

Third, the scope of objects is different. The right to privacy protects the tranquility of life and private secrets, and refers to personal private information that is not disclosed to the public. The object scope of the right to be forgotten is the personal information that has been disclosed on the Internet and the personal information that originally belonged to the public domain, but gradually becomes no longer relevant as time passes. There is an inclusive relationship between personal information and personal privacy[41].

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

[40] Meg Leta Ambrose, Jef Ausloos, “The Right to Be Forgotten Across the Pond”, 3 Journal of Information Policy, (2013)1, p.4.

[41] Chenxi Liang and Tiance Dong: "On the Attributes and Boundaries of the "Right to Be Forgotten" in the Background of Big Data, Academic Research, No. 9, 2015, p. 33.

Fourth, the institutional focus is different. The creation of the right to privacy is to prevent the disclosure of personal private information, not to protect the control and domination of privacy. The right to be forgotten emphasizes the control and domination of personal information, and attempts to reclassify the information that has been legally disclosed from the public domain to the private domain.

Fifth, the protection methods are different. The protection of the right to privacy relies on ex post remedies, and the scope of protection involves more personal interests, not public interests or public safety, and can only be carried out through laws. The protection of the right to be forgotten is an ex ante relief and should focus on prevention. The right to be forgotten sometimes involves not only personal interests, but also public interests and public safety. In addition to legal protection, it is also protected by administrative means.

2.4.5 Right to be forgotten and right of reputation

Although the creation of the right of reputation and the "right to be forgotten" both aim to maintain the social evaluation of the subject of the right, there are differences in the essential attributes of the objects of the right aimed at. What the right of reputation regulates is the use of false information to damage the social evaluation of the rights subject. The "right to be forgotten" is mainly aimed at objective and true information that cannot accurately reflect the personality image of the information subject due to the passage of time, and there is a difference between "false" and "true" information. If the media such as newspapers and the Internet publish false information about the information subject, thereby degrading the reputation of the information subject, the false content may be corrected or deleted in accordance with Article 1028 of the Civil Code. However, if others disclose the information subject's

bad credit record to the public in a legal way, the information subject cannot seek protection by claiming the right of reputation.

CHAPTER 3 Challenges of protecting a "right to be forgotten" in a digital era

In the era of big data, the Internet is developing rapidly, advanced network technology makes the collection and processing of information extremely easy, and personal information security faces unprecedented threats. The right to be forgotten is mainly aimed at personal information that has been legally disclosed, and it aims to return the disclosed personal information to the field of privacy[42]. It attempts to reverse the network system with permanent memory, allowing data subjects to selectively "forget" data through special means. However, there appears several legal and technical challenges in protecting and enforcing the right to be forgotten in the internet era.

3.1 Theoretical challenges

First of all, as mentioned earlier, from a practical point of view, it is almost impossible to completely achieve "forgotten" in cyberspace. Because compared with traditional hard-copy media, data in cyberspace can be transmitted, replicated and stored at low cost, unlimited, and across geographies once it is generated.

3.1.1 Publicly accessible personal data published on the internet

Under such an information environment, the information on the Internet is everywhere, and it is difficult to effectively delete the information completely and realize the protection of the right to be forgotten. Second, the territorial nature of the protection of the right to be forgotten makes it difficult to ensure that the right to be

[42] Meg Leta Ambrose and Jef Ausloos, The Right to Be Forgotten Across the Pond, 3 Journal of Information Policy (2013), p.14.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

forgotten can be realized in a borderless network[43]. Different countries and regions have different attitudes towards the right to be forgotten, the laws applicable to one country and region cannot be used in other countries, and the protection strengths in countries and regions that recognize the right to be forgotten are also different. And in fact, if personal information uploaded in China is spread to overseas online platforms, it will be very difficult to force overseas network service providers to delete it. The main reason is the lack of legal jurisdiction. Unless the relevant laws and regulations of the local country stipulate that the relevant information can be deleted in this case, the laws and regulations of China cannot govern the behavior of other countries. However, given that some overseas countries are more relaxed about the dissemination of online information, in practice, the "right to be forgotten" is difficult to enforce.

3.1.2 Unequal protection in different jurisdictions

In 1968, when the United Nations celebrated the 20th anniversary of the Universal Declaration of Human Rights, the issue of protecting citizens' data privacy has been raised, and it has received the attention of developed countries in information technology. It is worth noting that the Universal Declaration of Human Rights only provides a template for the formulation of national constitutions.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

The rights referred to the UN document are not necessarily legal rights in any country, so some countries have not written the protection of personal information into the law[44]. However, in 1980, the Organization for Economic Co-operation and Development (OECD) formulated the Guidelines for Privacy Protection and Cross-Border Flows of Personal Data, which became the first important international

43 Danna Hong, The legitimacy of the right to be forgotten in the era of big data, Journal of South China University of Technology (Social Science Edition), Vol. 23 No.1 , January,2021.

44 Perry, Michael J . The Idea of Human Rights: Four Inquiries

regulation on personal data protection. On December 14, 1990, the General Assembly of the United Nations adopted the Guidelines on Computer Processing of Personal Data Documents. Under the guidance of these rules, most countries have established their own personal data protection systems. As an important part of personal information protection, the protection of the right to be forgotten has a certain legal basis in the entire international and regional development.

3.2 Practical challenges

The Google vs. Spain case reveals how personal data that was deleted by an original publisher may be a challenge of being removed by a search engine on the internet such as Google or *vice versa*. In addition, a case study from Japan enforcing a right to be forgotten may face difficulties in determination of period of time especially when the personal data in question has been published for a long period of time and may be “no longer” needed to be processed. Lastly, legal development carried out by the EU reveals how sufficient “legal text” is necessary for adequate protection.

3.2.1 Personal data electronically published by a search engine on the internet

In 2014, the Court of Justice of the European Union established the concept of the right to be forgotten in the Google-Gonzalez case. In this case, the Court of Justice of the European Union held that Google, as the data controller, is responsible for the information on web pages with personal data published by third parties that it processes and is obliged to delete it. Although the judge's final decision in the Google Spain case was that the document related to the applicant must not appear in the search engine's search list, the document itself (the Spanish newspaper article) was still publicly accessible. Of course, there is no way to search for the public documents

by searching the names of the information subjects, which reduces the impact of the disclosure of these documents to a certain extent. In this sense, the information related to the information subject is not really forgotten, but deleted from the "positive memory" of the Internet[45].

The judgment in the Gonzalez case reflects two points: on the one hand, it represents the restrictive effect of the EU Data Protection Directive (95/46/EC)[46] on network service operators, and it is clear that search engines are responsible for "inappropriate, irrelevant, Obsolete information". On the other hand, the EU recognized for the first time that information subjects enjoy the right to be "forgotten", and the expanded interpretation of the "EU 95 Directive" opened the door to a "new world" for the right to be forgotten[47],1 triggering strong repercussions in the international community.

After the "Gonzalez case" judgment was published, when data subjects in the EU searched for their names with Google, as long as there were links to personal-related information in the search results, the data subjects had the right to ask Google to delete them. All are subject to the right to be forgotten unless there are legitimate reasons for immunity. This also brings two problems. Firstly, all Google can do is enter Gonzalez's name in a search without a link to the original information, but Gonzalez's original personal information will not be completely wiped from the online world[48], the reasons include three aspects: First, even if users enjoy the

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

---

[45] Chris Jay Hoofnagle et al., The European Union General Data Protection Regulation: What It Is and What It Means, 28 Info. & Comm. Tech. L. 65, 90 (2019).

[46] Article 12 of the EU Data Protection Directive (95/46/EC) of 1995 ("EU 95 Directive"), Article 12(b) provides that the data subject has the right to rectify, delete or block the processing of the data when it is incomplete or inaccurate.

[47] Ioana Stupariu, "Defining the Right to be Forgotten. A Comparative Analysis between the EU and the US", LL.M. Short Thesis, Central European University, 2015, p.1.

[48] "Google Must Delete Search Results on Request, Rules EU Court", Rich Trenholm, CNET, last modified December 20，2017. https://www.cnet.com/ news/google-must-delete-search-results-rules-european-court/.

protection of the right to be forgotten, they do not necessarily require to delete or forget their personal information, but to make the information no longer easily obtained by others[49].

Secondly, even if Google removes the link, the original information is still available in the server cache backup. Strictly speaking, it is difficult for Google to guarantee a complete disconnection between the data publisher and the data subject. Third, the judgment requires Google to delete only the results of the European Google search engine[50], It is difficult to completely erase reports and information that have been posted on social media. Secondly, search engine companies such as Google have too much responsibility for censorship. The subjects involved in the right to be forgotten are: the data subject Gonzalez, La Herald, Google Spain, users of Google, the Spanish Data Protection Authority, the Spanish High Court and the Court of Justice of the European Union. Among these subjects, it should have been more effective for the Herald to delete or hide personal information, which could better prevent the occurrence of the "Streisand Effect[51]". But in reality, the "Pioneer" is only the result of being notified that the link has been deleted, and all obligations are basically borne by the Google search engine.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.2.2 Determination on the period of time

On February 28, 2016, it was reported that a Japanese court had acknowledged the "right to be forgotten", asking Google to delete old news about a man who was

[49] "The Right to Be Forgotten", Peter Fleischer, Seen from Spain, last modified December 18, 2017, http://peterfleischer.blogspot.co.uk/2012/01/right-to-be-forgotten-or-how-to-edit.htm

[50] "Google Keeps Its Limitations on "Right to Be Forgotten" Requests", Vlad Tiganasu, Articles Informer, last modified December 18, 2017. https://articles.informer.com/google-keeps-its-limitations-on-right-to-be-forgotten- requests.html.

[51] The Streisand effect is a phenomenon that occurs when an attempt to hide, remove, or censor information has the unintended consequence of increasing awareness of that information, often via the Internetx. https://en.wikipedia.org/wiki/Streisand_effect

arrested three years earlier. The man claimed personal rights were violated because just typing his name and address into a Google search engine brought up news stories from more than three years ago. He was previously convicted of violating anti-child prostitution and pornography laws and fined 500,000 yen. In June last year, the Saitama Prefecture District Court had ordered Google to delete search results for the man, saying his right to restoration had been violated. Google objected to this. After reviewing the case, the court made the same decision[52]. Saitama prefectural judge Hisaki Kobayashi said that, depending on the nature of the crime, the right to be forgotten should be recognized over time. “Criminals exposed by media coverage of their arrest have the right to have their privacy respected and their restoration unimpeded.

In modern society, once information is published on the Internet, it is difficult to live a peaceful life, which This should be considered when deciding whether information should be deleted." The Saitama Prefectural Court in Japan upheld the plaintiff's request and ordered Google to delete the search result link. After that, Google asked to review the case, but the court still upheld the original judgment. The plaintiff's lawyer believes that the previous similar cases all invoked the right to privacy.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

In fact, the case in Japan is very similar to the "Gonzalez case" in Spain. She also argued that the European Supreme Court ruled that Google should delete negative information that was no longer relevant in the past, and that Japan could refer to the European ruling on the "right to be forgotten" in the Gonzalez case and use the logic and language of the ruling[53]. It can be seen that the EU's right to be forgotten

---

[52] Available at: http://japan.people.com.cn/n1/2016/0229/c35467-28156803.html

[53] "To Protect "Right to Be Forgotten" Japanese Court Asks Google to Delete Old News," Phoenix.com, http://news.ifeng.com/a/20160229/47621921_0.shtml, last accessed: June 10, 2022.

indirectly affects Japan's judicial practice, but the EU Court of Justice protects the right to be forgotten, citing Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the EU Charter on Fundamental Rights. Personal Privacy and Information Protection Regulations. Japan's protection of online privacy is based on Japan's Personal Information Protection Law. Therefore, the EU and Japan share the same basic concept of protecting citizens' right to be forgotten, but Japan did not choose to directly transplant the concept of the EU, but explained it through its own laws.

The retention of data may cause damage to the data subject at some time in the future. In order to prevent outdated data from causing adverse consequences, the data subject can act in advance to ensure that the data processor deletes the data that no longer needs to be retained through the governance system of the network platform. If the user sets an expiry date - "expiration date" when disclosing the data, to ensure that the data will be automatically deleted when it expires[54]. However, this approach has shortcomings in practice, including the following three aspects: First, it is difficult for users to make a thoughtful choice on the length of the "expiration date", and the "expiration date" Digitizing Shadows" doesn't do anything. Secondly, in the era of big data, how to accurately grasp what kind of data is "outdated" lacks a clear measurement standard. Finally, it is not only outdated data that can cause harm to data subjects, but some data can also cause harm to data subjects in the process of lawful processing, which cannot be solved by relying solely on the right to forget, which can only delete outdated data.

[54] Bert-JaapKoops, "Forgetting Footprints, Shunning Shadows.A Critical Analysisi of "the Right to be Forgotten" in Big Data Practice", 8 SCRIPTed (2011) 229, p.241-242.

3.2.3 Insufficient legal text

The General Data Protection Regulation (GDPR), finally passed in 2016, enshrined the right to be forgotten in the 28 EU member states identified as statutory rights. Article 17, paragraph 1 stipulates: "The data subject has the right to request the data controller to delete the personal data information of the data subject, and the controller shall not delay deliberately. Moreover, the data controller is obliged to delete the personal data information". Compared with the provisions of Article 17(1) of the General Data Protection Regulation (Draft) 2012, the provision "especially when the data subject of the personal data that has been disclosed is a minor" has been deleted, which the reason for the deletion is to avoid misleading people into thinking that the right is limited for adults, and to make the right equally applicable to all subjects. However, this does not mean that the Regulations ignore the protection of minors' right to be forgotten.

Under Article 17 of GDPR, the “right to be forgotten” means:

> *Individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’.*[55]

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Paragraph 1 stipulates that the data subject has the right to request the data controller to delete his personal data, and the data controller is obliged to delete the personal data information in the following cases without undue delay: It stipulates 6 situations in which data can be deleted: First, the personal data information collected is no longer necessary for the purposes for which the data was collected and processed;

[55]From the website:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

second, the expiry of the data storage period and the act of collecting the data no longer have legal justification; third, the revocation of the data subject Consent regarding data processing or refusal by the data subject to process personal data; fourth, acts of unlawful processing of personal data; Fifth, the data controller has to delete personal information according to the EU law or member state law's legal obligations to the data controller; sixth, the personal information data collected in information society services (e-commerce). In addition, the memorandum of the 2012 GDPR legislative proposal mentions that the data controller is obliged to notify third-party websites that are processing the data, that the data subject requests the removal of links, original data and replicated data related to personal information. The 2013 legislative proposal made changes. First, the "obligation to notify" of deleting information is changed to "the responsibility to delete the information published by a third party". Second, it is clarified that in special circumstances, the data controller is obliged to notify the data subject of the third party's actions and make compensation to the data subject. Third, it further proposes that the final judgments and rulings of courts and public management agencies can be the reasons for deleting data, which increases the possibility of implementation of the right to be forgotten[56]. These obligations increase the responsibility of the data controller, and ensure that the data can be deleted and forgotten practicably[57].

However, GDPR also has drawbacks. Firstly, the GDPR does not clearly distinguish between "right to erasure" and "right to be forgotten". The title of Article 17 of GDPR is "right to erasure (right to be forgotten)". As for the relationship between the right to erasure and the right to be forgotten, there is no more clearly defined. Secondly, GDPR regulates both personal data that has been disclosed and personal data that has

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[56] Xia Yan: "The "Right to Be Forgotten" Debate: An Investigation Based on the Reform of EU Personal Data Protection Legislation," Journal of Beijing Institute of Technology (Social Science Edition), 2015, No. 2, p. 130.

[57] Serge Gutwirth, Ronald Leenes, Paul de Hert, Reforming European Data Protection Law (Berlin:Springer Netherlands Press, 2015), pp.206-208.

not been disclosed. Article 17(2) of the General Data Protection Regulation sets out the data controller's obligation to delete, notify and take reasonable measures when data has been made public. Article 17(1), on the other hand, covers the processing of unpublished data. Thirdly, the GDPR does not distinguish between lawful and unlawful processing of the data in the original processing. It is worth noting that in the fourth and fifth cases, the deletion of the data can be requested because the processing of the data is unlawful in the first place.

In the other four cases, the data processing is legal at the beginning, and then the legitimate basis for processing the data is lost due to the data subject's withdrawal of consent, refusal to continue processing, etc. Fourth, the right to be forgotten does not impose a heavy burden on the data subject. The data subject does not need to provide a basis for data deletion, nor to provide evidence to prove that the website publishes information that is illegal or defamatory.

In terms of legal practices, China’s attitude towards the right to be forgotten appears to be more cautious. At present, there is no right to be forgotten in Chinese legislation. However, the provisions on the right to erasure can also reserve a certain space for the generation of the right to be forgotten. Article 47 of the Personal Information Protection Law of China, to some extent, draws on the relevant provisions of GDPR Article 17 on the right to be forgotten. However, in terms of the reasons for deletion, it still has defects, and the listed circumstances are too narrow. For example, Article 47 states that if an individual withdraws consent, the personal information processor should delete his or her personal information, but under section 17 of the GDPR, the information can only be deleted if the individual withdraws his or her consent for a valid reason.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Tab. Comparison table of GDPR and PIPL of the right to be forgotten in the EU and China

	GDPR (article 17)	Personal Information Protection Law of China [PIPL(Article 47)]
Exercising situation	a.The personal data is no longer necessary for the purpose for which it was collected or processed. b. the data subject withdraws consent and there is no other lawful basis; c. The data subject exercises the right of objection; d. There is already illegal processing of personal data e. Personal data needs to be erased in order to comply with the legal liability set by EU or Member State law for the controller	a.The purpose of processing has been achieved, cannot be achieved, or is no longer necessary to achieve the purpose of processing; b. Withdrawal of consent by the individual; c.The person who processes personal information violates laws, administrative regulations or agreements d.The personal information processor ceases to provide the product or service, Or the storage period has expired e. Other circumstances prescribed by laws and administrative regulations
Restrictions on the right to erasure	a. To exercise the rights to freedom of expression and freedom of information; b. Based on public interest, statutory duty and public health c. To bring, enforce, or defend a legal claim	a.The preservation period prescribed by laws and administrative regulations has not expired. b.Deleting personal information is technically difficult to achieve

Chulalongkorn University

Highlight the features	Focus on legal interest balance	The right to erasure overrides the right to be forgotten model

Certain communication behaviors or more explicit information flow in the public domain are more emphasized in China, or that the reasonable flow of information entrusts human rights, and China understands the reasonable flow of information and the expectations of individuals and communities as the embodiment of existing laws and regulations. For the legislation itself, it only protects the flow of information in line with the public interest and individual expectations, rather than the social atmosphere of complete freedom of speech. China's legal practice on this issue shows a different way of thinking from that of Europe.

Oblivion vs erasure; put beyond use and deletion

Across the literature and political discussions, there is a lack of uniformity in defining the overall concept of "deletion" of personal data. While some use the terms "the right of "the right to "the right to be forgotten," or the "right to erasure" as synonyms, or at least sometimes interchangeably[58], Some people distinguish between legal principles and legal scope. Based on the above analysis of Article 17 GDPR[59], the

[58] Cf. e.g. Napoleon Xanthoulis, Conceptualizing a Right to Oblivion in the Digital World: A human rights-based approach, research essay at University College London, May 2012, pp. 16 et seq., who argues that the right to be forgotten of the Draft Data Protection Regulation dated 25.1.2012, COM(2012) 11 final constitutes. GiusellaFinocchiaro/Annarita Ricci, Quality of Information, the Right to Oblivion and Digital Reputation, in: B. Custers et. al. (eds.), Discrimination and Privacy in the Information Society, Berlin 2013, pp. 289-299; Cédric Burton/Christopher Kuner/Anna Pateraki, The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report, Bloomberg Privacy and Security Law Report, January 21, 2013 state that the right to be forgotten is viewed by the Albrecht Report (cf. chapter B.III.2) as an extension of the right to erasure.

[59] Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

name of the "right to be forgotten" has undergone changes, but the content of the power has not changed. According to the GDPR, the EU judges that the "right to be erasure" is essentially part of the "right to forgotten." But in the digital field, oblivion and erasure are similar but different. For example, in the implementation of the Google case, in the version of Google in countries outside the EU, the information and links that were sued for deletion still exist. At the same time, for search engine companies, the burden of censorship or subsequent erasure adds a huge financial burden. In addition, since the deletion and identification of the relevance of links require a professional team to carry out, this will bring about a lag in the implementation time, which is often one of the reasons for the complaints of information subjects. In addition, in terms of practical effect, since the original linked article and the operation of the search engine are separate and the original linked article and blog users can often be exempt from the principle of freedom of news reporting, it should be added to the search engine at this time. What is the significance of a company's erasure obligation? If you don't want to use it and want to delete it, the Internet only has memory for certain types of information, or for specific websites and regions. For example, following the Google Spain case, citizens of EU member states learned to use Google sites in the United States to search for material not accessible from their own Google sites[60]. Once the data is published to the network, it is almost impossible to permanently remove it from search. In practice, especially in the digital era, oblivion, erasure, and deletion are different.

3.2.4 The complexity of social media users

One of the characteristics of social media is the large number of people, and the second is spontaneous transmission. With the passage of time and the development of

[60]Zhifeng Zheng: "Research on the Right to be Forgotten in the Network Society", in "Law and Business Research", No. 6, 2015.

the Internet, the user groups of social media show complex and diverse trends, that is, user gender, user age group, geographical location, education level, occupational background, religious belief, social roles, etc. are not the same. , which brings difficulties to the exercise of the right to be forgotten. Example analysis: A minor and a public figure both request the deletion of their outdated information, how do we determine whether they can exercise the right to be forgotten; a criminal requests the deletion of his past criminal records, and a terrorist records of terrorist activities, whether they have this right. It can be said that the right to be forgotten is reasonable in theory, but it also ignores the unknowingness brought by the huge user group to some extent.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

CHAPTER 4 The protection of the right to be forgotten

China has reached the world's leading level in the Internet field, and has surpassed many western developed countries in the development of the platform economy and sharing economy, but the legislation on personal information protection is out of touch with economic development. Whether China has created the right to be forgotten can be analyzed from the perspective of whether the current laws can comprehensively protect citizens' personal information. The creation of the right to be forgotten would be unnecessary if China's existing legal provisions were sufficient to ensure the security of citizens' personal information, but it is not. In China's current legal system, there is no "right to be forgotten" system, and "erasure" is used as a protection of rights and interests. Until November 2021, the personal information protection law has come into effect, but it only stipulates the right to delete, and does not officially raise the right to be forgotten to a formal right. In addition, by comparing with the legislation of GDPR and the judicial practice of Japan, we can refer to the experience and guide the way forward for the establishment and implementation of the right to be forgotten in China.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

4.1 Legislative basis for the protection of the right to be forgotten in China

4.1.1 Civil Law

Article 1195 of Title VII Tort Liability of the Civil Code, which will be implemented in 2021, stipulates the tort liability of Internet users and network service operators, and protects network service operators through the "Safe Harbor Treaty"; as can be seen from the provisions of the Civil Code, after the occurrence of network infringement, many people can be held liable, including network users and network

users' providers, etc. However, there are no provisions on the specific legal liability to be borne, so we need to refer to the provisions of other laws, The liability for network infringement generally includes civil liability, administrative and criminal liability, but the negative impact on personal interests caused by the disclosure of personal information due to network infringement has not been eliminated. Due to the characteristics of fast dissemination and wide dissemination of data, it is difficult to completely eliminate the impact in lawsuits violating the "right to be forgotten". Therefore, the tort liability method that eliminates the impact is not very enforceable in these cases, because once the data is spread out, one data controller will be transformed into an infinite number of data controllers, and it is difficult to determine and control.

Articles 1225[61] and 1226[62] stipulate the responsibilities of medical institutions and medical personnel for the protection of patients' personal data, but the law only stipulates the protection of special personal information, and does not stipulate the protection of general personal information. Therefore, for the special group of patients, medical staff who disclose the personal privacy of patients need to bear the tort liability. The patient can negotiate with the hospital about compensation. If the negotiation fails, they can collect relevant evidence and sue the court for medical tort. However, even if property compensation is obtained, traces of the leaked personal information cannot be removed online and restored to its original state, which may cause more than reputation damage to the person whose information was leaked. It

[61] "Medical institutions and their medical staff shall fill in and properly keep hospital records, doctor's orders, inspection reports, operation and anesthesia records, pathological data, nursing records and other medical records in accordance with regulations. If a patient requests to consult or copy the medical records specified in the preceding paragraph, the medical institution shall provide it in a timely manner."

[62] "Medical institutions and their medical staff shall keep patients' privacy and personal information confidential. Those who disclose patients' privacy and personal information, or disclose their medical records without their consent, shall bear tort liability."

can be seen that it is not enough to only stipulate the liability for online infringement, and it is necessary to establish the right to be forgotten in legislation. The right to be forgotten can better protect privacy. And the regulations pointed out that medical institutions shall not sell the personal information of citizens obtained in the process of providing services to businesses, but the relevant administrative regulations only stipulate the confidentiality of medical records, not the confidentiality of names and telephone numbers. For illegal acts, it still needs to be discussed.

Article 1037, paragraph 2, of the Civil Code, which came into effect in 2021, stipulates: "If a natural person discovers that the information processor violates the provisions of laws, administrative regulations, or the agreement between the two parties to process his personal information, he has the right to request the information processor to delete it in time."[63] The data controller shall delete the information and data in its possession. But it's worth noting here that it's not enough to simply delete the information it controls. In the context of today's big data, information is shared between different platforms and subjects. This is the main reason why information spreads so fast. It may not take an hour for a photo to be uploaded to the entire network. Therefore, if you really want the data controller to completely control the information, in addition to letting itself delete the relevant data, other platforms and controllers that obtain information from the data controller also need to delete such information.

Article 1195 of the Civil Code stipulates that the infringed has the right to require the Internet service provider to take necessary measures such as deletion, shielding and disconnection, which is enough to ensure that the infringing information will be deleted on the network. This involves the information subject's right of reputation, privacy and other personal rights or personal dignity is violated, the relevant

[63] Article 1037, paragraph 2, Civil Code of the People's Republic of China.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

information processing obligation to delete. Some people argue that the current provisions on the right to delete are based on the premise that the network service providers take such measures as deleting and disconnecting if there is an illegal and infringing act, and do not recognize the information subject's right to apply for deleting information under any circumstances, so it is essentially different from the right to be forgotten[64].

4.1.2 Economic law

The "Consumer Rights Protection Law of the People's Republic of China" specifies the basic conditions for the collection and use of consumer information in Articles 14[65] and 29[66]. Article 50[67] further stipulates the legal consequences for breaching the above obligations. With the rapid development of network technology and the fierce competition of network platforms, the security of consumers' personal information is becoming more and more serious. For example, many apps force users to submit personal information to participate in data processing activities, precise positioning services that users cannot refuse, and inability to close advertising pop-ups. In terms of sharing personal information with third-party software development tools, inducing users to click to download or directly enter the corresponding service to obtain mobile

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[64] Weili Duan: "Conceptual Analysis of the Right to Be Forgotten: Using the Right Theory of Analyzing Jurisprudence as a Tool", in Journal of Henan University (Social Science Edition), No. 5, 2018.

[65] Article 14 of the Law of the People's Republic of China on the Protection of the Rights and Interests of Consumers: Consumers have the right to respect their personal dignity, national customs and habits, and the right to protect their personal information in accordance with the law when purchasing, using goods and receiving services.

[66] Article 29: When operators collect and use consumers' personal information, they shall follow the principles of legality, legitimacy and necessity, expressly state the purpose, method and scope of the collection and use of information, and obtain the consent of consumers. When operators collect and use consumers' personal information, they shall disclose their collection and use rules, and shall not collect and use information in violation of laws, regulations and agreements between both parties.

[67] Article 50: If an operator infringes on the personal dignity of consumers, infringes on consumers' personal freedom, or infringes on consumers' rights to be protected in accordance with the law, they shall stop the infringement, restore their reputation, eliminate the impact, make an apology, and compensate for losses.

phone user information, etc. Therefore, for the infringement of consumers' personal information rights and interests described in Article 50, the infringement shall be stopped, the reputation shall be restored, the impact shall be eliminated, the apology shall be made and the loss shall be compensated. These punishments, for consumers whose personal information has been leaked, cannot really erase their personal information from the big data. And they don't want to be others know information may have been other websites or software company analysis and spread out, consumers' rights and interests protection law has no specific punishment standard, has certain difficulty in the actual implementation, not fully protect citizens' personal information from the violation or reduced, and the rules more general, At this time, if there are laws on the right to be forgotten, individual privacy can be better protected from the perspective of legislation, thus guaranteeing human rights and personal dignity.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

4.1.3 Cybersecurity Law

The Cybersecurity Law of China has made comprehensive and systematic provisions on the personal information protection system. For example, Article 40 of the Cybersecurity Law of China stipulates that network operators shall keep the user information they collect strictly confidential, and establish and improve user information protection systems. Article 41 stipulates: "In collecting and using personal information, network operators shall follow the principles of legality, legitimacy, and necessity, disclose the rules for collection and use, express the purpose, method and scope of the collection and use of information, and obtain the consent of the person being collected. " Then, if the information collected and used by the network operator is outdated, irrelevant or no longer relevant, there is no point in continuing to store that information, which is consistent with the basic idea of the right to be forgotten.

Article 43 stipulates: "Individuals who find that network service providers violate the provisions of laws, administrative regulations or both parties to collect and use personal information have the right to request deletion of their personal information, and have the right to request corrections during network operations if they find errors. The service provider should take steps to remove or correct it." The scope of deletion right in this provision is very limited, and there is no detailed provision on the scope of information that can be required to be deleted and the identity of the subject, so there is room for further refinement. In the provisions of network infringement dispute cases, the exception provision that network users and network service providers can claim compensation for damages caused by disclosing personal information of natural persons on the Internet is actually similar to the exception applicable to the right to be forgotten in the European Union, but it is still doubtful whether the information obtained through legal channels can be used again.

4.1.4 Personal Information Protection Law

The Personal Information Protection Law came into effect on November 1, 2021, and comprehensively regulates the collection, use, provision and deletion of personal information in the form of special legislation. Throughout the evolution of the Personal Information Protection Law, the relationship between the right to erasure and the right to be forgotten has always received much attention and discussion. The right to be forgotten is a right design granted by law to information subjects to deal with the loss of control of information. Information subjects can use information to clear and recycle information when the legally disclosed personal information is outdated, irrelevant, inaccurate and has a negative impact on individuals.

Article 47 of the Personal Information Protection Law establishes the right to delete personal information, allowing information subjects to request deletion of personal information under specific circumstances, and requiring personal information processors to fulfill their deletion obligations. In the third paragraph of Article 47, the exercise condition of "individual withdrawal of consent" is clarified, and individuals can achieve the purpose of protecting their "right to erasure" through this law. To protect the "right to be forgotten", it is necessary to make relatively clear provisions on the other four paragraphs of Article 47, such as the first paragraph: "The purpose of processing has been achieved, cannot be achieved or is no longer necessary to achieve the purpose of processing". Therefore, the protection of the "right to be forgotten" in the Personal Information Protection Law can be improved through legal interpretation.

Throughout the evolution of the Personal Information Protection Law, the relationship between the right to erasure and the right to be forgotten has always received much attention and discussion. The right to be forgotten is a right design granted by law to

information subjects to deal with the loss of control of information. Information subjects can use information to clear and recycle information when the legally disclosed personal information is outdated, irrelevant, inaccurate and has a negative impact on individuals.

4.2 China's first "right to be forgotten" case -Ren Jiayu V. Baidu

In December 2015, the Haidian District Court of Beijing concluded the case of Ren X suing Beijing Baidu Netcom Technology Co., Ltd. for infringing on his right of reputation, name and general personality. After the plaintiff Ren entered his name in the Baidu search engine, before clicking the search button, the "Related Search" list that appeared at the bottom of the search bar displayed key words such as "Ren from Dow Education" and "Ren from International Super Education". word. Ren believes that Dow Education has a bad reputation in the industry, and in 2014 she had terminated the labor relationship with Wuxi Dow Biotechnology Co., Ltd., and Baidu publicly associated her name with Dow Education, which would mislead the public into thinking that she Still working at Dow Education. Ren worried that the negative information of Dow's education would affect her work, future employment and daily life. After repeatedly claiming to Baidu to delete the "related search" to no avail, Ren sued the court, claiming that Baidu violated his right to reputation, name and general personality (right to be forgotten). In this regard, the Haidian District Court made a judgment and ruled to reject all the plaintiff's claims. Ren refused to accept the judgment and appealed to the Beijing No. 1 Intermediate People's Court. The court of second instance dismissed the appeal and upheld the original judgment.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

The judge in this case made a ruling to reject the plaintiff's claim, including three reasons: First, the related words appearing in the "Related Search" column were not

manually set by Baidu, but were collected by high-frequency words over a period of time. The system automatically generates. This automatically generated data does not have any intention of insulting or defaming the plaintiff, so Baidu did not infringe on the plaintiff's right of reputation[68]. Second, Ren's name is a combination of genetic characters in the search engine, and there is no reference to the meaning of the name. Therefore, Baidu's technology neutrality does not involve interference, misappropriation, or impersonation of others' names, nor does it infringe upon the plaintiff's right to name. Third, there is no right type of the right to be forgotten in the existing legal provisions in my country. Individuals have no right to delete personal information controlled by others, and can only classify the right to be forgotten into the abstract protection of general personality rights. However, Ren's claim that "forgotten" information does not have the dual importance of "legitimation of interests" and "necessity for protection", so the court does not support it.

In terms of argumentation, the judge advocated that the public's right to know takes precedence over the plaintiff's right to be forgotten. He believed that there was an objective necessity for the public to know the plaintiff's work experience, and the plaintiff's claim to delete relevant information was not justifiable and necessary. Since Ren Jiayu still works in the education industry, the information of past employment is closely related to his current occupation, which can become an important personal credit for relevant groups to refer to, and it is also an important manifestation of teachers' honesty and credibility. The reservation of this information can not only ensure the freedom of public speech, but also ensure the normal play of the supervision role of public opinion. Some scholars argue that the "right to be

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[68] Changyi Chen: "Thoughts and Protection Paths of "Right to Be Forgotten" Cases under the Existing Legal System: Starting from the First Case of "Right to Be Forgotten" in my country", Application of Law, No. 2, 2017, Nos. 41-42 Page.

forgotten" is the regulation of information that does not involve public interests[69]. However, how to divide the boundary between public welfare and non-public welfare information has become a new difficult problem. As in the case of "Google Spain", after Google responded to some netizens' claim of "right to be forgotten", many news reports published by news media could not be retrieved by netizens. As a result of the existential crisis, these news media turned to sue Google for violating its freedom of the press, putting Google in a dilemma and later restoring some "forgotten" links. It can be seen that even the exercise of the "right to be forgotten" system in the EU has not found a more effective method to balance the relationship between search engine service providers, original information publishers and information subjects. Removing links containing personal names and related deeds reports will make it unsustainable for some news media, and the news they have worked so hard to publish will be easily removed due to the requests of some information publics, cutting off their access to traffic sources. At the same time, the quality of the information released by the news media will also decline. Because the news media are afraid of the risk of “shielding” relevant personal information after reporting, they try to erase specific personal identities that may be involved in the news. When reading news, the information counterpart of the news will be lost, which greatly reduces the credibility and clarity of the news.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

But some scholars pointed out that the judge denied the plaintiff's right to be forgotten because of the priority of the public's right to know. The theoretical basis is not sufficient, and the legal interpretation is too conservative[70]. There are two main reasons: First, the public's right to know is not necessarily superior to the right to be

[69] Rongzhi Wen and Longjie Zhou: "The Creation of the Right to Be Forgotten in European Law and Its Enlightenment to my country", Journal of Changchun University of Science and Technology (Social Science Edition), No. 3, 2019, p. 36.

[70] Weili Duan: "On the Judicial Relief of the Right to Be Forgotten: Taking the Judgment of the First Domestic "Right to Be Forgotten" as an entry point", Application of Law, No. 16, 2017, p. 58.

forgotten. In the Gonzalez case, the European Court of Justice asserted that the fundamental rights in the EU Charter of Fundamental Rights take precedence over the public's right to know, that is, privacy and personal data protection take precedence over the public's right to know. In fact, the European Court of Justice also protects the right to be forgotten through the protection of private life and personal data[71]. Second, safeguarding the public's right to know does not conflict with Baidu's deletion of related words in "related searches". This case is different from the plaintiff's claim in the Gonzalez case. Ren did not ask the search engine to delete the original link of the news report, nor did he ask the search engine to disconnect the relevant link in the search results, but only asked the search engine to delete the original link of the news report. Related words in Related Searches. Deleting related words in "Related Searches" will not affect users' retrieval through web pages, nor will it affect the ability of search engines to collect information, but the keywords in "Related Searches" will not include "Ren" and "Dow Education". "Together, this appeal is reasonable. Therefore, the plaintiff's right to be forgotten does not have a huge conflict with the public's right to know.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

[71] Hui Zhou: "Summary of the EU's "Right to Be Forgotten" First Case," Cyber Law Review, No. 2, 2015, p. 331.

4.3 Foreign Legislation and Judicial Practice

To recommend possible ways forward to develop the legal protection regime in China, this research explores and examines existence, evolution, and application of the right to be forgotten in the European Union. It is important to note that the term "forgotten" was not originally recognized by subsequently added to the protection regime.

4.3.1 GDPR legislative experience on protecting the "right to be forgotten"

4.3.1.1 Legislative history of the "right to be forgotten"

Before the era of big data fully arrived, the European Union had already started to draft data protection directives. In 1995, the "EU Data Protection Directive (95/46/EC)" (referred to as "EU 95 Directive") promulgated by the European Union already contained provisions on the concept of the "right to be forgotten". The purpose of this directive is to solve the problems exposed by the differences in the national laws on which data protection is based between member states[72], and to unify data protection legislation in the EU region. This was because Germany, France and the United Kingdom had a say in privacy protection at that time, but Greece and other countries had no policies or regulations on data protection at that time. Therefore, the Directive requires each member state to adopt domestic legislation that not only protects the fundamental right of individuals to process information under the right to privacy, but also ensures the lawful processing of personal data and the free flow of data[73]. The Directive came into effect in 1998 and further clarified the lawful use of personal data processing, judicial remedies, data transfer between countries, and data application monitoring and enforcement. The basis for the European Commission to

[72] Douwe Korff, "EC Study on Implementation of Data Protection Directive", 34 Comparative Summary of National Law (2002)1, p.47.

[73] Michael L. Rustad, Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow", 28 Harvard Journal of Law, Technology (2015) 349, p.359.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

formulate the "EU 95 Directive" in a unified manner mainly includes three aspects. First, the right to privacy in European Member States is based on human dignity and reflects the preservation of a person's likeness, name and reputation[74]. Second, the right to privacy originates from a concept in the German constitution—"information autonomy", which is defined as the right of individuals to control information about themselves[75]. This right not only reflects how the subject of the right presents personal information to third parties or the public, but also confirms that personal information is valuable property. Third, the "EU 95 Directive" states in the preface that the original intention of the European Commission's directives is the same as that of the Human Rights Convention, which is to protect basic human rights including the right to privacy. Therefore, all member states have the same goal of legislating on the processing of personal information, focusing on protecting the right to privacy on the basis of protecting basic human rights. For this reason, the legislative protection of each country will not reduce the protection, but will seek a higher standard of protection[76]. (e) Data collection is done to accomplish a task based on the public interest, or the authority of the data controller, third party, for the disclosure of personal information. (f) Data is collected to protect the legitimate interests of the data controller or third party that discloses personal information. However, when the rights of the data subject to be protected under Article 1 are based on fundamental human rights and freedoms, they are not limited by this right.

Article 7 of Directive 95 states that the processing of personal data is lawful and restricts the exercise of the rights of the data subject if the following six circumstances

[74] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty", 113 The Yale Law Journal (2004)1151, p.1161.

[75] Paul Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 American Journal of Comparative Law (1989)675, pp.686-687.

[76] Michael L. Rustad, Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow", 28 Harvard Journal of Law, Technology (2015) 349, p.360.

arise. (a) The data subject expressly consents. (b) if the data subject is a party to a contract or the data subject has previously joined the contract, the processing is for the performance of the contract. (c) The data processing is based on a legal obligation of the data controller. (d) Data collection is processing that is necessary to protect the vital interests of the data subject.

EU officials have been stressing that the right to be forgotten is not a new right. First, the use of the word "strengthening" by the Vice-President of the European Commission, Vivinie Redding[77], in her 2012 speech entitled "EU Data Reform: Making Europe a Maker of Modern Data Protection Standards in the Digital Age" She believes that the right to be forgotten already exists and needs to be strengthened rather than created[78]. Second, Koops sees the right to be forgotten as a legal right rather than an abstract value, noting that the right to be forgotten had a good start as early as in the 1995 Data Protection Directive[79]. In January 2012, the European Commission issued a legislative proposal for the General Data Protection Regulation (GDPR), which improved the original EU Data Protection Directive (95/46/EC) (referred to as the "95 Directive"), in the following areas: Breakthroughs have been made in the following aspects: First, it is determined that the "right to be forgotten" is the right of every Internet user to delete the information published by themselves[80]. Second, this regulation is specially formulated for the protection of user privacy rights to enhance the level of privacy protection for all citizens of the EU. Third, in the Google v. Gonzalez case in 2014, the European Court of Justice, in its decision basis,

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[77] V Reding, “The Upcoming Data Protection Reform for the European Union” 1 International Data Privacy Law (2011)3, p.4.

[78]Bert-Jaap Koops, Forgetting Footprints, Shunning Shadows: A Critical Analysis of the Right to Be Forgotten in Big Data Practice, 8 SCRIPTed (2011), p.232.

[79] Bert-Jaap Koops, Forgetting Footprints, Shunning Shadows: A Critical Analysis of the Right to Be Forgotten in Big Data Practice, 8 SCRIPTed (2011), p.230.

[80] Michael L. Rustad, Sanna Kulevska, “Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow”, 28 Harvard Journal of Law, Technology (2015) 349, pp.353-354.

based on Articles 12 and 14 of the EU95 Directive, raised the implied right to be forgotten, clarified that Google's responsibilities as a data producer[81].

4.3.1.2 Provision of "right to be forgotten"

Article 17 of the GDPR provides for the right to be forgotten, but it also provides for several situations that limit this right, such as for freedom of information or expression, for compliance with EU or member state laws, for the public interest or for the exercise of public powers entrusted to them When, in the public interest in the field of public health, for archival purposes in the public interest, for scientific or historical research purposes, or for statistical purposes, etc. Obviously, the EU recognizes the existence of public interests and implements the principle of public interest in the relevant provisions of GDPR, which coincides with the legislative spirit of China. In fact, it can be seen from the provisions of the GDPR on the right to be forgotten:

First, the six situations in which individuals exercise the right to be forgotten in the GDPR are not all new concepts. The limitation of purpose principle is similarly set out in Article 6 of Directive EU 95, and the "Data subject's right to object" and "Unlawful processing of personal data" can also be found in the framework of the Directive[82].

Second, the GDPR expressly withdraws consent has no effect on the processing of data prior to the withdrawal[83]. When an individual withdraws consent for data processing in Article 7 of EU95 Directive, it does not stipulate whether the data controller's past data processing behavior is valid or not, and the original consent

[81] Michael L. Rustad, Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow", 28 Harvard Journal of Law, Technology (2015) 349, p.360.

[82] Meg Leta Ambrose, Jef Ausloos, "The Right to Be Forgotten Across the Pond", 3 Journal of Information Policy, (2013)1, p.12.

[83] Ibid.

system fails to meet the stringent requirements of the Internet. The right to be forgotten in the GDPR fills the gaps in the consent system, Article 7(3) of the GDPR 2016 states: Data subjects have the right to withdraw their consent at any time without prejudice to the lawfulness of data processing based on prior withdrawal of consent. The European Commission seeks to create a balanced environment through the right to be forgotten, where individuals can permanently and effectively re-determine whether or not they can withdraw their consent.

Third, the GDPR uses the data controller as an intermediary that can link data subjects with third parties who have released information about the data subjects[84]. On the one hand, however, the GDPR applies only a vague rationale criterion that imposes an obligation on data controllers to require third parties to remove them.

4.3.2 The judicial practice of protecting the "right to be forgotten" in Japan

The internationalization of the right to be forgotten has not been smooth sailing. Some countries recognize the importance of the protection of the right to be forgotten, but they do not fully agree with the EU's solution and have no plans to directly transplant it. Japan has been long known for its tradition of reception from foreign legal systems: starting with the reception during the Meiji Restoration, where the goal was to gain independence from European invaders and unequal treaties by creating a modern legal system. To this day, comparative law plays an important role both in the creation of new rules and the interpretation of existing rules, going back to legal transplants. For example, Japan has made an attempt to localize the protection of the right to be forgotten in judicial precedents, and its ruling is in line with the concept of the right to be forgotten. However, this right was not explicitly stated, and they took a wait-and-see attitude and laid the foundation for the future standing of similar rights

[84] Michael L. Rustad, Sanna Kulevska, "Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow", 28 Harvard Journal of Law, Technology (2015) 349, p.370.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

in the form of judicial decisions.

It must be noted that Japanese law does not clearly stipulate the "right to be forgotten", the Japanese courts consider the balance of interests and the protection of honor and privacy in the case of the "right to be forgotten". Japanese cases are based on civil law, the Japanese liability regime under the 'Provider Liability Limitation Act' only covered intermediaries such as content providers, and not search engine providers[85]. The nature of the results of a Google search is an automatic output created by an algorithm that gives each person's name as an input to the search term, and the fact that the results link to more content, is considered to be different from other Internet service providers, and the Tokyo Court, under limited conditions, in the judgment The exercise of the right to erasure is allowed in the case, and the case discusses the right to know and the right to be forgotten. Although the case in Japan is a civil dispute, unlike the Google Spain case in the EU based on data protection, the reasoning of the Japanese courts may in some ways be inspired by Google Spain, with an explicit reference to the case and the right to be forgotten, in view of different views on the right to be forgotten, the key lies in the protection and jurisdiction of territorial areas in different places. For Japan, space is needed for social and cultural differences. The settlement of cases is not only at the level of substantive law, but also in the judicial practice with legal conflicts.

4.4 Comparison table of the Right to be Forgotten, existing restrictions and protection

[85] Frederike Zufall,Challenging the EU's 'Right to Be Forgotten'? Society's 'Right to Know' in Japan, EDPL 1, 2019.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Issue	Desired protection	Existing limitation
Data subject	Require the obligated subject to delete online information, give the subject the right to choose, and choose the applicable obligated subject; Determining the data subject's right to be forgotten	The obligated subject cannot completely eliminate the existence of information on the Internet; The data period is uncertain.
Protection scope	Legally circulated network information	It is difficult to define whether the transmission method is legal or not; Identifying information relevant to a particular individual; Different jurisdictions protect unequally; What is "unnecessary, irrelevant and outdated" personal information.
Protection exemption	Establish the boundaries of the right to be forgotten	reedom of information or expression, for compliance with EU or member state laws, for the public interest or for the exercise of public powers; Data subject's right to object" and "Unlawful processing of personal data
Right exercising	Article 17 of the GDPR provides for the right to be forgotten	The GDPR does not make a clear distinction between the right to be forgotten and the right to be deleted; China does not explicitly stipulate the right to be forgotten in the whole law system.
Data controller's challenges	There is a lawful basis for the processing of the data; The characteristics of network information flow increase the difficulty of realizing "right to be forgotten"	Illegal processing that does not distinguish between legitimate data in the original processing; The

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

		GDPR does not provide a reference template for how data controls determine when data is no longer relevant, the authenticity of public information, and which data deletion requests qualify for exemptions.

Data Subject: Under the background of the era of big data, operators of various websites, online applications, mobile applications and self-media continue to emerge. They use the permanent memory of the Internet and the power of science and technology to integrate fragmented personal information, Therefore, data controllers should be clearly defined and required to fulfill the obligation of being forgotten. In today's world, the specific provisions of the subject of the right to be forgotten obligation are different, but the scope is basically the same. For example, the EU defines the subject of the right to be forgotten as a data controller, including an individual or a person who jointly decides the purpose and means of processing personal data with others. It usually refers to a public or private institution, but it can also be an individual. And protection is not equal in different judicial districts. The concept of "data controller" was widely used when the "EU Directive 95" was adopted in the 1990s[86], However, with the changes of the times, in the current mixed information processing process, it is more difficult than before to judge which "data controllers" the purpose and means of data processing come from. It can be seen that it is necessary for countries to further define the data subjects' right to be forgotten.

[86] Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows.A Critical Analysisi of "the Right to be Forgotten" in Big Data Practice", 8 SCRIPTed (2011)229, p.237.

Protection scope: According to Article 3 of the GDPR, the right to be forgotten applies to personal data processing activities throughout the EU, so the application scenarios of the right to be forgotten are multi-field, multi-dimensional, and multi-level. In addition, European theoretical circles focus on the distinction between data protection and privacy protection, and believe that data protection is a balance between public interests and individual rights and interests, while privacy protection focuses on protecting individual rights and interests from infringement[87]. However, China's legislation on the right to be forgotten shows a centralized trend, which is mainly reflected in the field of personal information protection and personality right protection. Article 38 and Article 40 of the Constitution provide protection for citizens' personal dignity, freedom of correspondence and confidentiality of correspondence, which is the legal source of the enactment of the Personal Information Protection Act[88]. Article 43 of the Network Security Law clearly stipulates that individuals who find that network operators have collected or used their personal information in violation of laws and regulations have the right to ask network operators to delete their personal information. As the basic law in the field of civil affairs, the Civil Code has a comprehensive provision on the right to delete personal information. For example, Article 1037 (2) stipulates that if a natural person finds that an information processor has processed his or her personal information illegally, he or she "has the right to request the information processor to delete it in time". Paragraph 1 of Article 1195 stipulates that “where network users use network services to commit torts, the obligee has the right to notify the network service provider to take necessary measures such as deleting, blocking, and disconnecting links.” In addition, Article 47, Paragraph 1 of the "Personal Information Protection

[87] Fuping Gao, Personal Information Protection: From Personal Control to Social Control[J]. Legal Research, 2018(3): 84-101.

[88] Chenxin Ruan, Confirmation and Practice of the Right to be Forgotten as a New Type of Right[J]. Journal of Anhui University (Philosophy and Social Sciences), 2022(3): 98-105.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Law", Article 8.3 of the "Information Security Technology Personal Information Security Specification", and Article 22 of the "Network Data Security Management Regulations (Draft for Comment)" issued in November 2021 Paragraph 1 stipulates the specific applicable circumstances for the information subject to exercise the right to delete. It can be seen that China has not formally established the system of the right to be forgotten, but more to realize the protection of the right to be forgotten by the right of deletion.

Protection exemption: In the legal texts of EU and other extraterritorial regions, the right to be forgotten and the right to delete are mostly integrated. For example, Article 17 of the EU GDPR uses the expression "right to delete (right to be forgotten)". However, it should be noted that the scope of rights provided for in Article 17(1) and 2(2) is different, Taking the GDPR as an example, it stipulates exceptions when establishing the right to be forgotten, that is, the data controller can implement a defense against the right to be forgotten raised by the data subject based on the exceptions. However, China's "Personal Information Protection Law" stipulates that information controllers have the obligation to delete personal information actively under statutory conditions; if the information subject finds that it has not been deleted, it has the right to request its deletion. This means that the criteria for determining the right to delete is wider than that of the right to be forgotten, but at the same time, it also makes the information controller additionally assume the obligation of determination in practical operations, and it cannot be expected that the information controller can perform the deletion obligation in a timely manner.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Data controller's challenges: In reality, it is almost impossible to completely "be forgotten" in cyberspace. Because compared with traditional media, once generated, data in cyberspace can be transmitted, copied and stored at low cost, without limitation, across regions. In this information environment, information on the

Internet is everywhere, it is difficult to effectively complete the deletion of information. By using VPNS, Internet users can circumvent the restrictions imposed by domestic search engines on their search activities and obtain relevant information. Or it can then generate alternative links for network users to repost and share. This method of disconnecting links simply reduces the relevancy of the results directly retrieved by "name" within a certain range. In addition, search engine service providers have no law to prevent other network users from caching the relevant data content[89], nor can they prevent others from secondary transmission of cached content.

CHAPTER 5 Conclusion and Recommendations

5.1 Conclusion

In the era of big data, information is the factor of production, and information security and rational use have become the focus of the entire society. The proposal of the "right to be forgotten" attempts to limit the excessive preservation and use of personal information in the process of data development and utilization, and strive to safeguard the personal dignity and personal interests of the information subject, which itself has the basis of legitimacy. At present, there is no right to be forgotten in Chinese legislation.

This research analyzes China's relevant rights to personal information protection in other laws and compares foreign legislation and practical experience of the right to be forgotten. In contrast, China's right to be forgotten legislative protection is relatively weak. To determine protection weaknesses, this research, based on the comparative methodology, develops, and applies the below analytical framework:

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

[89] P.T.J.Wolters. The territorial effect of the right to be forgotten after Google v CNIL. International Journal of Law and Information Technology,2021,29(1):61.

Issue	Desired protection	Existing limitation
Data subject	Require the obligated subject to delete online information, give the subject the right to choose, and choose the applicable obligated subject	The obligated subject cannot completely eliminate the existence of information on the Internet; The data period is uncertain.
Protection scope	Legally circulated network information	It is difficult to define whether the transmission method is legal or not; Identifying information relevant to a particular individual; Different jurisdictions protect unequally; What is "unnecessary, irrelevant and outdated" personal information.
Protection exemption	Establish the boundaries of the right to be forgotten	reedom of information or expression, for compliance with EU or member state laws, for the public interest or for the exercise of public powers; Data subject's right to object" and "Unlawful processing of personal data
Right exercising	Article 17 of the GDPR provides for the right to be forgotten	The GDPR does not make a clear distinction between the right to be forgotten and the right to be deleted; China does not explicitly stipulate the right to be forgotten in the whole law system.
Data controller's challenges	There is a lawful basis for the processing of the data; The characteristics of network information flow increase the difficulty of realizing "right to be forgotten"	Illegal processing that does not distinguish between legitimate data in the original processing; The

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

		GDPR does not provide a reference template for how data controls determine when data is no longer relevant, the authenticity of public information, and which data deletion requests qualify for exemptions.

It finds that: firstly, the Google vs. Spain case between the search engine company and the original publisher (who has the responsibility to delete reports and protect personal data) is also a practical difficulty for China, the right to be forgotten is not absolute, but always needs to be balanced against other conflicting fundamental rights such as freedom of expression and freedom of the media, the public also needs truthful information reporting.

Secondly, a case study from Japan enforcing a right to be forgotten may face difficulties in determination of period of time, for this issue, article 22 of the "Regulations on the Administration of Network Data Security (Draft for Comment)" on November 14, 2021 stipulates that data processors shall delete personal information or perform anonymization within 15 working days, the time limit for deleting personal information is clearly defined. However, this is only a draft for comments at present, and the provisions themselves may change in the future, and additions and deletions cannot be ruled out. Thirdly, many provisions of Chinese laws do not fall into what should be done in practice, but are only general provisions, and China does not stipulate the right to be forgotten in the law, other laws are not sufficient to protect personal information and other rights. Although different countries and regions have different attitudes towards the right to be forgotten, there are also differences in the formulation of the value system of the right to be forgotten and the content of the judicial system. However, the basic principles followed in the

development process are the same, that is, by deleting the personal data that has already been made public, giving individuals the right to disclose their past without having to face others, and solving the problem of violation of human dignity caused by the lasting memory of the Internet, make public personal information into privacy information to be forgotten[90].

However, due to the difficulty of practical operation of the right to be forgotten, the consideration of various factors such as China's national conditions, traditional culture and legal and social development. In addition to the legislative level, we need to make more efforts at other social and corporate levels.

5.2 Recommendations

Throughout the world, there are actually few legal provisions for the emerging right of "the right to be forgotten" in various countries. The EU only introduced relevant laws to protect the "right to be forgotten" in 2016, it is GDPR. For China, the right to be forgotten should be determined legally. First, China cannot use the traditional comparative method to learn from the advanced experience of the West. China has already taken a leading position in the world in the field of Internet, and has surpassed most Western countries in the development of platform economy and sharing economy. Based on the principle that Western experience can be used for reference, but the right cannot be completely transplanted, China should give a new connotation to the right to be forgotten that is different from that of Europe and the United States. Try to find out the loopholes in the formulation and application of the right to be forgotten in developed countries such as Europe and Japan, and ensure that China's legislation takes this as a reference. Then Determine a specific period by which the

[90] Meg Leta Ambrose, It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten, 16 Stanford Technology Law Reviews (2013), p.371

data will no longer be relevant. Last, combined with the reality and long-term needs of Chinese social life, it is necessary to localize the right to be forgotten in China. Internally, while paying attention to economic development, it is necessary to ensure that citizens' human dignity is not infringed, ensure the security of citizens' online information, and reduce the possibility of personal privacy leakage while making personal information public; externally, countries will pass China's personal information protection standards determine whether to restrict the cross-border flow of information between countries. If China does not have a complete legal system for personal information protection, it will be under the dual pressure of domestic basic human rights and foreign trade barriers. Therefore, China needs to clarify the protection of the right to be forgotten through legislation, and can introduce the Western right to be forgotten to a limited extent, and formulate legislation on the right to be forgotten with Chinese characteristics to ensure the realization of the data subject's right to be forgotten[91]. The right to be forgotten could be added to the personal information Protection Law or the civil code by expanding the interpretation .When legalizing the right to be forgotten, it should be as specific and clear as possible. If the legal provisions are too abstract and vague, and the Supreme People's Court has not issued a corresponding judicial interpretation, judges tend to adopt a negative attitude and deny the parties' claims. In addition, we can actively promote self-regulation in the Internet industry, set a storage period for personal information, and establish a special data protection agency.

[91] Fang Wan: "The Right to Be Forgotten: Reflections on the Introduction of the Right to be Forgotten in my country", Law Review, No. 6, 2016, p. 161.

REFERENCES

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

1. Tu Zipei. Big Data [M]. Guilin: Guangxi Normal University Press, 2012: 162.
2. Yang Lixin, Zhao Xin. The local right to be forgotten under the Personal Information Protection Law and its protection. Journal of Henan University of Economics and Law, 2022, No. 1, 60-71.
3. Brian Geremia, “Chapter 336: Protecting Minors’ Online Reputations and Preventing Exposure to Harmful Advertising on the Internet”, 45 McGeorge Law Review(2013)
4. Meg Leta Ambrose and Jef Ausloos, The Right to Be Forgotten Across the Pond, 3 Journal of Information Policy (2013), p.14.
5. Translation: Personal Information Protection Law of the People’s Republic of China – Effective Nov. 1, 2021. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/
6. Michael L. Rustad , Sanna Kulevska, “Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow”, 28 Harvard Journal of Law, Technology (2015) 251, p.360.
7. Yang Lixin and Han Xi: "The Chinese Localization of the Right to Be Forgotten and the Application of Laws", "Application of Law", No. 2, 2015, p. 24.
8. Mei Xiaying: "On the Legal Positioning of the Right to Be Forgotten and the Limitation of the Scope of Protection", "Applicable Law", No. 16, 2017.

CHULALONGKORN UNIVERSITY

9. Viviane Reding: The EU Data Protection Reform 2012:Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age.
10. Wang Zejian: The Law of Personality Rights: Legal Interpretation, Comparative Law, and Case Studies, Peking University Press, 2013.
11. Duan Weili: "Conceptual Analysis of the Right to Be Forgotten: Using the Right Theory of Analyzing Jurisprudence as a Tool", in Journal of Henan University (Social Science Edition), No. 5, 2018.
12. Jiang Su. From memory to forgetting: the operation of the EU's right to be forgotten system and its enlightenment [J]. Journal of Nanjing Normal University (Social Science Edition), 2021,(4):122.
13. Duan Weili: "On the Judicial Relief of the Right to Be Forgotten: Taking the Judgment of the First Domestic "Right to Be Forgotten" as an entry point", Application of Law, No. 16, 2017, p. 58.
14. Wen Rongzhi and Zhou Longjie: "The Creation of the Right to Be Forgotten in European Law and Its Enlightenment to my country", Journal of Changchun University of Science and Technology (Social Science Edition), No. 3, 2019, p. 36.
15. Zhou Hui: "Summary of the EU's "Right to Be Forgotten" First Case," Cyber Law Review, No. 2, 2015, p. 331.
16. Gutwirth, Serge and Leenes, Ronald and Hert Paul de. Reforming European Data Protection Law. Berlin:Springer Netherlands Press, 2015.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

17. StevenC.Bennett. The“Right to Be Forgotten” :Reconciling EU and US Perspectives[J],[8]Berkeley Journal of International Law, 2012:166

18. Kelly, Michael J. and Satola David. “The Right to be Forgotten”, 2017 Univesity of Illinois Law Review (2017)1

19. Kranenbor, Herke, “Google and the Right to Be Forgotten”, 1 Eur. Data Prot. L. Rev. (2015)70.

20. Owings, Lisa. “The Right to Be Forgotten”, 9 Akron Intellectual Property Journal (2015)45.

21. Wan Fang: "The Right to Be Forgotten: Reflections on the Introduction of the Right to be Forgotten in my country", Law Review, No. 6, 2016, p. 161.

22. Liu Wenjie: "Right to be Forgotten: Traditional Elements, New Context and Interest Measurement", Legal Research, No. 2, 2018.

23. Bert-JaapKoops, “Forgetting Footprints, Shunning Shadows.A Critical Analysisi of “the Right to be Forgotten” in Big Data Practice”, 8 SCRIPTed (2011) 229, p.241-242.

24. Fu Yanshu. A Brief Talk on the "Right to Be Forgotten" in the Era of Big Data [J]. North Journal of Beijing Institute of Graphic Printing, 2020, 28(2):17-20.

25. Fu Xiaozhu. Research and thinking on the "right to be forgotten" in the era of big data [J]. Young Reporter, 2018:80-81.

CHULALONGKORN UNIVERSITY

26. Zheng Zhifeng. Research on the right to be forgotten in the network society[J]. New Vision of Law Wild, 2015(6):52-56.

27. Li Bing, Zhan Jiang. The United States and the European Union on the "Right to Be Forgotten" in Cyberspace different attitudes of [J]. Journalists, 2016, 12(406):63-69.

28. Ling Qian, Wang Xiaopei. Dignity, Speech and Privacy: Multiple Dimensions of "Right to Be Forgotten" in the Internet Age [J]. News and Communication, 2020:43-46.

29. Blanca R. Reitz: "Privacy Rights in Electronic Communications: A Comparative Perspective of European Law and American Law", translated by Lin Xifen et al., Shanghai Jiaotong University Press, 2017, p. 37.

30. Wang Xiuzhe: "Research on Public Law Protection of Personal Privacy Rights in the Information Society", China Democracy and Legal System Press, 2017 edition, pp. 100-101.

31. Meg Leta Ambrose, Jef Ausloos, “The Right to Be Forgotten Across the Pond”, 3 Journal of Information Policy, (2013)1, p.4.

32. Douwe Korff, “EC Study on Implementation of Data Protection Directive”, 34 Comparative Summary of National Law (2002)1, p.47.

33. Michael L. Rustad, Sanna Kulevska, “Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow”, 28 Harvard Journal of Law, Technology (2015) 349, p.359.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

34. James Q. Whitman, “The Two Western Cultures of Privacy: Dignity Versus Liberty”, 113 The Yale Law Journal (2004)1151, p.1161.
35. Paul Schwartz, “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 American Journal of Comparative Law (1989)675, pp.686-687.
36. Michael L. Rustad, Sanna Kulevska, “Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Date Flow”, 28 Harvard Journal of Law, Technology (2015) 349, p.360.
37. Abril, Patricia Sdnchez and Lipton, JacquelineD. “The Right to be Forgotten: Who Decides What the World Forgets”, 103 Ky. L.J. (2015)363.
38. Bunn, Anna. “The curious case of the right to be forgotten”, Computer Law & Security Review (2015)336.
39. Wu Fei, Fu Zhengke. Big Data and "Right to Be Forgotten" [J]. Journal of Zhejiang University (Humanities and Social Sciences Edition), 2015, 4(52):68-78.
40. Zheng Yuanmin, Li Zhichun. A conceptual analysis of the right to be forgotten [J]. Changchun Division Journal of Fan University, 2015, 3(41):30-34.
41. Zhang Hao. Can "forgotten" become a legal right? Discussion on Yang Lixin and Professor Han Xu[J]. Guangxi Social Sciences, 2016(7):101-105.

CHULALONGKORN UNIVERSITY

42. Wang Yan, Zhao Jie. The Realistic Logic and Origin of the Right to Be Forgotten in the Era of Big Data Civil Construction [J]. Journal of Nanchang University (Humanities and Social Sciences Edition), 2020, 5(16):103-111.

43. Xiao Youjing. On the localization of the right to be forgotten in China under the background of big data: need and embarrassment [J]. News Culture Construction, 202(0 17):19-21.

44. Zhang Ruikun. Reflection and Reconstruction of China's Right to Be Forgotten System [J]. Journal of Fujian Police College, 2020, 3(4 6):88-93.

45. Zeng Yan. Reflections on the Right to Be Forgotten in the Era of Network New Media [J]. Rule of Law and Society, 202(0 9): 62.

46. Zhang Jianwen, Gao Finish. Ontology and Indigenization of the Right to Be Forgotten [J]. Journal of Jishou University (Social Science Edition), 2016, 37(3): 76-81.

47. Jiang Su. From memory to forgetting: the operation of the EU's right to be forgotten system and its enlightenment [J]. Journal of Nanjing Normal University (Social Science Edition), 2021(4):122-130.

48. Luo Yong. On the Construction of the "Right to Be Forgotten" System in my country's Personal Information Protection Legislation [J]. Jinan Journal (Philosophy and Society), 2018(12):69-80.

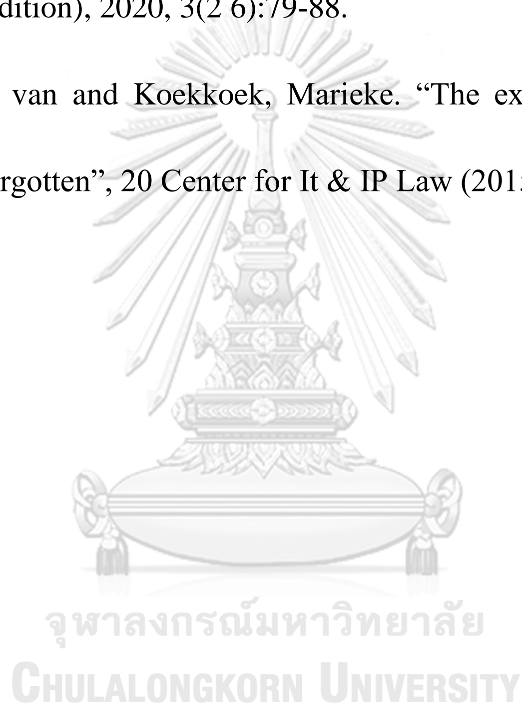
49. Shao Guosong. "Right to be Forgotten": New Issues and Countermeasures of Personal Information Protection [J]. Nanjing Social Sciences, 2013(2) .

CHULALONGKORN UNIVERSITY

50. Li Lijuan. British media condemns Google for abusing the "right to be forgotten" [N]. Legal Daily, 2014-07-08(9) . Zhang Lian."Right to be forgotten": New problems in the era of big data[J].Hebei Law, 2017(3).

51. Wen Ming, Yi Yonghao. On the Localization and Transplantation of the Right to Be Forgotten [J]. Journal of Chongqing University of Posts and Telecommunications (Social Sciences Edition), 2020, 3(2 6):79-88.

52. Alsenoy, Brendan van and Koekkoek, Marieke. “The extra-territorial reach of the EU’s right to be forgotten”, 20 Center for It & IP Law (2015)1.


จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

VITA

NAME	Yue Zhen
DATE OF BIRTH	02 Feb 1997
PLACE OF BIRTH	Shanxi Province, China
INSTITUTIONS ATTENDED	Shanxi Datong University
HOME ADDRESS	No.8, Lane 666, Jinxiu Road, Huamu Street, Pudong New Area District, Shanghai, China

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY