Master's Thesis

The Right to Be Forgotten in China?

With special reference to GDPR

GDPR에 비추어 중국에서의 잊혀질 권리에 관한 논의

February 2021

Graduate School of Seoul National University

Intellectual Property law, Department of Law

NA XIE

The Right to Be Forgotten in China?

With Special Reference to GDPR

Academic Advisor：Professor Sang Jo Jong

Submitting a master's thesis of Law

November 2020

Graduate School of Seoul National University

Intellectual Property Law, Department of Law

NA XIE

Confirming the Master'sThesis written by NA XIE

January 2021

Chairperson _____

Vice Chair _____

Examiner _____

TABLE OF CONTENTS

List of Table

Abbreviations:

CJEU: Court of Justice of the European Union

ECJ: European Court of Justice

ECtHR：European court of human rights

GDPR: General Data Protection Regulation

NPC: China’s National People’s Congress

Introduction

1. Background: Perfect Memory of the Internet

In the digital era, people have already got used to the ubiquitous collection of personal information by governments and incorporations in the name of public security and intelligent, personalized services, as well as advocacy from social media to share more information about private lives in order to promote interaction with friends. The result is that a massive amount of personal information has been exposed on the internet. What escalates the privacy crisis is the powerful search ability of search engines. Search engines can bring information from various places altogether, which breaks the spatial and temporal boundaries of the dissemination of information. The easy access and massive audience for information brought by search engines have dramatically changed the impact that a piece of information may have on the relevant data subject. Everything in our daily life has been recorded and never forget on the internet with its unlimited capacity. In the meantime, powerful search engines can keep bringing our past memory back to the present, regardless of a happy memory or embarrassing moments.

2. Purpose and Research Question

Facing the perfect memory of the internet, Professor MegLeta Ambrose calls on every country that it is time to reflect which values should be left, and how could

those values be left, and on the other side, what kinds of information are allowed to be takedown from the internet.[1] Concerning this matter, the European Union has taken an initiative to announce a right to be forgotten based on its data protection framework. In 2014, the Court of Justice of the European Union recognized the right to be forgotten as a workable legal right in the Google Spain case[2], confirming that European Union citizens have a right to request websites to delete their personal information on the internet if certain conditions are met. After the judgment was made, it immediately aroused widespread concerns and controversies in the global legal and technological circles. In 2016, the EU reconfirmed the right to be forgotten through article 17 of the General Data Protection Regulation (GDPR).

Scholars over the world have discussed and debated the nature, legitimacy, and scope of the right to be forgotten[3]. In China, the right to be forgotten is also on the agenda at the legislative and judicial levels. In 2015, in the case of Renjiayu v Baidu Netcom Technology of personality rights dispute, the plaintiff claimed not only that Baidu Company infringed his rights of name and right to reputation, but also claimed

[1] Ambrose, Meg Leta, Nicole Friess, and Jill Van Matre. "Seeking digital redemption: The future of forgiveness in the Internet age." *Santa Clara Computer & High Tech. LJ* 29 (2012): at p115.

[2] *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317 (2014).

[3] Discussion the right to be forgotten in country level, see. E..g, Kulk, Stefan, and Frederik Zuiderveen Borgesius. "Freedom of expression and right to be forgotten cases in the Netherlands after Google Spain." *Eur. Data Prot. L. Rev.* 1 (2015): 113., Singh, Ajay Pal, and Rahil Setia. "Right to Be Forgotten-Recognition, Legislation and Acceptance in International and Domestic Domain." *Nirma ULJ* 8 (2018): 37. Zufall, Frederike. "Challenging the EU's Right to Be Forgotten: Society's Right to Know in Japan." *Eur. Data Prot. L. Rev.* 5 (2019): 17. Chiou, Wen-Tsong. "Limits and Prospects of the Right to Be Forgotten in Taiwan." *The Right To Be Forgotten*. Springer, Cham, 2020. 311-318. Ambrose, Meg Leta. "Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception." *Telecommunications Policy* 38.8-9 (2014): 800-811. Slane, Andrea. "Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow." *Osgoode Hall LJ* 55 (2018): 349. Jacques, Sabine, and Felix Hempel. "The Right to Be Forgotten in the UK: A Fragile Balance?." *The Right To Be Forgotten*. Springer, Cham, 2020. 195-222.

that Baidu Company had violated the “right to be forgotten.” In terms of legislation, the "Legislation Plan" announced by the Standing Committee of the thirteenth National People’s Congress (NPC) on September 10, 2018, has confirmed the legislation of a specific "Personal Information Protection Law". Thus, regarding such a right, what kind of attitude should the Chinese legal system adopt? Should it follow the European Footsteps or maintain a more cautious stance on this right?

3. Review of the Scholars’ Opinions on the Localization of RTBF

Since 2014, there has been a surge of the study concerning the right to be forgotten among Chinese scholars, influenced by the famous Google Spain case.

3.1. Positive Attitude

Professor of the Remin University of China, Lixin, YANG believed that the establishment of the right to be forgotten could help to effectively balance the conflict between the increasing sharing culture of personal daily life and the phenomena of “the internet never forgets”[4]. Besides, the judicial case of “Ren vs Baidu” has shown a real need in china to establish the right to be forgotten. Moreover, the current practice of some network service providers in china coincides with the

[4] 杨立新,韩煦. 被遗忘权的中国本土化及法律适用[J]. 法律适用,2015(02):24-34.

spirit of the right to be forgotten[5]. And the current legislation of china has left room for the establishment of the right.

Professor Wenjie Man supported the introduction of the right to be forgotten from the perspective of the information life cycle. Since the eternity of the internet has disrupts the normal information life cycle, that the right to be forgotten can be introduced as an important correction mechanism to restore the normal metabolism of information, adjusting the retention of information according to the decline of information value, so as to avoid damage to personality rights or interest due to outdated or inaccurate information[6].

Lifeng Li affirmed the positive contribution of the right to be forgotten to "digital oblivion". The search function of the internet has given birth to a revolutionary force that redistributes the interest and rebuilds the class within the digital world. In the meanwhile, the private resistance of data subject to the search service providers cannot be adjusted based on existing personality rights, but can only be solved by constructing a new right[7].

After analyzing the conflict between the right to be forgotten and other rights and values, and the technical dilemma at the enforcement level, Shanshan Lei still

[5] For example, China's Search Engine, Baidu has launched a specialized service for accepting uses' complaints about search-related issues, which includes snapshot deletion and search keywords deletion in its "Privacy Issue Feedback" system. In the case where the content of the search results violates the privacy right or other legitimate interests of the user, a deletion service can be provided according to the user's request. After a deletion request is submitted by the user and is reviewed by a specialist in Baidu, the link to the webpage in question will be deleted within 24 hours. Here is the service link: http://tousu.baidu.com/webmaster/add#2

[6] 满洪杰. 被遗忘权的解析与构建:作为网络时代信息价值纠偏机制的研究[J]. 法制与社会发展, 2018, 24(02):199-217.

[7] 李立丰. 本土化语境下的"被遗忘权":个人信息权的程序性建构[J]. 武汉大学学报(哲学社会科学版), 2019, 72(03): 第 146 页.

embraced the value of the right to be forgotten in the over-connected era in which information is easily out of control. She believes that we should insist on the beneficial purpose of the legislation and further explore the solution of those conflicts and enforcement dilemmas that are not insurmountable[8].

3.2. Negative Attitude

ZeGang Liu questioned the legitimacy of the right to be forgotten from three kinds of freedom in political philosophy: the right to freedom, the freedom of general behavior, and Self-mastery. The right to freedom mainly refers to various traditional defensive rights represented by freedom of speech. The freedom of general behavior includes the freedom concept of non-interference and non-dominance. He criticized, although the right to be forgotten may provide the necessary safeguards for the freedom of expression if its scope is carefully defined and exercised, search engines represented by Google are suspicious for being arbitrary in carrying out mass applications of deletion which will directly harm the general freedom on the internet. Self-mastery emphasizes individuals' moral autonomy and autonomous control. The right to be forgotten restricts the freedom of commerce on the internet, thus, in turn, affects the freedom of users to obtain benefits and conveniences through the network.[9]

Xuelian He pointed out that the right to be forgotten encourages people to close themselves off by withdrawing information from the internet, but paradoxically

[8] 郭小安,雷闪闪."数据被遗忘权"实施困境与我国的应对策略[J].理论探索,2016(06):108-114

[9] 刘泽刚. 过度互联时代被遗忘权保护与自由的代价[J]. 当代法学, 2019, 33(01):91-100.

increases privacy anxiety. Second, its overly sentimental term covers up the possibility that there may be nothing behind the words, but a contemporary psychological feeling, such as what Freud called a “neighbor abyss”. Third, the invasion of data privacy is unpredictable and unpreventable. Overprotecting privacy is not only useless but may also trigger the Streisand effect. Thus, encouraging people to be more open and fostering social customs of tolerance is better than preventive legislation.[10]

Yuxiang Ding, the Vice president of Beijing No.1 intermediate people’s court thought the introduction of the right to be forgotten is an unnecessary burden. He explained that the consequences of infringing on the interests protected by the right to be forgotten can be classified into four types, namely the infringement of the right to privacy, reputation, name and personal freedom and dignity. Through seeking legal remedies from these four types of personality rights, the effect of the right to be forgotten can be achieved. Thus, there is no need to add an entity[11].

Liqiao Zhang thought that the right to be forgotten is too advanced relative to china’s national conditions[12]. Currently, improving free expression should be taken priority over the protection of privacy. At the same time, due to the scarcity of legislative resources, the value underlying the right to be forgotten could be embodied in the form of soft laws, standards, or industry norms.

[10] 何雪莲. 隐私的辩证:被遗忘还是被观望?[J]. 南京社会科学,2017(07):120-127.
[11] 丁宇翔. 被遗忘权的中国情境及司法展开——从国内首例“被遗忘权案”切入[J]. 法治研究,2018(04):27-39.
[12]. Liqiao Zhang believes that the right to be forgotten is at an advanced stage in the personal information protection legal system. The need for the right to be forgotten maybe not be so urgent than other data protection needs, such as protecting data security. See 张立翘：《被遗忘权制度框架及引入中国的可行性》，《互联网金融与法律》，2015 年第 2 期，第 6 页

Xuetao Liu and Yue Li believed that we should treat the right to be forgotten with caution after analyzing the risks of introducing the right to be forgotten in china and suggested to protect the interest in the right to be forgotten by enhancing the implementation of existing laws and regulations[13].

3.3. Analysis of Above Opinions

First, as a starting point for discussion, the concept of the right to be forgotten is still not clearly defined. The vagueness and confusion of concept have led to a large number of researches become less persuasive. For example, regarding the relationship between the right to be forgotten and the right to erasure, which are both stipulated in Article 17 of the GDPR, some scholars believe that the two rights are identical[14]. In contrast, some believe that the right to be forgotten only refers to a part of the right to erasure[15] or are totally different rights[16]. And some scholar believes that the right to be forgotten is only applicable for search engines. That is, the right to be forgotten is equivalent to the right to delisting[17]. In addition, some scholars believe that the current legal framework of personality right can already solve the cases relevant to the right to be forgotten, including the violation of the privacy, reputation, name, and personal freedom or dignity, therefore there is no need

[13] 刘学涛, 李月. 大数据时代被遗忘权本土化的考量——兼以与个人信息删除权的比较为视角[J]. 科技与法律, 2020(02):78-88.
[14] 刘文杰. 被遗忘权:传统元素、新语境与利益衡量[J]. 法学研究, 2018, 40(02):24-41.
[15] 李倩. 被遗忘权在我国人格权中的定位与适用[J]. 重庆邮电大学学报(社会科学版), 2016, 28(03):44-50.
[16]满洪杰. 被遗忘权的解析与构建:作为网络时代信息价值纠偏机制的研究[J]. 法制与社会发展, 2018, 24(02):199-217.
[17] 李立丰. 本土化语境下的“被遗忘权”:个人信息权的程序性建构[J]. 武汉大学学报(哲学社会科学版), 2019, 72(03):145-155.

to add more entities[18]. However, this view does not identify that the exercise of the right to be forgotten is not based on the premise of illegal or infringing, but from the data quality issues. Therefore, due to the issue of concept, the article will first take the EU's legislative history as a clue to clarify the connotation of the right to be forgotten.

Secondly, there are two main points of the dispute between Pros and Cons attitude towards the right to be forgotten: First is about the conflict between the right to be forgotten and other rights or interests. The second issues concern the impact on internet business at the level of enforcement. Thus, only when the controversy over the scope of the exercise of the right to be forgotten and the application of the law is clarified, can we build a bridge between supporters and opponents for rational communication and cooperation.

4. Outline

With that in mind, the rest of the work is structured as follows. It will firstly analyze the connotation, the value conflict, and enforcement dilemmas of the right to be forgotten based on the EU's legislation and practice. Due to its vague definition, the understanding of the right to be forgotten is not straightforward. Thus, it is better to focus on the concept of the right to be forgotten at its birthplace: Europe. By tracing its legislative history and judicial practice in the European legal system, I attempt to roughly delineate the root and scope of the controversial right. Then, it

[18] 丁宇翔. 被遗忘权的中国情境及司法展开——从国内首例“被遗忘权案”切入[J]. 法治研究, 2018(04):27-39.

will discuss the possibility of China's introduction of the right to be forgotten based on china's national conditions. More specifically, Chapter 1 will exams the rationale and foundation of the right to be forgotten, pondering what is the right to be forgotten. Then Chapter 2 will focus on legislation the right to be forgotten in GDPR, and distinguish the confusing relationship with the pre-existing right to erasure in data protection. Chapter 3 delineates the scope of the right to be forgotten and explore what kind of data is worth forgetting. Chapter 4 will discuss the Enforcement dilemma of the right to be forgotten, especially the role of search engines in the context of the right to be forgotten, and its ensuing obligations as a data controller. Chapter 5 will turn the focus back to China, reviewing the existing law and judicial practice relevant to the right to be forgotten, Especially the case of "Renjiayu vs. Baidu. The last Chapter explores the possibility of China's introduction of the right to be forgotten based on china's practical local backgrounds.

5. Methodology

Concerning the research methodology, the article mainly adopts the historical Analysis Method, Case Analysis Method, Normative analysis Method, and Comparative law approach.

Historical Analysis approach: The EU's right to be forgotten is rooted in the historical and cultural context of Europe. Therefore, by reviewing the legislative history of the right, it can help to grasp the underlying value of the right to be forgotten.

Case Analysis approach: The paper deeply analyzes the case of “Renjiayu vs. Baidu,” which is called the “First case of the right to be Forgotten” in china. Through the interpretation of the judgments of the two trials, it can clarify the path of the protection of the right to be forgotten under the existing Chinese law and the reject reasons, as well as the judges’ considerations behind the verdicts.

Normative Analysis approach: The paper conducts a deep analysis of the European Union’ legal norms involving the protection of the right to be forgotten, including the “*European Charter of Fundamental Rights*”, “*Data Protective Directive (Directive 95)”*, “*General Data Protection Regulation (GDPR)*”, particularly the provision of Article 17 of the GDPR. By analyzing the pros and cons of Article 17 of the GDPR, the paper draws insights from the European's right to be forgotten in the GDPR, reflecting on the extent and scope to which we can learn from the European data protection framework and the right to be forgotten under this protection framework.

Comparative law approach: Based on the consideration that the problems of loss of control over personal information in the era of big data are universal in such a tightly connected world, it is believed the study of EU’s attempts of constructing and implementing the right to be forgotten could shed light on the data protection legal framework in China. The paper takes a holistic view of the development of the right to be forgotten in the EU and scrutinized the relevant cases and theories. However, after comparing the legislative difference between China and the EU, it is concluded that based on china’s local legal resources and environment, the EU’s right cannot yet be entirely introduced in china.

Chapter 1 The Rationale of the Right to Be Forgotten

The right to be forgotten is a very eye-catchy terminology that not only raising attention in the legal world, but also becoming a buzzword in people's daily communication[19]. In the sense of enhancing the public awareness of data protection, the EU's proposal of the right to be forgotten is undoubtedly successful. However, when scrutinizing the parlance in a legal context, the definition of the right is frustratingly unclear. Each scholar has a slightly different perspective on the meaning of the concept. Moreover, it is like stepping into the maze of terminologies. There are too many similar but confusing terms. Therefore, this section first explores the root of the burgeoning right in Europe, which could provide an essential basis for understanding the complexity and rationale behind a right to be forgotten.

1. The Right to Be Forgotten in Dignity: Forgetting and Forgive

Leaving aside the numerous controversies brought by the conception of the right to be forgotten, let us first focus on the word "forgotten" in the term. Memory consists of numerous past events. Human beings have a natural physiological mechanism of forgetting, that allows us to selectively forget some memories, such as painful memory, or some trivial or stupid mistakes we made. Forgetting is the need to relieve us from past unpleasant memory, forgive ourselves or others, and

[19] Chris Moran, "Things to remember about Google and the right to be forgotten", Guardina, July, 3, 2014,
See https://www.theguardian.com/technology/2014/jul/03/google-remember-right-to-be-forgotten

regain the power to move on. In this sense, the virtue of forgetting can prevent the stagnation of self. The virtue of forgetting is not limited to individuals, but to the society as a whole. The society is benefited if individuals get chances to develop their identity freely[20]. For example, through granting forgiveness to juvenile offenders, society also benefits from cultivating society's future. Thus, when considered in this light, the right to be forgotten is connected with the past, as well as related to the purpose of forgiveness.

1.1. The Right to Oblivion

In the legal context, the interest of forgiveness has already been embedded in many laws that aims at protecting vulnerable groups from discrimination or unfairness, such as bankruptcy law, juvenile justice, crediting report law and rehabilitation. For example, the 'droit à l'oubli' in French law or the 'diritto al' oblio' in Italian law recognizes the "right of oblivion" of the judicial past. More specifically, the 'droit à l'oubli' allows a convicted criminal who has paid what is due and been rehabilitated to object to the publication of the facts of his conviction and incarceration[21]. The 'droit à l'oubli' in EU's case law is limited by its application to media activities, forbidding the media to make public, once again, about a person's private life in the past[22]. However, since the media pattern has changed with the rise

[20] Mayer-Schönberger, Viktor. *Delete: The virtue of forgetting in the digital age*. Princeton University Press, 2011.

[21] De Terwangne C. Internet privacy and the right to be forgotten/right to oblivion[C]//VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet,[monografía online], IDP, Revista de Internet, Derecho y Política, UOC. 2012 (13): P111

[22] Mantelero, Alessandro. "The EU Proposal for a General Data Protection Regulation and the roots of

of new intermediates such as social media and search engines. It is natural to think about extending the application of the right on certain key intermediates, such as search engines. In addition, concerning re-addressing the issue that happened in the past, the factor of time plays an important role in the notion of the right to oblivion.

The right to be forgotten has embraced the spirit of "a fresh start" or "a clean slate" from the right to oblivion, namely that people should not be tethered to his/her past action. It is easy to find such an inheritance from the name of the right.

1.2. Privacy Protection in Europe

For more general personal information other than judicial history, the interest of preventing unwarranted publication or disclosure reflects an aspect of the right to privacy. In this sense, the right to be forgotten is tied with privacy in the perspective of public disclosure of private facts.

In the traditional discussion of the private protection against public disclosure, scholars have gradually realized that de-contextualized personal information may lead to unfair judgement and the benefit of concealing one's past to the personal growth and reformation of identity[23]. For example, Certain sensitive information easily leads to stereotypes or discrimination or prejudice. If someone has AIDs, people tend to assume that the person has engaged in drug use, promiscuity, or homosexual sex.[24] In addition, since a person's identity is not fixed, and everyone

the 'right to be forgotten'." *Computer Law & Security Review* 29.3 (2013): P231

[23] Solove, Daniel J. "The virtues of knowing less: Justifying privacy protections against disclosure." *Duke LJ* 53 (2003): P1053

[24] Karas, Stan. "Privacy, identity, databases." *Am. UL Rev.* 52 (2002): P427

has some embarrassing moments where they have done things, then regretted later, being able to escape disclosure of their past conduct could prevent potential harm to "dignity, personality, reputation and identity" of an individual[25]. Also, as the core content of privacy, individuals need to enjoy a certain degree of tranquility of spirit, which refers to avoiding being disturbed by others and free from unwanted disclosure of personal information. Following this vein, the right to be forgotten can develop on the basis of the protection of life tranquility, which allows an individual to enjoy a kind of peace and quiet, so that he can develop his personality[26].

For Europeans, the core of the protection of the right to privacy is to protect human dignity and the typical manifestation of privacy is the individual has the right to protect their image in public and ensure others see themselves the way they want to be seen[27]. For example, in a French case, model Estelle Hallday has successfully sued a free service provider that kept her nude photos[28]. Although the massive storage capabilities of the Internet make the complete deletion of information almost impossible, the Court of Justice of the European Union still considers it necessary to prohibit the dissemination of these photographs in order to express the importance of the protection of the private life.[29] In the context of the right to be forgotten, most of the public information has already lost its privacy interest. But it is a matter of dignity concerning private life and personal image. Thus, it shows respect for human

[25] Tamò, Aurelia, and Damian George. "Oblivion, erasure and forgetting in the digital age." *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 5 (2014): 71.

[26] Henry, Michael. *International privacy, publicity and personality laws*. Butterworths, 2001.

[27] Whitman, James Q. "The two western cultures of privacy: Dignity versus liberty." *Yale LJ* 113 (2003) p1161

[28] ibid, at p1199

[29] ibid, at p1200

dignity to allow the request to withdraw information that has been made public.

2. The Right to Be Forgotten in Data Protection

The right to be forgotten can also find its root in data protection. The right to be forgotten does not only means deleting the past events, but has a more positive facet which refers to the capacity to make choices or to make informed decisions[30]. In this aspect, the right to be forgotten is linked to a concept related to informational self-determination. The necessity of data protection in Europe was realized as early as the emergence of data banks in the 1950s. When individuals faced the massive data collection of the industry and bureaucracy, European lawmakers realized the huge disparity of power between individuals and data controllers, and considered there is a need to give individuals greater control in balancing the asymmetric relationship.

2.1. Informational Self-determination: Control

Self-determination of personal information or so-called informational self-determination stems from the German Constitutional law. In the context of German law, informational self-determination is derived from the protection of human dignity, and refers to a kind of autonomy in which an individual has a right to decide which information about herself will be disclosed, to whom and for what purpose. The right of self-determination of personal information has been recognized as a constitutional

[30] De Terwangne C. The right to be forgotten and informational autonomy in the digital environment[M]//The ethics of memory in a digital age. Palgrave Macmillan, London, 2014: p88.

right in the "population Census Decision"[31] of the German Federal Constitutional Court and has a profound impact on the private law system by confirming its "third party effectiveness" through a series of subsequent judgments[32].

The core value of the informational self-determination lies in the control of personal information which is also inherited in the legislation of the GDPR. Following the theory of informational self-determination, if personal information about an individual is collected, processed, and used by others, but the individual has no knowledge or ability to stop it, it is equivalent to place the individual in a position of being dominated by others, which constitutes an infringement on the individual's autonomy. The right to be forgotten empowers individuals to control over one's personal information by means of deleting or blocking, which reflects the spirit of information self-determination.

2.2. The Fundamental Right to Protect Personal Information

Moreover, based on the informational self-determination, the right to the protection of personal data has been stipulated as a fundamental right in the "European Charter of Fundamental Rights",[33] which came into force together with

[31] Bundesverfassungsgericht, decisions volume 65, p. 1 ff.

[32] 李承亮. 个人信息保护的界限——以在线评价平台为例[J]. 武汉大学学报(哲学社会科学版), 2016, 69(04):111 页.

[33] Article 8 of the European Charter of Human Rights of the European Union: Protection of Personal Data:

1. everyone has the right to the protection of personal data concerning him or her,

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

the Lisbon treaty in 2009. Since that, the right to protection of personal data has been elevated to the level of a fundamental human right in Europe.

Compared with the privacy protection, the right to protect personal data is a more modern right focusing on constraining improper use of personal data[34]. In general, the hard core of the right to protection of personal data refers to the "informational self-determination" and dignity and personal identity (the principle of "non-discrimination").[35] Although the precise nature of the link between the privacy and data protection is not fully understood and is still being debated, the independent status of the right to personal data protection at least shows some added values of the data protection. One among others, compared with the opaque notion of privacy, data protection provides more normative and objective guidelines which refer to requirements for fair processing, consent, or legitimacy.[36] Especially, fair Information Principles constitute the core framework of data protection. There are mainly seven data protection principles which are (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimization; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality; (g) accountability.[37]

In addition, as a broader right than the right to privacy, the right to protect personal data facilitates to reduce the asymmetric relationship between data

[34] Forde, Aidan. "Implications of the Right to be Forgotten." *Tul. J. Tech. & Intell. Prop.* 18 (2015): at p90

[35] Tzanou M. Data protection as a fundamental right next to privacy? 'reconstructing' a not so new right[J]. International Data Privacy Law, 2013, 3(2): p98.

[36] Forde, Aidan. "Implications of the Right to be Forgotten." *Tul. J. Tech. & Intell. Prop.* 18 (2015): at p91

[37] GDPR article 5

controller, processors and data subjects. As data processing has now reached an unprecedented scale, by granting data subjects more rights over types of data, the right to protect personal data aims at preventing negative impacts on individual autonomy during data processing[38].

3. Summary

Then, by delving into the root of the right in Europe, it shows that the emergence of the right to be forgotten in Europe was a natural consequence of its strong protection of privacy centered on honor and dignity and data protection centered on informational self-determination.

[38] Lynskey, Orla. "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order." *International & Comparative Law Quarterly* 63.3 (2014): p597.

Chapter 2 The Right to Be Forgotten in GDPR

In this section, by using a historical analysis methodology and tracking back the legislative history of the right to be forgotten in the EU, it shows how the right has been conceptualized over time and attempts to clarify the underlying values in the right to be forgotten, and set this conception as the keystone in this paper, for the convenience of the following discussion.

1. Lack of uniformity in the conception of the right to be forgotten

The right to be forgotten was stipulated in Article 17 of GDPR. However, the right to be forgotten is placed inside the parenthesis after "the right to erasure," which has led to a confusing relationship between the right to be forgotten and the right to erasure, as well as the precise connotation of the right to be forgotten. In practice, the term "right to be forgotten" has been used for multiple ends. Among them, the right to be forgotten is described as a specific enforceable legal right, as well as the broader, socio-philosophical concept underlying this and related right".[39] Thus, what is the relationship between the right to be forgotten and the right to erasure? Against whom can the right be invoked? When and why can the right be invoked? Encompassing perspectives on the right to be forgotten in literature, the academic

[39] Garstka, K., & Erdos, D. (2017, October). Hiding in Plain Sight? The'Right to Be Forgotten'and Search Engines in the Context of International Data Protection Frameworks. In *The'Right to Be Forgotten'and Search Engines in the Context of International Data Protection Frameworks (October 2017). Forthcoming in Report of the 2017 Internet Governance Forum (IGF) Dynamic Coalition on Platform Responsibility*.

circle has not yet formed a unified definition of the right to be forgotten.

1.1. Unique Meaning

The majority of Chinese scholars tend to define the right to be forgotten as a right to delete outdated and negative personal information which may harm the social evaluation of relevant individuals.[40]

1.2. Binary Meanings

Ambrose and Ausloo think that the right to be forgotten is an umbrella term for the right to oblivion and the right to erasure[41]. Professor Lian Zhang also believes that the right to be forgotten has two dimensions: the right to oblivion and the right to erasure, which is the restatement and the improvement of the two rights in the era of big data[42].

1.3. Multiple Meanings

David Erdos suggested that the right to be forgotten refers to a right to restrict access to identified or identifiable personal information to prevent actual or potential damage, as long as there is no legitimate reason to oppose such a removal. However, he also admits that due to such a broad understanding of the right, the right to be

[40] 李倩.被遗忘权在我国人格权中的定位与适用[J].重庆邮电大学学报(社会科学版),2016,28(03):44-50,杨立新,韩煦.被遗忘权的中国本土化及法律适用[J].法律适用,2015(02):24-34.

[41] Ambrose, Meg Leta, and Jef Ausloos. "The right to be forgotten across the pond." *Journal of Information Policy* 3 (2013): 1-23.

[42] 张里安,韩旭至."被遗忘权":大数据时代下的新问题[J].河北法学,2017,35(03):35-51.

forgotten is not a specific legal right, but refers to a number of specific legal rights and provisions.[43] Koops summarized the contents of the right to be forgotten into three aspects: The first one emphasized the "Clean-slate" from the perspective of society, that individuals should not be over-trapped by outdated negative information. The second one means that personal data should be deleted in its appropriate due time. The third one is mentioned from the perspective of personal self-development, that people should be able to express themselves unstrained[44]. A right allows you to speak and write freely without fearing your personality being fixed by what you express. It is a sense of liberty of writing today, and being able to change your mind tomorrow. Focusing on these three aspects, Xanthoulis thought the right to be forgotten could be conceptualized as a multidimensional privacy, as a human right[45]. W. Gregory Voss, et al proposed a taxonomy on the various forms of the right to be forgotten, which includes the right to rehabilitation and the right to erasure in a general context, the right to delisting, the right to obscurity and the right to digital oblivion in the digital context.[46]

---

[43] Garstka, Krzysztof, and David Erdos. "Hiding in Plain Sight? The 'Right to Be Forgotten' and Search Engines in the Context of International Data Protection Frameworks." *The 'Right to Be Forgotten' and Search Engines in the Context of International Data Protection Frameworks (October 2017). Forthcoming in Report of the 2017 Internet Governance Forum (IGF) Dynamic Coalition on Platform Responsibility*. 2017.

[44] Concerning the third meaning, Koop also admits that such an abstract concept is difficult to develop into a legal right, but a reflection of philosophy and psychology. However, it still matters for legislators and designers to remember the virtues of forgetting, when collecting and processing data. See: Koops B J. Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice[J]. SCRIPTed, 2011, 8: 229.

[45] Xanthoulis, Napoleon. "The right to oblivion in the information age: A human-rights based approach." *US-China L. Rev.* 10 (2013): at 87.

[46] Voss, W. Gregory, and Céline Castets-Renard. "Proposal for an International Taxonomy on the Various Forms of the Right to Be Forgotten: A Study on the Convergence of Norms." *Colo. Tech. LJ* 14 (2015): 281.

Therefore, the current literature is still confused about the concept of the right to be forgotten. The main reason is that the Google Spain case was decided in 2014. At the time, the GDPR has been drafted but not yet voted on. Thus, the Court of Justice of the European Union (CJEU) relied on Directive 95 to deduce the right to be forgotten. Such a "Original legislation- Jurisprudence-New legislation" has led to an understanding of the EU's right to be forgotten only relies on existing legislative provisions is inevitably biased.[47] The following will examine relevant documents, including the law, cases, preparatory documents, and official press releases, from the proposal of the right to the final inclusion into the GDPR. In doing so, it reveals what kind of concerns and context in which the EU established the right to be forgotten.

2. The Evolution of the Right to Be Forgotten in GDPR

2.1. Proposal of the Right to Be Forgotten: Withdraw Information Published by the Data Subject

The right to be forgotten has been brewing for quite a long time in the data protection community. The right to be forgotten was proposed in early 2010, when the vice-president of European Commission Viviane Reding proposed a new right to personal data at the European Data Protection and Privacy Conference. The right to be forgotten was described as enshrined with the spirit of "God forgives and forgets". In her speech, she listed two situations in which the right to be forgotten should be applied: one is when people want to quit from a certain service, people have the right

[47] 蔡培如. 被遗忘权制度的反思与再建构[J]. 清华法学,2019,13(05):第 171 页

to wipe out their profile, especially on social networking site. The other one is when the pre-determined expired time is termed, the user's data should be deleted.[48]

In the "Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (hereinafter referred to as "Proposal for GDPR") in 2012, the Article 17 stipulates the "right to be forgotten and to erasure" which empowers data subject to obtain from the controller "the erasure" or the "abstention from further dissemination" of their personal data. The "abstention from further dissemination" of their personal data, seemingly can be regarded as the "right to be forgotten" literally. The Proposal for GDPR stipulates the grounds where the right to be forgotten can be invoked, including when the data are no longer necessary in relation to the purpose of data processing, withdraw consent or the storage period has expired, and when the data subject object to the processing.[49]

---

[48] See the complete transcript of Viviane Reding's speech at : https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_10_700

[49] Article 17(1) Proposal for GDPR

The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;

(d) the processing of the data does not comply with this Regulation for other reasons.

According to the European Commission, the proposal of the right to be forgotten is a result of a growing frustration regarding the lack of control over their personal data. Thus, the right to be forgotten, along with the right of access, right to rectification and object, is expected to strengthen individuals' control over their personal data. "It aims to protect the privacy interest of individuals, instead of erasing past events or restricting the freedom of the press"[50].

More specifically, the European Commission itself stated that it has received a lot of inquiries because individuals cannot retrieve personal data from the online service providers, such as their photo.[51] In practice, although the data has been deleted on the surface, the data stored on the server of the social platform has not been completely deleted. It is still used for other purposes based on the general terms and conditions in their privacy terms. The sad story of "Drunken Pirate" is a good example to show the need to delete information when the data subjects withdraw their consent. In 2006, Stacy Snyder, a single mother who was expecting to become a teacher, was disqualified as a teacher from her favorite university because her behavior was inconsistent with a teacher. The blasting fuse was a picture on her Myspace personal webpage in which she was wearing a pirate hat and holding a plastic cup, seems like being drunk. When Stacy wanted to delete the photo, she found that her personal web page had been cataloged by search engines and indexed by a web crawler program. Thus, even she deleted the picture on her Myspace Page,

[50] Questions and answers on data protection reform: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_6385

[51] European Commission Communication, 'A comprehensive approach on personal data protection in the European Union' 4 November 2010, COM (2010) 609 final, p. 7

the picture still be searched on the search engine. Thus, the European Commission believed that they should grant individuals a right to have their personal data erased completely if they withdraw their consent for processing. Especially for young people, they often without fully understand the consequence, they should not be trapped by the consequence caused by their stupid behavior for the rest of their lives. Thus, withdrawing consent has become the major ground of the right to be forgotten, especially in the context of social networks or some processing that only relies on consent. Google's transparency report also shows that the most links it removed come from social platforms such as Facebook, Twitter and YouTube[52].

Therefore, at the outset of its conceptualization, the right to be forgotten aims at strengthening the data subject's control over data originally posted by data subjects themselves.

2.2. Google Spain Case

The right to be forgotten caused a lot of controversies since it is proposed. Scholars have argued it's a too sentimental word which is easy to cause unfounded panic or excessive fanaticism, rather than rational reactions[53]. In the face of a huge controversy, In March 2014, the European Parliament has decided to fully replace the "right to be forgotten" with "the right to erasure" and deleted all the expressions of the "right to be forgotten" in the proposal for GDPR.[54] Thus, the title of Article

[52] Bertram, Theo, et al. "Five Years of the Right to be Forgotten." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019. P966

[53] Bernal, P.A., 'A Right to Delete?', European Journal of Law and Technology, Vol. 2, No.2, 2011

[54] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing

17 was directly named as "right to erasure" in the consolidated text of GDPR in 2014.

The Google Spain case in 2014 has taken the limelight. In this case, a Spanish citizen, Costeja Gonzalez, when typing his name into the Google Search engine, has found his name was linked to two articles published in 1998 in the search results. The two articles, which contained Mr. Gonzalez' name, were published in the Spanish newspaper La Vanguardia about an announcement of a real-estate auction due to social security debts.[55] The announcement was based on the order from the Ministry of Labor and Social Affairs, which is legally published. Mr. Gonzalez thought that the auction process had been completed years ago and was now completely irrelevant to him.[56] There, he requested Google to remove or conceal the personal data relating to him from the search result.[57] In the case, the Court of Justice of the European Union ("CJEU") upheld the complaint lodged by Mr. Gonzalez and ruled that Internet search service providers are obliged to delete "inadequate, irrelevant or no longer relevant or excessive" information. Thus, the judicial decision has confirmed the legitimacy of the right and declared that the right to be forgotten is no longer a law in the paper, but a law in action.

There are three significances of the Google Spain case, compared with the right to be forgotten proposed previously. First, it has shaped Google as a data controller. Second, it expanded the applicable condition to disclosed information by third

of personal data and on the free movement of such data (General Data Protection Regulation) , accessible at: Texts adopted - Protection of individuals with regard to the processing of personal data ***I - Wednesday, 12 March 2014 (europa.eu)

[55] Case C-131/12 *Google Spain v Gonzalez* [2014] "Google Spain judgment", paragraph 14, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

[56] Ibid, paragraph 15

[57] Ibid.

parties legally, through extensive interpretation of the purpose limitation principle and the right to be an object (Article 14 (a) of Directive 95/46/EC). Third, the right can be exercised by removing links from the name-based search result. The content at issue remains available at the source and can be located using other search terms or through other search platforms. The right to ask Google to delist certain links only make information harder to find or obscure the connection between one's own identity and particular information concerning the person. Thus, due to the method of exercise, some scholars refer to the right to be forgotten as a "the right to delisting"[58] or "the right to obscurity."[59]

2.2.1. Search Engines as a Data Controller

The court interpreted Google as a data controller from the perspective of the actual role and influence of search engines. First, the court pointed out that search engines have played a decisive role in the dissemination of personal data.[60] Second, through integrating information, it is possible to construct a person's profile by a name-based search[61], while restricting improperly profiling is one of the incentives of the development of the modern data protection law. Third, in the information society, the interference of the Internet and search engines with the fundamental rights of data subjects is profound. In the case, the court specially emphasized the

[58] Voss, W. Gregory, and Céline Castets-Renard. "Proposal for an International Taxonomy on the Various Forms of the Right to Be Forgotten: A Study on the Convergence of Norms." *Colo. Tech. LJ* 14 (2015): 281.
[59] Hoffman, David, Paula Bruening, and Sophia Carter. "The right to obscurity: How we can implement the google spain decision." *NCJL & Tech.* 17 (2015): 437.
[60] "Google Spain judgment", paragraph 36
[61] ibid, paragraph 45

easy access provided by the search engine and its massive audience (hundreds of millions of internet users), which may pose a significant effect to the fundamental right to privacy and the protection of personal data on the basis of an individual's name[62]. More specifically, the court noticed that the harm came from the search engine, instead of the original newspaper. Since after so many years, the old issue of a newspaper has been unlikely to be accessed by people. It is due to the effort of the search engines that brings the information to the surface, which has already faded out in public eyes. In other words, the powerful search function provided by search engines has broken the spatial and temporal boundaries of information spread on the network, which makes the information that might not be discovered by third parties become visible. As far as its influence is concerned, the impact of Google's processing on the fundamental rights of the data subject, especially the right to privacy, is far more profound than the original publication behavior. Thus, the role of search engines is not as a purely "intermediary" that indexes and provides access to internet users, but a data controller that provides "value-added processing" during the secondary publication. By organizing, combining, the search engines ultimately profile an individual based on its name-based search service.

Following this mind, the court determined the nature of the content location service provided by search engines as information dissemination, which is an independent, additional behavior from the original publication of information, thus search engines service provider is a data controller who determines the purpose and

[62] "Google Spain judgment", paragraph 80

means of information processing[63]. In other words, due to its decisive role in the overall dissemination, Google was confirmed its legal status as a data controller described in Directive 95 and subjected to the European data protection framework. It is a major step forward in adapting the data protection law to the current social-technological environment, a world where "you are what Google says you are"[64]. Thus, EU citizens are empowered to ask Google directly to remove their personal information without going through expensive and time-consuming litigation procedures.

2.2.2. Expand to Information Legally Published by Third Parties

Although Directive 95 does not explicitly stipulate a right to erasure, some provisions already implied situations in which data should or could be deleted. Article 6 of the directive 95 declares the data minimization principle that the processing of personal information must be appropriate, relevant, and necessary for the purpose of processing for which the data were collected or for which they are further processed[65]. Article 12 (b) of the directive is the most direct provision related

[63] ibid, paragraph 93

[64] Jones, Meg Leta. "You are what Google says you are: The right to be forgotten and information stewardship." *International Review of Information Ethics* 17 (2012).

[65] Article 6: The controller should ensure the data processing is complied with the following standards:

a) fairly and lawfully,

b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purpose shall not be considered as incompatible provided that member states provide appropriate safeguards

c) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed

to the right to erasure, that when the processing does not comply with the provisions of this directive, in particular, because of the incomplete or inaccurate nature of the data, the data subject can have the right to rectification, erasure or blocking of the data. Article 12(b) defines the nature of the pre-existing right to erasure as a tool against non-compliant of fair processing.

In Googles Spain, the CJEU broadly interpreted the meaning of "inaccurate" data. The court illuminated that information may become "inappropriate, irrelevant or excessive" for the processing purpose at the current moment due to the elapse of time, although the information at issue is accurate at the time of publication.[66] In this case, it is also counted as a failure to meet the requirement of Article 6 in directive 95. Thereby according to Article 12(b), it is eligible to be deleted. Thus, by pointing out initially lawful information may become illegal because it is "inappropriate, irrelevant or excessive" over time, the scope of the right to be forgotten has been significantly expanded. In other words, the court deduced the existence of the right to be forgotten by interpreting the "purpose limitation" principle as a dynamic test that is not only applicable to the initial data processing but also to the subsequent processing.

d) Accurate and where necessary, kept up to date, every reasonable step must be taken to ensure that date which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer period for historical, statistical or scientific use.

[66] "Google Spain judgment", paragraph 92

In addition, according to the Article 14(a), the data subject may object to data processing in cases referred to article in Article 7(f) on "compelling legitimate grounds relating to his particular situation." If the objection is justified, the processing must be stopped. Since the legitimate basis for search engines to collect and process personal information, usually falls within the Article 7(f) of the directive,[67] the data subject can invoke Article 14(a) to object to search engines' search service. In the situation of invoking the right to object, it is necessary to weigh the data subject's fundamental rights against the economic interest of the search engine on a case-by-case basis. In this case, the Court pointed that data subject's fundamental rights (particularly the right to respect of privacy and family life and the right to data protection which enshrined in the Article 7 and 8 of the European Charter of Fundamental Rights) generally override the economic interests of the operate of the search engine, as well as the interest of the general public in finding

[67] Article 7 of directive 95/46/EC: Personal data may be processed only if:

a) The data subject has unambiguously given his consent; or

b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or

d) processing is necessary in order to protect the **vital interests** of the data subject; or

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interest is overridden by the interests for fundamental rights and freedom of the data subject which require protection under article 1(1)

that information[68]. In other words, the general rule set in the case shows the paramount value of the individual's private interest. Although if the subject is a public figure or plays an important role in the public, the situation may be reversed.

Thus, although the google Spain decision is made based on the erasure mechanism in the Directive 95, the CJEU interpreted it in a broad way. The traditional right to erasure under the data protection has a procedural nature and is targeted as the collection or processing of information that lacks a legal basis. In this sense, the traditional right to erasure does not deal with the relationship between memory and oblivion, but is related to the fair processing principles, such as data quality principle, purpose limitation principle and so on. The right to be forgotten established in the Google Spain case brings the right to erasure to the online environment and grants the dynamic attribute to the data quality principle, with the spirit of protecting fundamental rights, including the right to privacy and the right to informational self-determination.

2.2.3. Delisting and Contextual Integrity

The effect of delisting can be justified by the theory of "contextual integrity" proposed by Professor Helen Nissenbaum. With the advent of web 2.0 and powerful search engines, what data subjects lose is the assurance that the internet will present information about them in an appropriate context.[69] According to Nissenbaum's

[68] "Google spain judgment", paragraph 97.

[69] de Mars, Sylvia, and Patrick O'Callaghan. "Privacy and search engines: forgetting or contextualizing?" *Journal of Law and Society* 43.2 (2016): 257-284.

interpretation, there are at least two types of informational norms: Norms of appropriateness and Norms of flow or distribution. When personal information flows among different parties, each context is correlated with specific informational norms. A breach of either the norms of appropriateness or the norms of flow or distribution will lead to an occurrence of privacy invasion.[70]. The Unconstrained flow of information may generate some "unexpected results," sometimes even raise a negative impact on the data subject. In this sense, the theory of contextual integrity can justify imposing restrictions on the distribution of personal information in search engines.

In the Google Spain case, Mr. Costega's information about a real-estate auction of his property is undoubtedly appropriate in the context of T1: the year 1998. At the time T1, the information is relevant and has public interest. However, when considering the information in the context of T2: 12 years later, the information became inappropriate to be further disseminated as it is no longer relevant and serves public interests. Thus, the information is less appropriate for reappearing in the public domain. Thus, there is a sound argument that the right to be forgotten cannot be narrowly understood as a right to delete information on the internet to make it impossibly accessible, but about imposing control on the access to information.[71]

2.3. Integration in the GDPR: Article 17

In 2016, the General Data Protection Regulation (GDPR) was finally adopted

[70] Nissenbaum, Helen. "Privacy as contextual integrity." *Wash. L. Rev.* 79 (2004): P138.

[71] de Mars S, O'Callaghan P. Privacy and search engines: forgetting or contextualizing? [J]. Journal of Law and Society, 2016, 43(2): p269.

and the right to be forgotten appeared again in the final text of GDPR The special reference to "the right to be forgotten", according to the Council, was due to the necessity to adapt the right to erasure in a digital context.[72] Thus, in terms of the evolution in the legislative history, corresponds to Article 17 of GDPR, the right to be forgotten is mainly embodied in the first three grounds of Article 17.1 (No longer necessary, withdrawing consent, right to object). It is worth noting a shift of the burden of proof in the stipulation of the "right to object" under the GDPR. When raising an objection under Article 17.1.c, a data subject only needs to provide a "particular situation". According to the guideline offered by the European Data Protection Board (EDPB), some examples can be qualified as particular situations such as "creating detriment for applying for a job, or undermining his or her reputation in his or her personal life".[73] On the other hand, it belongs to the data subject to demonstrate there are compelling public interests in retaining the information.[74] Thus, it provides more inclined protections for internet users.

Moreover, in consideration of multiple copying and cross-reference of data processes, it is not sufficient to protect the personal data by only deleting data in the source. Thus, in order to effectively control the further publication or dissemination of one's personal information, Article 17(2) required that the data controller who has

[72] Statement of the Council's reasons: Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), EUR-Lex - 52016AG0006(02) - EN - EUR-Lex (europa.eu)

[73] "Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the GDPR" issued by European Data Protection Board on 2 December 2019, accessible at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en

[74] European Data Protection Board (EDPB) , Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR

made the data public, and if the data is satisfied for erasure, shall take an extra obligation to "take all reasonable step" to inform third parties who may have copied or replicated or linked to those personal data. The second paraphrase of article 17 is totally newly added in the GDPR, which also reflects the spirit of the right to be forgotten to control further dissemination[75].

Therefore, with the enactment of the GDPR, the right to be forgotten has been officially recognized in the statutory law after years of controversy.

3. Summary: Value of the Right to Be Forgotten

By tracing the evolution of the right to be forgotten in the history of European legislation, the right to be forgotten is developed based on the European's data protection framework. The right to be forgotten can be broadly regarded as a right to request deletion or restriction of the processing of personal data in the online environment. However, the right has undergone an expansion both in terms of when and against whom the right could be invoked. The scope of the right to be forgotten has been expanded from withdrawal information posed by data subjects themselves to personal information that has been lawfully processed by a third party. And the subject of the obligation was also expanded to search engines due to their decisive role in the dissemination.

The relationship between the right to be forgotten and the right to erasure is confusing. Through comparing the right to erasure in the history of the European

[75] Some scholars believe the right to be forgotten just belongs to the Article 17(2). See Ausloos, Jef. *RIGHT TO ERASURE IN EU DATA PROTECTION LAW*. OXFORD University Press, 2020.

data protection system the novel right to be forgotten, we found out that the traditional right to erasure (in a narrow sense) and the right to be forgotten is closely related but not synonymous. The main difference between the right to be forgotten and the right to erasure lie on the ground for erasure, applicable environment and the effect of implementation.

First, the traditional right to erasure has a procedural nature and is targeted as the collection or processing of information that lacks a legal basis. However, by reviewing the legislative history of the right, in the discussion of the right to be forgotten, it never refers to situations where the initial data processing was lack of legitimate grounds. Instead, the core of the right to be forgotten is the discussion about whether the previous legally collected data can be further processed or disseminated. In this sense, the added value of the right to be forgotten is that it provides data subjects more informational autonomy to re-exam subsequent data processing in facing the eternity effect of the internet. More specifically, on the basis of the principle of data minimization principle and Google Spain case, GDPR stipulated irrelevant, incorrect or unnecessary data in respect to the purpose of processing as the first scenario of the application of the right to be forgotten. Furthermore, the right to be forgotten further added removal situations based on the withdrawal of consent by giving data subject a second chance to restricting processing after one quick click of the consent button and when a data subject raises an objection to a particular processing behavior.

Second, the traditional right to erasure acts in the situation of automated processing, as a defense to the massive collecting by tech giants or bureaucracy.

However, the right to be forgotten can be applied to the online environment.

Third, the effect of the excise of the right to be forgotten is more nuanced and varied than the right to erasure. Deletion is only one among the multiple choices. Delisting, flagging, updating or correction, restricting access can also be taken as alternative ways to achieve an effect of forgotten to some extent.

The below table summarizes the similarities and differences between the right to be forgotten and the right to erasure (in a narrow sense).

		The right to erasure	The right to be forgotten
Similarity		Both for protecting personal information, and for deleting information	
Difference	Grounds for erasure	Processing lack of a legal basis; "When the processing does not comply with provisions of the directive"	Work on lawful ground: (No longer necessary, withdrawing consent, right to object) In facing the eternity effect of the internet, an opportunity to exam subsequent data processing after data has been lawfully collected
	Applicable Environment	Automated processing, Data of user behaviors on the web	Online environment Personal information created by others or by the data subject themselves
	Effect	Erasure	More nuanced: delisting, flagging, updating (may be further developed in any form, that achieves an effect of obscurity)

Table 1 Comparison between The Right to Erasure and The Right to Be Forgotten

From the Google Spain case, the jurisprudence behind the right to be forgotten is based on both “informational self-determination” as enshrined in Article 8 of the EU Charter of fundamental rights and the “forgiveness and the preservation of tranquil of life” in the Article 7 of the charter. Balancing among each conflicting interest is always present in the decision. The balance between conflicting rights and interests will be discussed further in the next chapter.

In order to facilitate the following discussion, we summarize that the right to be forgotten in the EU has three characteristics. First, the information required by the right to be forgotten is legally circulating on the internet. Second, the right to be forgotten is directed to all data controllers, including information collectors, information publishers, and search engines. Third, the information targeted for deletion is “Inadequate, irrelevant or no longer relevant or excessive”.

Chapter 3 Value Conflict: What is worth forgetting?

The legal challenge has never been to identify which interest needs to be protected, but rather how to balance the competing interests that are also worth protecting.[76] Chapter 3 analyzes the value conflict of the right to be forgotten and explore what kinds of data are worth forgetting, based on guidelines given by European data protection authority (Article 29 Working Party) in implementing the right to be forgotten, as well as relevant case laws.

1. Digital footprint and digital shadow

According to the creator of personal data or content, Professor Koop categorizes data into digital footprints (data generated by users themselves) and digital shadows (data about users created by others). According to an IDC report, the number of digital shadows has exceeded digital footprints, which means that more information about users is created by others than by users themselves[77]. Moreover, with the practice of big data technology, more and more information about users (digital shadows) in the future may not even be generated by humans, but by algorithms (e.g.., Issue of automated suggestion function of search engines in the algorithmic

[76] 苏力.隐私侵权的法理思考——从李辉质疑文怀沙的事件切入[J].清华法学,2019,13(02):第112 页

[77] IDC, *The Digital Universe Decade* (2010) available at http://www.emc.com/collateral/demos/microsites/idc-digital-unmv erse/iview htmn (accessed 1Nov 2011)

society. Therefore, in the era of big data, the issue of digital shadow should be at least received equal attention as that of digital footprints[78].

Jef Asloo further divided User-generated data (digital footprint) into passively created data and actively created data such as expressive content authored by users on their social media. The former categorize may include data such as location data or cookies generated when using certain services provided by data controllers. The deletion request for the data passively generated by users is less controversial. And the relevant regulation on the transaction of this kind of data is relatively mature. Thus, this article focuses on the discussion of the deletion of content created by users themselves and digital shadows created by a third party. Under the traditional privacy framework, information that has been published is usually cannot be protected, which is precisely the kind of information that the right to be forgotten aims to work on. The below table shows the categorization of data.[79]

	Internal (created by users)		External (created by others) (Digital shadow)	
	Data (passive created by users) (Digital footprint)	Content (Active created by users)	Data	Content
Initial	Clickstream	Tweet	N/A	Tweet
Down stream	Click stream	Retweet	N/A	Retweet

Table 2 Categorization of Data

[78] Koops, Bert-Jaap. "Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice." *SCRIPTed* 8 (2011): 229.

[79] The table is from the article Ambrose, Meg Leta, and Jef Ausloos. "The right to be forgotten across the pond." *Journal of Information Policy* 3 (2013): at p15

Thus, the question going to discuss in this part is whether the data subjects still have control over their personal content after it is posted to the internet and, if yes, to which degree the control can extend. After all, the right to be forgotten represent an effort to bring information that already entered the public domain back to the private domain again under specified circumstances.

2. Conflicting interests and rights

The right to be forgotten is not an absolute right. Instead, balancing is an inherent part of the Right to Be Forgotten. Article 17 (3) stipulates five kinds of exceptions that the unconditional removal obligation specified in article 17. (1) Shall not apply. They are processing (a) for exercising the right of freedom of expression and information, (b) for compliance with a legal obligation or in the public interest of official authority vested in the controller, (c) for the public interest in the area of public health, (d) for archiving purpose in the public interest, scientific or historical research purpose or statistical purpose, (e) for the defense of the legal claim.

2.1. Freedom of Expression

The conflict between the freedom of expression and the right to be forgotten is at the heart of the controversy surrounding the novel right. It is also the reason that hinders the development of the right to be forgotten in the United States. In the United States, where freedom is highly respected, comparing personal dignity, the constitutional spirit of freedom of speech has been respected in a more sacred and

unshakable status. Scholars concern the right to be forgotten has a risk of being abused as a means to impose censorship. For this reason, the right to be forgotten must be balanced well with freedom of expression. The first derogation of the right to be forgotten is pointed to freedom of expression, especially with respect to processing carried for the journalist, artistic or literary expression.

Each legal system handles such a conflict in different ways. On the other side of the Atlantic, the right to be forgotten can coexist alongside the freedom of speech in Europe,[80] especially the jurisprudence of ECtHR is relevant is balancing private interest and public interest in access to information. Behind the transatlantic clash is the value disparity between liberty versus dignity in traditional privacy culture[81]. The theoretical risk of the right to be forgotten in balancing with freedom of expression has largely determined the ultimate destiny of the right.

The public's right to know is also closely linked with the freedom of speech. The realization of the public's right to know depends on two aspects: First, it depends on the freedom of expression of traditional media. Second, the public's right to know depends on the free flow of information. The right to be forgotten makes public information re-incorporated into the private domain, which may restrict/disturb the free circulation of information, therefore, violates the public's right to know. Therefore, the right to be forgotten must have a certain degree of derogation in this

[80] Singleton, Shaniqua. "Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD." *Ga. J. Int'l & Comp. L.* 44 (2015): 165.

[81] The concept of privacy in the United States is liberty-oriented, particularly the freedom of individuals in the face of governmental authority. Contrary to a deep wariness of government, United States citizens have full respect for market and technology and value industry self-regulation. See: Whitman, James Q. "The two western cultures of privacy: Dignity versus liberty." Yale LJ 113 (2003): 1151.

dimension.

2.2. Public interest

On the other end of the scales of data protection is public interest. Especially for data that has already entered the public domain, they naturally carry a certain degree of public interest, more or less. A proper and effective data protection framework must take into account the relevance between individuals and society. As far as society is concerned, the free flow of information is the key to the normal operation of a society.[82] Without the free flow of information, effective communication is impeded, further hindering the formation of reasonable social norms.

In contemporary society, governments are increasingly adopting modern technologies to collect and use personal information for public interest reasons, such as the need for public security, government information disclosure, judicial information disclosure. While the right to be forgotten has given citizens a great deal of control over their information. Therefore, the exercise of the right to be forgotten needs to be weighed against the public interest protected by official authority behaviors.

Moreover, the benefit of removing personal information needs to balance with the public interest in archiving, scientific or historical research purposes, or statistical purposes. History is the common property of the whole society. Thus, no one can

[82] Post, Robert C. "The social foundations of privacy: Community and self in the common law tort." *Calif. L. Rev.* 77 (1989): 957.

prohibit the description of historical events based on "control" over their personal data. In addition, in the case of withdrawal of consent, the effect of withdrawing consent does not necessarily lead to the removal of contested data. In the field of Biobank, the complete deletion may result in a waste of resources[83]. Some research data can be archived for secondary analysis[84].

3. Balancing mechanism

In carrying out specific balancing in individual cases, the principle of proportionality combined with the specific balancing criteria is mainly adopted in the EU's practice of the right to be forgotten.

3.1. Principle of Proportionality in data protection

The principle of proportionality has been highly important in interpreting data protection law by the European Court of Justice[85]. The principle of proportionality includes three criteria: Suitability, necessity, and balancing. The suitability principle emphasizes the relevance of the purpose and means. The relevance here only requires that the means contribute to the realization of the goal and does not require that the means must be able to realize the goal. For example, in the case of the right to be forgotten, if the goal is to achieve an effect of being forgotten, the means of delisting

[83] Kaye, Jane. "The tension between data sharing and the protection of privacy in genomics research." Annual review of genomics and human genetics 13 (2012): 415-431.
[84] Parry, Odette, and Natasha S. Mauthner. "Whose data are they anyway? Practical, legal and ethical issues in archiving qualitative research data." *sociology* 38.1 (2004): 139-152.
[85] Tranberg, Charlotte Bagger. "Proportionality and data protection in the case law of the European Court of Justice." *International Data Privacy Law* 1.4 (2011): 239-248.

fulfills the suitability principle since it reduces the visibility of content. The necessity principle requires choosing the less intrusive one among all the means that are capable of producing the desired result. For example, if the original website agrees to anonymize or delete a part of controversial content while keeping other parts intact, the less invasive means to freedom of expression should be selected. The balancing principle takes a subjective approach to the question of whether the proportionality between the protected interest and incurred costs is justified. The balancing principle is the most critical and difficult part which belongs to value judgment.[86]

The principle of proportionality itself is still relatively abstract. Therefore, it still leaves a large space for the judge's discretion. Thus, it is also necessary to consider multiple factors to make a fair and reasonable judgment. The following specific criteria can further complement the lack of objectivity and normalization brought by the principle of proportionality.

3.2. Specific criteria

The EU's data protection authority Article 29 Data Protection Working Party (hereinafter referred to as "Article 29WP") has played an important role in its interpretation of the standard of the "Inadequate, irrelevant or no longer relevant or excessive" proposed in the Google Spain case. In November 2014, Article 29 WP published a guideline in the implementation of the right to be forgotten and specifically provided 13 "common criteria" which can be used as a flexible toolbox

[86] 郑晓剑.比例原则在民法上的适用及展开[J].中国法学,2016(02):第 146 页

during the decision-making process. These 13 criteria will evolve over time, and none of them is conclusive.[87] Moreover, In February 2015, Google published an instructive and an operable advisory report with the reference of the Article 29 Working Party's guideline[88]. Based on the Advisory Council Report, the advisory

[87] See the "Guidelines on the implementation of the court of justice of the european union judgement on "Google Spain and INC V. AEPD and Mario Costeja Gonzalez C-121/12. And The 13 criteria are:

1. Does the search result relate to a natural person – i.e. an individual? And does the search result come up against a search on the data subject's name?
2. Does the data subject play a role in public life? Is the data subject a public figure?
3. Is the data subject a minor?
4. Is the data accurate?
5. Is the data relevant and not excessive?
   a) Does the data relate to the working life of the data subject?
   b) Does the search result link to information which allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant?
   c) Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?
6. Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?
7. Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?
8. Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?
9. Does the search result link to information that puts the data subject at risk?
10. In what context was the information published?
    a) a. Was the content voluntarily made public by the data subject?
       b. Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?
11. Was the original content published in the context of journalistic purposes?
12. Does the publisher of the data have a legal power – or a legal obligation– to make the personal data publicly available?
13. Does the data relate to a criminal offence?

[88] Luciano Floridi, Sylvie Kauffman, et. "the advisory council to google on the right to be forgotten" (hereinafter "Advisory") , 6 February 2015, accessible at: https://static.googleusercontent.com/media/archive.google.com/zh-TW//advisorycouncil/advisement/advisory-report.pdf

council also provided four criteria for accessing delisting requests: data subject's role in public life, the nature of information, source, and time. Therefore, based on these two documents, the following sub-section will examine the criteria for balancing the conflicts of interests underpinning the right to be forgotten and citing relevant case laws as supporting materials.

3.2.1. Data Subject's role in public life

Data subject's role in public life affects the balance between the right to be forgotten and freedom of expression. According to the attributes in playing a public role, data subjects can be further divided into public figures and limited or context-specific role in public (or involuntary public figures)[89]. The former includes celebrities, sports stars, political persons whose right to be forgotten relatively difficult to get affirmed. While the latter refers to who has been put into the public eyes because of events beyond their control. In the latter situation, the balancing result is uncertain and needs to consider other factors.

3.2.2. Nature of information

According to the nature of information, the advisory council divides information into "Type of information that biases towards individuals' privacy interest" and "Type of information that biases toward public information" in an enumerated way.[90] Logically, although all types of personal information are

[89] "Advisory", at p8
[90] "Advisory", at p9-p13

deserving of protection, it doesn't mean that all types of personal information should be treated equally.

Information that bias toward *an* individual's strong privacy interest	Information that bias toward a public interest
1. Information related to an individual's intimate or sex life. 2. Personal financial information. 3. Private contact or identification information. 4. Information deemed sensitive under EU Data Protection law. 5. Private information about minors. 6. Information that is false, makes an inaccurate association or puts the data subject at risk of harm. 7. Information that may heighten the data subject's privacy interests because it appears in image or video form.	1. Information relevant to political discourse, citizen engagement, or governance. 2. Information relevant to religious or philosophical discourse. 3. Information that relates to public health and consumer protection. 4. Information related to criminal activity 5. Information that contributes to a debate on a matter of general interest. 6. Information that is factual and true. 7. Information integral to the historical record. 8. Information integral to scientific inquiry or artistic expression.

Table 3 Nature of Information

For example, the more sensitive, more private the information is, the more it favors the privacy interest. On the contrary, the information with a nature of political, religious, or philosophical discourse or speech, or professional information favors the public interest. The above categorization improves the absolute theory of "public" and "private" with more nuanced dimensions and helps to quickly identify the sensitivity of personal information.

Based on Google's transparency report[91], the success rate of delisting requests involving professional information or professional wrongdoing is relatively low, roughly remaining around 10-20%. For example, in the Manni case[92], Manni believed that the company registration information, which related to facts in more than ten years ago, has caused him to lose potential buyers, therefore claimed for the deletion of the information. The European Court stated that the company registration information belonged to a person's professional information and was disclosed voluntarily by the individual himself. In other words, the legitimate and correct professional experience does not have the sensitivity required for privacy protection, so the information should not be deleted.

3.2.3. Source

The source of information and the motivation for publishing the information also should be considered in the balancing. Assuming the information comes from an authoritative and professional news organization, there may be substantial public interest contained in the information, such as information involving crime, professional information, or professional wrongdoing. It is also true in cases where the source of information is government publication or bloggers or individuals with

[91] https://transparencyreport.google.com/eu-privacy/overview?hl=en

[92] See Case C398/15, Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=80219

substantial credibility.

According to Google's Transparency Report, the information with the highest percentage of deletion is information on Directory, which aggregates information such as postal addresses or phone numbers for businesses or individuals. Because such information is objective personal information and often lack a clear purpose of processing, it is justified to be deleted. In addition, information on social media such as Facebook or Twitter also relatively favor being delisted since the majority of the information on social networks is self-authored.

3.2.4. Time

The factor "Time" is a critical element in the right to be forgotten since the initial purpose of the right is to counter the effects of long retention of personal information on the internet. In the Google Spain case, the court has noticed the effect of time on data accuracy, which data's relevance could decline over time and lead to unintended results to the data subject. What's more, in the aspect of forgiveness, although forgiveness is a virtue, either offer it too early or too late will disrupt the benefit of forgiveness.[93] Not to mention, it takes a certain amount of time for human's natural oblivion. Thus, a question could be derived from the above statements, that is, whether the data that is qualified for the right to be forgotten is conditioned by time? In other words, only information that happened a long time ago

[93] Jeffrie G. Murphy, Forgiveness in Counseling: A Philosophical Perspective, in BEFORE FORGIVING: CAUTIONARY VIEWS OF FORGIVENESS IN PSYCHOTHERAPY 41 (Sharon Lamb & Jeffrie G. Murphy eds., 2002).

is qualified for being forgotten? Then how long should be considered as a fair length? The ambiguity of the answer leaves great subjectivity and uncertainty to a decision-maker. In fact, taking time as a factor in the balancing might result in favor or against a removal request.

3.2.4.1. Time and Data Quality

The factor of time gives the right to be forgotten a dynamic characteristic. People in society are developing dynamically. If looking back at every decade of life, people may be surprised by the tremendous changes that happened to them. Therefore, it is expected that the plain name-based search would reflect such a dynamic change over time. Otherwise, it would be misleading and deserve to be deleted according to the principle of data accuracy.

However, the influence of time on the relevancy of information is a tricky issue, as well as with a certain degree of subjectivity. For example, in the United States, the value of news usually does not fade over time.[94] And in the case of A&B v El Pais,[95] the Spanish court took great pains in reasoning about the effect of time on relevance. The court provided a good suggestion for assessing the relevancy in relation to its original purpose, noting that, while the information remains true as time goes by, it might become inadequate in terms of its original purpose for which it was intended to keep the public informed of the crime. But the court failed to give a more standardized set of time to distinguish the difference between a piece of news

[94] McNealy, Jasmine E. "The emerging conflict between newsworthiness and the right to be forgotten." *N. Ky. L. Rev.* 39 (2012): 119.
[95] Spanish Supreme Court Judgment 545/2015 of 15 October 2015

in 20 years and that in 15 years[96].

3.2.4.2. Information value and the information lifecycle

A study on the factor of time in the right to be forgotten has also shown the complexity and diversity of the balancing results between public interests and personal interest carried by information among different time stages[97], thus that there is no definitive rule to determine whether the information becomes no longer newsworthy over time. Because any judgment based on the timeline solely actually negates other value of news, such as the historical or statistical value.[98] For example, for convenience of analyzing the changing balance of different interest over time, Meg leta Ambrose categorized the value of information into immediate needs and remoted needs and divided the information life cycle into three stages: Distribution phase, Record phase, and Expiration phase.[99] An immediate need is relevant to an immediate decision based on the current state of the world. In contrast, a remote need is relevant to uncovering unknown insights by reviewing the past, such as for historical or predictive study.

The study has shown the immediate and the remote need of the information changes alternately during the information life cycle.[100] For outdated information,

---

[96] Sanchez Abril, Patricia, and Eugenio Pizarro Moreno. "Lux In Arcana: Decoding the Right to Be Forgotten in Digital Archives." *Laws* 5.3 (2016): 33.

[97] Korenhof P., Ausloos J., Szekely I., Ambrose M., Sartor G., Leenes R. (2015) Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In: Gutwirth S., Leenes R., de Hert P. (eds) Reforming European Data Protection Law. Law, Governance and Technology Series, vol 20. Springer, Dordrecht

[98] 万方.终将被遗忘的权利——我国引入被遗忘权的思考[J].法学评论,2016,34(06):155-162.

[99] Ambrose, Meg Leta. "It's about time: privacy, information life cycles, and the right to be forgotten." Stan. Tech. L. Rev. 16 (2012): 369.

[100] Ibid.

the immediate need may be low, but still has a remote interest, which can be stored for historical or predictive study. Based on the current study, it is difficult to predict which information is relevant, useful, or valuable until time has passed by. Not to mention, other factors may reverse the value of data over time. For example, what if an ordinary person runs for a government officer in the future? The less valued personal data may become important again due to the change in personal identities. Thus, studies on the value of information over time would give us more insights in constructing the right to be forgotten.

With the breakthrough of data science, when the study of the relationship between data value and time can draw a practical and operational rule, the time theory approach could greatly shape the theoretical pattern of the right to be forgotten.

3.2.5. Harm: A Level of Severity and Pervasiveness?

As mentioned above, the right to object can be invoked simply based on a particular situation of the data subject. Thus, "the right exists regardless of whether the processing at issue cause harm or is prejudiced in some way to the data subject."[101] Also, it has been clearly stated in the Google Spain case that it is unnecessary for the data subject to show that the disclosure of the information in the search result caused prejudice[102].

However, although prejudice is not necessary, if there is prejudice, it is undoubtedly favor delisting. The criteria of whether the data processing causes

[101] Advisory, p5
[102] Case C-131/12 *Google Spain v Gonzalez* [2014] Paragraph 94, 96

prejudice to the data subject, or does the data have a disproportionately negative privacy impact on the data subject, is also listed as one criterion in the guidance in the WP29. For example, a disproportionate negative impact caused by a "trivial or foolish misdemeanor" which is not the subject of public debate or without wide public interest would be a favorable factor for delisting[103]. And the advisory report also stated that accessing harm to the data subject is still recommended when balancing public interest.

Thus, the standard of specific harm is still very vague in the context of the right to be forgotten.

4. Balancing scenario

After expanding the coverage of the right to be forgotten to information which is legally released by a third party, the most influential parties are search engines and online archives. Therefore, in the following two cases, we will take a closer look at how the balancing test was exercised in these two contexts.

4.1. Against Search engines: NT1 & NT2

In the guidance given by the EDPR, it has concluded that it less possible for search engines to invoke any of the exceptions listed in the 17 (3). Thus, the main defense for search engines to invoke is based on the interest of internet users in accessing the information through the search engine.

[103] See the "Guidelines on the implementation of the court of justice of the European union judgement on "Google Spain and INC V. AEPD and Mario Costeja Gonzalez C-121/12

In April 2018, the British High Court ruled a crucial case of the right to be forgotten: NT1 &NT2 v Google[104]. In the 76-page judgment, the British court established and clarified under which circumstance a person can successfully erase unwanted information from the Internet under UK law. The British Court used the 13 criteria specified in the WP29 guideline and analyzed the application of each criterion when dealing with the Google Spain compliance issue. At the same time, the two plaintiffs in the case, NT1 and NT2, both required delisting information relevant to their criminal convictions. Nevertheless, they have received opposite verdicts, which lends itself well to a comparative analysis of the factors affecting forgetting.

In the unsuccessful case of NT1, the businessman NT1 committed a conspiracy to false accounts and then was sentenced to four years. Following the 13 criteria specified in the WP29 guideline, the court found the overwhelming public interest in the case, which supports the retention of the link. First, NT1 was a businessman and is counted as a public figure with a certain public influence in society. Second, as to the relevancy of the information, the information at issue is still relevant since he continues to work in the same business, though the specific work position has changed over time. Third, the court held that crime information is historical, so it should not be measured by time. Although the crime is spent after the amendment of the rehabilitation law, it was not the case when he was prosecuted, charged, and sentenced. And even after the law is revised, if his sentence is one day longer, he

[104] Supreme Court of the United Kingdom – NT1 &NT2 v. Google LLC ([2018] EWHC 799 (QB))

would not be able to spend. Thus, the severity of his crime has justified the need for retention. Fourth, NT1 was trying to mislead the public by posting content on the network to describe him as an upright person and misstatement on the court. And NT1's attitude was arrogant, dishonest, and failure to acknowledge the guilty. Due to the above reasons, the court held that NT1 has no reasonable expectation of privacy and refused his claim.

On the other side, the fact of NT2's case is roughly similar to NT1. The plaintiff was sentenced to 6 months in prison for phone tapping and computer hacking. First, concerning the nature of the crime, the crime of NT2 is an infringement of privacy, thus has nothing to do with consumers. And NT2 has only been sentenced to six months. Thus, he has a reasonable expectation of rehabilitation. Second, as to the relevance of data, the industry that NT2 is currently engaged in is completely different from that when he committed the crime. Thus, the information is less relevant over time. Third, NT2 has pleaded guilty at an early stage and expressed genuine remorse. And he has not tried to conceal the crime fact. Fourth, as to the prejudice or negative impact: NT2 has suffered substantial damage and distress due to the information. Particularly, he has a child of school age. The information further raises a negative impact on his family. At last, the interview was based on his consent. And there are no obstacles to prevent the withdrawal consent. NT2 has withdrawn the consent, and there is no other reason to make it legitimate to continue processing personal data. Thus, the court has affirmed the NT2's request for delisting.

Compared with other personal information, the criminal record is particularly special and sensitive. The debate over whether criminal information stored on the

Internet can be forgotten has never stopped. In this case, the court adopted a specific analysis that took into account all factors. Besides, compared with the 13 criteria given by WP29, the judge also added the state of mind to the guilt during the balancing. As opposed to a severe criminal, the interest of "the right to be forgotten" should be supported when the information may have a disproportionately negative impact on the person concerned or even their family, while there is no broader public interest as time passes.

4.2. Against Original Website: ML and WW v Germany

In 2018, the European Court of Human Rights (ECtHR) made a judgment of "M.L. And W.W. vs Germany".[105] The two applicants were sentenced to life imprisonment in 1993 after murdering a famous German actor Walter Sedlmayer in 1991 and were subsequently released on parole in 2007 and 2008. The German radio station 'Deutschlandradio' published a report about the murder and the full names of the applicants were mentioned. A transcript of the report was available in the radio's archive.[106] They demanded to have their names be anonymized or removed from the transcript. In 2008, the Hamburg Regional Court upheld M.L. and W.W.'s request, noting that information was no longer relevant. In 2009, the Federal Court of Justice reversed the judgment, finding that the court had failed to consider the freedom of

[105] M.L. AND W.W. v. GERMANY *(Applications nos. 60798/10 and 65599/10)* (ECtHR, 28 June 2018)

[106] Holger Hembach, Article 8 ECHR and the 'right to be forgotten' – M.L. and W.W. v. Germany, July 17, 2018.,https://human-rights-law.eu/article-8-echr-and-the-right-to-be-forgotten-m-l-and-w-w-v-germany/

the press and the public interest in being informed about the convictions. Thus, in 2010, the two plaintiffs brought the case to the ECtHR, arguing that the failure to the anonymization was a violation of the right to privacy under article 8 of the European Convention on Human rights. The Court of Human Rights dismissed the plaintiffs' request.

It is worth noting that the plaintiff invoked the RTBF directly to the original website, instead requesting to delist the website link in the search results. The original report was protected by the freedom of Press under Article 10 of the European Convention on Human Rights. Thus, the plaintiff's request caused a direct confrontation between the right to be forgotten and the freedom of press, which is the issue the European court deliberately circumvented in the case of Google Spain. Compared with the search engine, the claim of "right to be forgotten" to the original website is obviously more difficult to affirm, since the press played a crucial role in a democratic society. Maintaining the public archives of news is necessary for educational and historical research.[107]

Besides the freedom of press of the original websites, the court further added other factors that show the public interest in retaining the news. First, the content about criminal proceedings undoubtedly contributes to a debate of public interest. Second, the notoriety of the two plaintiffs is outrageous and unforgivable. The notoriety, while diminishing over time, has not entirely disappeared. Third, the plaintiffs' previous conduct for actively exposing themselves in public has made

[107] Corcione, Elena. "The Right to Be Forgotten, between Web Archives and Search Engines: Further Steps at the European Court of Human Rights." Eur. Data Prot. L. Rev. 5 (2019): 262.

them already a public figure. Fourth, regarding the consequence of publication, the negative impact is restricted by the fact the full content is only accessible after subscription. Thus, in this case, the public interest outweighs the individuals' interest.

5. Summary

Through the above analysis, whether pertinent information can be requested to be forgotten is a result of balancing with conflicting interests. And it can be seen that the balancing test handled in Europe can be integrated into a systematic framework. The main criterion is the data Subject's role in public life, Nature of information, Source, Time, and potential or substantial Harm to the data subject. Besides, it can also borrow ample experience from the case laws in the European Court of Human rights (ECtHR) and European Court of Justice (ECJ). Thus, as said by Google's executive "learning as we go",[108] the framework is liable to evolve with the accumulation of experience.

However, on the other hand, it also reflects that it leaves substantial discretion and opens to interpretations when handling the balance between conflicting interests. For example, the effect of time could both favor or disfavor the claim of forgetting. Also, the subject's role in public life has a dynamic character. Thus, accessing what should be "forgotten" in reality "is anything but straightforward."[109]

[108] Matthew Weaver, "Google 'Learning as we go' in row over right to be forgotten", The Guardian, https://www.theguardian.com/technology/2014/jul/04/google-learning-right-to-be-forgotten

[109] Sanchez Abril, Patricia, and Eugenio Pizarro Moreno. "Lux In Arcana: Decoding the Right to Be Forgotten in Digital Archives." *Laws* 5.3 (2016): 33.

In addition, as a region with the most stringent protection of personal information in the world, the right to be forgotten under GDPR can be invoked at a relatively low threshold. Claiming relief of the right to be forgotten does not need to reach the level of severity as infringing on the right to reputation, right to privacy, or other specific personality rights. The absence of harm or prejudice to the person concerned is not determinative. As long as the information on the internet is no longer necessary and there is no legitimate reason for its continuing process, the data subject can request the data controller to remove it in order to achieve an effect of obscurity. Thus, the right to be forgotten has greatly expanded the scope of the data subject's interests. But also, due to its light burden of proof for request removal, it would cause a frequent conflict of other interests.

Chapter 4 Effectiveness: Enforcement Dilemma

As we can see from the previous chapter, the internal structure of the right to be forgotten is based on a flexible and context-reliable balancing mechanism. Theoretically, through reasonable balancing, it can achieve an ideal result of protecting the individual's interest while not disturbing other legitimate rights and interests. Thus, in this chapter, taking search engines as representatives of data controllers, we observe the obligations of search engines under the right to be forgotten and their compliance, and then outline some of the key issues involved in implementation. We find that, because of the ambiguity of the legal provisions, compared to its theoretical crisis, the enforcement issue is the biggest problem of the right.

1. Search Engines and ensuing obligations as data controller

1.1. Assess the validity of the request

A critical question in implementing the right to be forgotten is who should review the subject's deletion request. Currently, in practice, the burden is almost entirely on search engines, which grants search engines a kind of power as a new governor of the online content. It is even criticized that search Engine is now responsible for "censorship" online content, therefore, shaping our new digital and

democratic culture[110].

In handling the assessment work, Google has developed a specific system according to the data protection law with regularly updated rules and publishes its transparency report timely. Moreover, Google has organized a so-called “removal teams” to deal with these requests[111]. This removal team consisting of Google's staff is responsible for easy cases, generally. At the Brussels meeting on the right to be forgotten, the Google's Chief Legal Officer, David C**.** Drummond, acknowledged that most delisting requests are easy to solve[112]. In addition, Google also sets up a “senior google panel consisting of senior lawyers, engineers, and product managers to handle complex cases[113]. Sometimes, the senior google panel will also consult external experts for advice. In addition, it will contact the original web site for inquires or ask the requester for more information in order to make a reasonable decision. Also, Google has established an external advisory council for further advice and guidelines on making delisting decisions.

1.2. Notification

Notification, as a safeguard mechanism of “transparency,” can effectively correct errors in the inform-takedown procedure. However, the notification

[110] Abril, Patricia Sánchez, and Jacqueline D. Lipton. "The Right To Be Forgotten: Who Decides What the World Forgets." *Ky. LJ* 103 (2014): 363.

[111] Although there is no accurate number, there are roughly 100 people in the team in November 2014 consisting of lawyers, paralegal assistants, and other full-time employees.

[112] David Drummond, Chief Legal Officer, Google, Address at the Brussels Meeting of the Advisory Council to Google on the Right to Be Forgotten (Nov. 4, 2014), https://youtu.be/OTAbo3n3BJ8

[113] Lee, Edward. "Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten." *UCDL Rev.* 49 (2015): at p1040

obligation in the context of the right to be forgotten is a pretty tricky issue since there is a natural tension between the right to be forgotten and further dissemination. Any less deliberate transparency requirements may cause the right to deviate from its good practice and fail to reach its pro-privacy goal. In general, the notified objects include a third party who is processing the data, original website, and public, which will be addressed one by one.

1.2.1. To the Other Controllers

After the search engine provider supports an applicant's claim for removal, the search engines should notify other controllers who are processing the data in a "best-effort" under Article 17 (2). Leave aside the technical hurdles this step may still face, it may go against the purpose of the data subject from the perspective of privacy protection. Since the right to be forgotten requires data controllers to stop processing her information if the request is valid. Thus, the continued dissemination of information about the data subject to other controllers continuing to process data. Especially if the right to be forgotten, involves information on social media, such notification still has the potential risk to raise secondary social attention.

1.2.2. To the Original Website

The Directive 95/46/EC does not directly request search engines to routinely communicate de-listing decisions to original publishers either before or after decision makings. Although WP29 considers that it is helpful to contact the original publisher, particularly in complicated cases, so as to have a better understanding of

the circumstance of the case[114], in that case, search engines need to take all necessary measures to safeguard the data subjects' rights. Because the legitimate grounds for processing between the search engines and the original publishers have a "crucial difference." WP29 mentioned two reasons for explaining why the search engines don't need to notify the webmasters. First, removing a link from a search result in terms of a person's name only generates a limited impact in accessing the information[115]. The news can still be searched based on other search terms. Second, publishers and search engines are two independent entities. Thus, publishers cannot control a search engine to have their content indexed and displayed, or display in a particular order as they want.

1.2.3. To the Public

A notification to unspecific third parties would, in turn, stimulates the public's curiosity and thereby induces the "Streisand Effect"[116]. A typical example of the "Streisand Effect" is a case about two German criminals who asked Wikipedia to remove their names from the page of the victim, who happened be to a famous actor, Walter Sedlmayr[117]. When the two German men attempted to remove their names

[114] Article 29 Data Protection Working Party, Guidelines on the implementation of the court of justice of the european union judgment on "google spain and inc. V.agencia española de protección de datos (aepd) and mario costeja gonzáles" c-131/12 at 5 (2014), at paragraph 22.

[115] ibid, at paragraph 23

[116] "The "Streisand effect" is a social phenomenon that occurs when an attempt to hide, remove, or censor information has the unintended consequence of further publicizing the information." See Wikipedia: https://en.wikipedia.org/wiki/Streisand_effect

[117] Charles Arthur, " *Wikipedia sued by German killers in privacy claim",* The Guardian, Nov. 13, 2009, https://www.theguardian.com/technology/2009/nov/13/wikipedia-sued-privacy-claim

from Wikipedia's page based on privacy reasons, Wikipedia in the German-language version agreed with their requirement and deleted their names. After a few media reported the delete-movement, the views of the English-version page of Walter Sedlmayr, which did not delete the criminal names, dramatically increased from about 20 daily views to more than 10,000 times per day. Thus, it warns us that one possible result of exercising the right to be forgotten is that, after spending a great deal of effort by the data subject and the data controller, paradoxically, the "right to be forgotten" achieve an effect of "right to be remembered."

Thus, in order to effectively prevent unintended secondary social media attention, the GDPR requires transparency only in a way that cannot identify the requesting party. Under the regulation, the current practice of Google is to disclose the RTBF removal as a copyright removal action. It shows a little notice at the bottom of its result implies that some URLs may be missed under the data protection law[118]. And in the transparency report offered by Google only contains statistical data, such as how many requests have been received and the number of links removed. There are only a limited number of typical examples for giving a rough idea about how Google has responded to RTBF requests. Thus, only a very limited and unsatisfactory public transparency is available now.

2. Issues:

2.1. Role of Google: A Data Controller or Neutral Intermediary

[118] Danny Sullivan, How Google's new "right to be forgotten" form works: an explainer, May 30, 2014, *https://searchengineland.com/google-right-to-be-forgotten-form-192837*

2.1.1. Passive role or Active role?

By identifying the search engine as a data controller based on its search service, an issue will arise: the conflict with intermediaries' neutral and passive service position under the "inform-and-takedown" mechanism.

In traditional tort law, the responsibilities between publishers and distributors of information are different. The publishers have the ability to edit content, such as newspapers. Thus, publishers are liable for the information they displayed to the public[119]. The distributors of information only play a passive role in making the information available to others, such as public libraries. They lack actual control over the contents. Therefore, it is not easy to know the existence of infringing information. Thus, it is necessary to restrict the liability of distributors. More specifically, the distributors shall be liable only if it shows that it had actual knowledge of inappropriate content or should have known the infringing information under a reasonable presumption.

In the network infringement, the distinction between the publishers and distributors is embodied as the distinction between Internet Service Providers (ISPs) and Internet Content Providers (ICPs). ISPs, similar to the traditional information distributors, are in a passive position on the control of the contents. For example, in EU eCommerce Directive 2000 lists three types of intermediaries: mere conduit, caching, and hosting. Generally, online intermediaries are shielded from most forms of liability as long as it could take action to remove or disable access to information

[119] 韩旭至.搜索引擎对侵扰性自动提示内容的责任——兼评北京市第一中级人民法院(2015)一中民终字第 09558 号民事判决[J].私法研究,2016,20(02):249-270.

once it acquired knowledge (actual knowledge) of a legal problem by the so-called "inform and takedown" mechanism. While the ICPs have greater control over the information on the web pages, thus they are similar to the traditional publishers and can be liable directly for the contents they create.

In general, search engines for providing search services should be categorized as ISPs. Thus, as a passive role for only making published information more accessible, the search engine's liability is subordinate to the publisher's operation. However, in the case of Google Spain, the court saw Google's role in another way, which is independent of the publisher's operation. Internet users will form a brief evaluation of the individual based on the information presented in the search results.

Thus, how the intermediary liability in the future should be structured to reconcile direct liability under the data protection framework and indirect liability as a passive conduit is an issue that needs to be addressed in the development of the right to be forgotten.

There is a tendency to tailor the extent of the obligation of search engines to maintain technological neutrality. For example, in the GC and Others v (CNIL) case,[120] concerning the issue of sensitive information, since it is impossible for google to examine whether there is any sensitive data on its search result, the Court set a different regime of special categories of data applicable to search engines. That is, the compliance for the general prohibition of processing sensitive data only applied upon request of the data subject or under the supervision of authorities.

[120] C-136/17-GC and Others v Commission nationale de l'informatique et des libertés (CNIL)

2.1.2. Algorithm as Speech

Regarding Google's added value of its organizational behavior of online information as a closer role of creators will lead to another question, which is whether the search algorithms can be treated as Google's speech and thus falls within the protection of freedom of speech. For example, in American, the case of Search King v Google Technology Inc (2003)[121] has confirmed that Google's algorithm is an opinion and, therefore, it is protected by the first amendment law. However, it brings back the discussion of the conflict between data protection and freedom of speech, which can be resolved through a balancing mechanism.

2.2. Fair Balancing: An Illusion?

2.2.1. Difficulty in Striking A Balancing

First of all, balancing tests are inherently embedded in the right to be forgotten, which are almost inevitable. Some of the balancing are simple. Some are complex, especially for balancing involving privacy interest. Actually, balancing privacy interests with the public interest is not a simple matter even in the view of professional judges, not to mention the task for search engines that have not enough legal knowledge. In addition, when evaluating the necessity relative to original processing purposes, it is not so straightforward to find out whether the information is irrelevant or outdated. Compared with the original website, search engines are not professional media. Thus, they are not equipped with the same level of professional

[121] *Search King, Inc. v. Google Tech., Inc.*, 2003 W.L. 21464568, 2003 U.S. Dist. L.E.X.I.S. 27193 (2003).

qualities in dealing with the scope of the disclosure. Thus, whether search engines can become a qualified judge and strike a balance is still doubtful.

2.2.2. Over-Compliance: Uncertainty and Stick

From the previous analysis, it can be seen that the data worthy of forgotten is not an objective standard. On the contrary, the standard is relatively abstract and subjective by adopting a flexible framework for balancing different interests, which brings a lot of legal uncertainty on the outcome of each removal request. In addition, there is a severe penalty for untimely response and the potential litigations following decisions of rejection[122]. Thus, in facing the legal uncertainty and awaited stick, the data controller is virtually given an incentive of over-compliance with the data subjects' takedown request. In the most extreme case, the data controller may even skip the balancing test and direct block entirely legitimate content when receiving removal applications, which will impose inestimable harm to the abundance of online information.

2.2.3. Heavy Burden

At the same time, because the balancing can only be conducted on a case-by-case basis manually, it cannot be automated processing through a pre-filtering measure like that in the field of copyright infringement or trademark infringement. Google is expected to update its balancing criteria from time to time according to the

[122] Under the GDPR, potential penalties are up to 1% of a company's global annual revenue.

complex situation in reality, which bears high compliance costs. In the report from 19 member states after two years of implementation of GDPR[123], one criticism is that the high enforcement expense. Most countries complain that their law enforcement budgets need to be increased, as well as recruiting more professionals to meet the requirement of data protection law.

2.2.4. Due Process

There is no legal hearing available for the relevant third party in such a private content censorship model. Without adequate defense mechanisms provided, links to the contents can be removed from search results without the content provider's knowledge. It may make sense in terms of data protection, but from the perspective of due process and speech protection, it is obviously problematic for taking down content based on an accusation on one side without any notice to the accused party or providing opportunities for defense[124].

2.3. Limited Effect

Finally, from the presentation of the results, the effect of delisting is very limited. For data in closed systems like healthcare sectors or the banking industry, to achieve the erasure of data is workable in principle, although it is not without any challenges. However, in an open system such as the internet, data erasure is almost impossible.

[123] Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States, https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf

[124] Keller, Daphne. "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation." *Berkeley Tech. LJ* 33 (2018): at p338

Since there are different subject can continuously upload data from local, the deletion job is similar to a kind of Sisyphus's work[125]. Therefore, although requesting delisting vis-a-vis search engine effectively reduces the scope of dissemination and damage to the data subject, there is still a great distance to achieve an effect of "forgetting." It is at most a kind of subjective deletion. Information is still available on the internet and can be linked with other search terms or using other search engines. In addition, from the geographical scope of the application, in the ruling of Google v CNIL, the decision clarified that the right only applies within the European territory which undoubtedly increases of the risk of "Streisand Effect".[126] Although the court declared that Google should "prevent or at the very least seriously discourage" users from searching elsewhere for the link in order to ensure the enforcement of the right, it failed to suggest any effective measures. Such an ambiguous rule only puts Google in a dilemma and leaves the enforcement up in the air. Relative to the tremendous labor and economic cost, the efficiency of the implementation is questionable.

Thus, the right to be forgotten has been criticized as having little effect in protecting personal information, but exacerbating information asymmetries. It widens the gap between those who can afford to spend resources to obtain information and those who do not know how to find it directly and fall back on general search engines. It is equivalent to tax to people who want access to data in

[125] Druschel P, Backes M, Tirtea R. The right to be forgotten-between expectations and practice[C]//I Congreso sobre retos sociales y jurídicos para los menores y jóvenes del siglo XXI. 2013: 5.

[126] G*oogle Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*, case C-507/17

the public domain, which goes against the purpose of openness of the internet.[127]

3. Summary

This chapter discussed the enforcement dilemma of the right to be forgotten from the perspective of search engines. It revealed the key issues such as lack of transparency, lack of oversight, and lack of error correction mechanism, which would pose a significant threat to freedom of expression and operative burden when being put into practice.

The complexity of the right to be forgotten began to unfold since the search engines were identified as the data controller in the Google Spain case. It is conceivable the enforcement challenges will be leveled up if the right applies to Facebook, Twitter, or any other platforms for user-generated content. The effectiveness of the right to be forgotten has yet to be tested and refined over time.

[127] Post, Robert C. "Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere." *Duke LJ* 67 (2017): 981.

Chapter 5 China's Privacy and Data Protection Framework

Chapter 5 sketches the legal framework of privacy and data protection law in China, comparing the "Right to Erasure" in china with the Right to Be Forgotten in the EU. More specifically, this chapter first draws an overview of the legal protection of online privacy and examines whether search engines are required to remove or block search results that invade privacy. It further addresses legislative measures and trends of personal data protection in recent years, then assesses whether such legislative actions imply the right to be forgotten.

1. Online privacy protection

1.1. Cultural backdrop

Compared with the history of privacy protection in Europe and the United states which for more than 100 years, China did not have a tradition of privacy protection. Affected by the cultural traditions of Confucianism and collectivism, personal freedom, the most important cornerstone for forming the right to privacy, has not been valued.[128] As Confucian culture advocates, the traditional cultural concept of "The interest of the state and social are superior to those of the individual" has been deeply rooted in the protection of privacy. Although the value of the self-

[128] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(01):130-149.

development of personality has been reflected in traditional Chinese culture,[129] the reason behind the value is different from western countries. The purpose of self-development or introspection advocated by Confucian culture is not for discovering uniqueness, but in the hope of finding what he has in common with other men.[130] In other words, the goal of introspection is still for promoting connections with the public, which is consistent with the collectivist culture.

In the early years of the new nation, in order to strengthen the organization of society and to increase the solidarity and efficiency of social groups, Chinese society emphasized collectivism in policy, and implemented the state-owned and planned economic system in the economy. As a result, citizens enjoy weak privacy interest. In addition, the media resource is strictly controlled by the state, which means that social organization or individual citizens other than government and quasi-governmental agencies did not have access to media resources. Therefore, there was a little conflict of privacy interests among citizens, so as the need for privacy protection.[131]

In judicial practice, some behaviors which are obvious infringements of the right to privacy did not receive judicial protection due to the influence of traditional ethical thinking that overemphasizes social interest, which weakens the public

[129] For example, when Zilu asked Confucius for advice on how to become a complete and mature human being, Confucius believed that only when a person grows up to the point where he can require himself with the standard of "benevolent"(仁) and "righteousness"(义), will he possess the essence of a human being and become a man of noble character. With this vein, we can see the personality embodies the process and value of a person's continuous development, until forming a personality of a gentleman. 白奚."仁者人也"——"人的发现"与古代东方人道主义[J].哲学动态,2009(03):77-79.

[130] Whitman, Christina B. "Privacy in Confucian and Taoist thought." (1985). at p96

[131] 吴伟光.从隐私利益的产生和本质来理解中国隐私权制度的特殊性[J].当代法学,2017,31(04), p54

consciousness of the concept of privacy.[132] In the meantime, the dilemma of regulating the problem of human search reflects the conflict between the culture of Chinese netizens and the privacy of individuals. The Chinese Netizens, inheriting the tradition Chinese culture of acquaintance community, has a strong tendency to form an ethical community online to expose individuals' scandals.[133]

Therefore, the understanding and construction of china's privacy system cannot be separated from the consideration of traditional Chinese collectivism, which is in sharp contrast with Europe's more individual-oriented privacy protection framework.

1.2. Legislation on the right to privacy

Since the implementation of the "reform and opening-up" policy in 1979 and the rapid development of the internet, internet users' ability to disclose themselves and others' information has improved significantly. In the meantime, many market-oriented media have emerged, which have changed the pattern of traditional media dominating the news market. Privacy protection began to gain attention.

The right to privacy in china is not directly stipulated in the Constitution, but Article 37, 38, 39, and 40 of the Constitution in 1982 has guaranteed protection regarding the general personal dignity of citizens and the specific protection to people's bodies, houses, letters. "Illegal searches of citizens' bodies are forbidden (Article 37)", "Human dignity shall not be infringed (Article 38)", "illegal searches or illegal intrusions into citizens' houses are forbidden (Article 39)" "No

[132] 张礼洪.隐私权的中国命运——司法判例和法律文化的分析[J].法学论坛,2014,29(01):11-19.
[133] 刘晗.隐私权、言论自由与中国网民文化:人肉搜索的规制困境[J].中外法学,2011,23(04):870-879.

organization or individual may violate the freedom and confidentiality of citizens' communications for any reason (Article 40)". Therefore, since the Constitution does not explicitly establish the right to privacy, privacy protection is scattered in various departments of law, with a particular focus on civil protection.

Before 2009, infringing on privacy normally sought legal remedies under the protection of the right to reputation or through inclusion within a "personality right" as a kind of civil interests. The "General Principle of civil law" of 1986 only stipulated the right of the name, right of reputation, right of portrait, which leaves no words to the protection of privacy. In order to fill the hidden loophole in the General Principle of civil law, the Supreme People's Court issued a judicial interpretation which stipulated that publicizing other person's privacy in writing or orally, or publicly scandalizing other person's personality by fabricating facts or damaging other person's reputation by means in a manner of insult or defamation, thereby causing a certain impact, those above act shall be considered an infringement of a citizen's right to reputation".[134] However, the problem with using an analogous approach to the right to reputation is the heterogeneity between the right to privacy and the right to reputation. The disclosure of privacy does not necessarily lead to a decrease of a person's social reputation. On the contrary, sometimes it even leads to an increase in a person's reputation.

[134] Article 140 of "Opinion of the Supreme People's Court on several issues concerning the implementation of the "General Principle of the civil law of the People's Republic of China.

Until 2009, with the promulgation of the "Tort liability law", the right to privacy was formally confirmed as an independent and specific civil right.[135] And in the "General Principle of the Civil Law" enacted in 2017, the right to privacy has been officially recognized as one of the statutory personality rights in Article 110.[136] In May 2020, the Tort Liability Law was codified in the Chinese first Civil Code, as one of seven books(编) in the civil code. Thus, along with the "General Principle of Civil Law" as the introductory book, the right to privacy has secured its protection in the civil code as a stipulated civil right.

In sum, influenced by the collectivist culture, the cultural and legal foundations of privacy protection in China are relatively weak. Although the demand for privacy protection of individuals has increased with the booming of markets and the development of internet technology, based on the cultural tradition of collectivism, China cannot establish a privacy protection system like Europe, which pays highly respect to the position of everyone in the society and the "honor" of everyone.[137] In the future, China's privacy system still tends to focus on enhancing the cooperation of social members and promoting the exchange and communication of information.

[135] Article 2 of Tort liability law: Those who infringe upon civil rights and interests shall be subject to the tort liability according to this law , wherein the "Civil rights and interest" used in this law shall include the right to life, the right to health, the right to body, the right to name, the right to reputation, the right to honor, right of portrait, right to privacy, martial autonomy, guardianship, ownership, usufruct (用益物权) security interest（担保物权）, copyright, patent right, exclusive right to use a trademark, right to discovery（发现权 ）equities (股权)，right of succession(继承权) and other personality and property rights and interests.

[136] Article 110 of General Principle of the Civil Law：A natural person shall enjoy the right to life and the rights to his/her body, health, name, portrait, reputation, honor, privacy, and marriage by choice. A legal person or an unincorporated organization shall enjoy the rights to name, reputation and honor.

[137] Whitman J Q. The two western cultures of privacy: Dignity versus liberty[J]. Yale LJ, 2003, P 1220.

1.2.1. Concept of the right to privacy

Although the concept of the right to privacy is recognized, either the tort liability law or the General Principle of civil law has not offered a normative definition of the right. The civil code adopted in June 2020 has for the first time clearly defined that the privacy refers to the tranquility of a natural person's private life, and the information about private space, private activities, and private information that the natural person does not want to disclose to others.[138] Thus, the core content of privacy focuses on the tranquil of life and life secrets.

Protection of life secret refers to free from illegal disclosure or interference by others over their private activities, private space, private information. The infringement on life secrets is mainly manifested in snooping, eavesdropping, and other illegal acquisition or unauthorized public disclosure of other's privacy. According to Professor Liming Wang, life secret covers a wide range and is constantly changing with the development of technology and social life.[139] As long as the information does not belong to the public domain and the information subject unwilling to disclose to others can be regarded as life secret.[140] Thus, life secrets emphasize on private and non-public information. Here, the "unwilling to disclose to others" should be judged from the right holders' subjective will. For example, the willingness to be known by a certain group of people is not equivalent to the

[138] Article 1032 of the civil code

[139] For example, the life secret includes personal biological data, physical data, health information, property information, conversation information, genetic information, phone numbers, as well as information about the family, relatives, or marital status， see：王利明.隐私权概念的再界定[J].法学家,2012(01):第 117 页

[140] 张新宝:《隐私权的法律保护》(第 2 版)，群众出版社 2004 年版，第 8 -9 页

willingness to be known by everyone[141]. Thus, disclosing information on the internet that the individual only agrees to share with a specific person can still constitute a violation of privacy.

The tranquility of private life indicates a right of a natural person to maintain a stable and peaceful private life and exclude others from harassment or disturbance of private life[142]. Similar to the meaning of the right to let alone, it implies the tranquility of spirit, which is a lack of external interference. Although our current law does not explicitly provide an interpretation of the tranquility of private life, the mainstream theory encompasses the tranquility of private life in three aspects: (1) the tranquility of private space, both physical and virtual. (2) The tranquility of daily life. In this sense, the right to privacy refers to the rejection of others' prying, stalking, and other forms of illegal interruption. It also includes the tranquility of communication. For example, phone harassments and online spam advertising harassment are increasingly affecting people' life, particularly people's tranquility of communication. (3) Self-determination of personal matters, such as the patient's self-determination rights. Self-determination is critical for guaranteeing the tranquility of private life, which shows respect and protection of personal freedom.[143] In this sense, the information under the protection of life tranquility does not need to be private or undisclosed. As long as other people's behaviors disrupt the peaceful life of the

[141] 参看：江苏省南京市鼓楼区人民法院［2005］鼓民三初字第 366 号民事判决书。The ruling held that the privacy information of once-publicized information does not automatically mean that others can re-disseminate, but still enjoy the protection of privacy.
[142] 王利明. 生活安宁权：一种特殊的隐私权[J]. 中州学刊, 2019(07):46-55
[143] Ibid.

information subject, such as conducting human flesh searching on the internet, it is also within the scope of privacy protection.[144]

1.2.2. Comparison with the right to be forgotten

By reviewing the concept of the right to privacy, the question that follows is whether the right to be forgotten can be included in the scope of the right to privacy?

Undoubtedly, the right to privacy and the right to be forgotten is closely related. Both the right to privacy and the right to be forgotten are enshrined as a value for maintaining human dignity and freedom, and both have emerged as a legal response to the development of modern communication technology. Privacy was born in an era when photographic technology and the press invaded aggressively into the sacred space of private and family. In the age of big data, social network, e-commerce, and communication technologies have brought human society into an "era of mass-producing, sharing and processing of data."[145] Thus, the right to be forgotten has been created in response to a new social-technic context, which still embodies the same value as traditional privacy.[146]

However, despite these similarities, there are still differences between the right to be forgotten and the right to privacy.

---

[144] As shown in the case of Wangfei v Hainan Tianya Network Technology Co., Ltd for right to reputation and privacy dispute, after the plaintiff's home address and other information were disclosed on the Internet, many netizens came to plaintiff's residence, which caused great distress to the plaintiff's tranquil of spirt. The court held that the plaintiff's right to private should be protected. 王菲诉海南天涯在线网络科技有限公司名誉权、隐私权纠纷案"(北京市朝阳区人民法院(2008) 朝民初字第 29277 号民事判决书

[145] Mayer-Schönberger, Viktor. *Delete: The virtue of forgetting in the digital age*. Princeton University Press, 2011.

[146] 张建文.被遗忘权的场域思考及与隐私权、个人信息权的关系[J].重庆邮电大学学报(社会科学版),2017,29(01)，第 28 页

Essentially, the right to be forgotten doesn't address the disclosure of information, but rather the control of the flow of information or how the information is shared. Therefore, the information protected by the right to be forgotten is not only already publicly available, but was legally published originally. The lawful disclosure becomes inappropriate during the change of context or with the elapse of time. In comparison, in the case of violation of the right to privacy, the disclosure is illegal at the moment when the information is disclosed. In addition, in the context of search engines, the issue of the right to be forgotten is to question the search results derived from a search engine's search algorithm, rather than to assess whether a particular search result violates the right to privacy, which goes beyond the traditional definition of "disclosure behaviors" targeted by privacy infringements.

Second, in terms of the object of protection, the information protected by the right to be forgotten is not necessarily private in nature. Widely published information already lost its secrecy which is out of the scope of privacy. Although the right to privacy has gradually expanded its scope with the development of society over time, the privacy right in Chinese law, as a specific personality right, has a relatively fixed connotation and extension. The core of privacy still lies in the tranquility of private life and private information, which is what the future development should also adhere to. Therefore, it is not comprehensive to cover the right to be forgotten under the right to privacy.

Third, in the way of protection, privacy protection is negatively defensive in nature. Both in the context of the life secret of the tranquility of private life, the defensive function of the right to privacy is emphasized. Specifically, the protection

of life secrets emphasizes that personal information is not made public without authorization or is not illegally obtained by the public. While the protection of tranquility of life emphasizes not being disturbed or harassed. Thus, before the right is infringed, the individual cannot exercise the right. Only after the damage has been caused, the right holder has the right to request the removal of interference. The right to be forgotten, on the other hand, is a proactive right to challenge the legitimate grounds of the continued dissemination of personal data.

Besides, in the past judicial practices, courts tend to deny the "right to be forgotten" of the personal information involved in criminal convictions under the approach of privacy, although those cases were not proposed in the name of "the right to be forgotten." For example, in a case where a claimant requested to remove a criminal conviction relevant to him from a website (unofficial), the court held that information about a person sentenced for contract fraud is not private information that is protected by law and directly rejects the claimant's claim.[147] In another case involving whether the quoting information related to a criminal judgment could constitute an invasion of privacy, the court emphasized that the privacy of citizens protected by law must not be associated with the public interest. The information that a person has been sentenced to punishment for a criminal act is an objective fact confirmed by the people's court. The judgment document issued by the people's court is not only legally binding, but also has a publicity effect on unspecified membered of the public. Thus, the information is related to the public interest,

[147] 参见杭州市拱墅区人民法院（2014）杭拱民初字第 281 号民事判决书

thereby not belonging to the scope of privacy.[148] Although China is not a common law country, the past judicial practice still generates a relatively conservative effect in recognizing the right to be forgotten under the protection of privacy.

1.3. ISP Responsibility

Article 36 of the tort liability law of the PRC, as a "specific provision for network infringement", clarifies the responsibility of network operators and establishes a general principle of online privacy protection[149]. Under the tort liability law, the ISP embraces indirect civil liability for a third party's infringement behaviors based on fault. Since the ISPs have no general obligation to review the infringing content, the fault of ISP only exists in cases where the ISPs failed to respond in a timely manner and take necessary measure to prevent the right holder from an expansion of the damage after being aware that network users have used their network service to infringe civil rights and interests of others. Therefore, the ISPs only bear joint and several tort liabilities for the damage caused by infringement of a third party and responsible for the enlarged damage by failing to take necessary

[148] 参见天津市第二中级人民法院（2015）二中保民终字第 65 号民事判决书

[149] Article 36 of tort law stipulates that 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.

Wherein a network user commits a tort through the network services, the victims of the tort shall be entitled to notify the network service provider to take necessary measures as deletion, block, or disconnection. If the network service provider fails to take necessary measure in a timely manner after being notified, it shall be jointly and severally liable for any additional harm with the internet user;

Wherein a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.

measures in time after receiving effective notice.

In addition, Article 15 of the tort liability law rules the method of assuming tort liabilities, which includes cessation of infringement, elimination of consequences and restoration of reputation, and so on.[150] Thus, the "elimination of consequences and restoration of reputation" has different manifestation forms based on the specific case and the corresponding personality rights. For example, individuals can request to delete the original content or block or delink the infringing content to prohibit the continued spread of the information. Thus, if the ISP is eventually found liable for invasion of privacy or the right to reputation, tort victims can also rely on Article 15 in demanding the ISP to remove, block or delink the infringing content.

Although the provision grants individuals to request deletion of personal information vis-a-vis internet service provider (such as search engine), as a remedy of infringement, the exercise of the request is at the premise of "infringement behavior," which creates the substantial difference between the deletion in the right to be forgotten and delete based on Article 36 of tort law.

The right to be forgotten in the GDPR is considered in terms of data quality and the purpose of data processing, which is mainly targeted to de-contextualized or inaccurate personal information on online platforms such as search engines. Therefore, the deletion embedded in the right to be forgotten does not require the existence of an infringement. Even if no damage has occurred, the data subject may

[150] Article 15 of tort liability law of PRC: The methods of assuming tort liabilities shall include: 1. cessation of infringement; 2. removal of obstruction; 3. elimination of danger; 4. return of property; 5. restoration to the original status; 6. compensation for losses; 7. apology; and 8. elimination of consequences and restoration of reputation. The above methods of assuming the tort liability may be adopted individually or jointly.

still request the data controller to delete his or her personal information as long as it fulfills the grounds listed in Article 17 in GDPR. In addition, as in the Google Spain case, the court categorized the search engine as a data controller. It is responsible for its own dissemination behaviors independently, instead of indirectly liable due to other third parties. In this regard, it is questionable for some Chinese scholars believe that the right to be forgotten can be established based on Article 36 of the tort law.[151]

Besides, currently, the control of search engines in china basically relies on industry self-discipline. For example, there is "Search Engine Service Providers self-regulation for resisting illegal and harmful information" and "Convention on the self-regulation on Internet Search Engine service." The former was stipulated by the Chinese internet Association in 2004 for controlling the dissemination of obscenity, pornography and other illegal and harmful information through search engines. The latter one was initiated in 2012 by Baidu and other 11 search service provider companies. Although the "Convention" also stipulates several provisions of the obligations of blocking or delinking, the content and scope do not exceed the regulation of article 36 in tort law.[152]

2. Personal data protection in the PRC

In recent years, with the advent of the internet age, China has strengthened the

[151] 周頔. 朱巍: "被遗忘权"应成为网络时代个人信息的保护伞[N]. 民主与法制时报, 2016-06-02.

[152] Article 10 of "Convention on the self-regulation on Internet Search Engine service":
Search engine service providers are obliged to assist in protecting user privacy and personal information security. Upon receiving valid notification from the right holder, the search engine service providers shall promptly remove or delink infringing content.

protection of personal information. Several legislations involving personal information have been issued successively. The sub-section will first introduce the recent initiatives regarding protecting personal information, then discuss the Chinese scenarios of deletion of personal information under the current legal system.

2.1. Recent initiatives

In 2012, the Standing Committee of The National People's Congress (NPCSC) passed the "Decision on strengthening Network information Protection" (hereinafter referred to as "Decision 2012") which stipulates the principle of information processing and the responsibilities of network service providers in protecting personal information.[153]

In 2014, the Supreme People's Court issued the "Provisions of the Supreme People's Court on Several Issues concerning the application of the Law in the trials of cases involving civil disputes over infringement upon personal rights and interests through information network" (hereinafter referred to as "Provision 2014"). The Provision 2014 enhances protection of personality rights in cyberspace and regulation on ISP's liability for the breach of personal rights and interests through the approach of tort liability law.

In 2016, the Standing Committee of the National People's Congress promulgated the "Cybersecurity law." The Cybersecurity Law defines the protected

[153] According to China's legislative law, there are seven types of laws enacted by the National People's Congress and its standing committee: Law(法), resolution(决议), Decision(决定), Regulation(条例), Provision(规定), Measure(办法), Plan(方案). Therefore, the decision is one type of laws and has the force of law.

scope of personal information and stipulates how to collect, store, or transmit personal information electronically. Chapter Four of the Cybersecurity Law focuses on the network operator's obligation in protecting personal information and the rights of data subjects.

The "General Provision of Civil law of PRC" has introduced in 2017. Article 111 of the General Provision of Civil Law makes a firm declaration that personal information shall be protected by law and that No one may illegally collect, use, process, transmit personal information, No one may illegally trade, provide or publicize the personal information of others.[154] Although some scholars have criticized the provision for using negative specification instead of affirmative statement, it was the first time that personal information had been regulated at the basic civil law level as a personality interest which is worthy protection, the meaning of Article 111 should not be underestimated. Article 111 in the General Provisions of the Civil Law includes the interest in personal information in the scope of protection of civil law and provides a remedial basis for individuals in case of misuse of the personal information.

The Chinese first Civil Code has been formally enacted on May 28, 2020. The civil code opened a separate chapter on the right to privacy and personal information protection. The newly adopted Civil Code has made up for the shortcoming of Article 111. It stipulates more detailed regulations in conjunction with personal information

[154] Article 111 of the General Provision of Civil Law: "the personal information of a natural person shall be protected by law. Any organization or individual that needs to acquire the personal information of an individual shall obtain such information in accordance with law and guarantee the safety of such information. No one may illegally collect, use, process, transmit, trade, provide or publicize the personal information of others.

processing, particularly the principle of personal information processing and the rights of data subjects.

The "GB/ T35273-2020" Information Security Technology-Personal Information Security Specification (hereinafter referred to as "Specification")[155] is issued by the Standardization Administration of China, an organization under the State Council that oversees the coordination of standardization work in China. The Specification GB/ T35273-2020 was promulgated on March 6, 2020, after three revisions on the 2017 version and came into force on October 1, 2020. The Specification provides more detailed regulations on fair data processing and clarifies the data subjects' rights and the responsibility of data controllers. Although the Specification is not legally binding, in the absence of a comprehensive personal information protection law in china, the national standard can provide companies with what the Chinese regulators consider to be best practice for personal information protection and reflect the direction in which China's data protection regime is heading[156].

Since the legislation of a specific "Personal Information Protection Law" was listed in the "Legislation Plan" announced by the Standing Committee of the thirteenth National People's Congress (NPC) on September 10, 2018, the draft of the "Personal information protection law" (herein after referred as “draft”) was freshly published for public consultation on October 21, 2020.

The draft indicates the two primary purposes of personal information protection,

[155] Full text of “Specification” is available at: the https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf

[156] It noted that there are no penalties imposed for breach of the “Specification.”

which both protect personal information and promote the fair use of personal information. The structure of the draft basically follows the general principle of personal information protection proposed by Professor Xinbao, Zhang, which is "bilateral strengthening, tripartite balance."[157] The "bilateral strengthening means strengthening both the protection of personal sensitive personal information and the use of general personal information (non-sensitive information). "The tripartite balance" refers to balancing interests among individuals, information industries and government. More specially, the interests needed to be balanced include individuals' interest in protecting their personal information, the interest of the information industry in using personal information, and the public interest of the government in managing the whole society. Following this vein, the draft first stipulates rules for processing personal information in terms of general personal information and sensitive personal information, respectively. Then it stipulates the right of individuals, obligations of personal information processors, and the national department responsible for personal information.

2.2. Protection Approach: Growing Independent from Privacy

Due to a lack of comprehensive personal information law in china, in order to enhance the protection of personal information, there is a tendency to protect personal information by expanding the scope of privacy. The concept of tranquility of life gives a certain degree of openness to the concept of privacy and leaves judges

[157] 张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学,2015(03):38-59.

with discretion in its application.[158] In judicial practice, the right to privacy also serves the function of protecting personal information.[159] However, unless completely ignore the literal meaning of the right to privacy, no matter how to expand the scope of privacy protection, it is impossible to include all personal information under the scope of privacy protection.[160] In addition, the right to privacy is a passive personality right, which can claim relief only after the occurrence of damage. However, in the era of big data, many privacy risks are determined at the design stage.[161] Thus, scholars in china also began to seek to propose a more proactive personal information protection system, independent from the protection of privacy.

Since the introduction of the "General Provision of Civil law of PRC" in 2017, personal information began to gain protection independent of privacy. The General Provision of Civil law uses two clauses to stipulate the protection of the right to privacy (Article 110) and the protection of personal information (Article 111), respectively. In addition, in the civil code, Article 1034 affirms the legal protection of personal information, separate from the right to privacy.

Although both the General Provision of Civil law or the civil code does not

[158] 谢远扬. 信息论视角下个人信息的价值——兼对隐私权保护模式的检讨[J]. 清华法学, 2015, 9(03):94-110.

[159] 参见 "孙某某诉中国联合网络通信有限公司上海市分公司侵害隐私权案",(2009) 浦 民一初字第 9737 号. In the case "Sun weiguo vs China Union Ltd. (shanghai Branch) for the invasion of privacy, the plaintiff's personal information, including name, address, telephone number, and ID number, was disclosed to a third party without the plaintiff's permission. And the subsequent processing by the third-party exceeded the original purpose of collection. The court ruled the defendant's behavior constituted an infringement of the plaintiff's privacy. More specifically, the court held that "the purpose for laws and regulation in protecting the right to privacy is to give right holder a right to control the extent to which others may intervene in their private lives, and the right to determine whether and to what extent they disclose their privacy to others."

[160] 李承亮.个人信息保护的界限——以在线评价平台为例[J].武汉大学学报(哲学社会科学版),2016,69(04):109-120.

[161] 郑志峰.人工智能时代的隐私保护[J].法律科学(西北政法大学学报),2019,37(02):51-60.

clearly define whether the protection of personal information is a civil right or legitimate interest, the protection of personal information is different from the protection of privacy as follows:

First, protection of personal information is related to the processing of personal information. Since personal information has a natural character of circulation, data protection does not deny the value of processing personal information at the inception of its conceptualization. Thus, the personal data is protected through imposing a series of objective and followable rules of conduct during all stages of data processing.[162] In other words, how the data processing should be undertaken.[163] On the other hand, the data subject is not completely passive. By endowing a bundle of rights, data subjects can impose restrictions on the data controller/data processor's behavior to protect their autonomy. Thus, besides the privacy interests, the underlying value of protection of personal information also includes interests in knowing that personal information is being processed, interests in the accuracy and integrity of personal information, and interests in maintaining the processing of personal information is subject to a specific purpose.[164]

Second, information under the scope of personal information protection is not limited to information of a private nature. According to Article 1034 of the civil code, any information that identifies or is identifiable an individual falls into the scope of

[162] 叶金强. 《民法总则》“民事权利章”的得与失[J]. 中外法学,2017,29(03):645-655.

[163] Fuster, Gloria González, and Raphaël Gellert. "The fundamental right of data protection in the European Union: In search of an uncharted right." *International Review of Law, Computers & Technology* 26.1 (2012): P80.

[164] 杨芳. 个人信息保护法保护客体之辨——兼论个人信息保护法和民法适用上之关系[J]. 比较法研究,2017(05):第 81 页.

personal information protection.

Third, compared with the ex-post remedy of privacy protection, the protection of personal information place emphasis provides more ex-ante remedial measures. Data protection aims at preventing abstract dangers or harm that may arise from the misuse of personal information. Due to the complexity and diversity of data processing, it is difficult to distinguish which data would significantly impact private life. The traditional categorization of sensitive information also faces new challenges in the big data era in which small pieces of information can be accumulated to form a complete profile. Thus, the protection of personal information intervenes when the risk is approaching, or the likelihood of the risk is high enough, instead of waiting until actual dangers happen.

Thus, the current legislation for protecting personal information in an independent approach of the right to privacy can better fit for the development of the big data era and provide more comprehensive protection of personal information.

2.3. Principles and conditions for lawful processing

Article 41 of the cybersecurity law for the first time establishes the principles of data processing are lawfulness, fairness, and necessity.[165] Here the "lawfulness" is not limited to the cybersecurity law, but includes provisions of personal

165 Article 41 of cybersecurity law: Collection and use of personal information must be lawful, legitimate and necessary. Network operators must clearly state the purpose, method, and scope of collection and use, and obtain consent from the person whose personal information is to be collected; personal information irrelevant to the service provider shall not be collected.

information protection involved in other departmental laws and relevant judicial interpretations. “Fairness” means that the purpose and means of processing should be proper, in line with the principle of good faith, and ensure the individuals’ right to be informed. The “necessity” implies the principle of purpose limitation and data minimization in the GDPR. That is, the collection and processing should be necessary relative to the purpose. The second paragraph rules that consent is the only condition for lawful processing.

Article 1035 of the civil code follows the principles and conditions for the lawful collection and processing of personal information stipulated in the Cybersecurity law, which is lawfulness, fairness and necessity.[166] At the same time, the first paragraph regards users' consent as the only legal basis for lawful processing, which fully embodies the concept of information self-determination and guarantees individuals' control over their personal information. The processing here should be understood in a broad sense, including all processing stages from the collecting, using, processing, transmitting and disclosure. Therefore, the data processor in the civil code includes both the definition of data controllers and the data processors in

[166] Article 1035 of civil code: the processing of personal information shall follow the principles of lawfulness, fairness and necessity, shall not excessive and meet the following requirements:

1. With the consents of the natural person or his/her guardian, unless otherwise prescribed by laws or administrative regulations.
2. Disclosure of processing rules
3. Clearly state the purpose, method and scope of the processing
4. Shall not violate the provisions of laws, administrative regulations or the agreement between the parties

The processing of personal information includes the behaviors of collection, storage, use, processing, transmission, provision, and disclosure of personal information.

the GDPR. However, it remains unclear whether such a definition would be interpreted, as it was in the Google Spain case, to include search engines that lodge personal information on their platforms. Article 1036 of the civil code stipulates exemptions for collecting, processing, and disclosing personal information.[167] The first situation is for processing based on the consent of natural persons. The second situation refers to the information that has been made public. The third situation is processed for the protection of the public interests or legal rights of natural individuals.

Based on the principles "lawfulness, fairness, and necessity", the "specification" refines the principles into the following seven principles: accountability; data minimization; purpose limitation; inform-consent; transparency; security ensuring and individual participation.[168] Like the provisions in the civil codes, the basic basis for lawful processing in the "specification" is the consent of the data subject. But the "specification" further provides more exceptions which are consistent with the civil code but more detailed. Noteworthy, information is disclosed to the public by the data subjects, and information collected from legally publicly disclosed information, such as news reports, government information disclosure websites, and other

[167] Article 1036 of the Civil Code: individuals do not bear civil liability for processing personal information under any of the following circumstances:

1） Based on the consent given by the natural person or his/her guardians

2）Processing on the information disclosed by the natural person or other legally disclosed information, unless the natural person raise an explicit objection or the processing infringes his/her vital interests (public data exemption)

3） Other reasonable processing behaviors carried out for the purpose of protecting public interest or the natural individuals' legitimate rights and interests.

[168] Article 4 of "specification"

channels, can be collected or used without individuals' consent.[169]

In the draft, personal information is defined as a variety of information related to an identified or identifiable natural person recorded electronically or by other means, as excluding anonymized information.[170] General exceptions to the personal information protection include natural persons when pursuing personal or household activities.[171] Principles for processing personal information include Lawfulness, fairness and integrity (Article 5), purpose limitation (Article 6), transparency (Article 7), Accuracy (Article 8) and accountability (Article 9). Noteworthily, Article 13, as one of the cores and most important changes in the draft, has extensively expanded the basis for lawful processing of personal information. The article stipulates six basis for lawful processing: (1) consent; (2) Necessary for the conclusion or

[169] Article 5.6 of specification **GB/ T35273**-2020: in the following circumstances, the data controller is not required to obtain consent from the data subject for collecting and using personal information:

1. processing for fulfilling obligations stipulated by laws and regulation,
2. directly related to national security and national defense;
3. directly related to public safety, public health, and major public interest;
4. directly related to criminal investigations, prosecution, trial and execution of judgments;
5. in order to protect the life, property and other vital legal rights of the data subjects or other individuals while having difficulties to obtain the authorization of the person;
6. the information is disclosed to the public by the data subjects;
7. necessary for signing and performing contracts according to the requirements of the data subject;
8. information collects from legally publicly disclosed information, such as news reports, government information disclosure websites and other channels;
9. the data controller is a news media, and the processing is necessary to carry out news reports;
10. the data controller is an academic research institution that the processing is necessary to conduct statistics or academic research for the public interest, and the personal information contained in the result is de-identified when providing the results of the academic research or description to others.

[170] Article 4 of the draft of personal information protection law

[171] Article 68 of the draft of "personal information protection law".

performance of a contract to which the data subject is a party; (3)Necessary for the fulfillment of legal duties or obligations; （4) Necessary for responding to public health emergencies, or for the protection of life, health and property of the data subject or other individuals in emergent cases; (5) For the public interest in the implementation of journalism or public opinion supervision and other acts within a reasonable extent; (6) Other circumstances. Thus, it ends the history that the consent has been the only legal basis for the processing since the enactment of the cybersecurity law. It can be seen as a development of the exemptions stipulated in Article 1036 of the civil code. In terms of content, it is similar to items (a) -(e) of Article 6 (1) in the GDPR, but there are certain differences. In particular, the basis for journalism and public opinion supervision has taken into account the public opinion environment of china, clearing certain legal obstacles for the press. Article 14 stipulates that the consent must be informed, specific, freely given, and indicate data subjects' intentions. Article 16 further adds the opportunity to withdraw consent to processing in cases wherein the processing solely on the user's consent.

Considering the inclined protection, Article 15 regulates special treatment for the protection of minors. In addition, in order to prevent personal discrimination or severe harm to personal and property safety, such as personal information about the race, ethnic group, religious beliefs, personal biometric data, health data, financial account data, and location data, Article 29 stipulated the special protection of the sensitive information. It is noted that the criminal conviction is not listed as sensitive information. Only with a specific purpose and sufficient necessity, the processing of sensitive personal information is allowed. The processing of sensitive information

needs separate consent and higher notification of the necessity and risk of the processing. Also, Article 32 implies that the processing of sensitive information may require an administrative license or more stringent restrictions if required by laws and administrative regulations.[172]

	Principle, rules and sensitive data	General legitimacy of processing
Cybersecurity law	Lawfulness, Fairness And Necessity	Consent
Civil code	Lawfulness, Fairness and Necessity	Consent
Specification	Lawfulness, Fairness and Necessity	Consent
Draft of personal information protection law	Lawfulness, fairness and integrity; Purpose limitation; transparency, Accuracy; Accountability	6 grounds (1) Consent; (2)Necessary for contract; (3) Necessary for legal duties or obligations (4) Necessary for public health emergencies, (5) For journalism within a reasonable extent (6) Other circumstances

Table 4 Principle and legal basis for processing

In sum, from the legislation mentioned above, the framework of personal information protection in china has been basically established, which is based on the principles of lawfulness, fairness, and necessity, and centered on informed consent. There, the principle of data minimization, and the principle of data accuracy are

[172] Article 32 of draft: Where laws and administrative regulations stipulate that the processing of sensitive personal information should obtain relevant administrative licenses or impose stricter restrictions, the provisions shall be followed.

explicitly stated. The draft timely addresses the over-reliance on consent set in prior legislation by providing more basis for legal processing, and stipulates what constitutes valid consent and the right to withdraw consent, which is largely in line with international rules for protecting personal information.

2.4. Public disclosure of personal information

Since the right to be forgotten is a right to request deletion or restriction of the processing of published personal data. The following sorts out the regulations regarding the processing of information disclosed by data subjects themselves or legally disclosed and the general rules of personal information disclosure.

Article 12 of the "Provision 2014" specifies that the legal liability for disclosing personal information online.[173] Pursuant to Article 12, internet users or internet

[173] Article 12 of the Supreme People's Court Provision 2014: If internet users or internet service providers use the internet to disclose personal's private information and other personal information such as a nature person's DNA, medical records, criminal records, residential address, or personal activities has online and cause harm to others shall be held for legal liability.

Exemptions for liability includes:

1. Disclosure is based on written consent by the individual and is within the agreed scope;
2. the disclosure aims to promote society's public interest and is within the necessary scope;
3. the disclosure is based on public interest for academic research or statistical purposes, with int written consent of the natural person, and in a way that is insufficient to identify the natural person.
4. information already disclosed online by the individual or other personal information lawfully disclosed,
5. personal information obtained through lawful means,
6. other situations specified in laws or administrative regulations.

wherein in situations refers to the item (4) and (5), internet users or internet service providers can still be held liable if the means used to disclose the personal information is against society's public interest or public morals, or the disclosure would infringe the individual's vital interests that are worthy of protection.

service providers shall bear the corresponding responsibility if they disclose personal information online and harm others. Several features concerning Article 12 of the 2014 judicial interpretation are noteworthy:

1. It is worth noting that Article 12 concerns not only private information, but also "other personal information that does not constitute privacy," which enhances the protection of personal information.
2. Article 12 is aimed at the direct infringement of internet users and internet service providers by disclosing personal information online, which should be distinguished from the indirect tort liability of ISP specified in Article 36 of the tort liability law.
3. Disclosing personal information that is voluntarily disclosed by the data subject or legally disclosed through other means is exempted from tort liability in principle.

Only if the disclosure infringes the individual's vital interest or is against public interest or public morals, users or internet service providers would be held liable for the re-publication of publicly available information. Thus, information voluntarily disclosed by the data subject or legally disclosed through other means is free to use in most cases. However, what constitutes the "vital interest that is worthy of protection" is a matter of discretion of the court and remains to be clarified. Some scholars have proposed that if an internet user conducted a human flesh search

through a search engine and caused harm to the right holder, the user should be held liable for legal responsibility.[174]

Article 13 of the "Provision 2014" stipulates the infringement by publishing judicial documents.[175] According to Article 13, since the judgment document is an authoritative source, the republication does not constitute infringement, as long as the content is consistent with the original content, and there is no improper use such as by adding insulting content, defamatory information, inappropriate titles, or adding or deleting information, adjusting structure, changing the order.

As mentioned above, Article 1036 of the civil code stipulates exemptions for collecting, processing, and disclosing personal information.[176] Especially, the

[174] 杨临萍,姚辉,姜强.《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》的理解与适用[J].法律适用,2014(12):22-28.

[175] Article 13 of the Supreme People's Court Provision 2014: Network users or network service providers infringe personality rights of others based on information from ex officio-document released by government offices or publicly implemented act of authority in the following situations:

1. The information published by network users or network service provider does not match the content of the aforementioned information from the source.
2. Internet users of internet service providers mislead the public by adding insulting content, defamatory information, inappropriate titles, or adding or deleting information, adjusting structure, changing the order, and so on;
3. The aforementioned information in the source has been publicly corrected, but the network user refuses to make the correction or the network service provider does not make the correction;
4. The aforementioned information in the source has been publicly corrected, the network user or network service provider still release the information before the correction.

[176] Article 1036 of the Civil Code: individuals do not bear civil liability for processing personal information under any of the following circumstances:

1）Based on the consent given by the natural person or his/her guardians

2）Processing on the information disclosed by the natural person or other legally disclosed information, unless the natural person raise an explicit objection or the processing infringes his/her vital interests (public data exemption)

second situation refers to the information that has been made public. The Article 1036 in Civil Code has strengthened the protection of publicly available information compared with Article 12 of Provision 2014. The proviso for the use of public personal information not only includes the situations where the information infringes on the individuals' vital interest, but also adds cases where users explicitly object to the processing. Thus, even if the information is legally disclosed, if the data subject explicitly refuses the use, the individual who insists on processing the relevant information cannot get an exemption from the civil liability.

Regarding the public disclosure of information in the "specification", the personal information is not allowed to be publicly disclosed, unless it is authorized by law or is necessary to be disclosed for legitimate reasons. In addition, even if the ground for public disclosure is valid, it still needs to obtain explicit consent from the data subject before the disclosure, and be responsible for damage to the data subjection due to the disclosure. However, for public disclosure of (f) information disclosure by the data subject or (g) information from legally disclosed information, such as information on newspaper, government websites, and other channels, such authorization or consent from the subject is not required.[177]

In the draft, Article 26 set general prohibition of disclosure of personal information, except for obtaining the individual's "separate consent" or as otherwise provided by law or administrative regulations and so on.[178] The key provision of the

3） Other reasonable processing behaviors carried out for the purpose of protecting public interest or the natural individuals' legitimate rights and interests.

[177] Article 9.5 of "personal information security specification"

[178] Article 26: processors shall not disclose the personal information they process. Except for

interest of the paper is presented in Article 28. Article 28 for the first time clarifies the requirement for processing personal information that has been made public. According to Article 28, the processing of personal information that has been disclosed shall not exceed the reasonable extent related to its original purpose. Otherwise, it needs to obtain the data subject's consent again. If the original purpose of disclosure is not clear, the processing still should be undertaken cautiously. If the potential risk is great, more ideally, the processor should inform the data subject and obtain consent.[179] The processing of published information has been included in the exemption in Article 1036 (2) of the Civil code. Unless the information infringes on the individuals' vital interest or users explicitly object to the processing. Thus, compared with stipulation Article 1036 (2) of the Civil code, the draft imposes a stricter requirement to process personal information that has been made public. The "published information" cannot justify unrestricted processing of personal information.

obtaining the individual's "separate consent" or as otherwise provided by law or administrative regulations and so on.

[179] Article 28 of the draft of personal information protection law of PRC:

the processing of personal information that has been disclosed by the personal information processor shall comply with the purpose when the personal information is disclosed; if it exceeds the reasonable scope related to the purpose, it shall notify the individual and obtain his consent in accordance with the law.

Wherein the purpose of disclosing the personal information is not clear, the personal information processor shall process the disclosed personal information reasonably and cautiously. If the use of publicly disclosed personal information to engage in activities that have a significant impact on individuals, the personal information processor shall notify the individual and obtain his consent in accordance with the law.

	Rules of disclosure of personal information	Processing of self or legally disclosed information
2014 Court Provision (Tort liability law)	N/A	Exemption from liability, unless infringes the individual's vital interest or is against public interest or public morals
Civil code	N/A	Exemption from the liability, except the situations where the information infringes on the individuals' vital interest or users explicitly object to the processing
Specification	Not allow in principle, unless it is authorized by law or is necessary to be disclosed for legitimate reasons	N/A
Draft of personal information protection law	Not allow in principle (except for "separate consent")	Not exceed the reasonable scope related to its original purpose; If the original purpose is not clear, the processing should be undertaken with reasonable care

Table 5 Disclosure of personal information

Thus, following the legislation process, individuals gradually gain more control to challenge the processing of published information. In provision 2012, data legally disclosed on the Internet by the data subject himself or by a third party is not protected by default, unless the use or republication of such personal information damages the vital interest of data subjects. The Civil Code empowers data subjects to control over disclosed information by raising an objection. And the draft of personal information protection law further sets the "reasonable care" and "compliance with the original purpose" as two critical elements in defining the

boundary of processing disclosed information. Due to the current prevalent secondary use of big data, it is necessary to set restrictions for the use of published information. In addition, both the “Specification” and the “draft” set general prohibitions for the publication of personal information online, which indicates a restriction on the disclosure of information at the source.

Although, overall, the level of protection for information disclosed by data subjects themselves or legally disclosed is relatively low, legislative protection is being strengthened as more and more personal information is made publicly available on the internet. In this sense, the legislative trend is consistent with the spirit of the right to be forgotten, although it does not reach the protection level afforded by the right to be forgotten.

2.5. Right to Erasure

At last, we analyze the right closest to the right to be forgotten, the erasure mechanism under the data protection framework.

Article 8 of the Decision 2012 stipulates that “Citizens who find that the disclosure of the personal identity or the dissemination of privacy and other personal information infringes their legitimate rights and interest, or suffer interference from commercial electronic information, has the right to request the network service providers to delete the information or take other necessary measures to stop it”. Thus, Article 8 implies a right to require ISPs, including search engines, to erase or stop further dissemination of online information based on the conditions of the infringement of their legitimate rights and interests.

Article 43 of the Cybersecurity law stipulates the circumstances of deletion and correction, that individuals are entitled to ask network operators to delete personal information if the collections or processing of the network operators have violated the laws, administrative regulations, or agreements between the parties.[180] Thus, based on Article 43, personal information that is illegal or unauthorized collected or used can be asked to delete. The "network operators" under the cybersecurity law refers to owners, managers, and network service providers of the network,[181] including telecommunication business operators, network service providers (ISP), and network content providers (ICP). In this sense, search engines fall within the scope of network operators.

Compared with the value of "dignity" or "Informational Self-Determination" in Europe, China's right to erasure in the Cybersecurity law enshrines a view of order. The reason is that the cybersecurity law is designed to maintain the cyberspace sovereignty and safeguard the security of the overall system of the network, so as to avoid instability of the network order caused by the leakage of personal information. Besides, due to the cultural foundation and legal traditions of privacy protection in china are relatively weak, the right to erasure in cybersecurity law does not adopt an individualistic approach which gives an individual a subjective right to apply for the deletion of personal information, but instead setting the violation of the law,

[180] Article 43 of cybersecurity law: Where individuals discover that network operators have violated the provisions of law, administrative regulations, or agreements between the parties to gather or use their personal information, individuals are entitled to ask network operators to delete such personal information

[181] Article 76 of cybersecurity law

regulation, and agreement as the pre-conditions to ensure that the use of personal data is in line with the overall expectations of the large community consisted by nations and people.[182]

Article 1037 of the Civil Code stipulates the rights of the data subject. The right to erasure under the civil code is regulated the same as the cybersecurity law. Pursuant to Article 1037, the data subject has a right to access or copy their personal information from information processors in accordance with the laws, a right to object or rectification if there are errors in the information, and a right to erasure if the personal information processor violates the laws, administrative regulations or the agreement between the parties.[183]

In the "Specification," the circumstances of deletion have been stipulated in more detail. The grounds involved in deletion mainly refer to the following four situations: (1) When the minimum period necessary to achieve the purpose is expired (Article 6. 1), (2) when a data controller ceases to operate its products or service (Article 6. 4), (3) where in cases of violation of the laws, administrative regulations, or agreements between the parties (Article 8.3), (4) After the accounted is canceled.

[182] 周冲.个人信息保护:中国与欧盟删除权异同论[J].新闻记者,2017(08):第 78 页.

[183] Article 1037 of civil law: natural persons can assess or copy their personal information form information processors in accordance with the laws. If there are errors in the information, the natural persons have the right to raise objections or request corrections or other necessary measures. If the natural person discovers the processing of his or her personal information by information processor violates the provisions of laws, administrative regulations or the agreement between the parties, the natural person has the right to request the information processor to delete the involved personal information in time

(Article 8.5.f).[184] However, as mentioned above, the "Specification" has no legal effect, thus cannot be used as a basis for claiming erasure.

Much development has been made in the draft of the personal information protection law. Chapter 4 of the draft stipulates the rights of data subjects. Article 47 defines the right to erasure. Compared with the previous legislation, the circumstance of application of deletion have been greatly expanded. In addition to the situation of violating the laws, administrative regulations, or agreements between the parties, the draft also adds other grounds for erasure, including those where the purpose of processing has been achieved, and consent has been withdrawn.[185] Thus, under the new draft, a user would have the right to withdraw her consent and thereby ask the data controller to delete personal information if the consent is the only basis for the processing. And the second deletion grounding mainly focuses on solving how to manage the personal information collected by various applications, larges, or small entities, after they cease operation.

	Right to erasure
2012 Decision	Infringes on their legitimate rights and interest, or

[184] Article 8.5.f of "personal information security specification": when a data subject cancels his or her account, his or her personal information shall be deleted or anonymized without delay.

[185] Article 47: The personal information processor shall take the initiative or at the request of the individuals to delete personal information where one of the following grounds applies:

1. the agreed retention period has expired, or the purpose of processing has been achieved
2. the person information processor stops providing products or services
3. the individual withdraws consent
4. the personal information processor violates laws and administrative regulations or violates the agreement to processing personal information
5. Other circumstances as provided by Chinese laws and regulations.

	suffer interference from commercial electronic information
2014 Court Provision	N/A
Cybersecurity law	Violating the laws, administrative regulations, or agreements between the parties
Civil code	Violation of laws, administrative regulations or the agreement between the parties
Specification	(1) When the minimum period necessary to achieve the purpose is expired (2) When a data controller ceases to operate its products or service; (3) Violating of the laws, administrative regulations, or agreements between the parties (4) After the accounted is cancelled.
Draft of personal information protection law	1. The agreed retention period has expired, or the purpose of processing has been achieved 2. The person information processor stops providing products or services 3. The individual withdraws consent 4. The personal information processor violates laws and administrative regulations or violates the agreement to processing personal information 5. Other circumstances as provided by Chinese laws and regulations.

Table 6 Right to Erasure

Thus, it can be seen the deletion system in personal information protection in China is being improved. From the previous general and abstract regulation of violation of the law, administrative regulations, and agreements, the right to erasure has finally been refined to the point where it is more consistent with data processing provisions and allow individuals to delete their personal information based on withdrawal of consent and when information is no longer necessary for the purpose.

However, the right to erasure under the current Chinese legal frame and the

right to be forgotten in EU rights have substantial differences. The right to erasure in china shows a strong a procedural nature and belongs to the negative facet under the protection of personal information[186]. Beginning from the collection stage, the data subject has the right to be informed through the consent mechanism and the right to decide whether to accept the processing or deny it. During the stage of processing, the data subject has the right to withdraw their consent to opt-out the processing. Also, the data subject has the right to access their information in order to understand the purpose of data processing, the type of data involved, the storage period, and its subsequent impact, and so on. On the other side, if the data subject found any breach of integrity, accuracy, or privacy of the personal information, the data subject has the right to correct, to restrict, to object, or to delete the personal information. Thus, the right to erasure under the draft is one of the remedial contents under the protection of personal information.

However, the right to be forgotten is the strengthening of the right to erasure to meet the demand for privacy protection in the digital context. The degree of protection of the personal information has deepened to “forgiveness of data subject’s past and giving the information subject an opportunity to restart”, which has gone beyond the right to erasure currently.

3. Summary

Under the influence of collectivism and Confucius culture, both the cultural

[186] 叶名怡.论个人信息权的基本范畴[J].清华法学,2018,12(05):143-158.

foundation and legal tradition of privacy protection in China are relatively weak. The future privacy system still tends to focus on promoting the exchange and communication of social information. As for the current legislation on privacy, due to the difference in the nature, the object of protection and the way of protection, the right to be forgotten cannot be included in the current right to privacy.

On the other side, the protection of the personal information protection system has been established, but is still in the fundamental stage. Although the recent initiatives show a trend to enhance the protection of published information, it still has a distance from the protection level afforded by the right to be forgotten. Thus, in the author's opinion that the right to be forgotten is slightly ahead of the legislative processes in china.

Chapter 6 Judicial practice of The Right to Be Forgotten in China: Renjiayu vs Baidu

Chapter 6 introduces the judicial practice of the right to be forgotten in China: Renjiayu v Baidu, which is called the “First case of the Right to Be Forgotten” in china. Through the interpretation of the judgments of the two trials, it can clarify the path of the protection of the right to be forgotten under the existing Chinese law and the reject reasons, as well as the judges’ attitude towards the right.

1. Fact

In a 2015 judgment, the No.1 Intermediate People's Court of Beijing of China upheld a dismissal of a request for deleting automated produced search suggestions from China's largest search engine Baidu made by the lower court. In the case, the plaintiff requested Baidu to delete search suggestions, which implied his professional experience on the claim of the "right to be forgotten". Thus, this case has also been called the first case of" the right to be forgotten" in China. Both the courts of the two levels refused the claim after thoroughly considering various factors.

1.1. Claim of Mr. Ren: Substantial Damage

The plaintiff Mr. Ren is a national senior human resource expert and specially invited as a senior engineer by the Chinese Academy of Sciences. Thus, he has a great reputation in the field of education and management. On March 12, 2015, Ren Jiayu ended his labor agreement relationship with the Beijing Daoyuxuan Commercial because

of a “Related search” suggestion feature provided by Baidu. These suggestions linked Mr. Ren with “Taoshi Education”, a company that had a reputation of being dishonest, with some arguments going as far as to claim that the company is a cult. Because Beijing Daoyuxuan Commercial Trading Company required performance by Mr. Ren with a high credit rating, both parties voluntarily terminated the contract.

Mr. Ren sued Baidu for seeking compensation for the loss of income resulting from the termination. He also wanted these six specific keywords to not appear in the "related search" suggestion when entering his name. In the court, Ren Jiayu admitted that although he did have business cooperation and media promotion with the "Taoshi Education" company, the cooperation between the two parties has ended already. However, the related searches did not reflect such kind of change in a timely manner. On the contrary, the content of related searches may mislead the public that Mr. Ren still cooperates with "Taoshi Education", thereby may scare off potential partners. Thus, Baidu's refusal to remove the information displayed in related searches has negatively impacted his life and subsequent job hunting, and even health. More specifically, he had applied for many jobs, but all be turned down since the relevant search suggestions have prevented him from obtaining trust from companies, causing his economic losses. Simultaneously, to maintain his reputation, he spends lots of time, money, and energy in contracting websites or online reputation management corporations and hiring lawyers, which significantly affects his daily life. Thus, He brought his complaint on the ground that Baidu was infringing his right to reputation, right of name. In addition, Mr. Ren claimed he had a "right to be forgotten." Because now Mr. Ren has no relationship with Taoshi

Company, the information should not continue to be widely on the internet. Instead, it should be forgotten.

1.2. Defense of Baidu: No knowledge, No intent, No human intervene

Baidu raised defenses from four aspects. First, the related suggestion provided by Baidu is an objective reflection of internet information and the relevant search. Baidu's related suggestion is automatically generated through a specific search algorithm based on two main factors: relevance and frequency of search queries at which people search the related terms. On the one hand, it will refer to the vocabulary that the user had entered in the search bar. On the other hand, it is predicted based on the big data generated by the previous search contents used by other users on the internet. Thus, the related suggestions will also dynamically change with the input by other internet users. Since there is no adjustment or human intervention, the service of "related search" is justified by its technical neutrality. Second, there was no infringement of Mr. Ren's right of name and the right to reputation. Third, the claimed right to be forgotten by Mr. Ren lacks a legal basis. Baidu believes that the right to be forgotten mainly refers to one's negative information, which does not apply in this case. Fourth, there is no evidence to prove that the spiritual suffering and economic losses were causally related to Baidu's search engine service.[187]

2. Judgement

[187] 参见北京市海淀区人民法院（2015）海民初字第17417号民事判决书（2015年7月21日）

2.1. Trial at first instance

The Court of the first instance, held that the legal disputes of the current case lie in the evaluation of the legitimacy of the technical model of "related searches." Specifically, it involves the factual judgment of whether Baidu's search service has been artificially interfered, and the legal judgment of whether the related business model of "related searches" violated Renjiayu's Right to reputation, right of name, and the so-called the "right to be forgotten." The Court first determined that there was no evidence of any human interference in generating the related search suggestion words. Then the Court focused on whether the Baidu's current technical model for "related searches" constitutes an infringement of the rights being advocated by Mr. Ren.

Regarding the right to reputation, the Court stated Baidu did not have any "specific intent" to harm Ren Jiayu. The generation of the related search suggestions may due to the media promotion carried out by Mr. Ren voluntarily or search keywords used by internet users. Furthermore, considering that Ren Jiayu did work with Taoshi Education, the related search suggestions, instead, has objectively reflected his work history. And the isolated keywords alone did not constitute independent expression. Thus, it cannot constitute an offensive or defamatory expression. Thus, the Court dismissed his claim of infringement of the right to reputation.

Second, obviously, there is no interference, misappropriation, or impersonation of Mr. Ren's name in this case. Thus, the use of the term "Ren JiaYu" in the related searches does not constitute an infringement of Mr. Ren's right to name.

Last, the court considered whether Ren Jiayu's right to personality was violated. Specifically, the court examined whether a new "Right to Be Forgotten" should be recognized under the framework of the "General personality right." The court stated: "The right of personality or the general personality right protects the subject's personality interests, including both the personality interests which have been categorized as statutory rights and the legitimate interests that have not been so categorized yet but should be protected by law". Concerning the latter, the following three criteria must be met simultaneously:

1. The personality interest cannot be contained by a typed right under China's law;
2. The personality interest must be legitimate; and
3. The personality interest must be necessary for protection

However, the court held that Ren Jiayu's "interest" in having information forgotten was not "legitimate and necessary for protection". Concerning the legitimate for protection, the judge believed that the plaintiff's interests to be forgotten contained two specific intentions: First is to confirm the reputation of a specific enterprise which he had cooperated with, either positively or negatively. The second is an attempt to conceal previous work experience from potential students and work partners on the internet.[188] For the first intention, the judge considered it was not appropriate to ask the court to confirm the company's reputation. The reputation of a company is protected by law and is subjective. Moreover, the

[188] 陈昶屹. 现有法律体系下“被遗忘权”案件的审理思路及保护路径——从我国“被遗忘权”第一案说起[J]. 法律适用(司法案例), 2017(02):41-46.

reputation of a company would change dynamically according to its operation. Thus, the claim for deleting relevant information is not legitimate since it implies to ask the court to confirm that “Taoshi company” has a poor reputation.

As to the latter intention, the work experience involved in the lawsuit is a reflection of the actual situation of the plaintiff's career one year ago, and the plaintiff still worked in the same industry. In addition, this information happens to form a portion of his professional history and his current individual credibility. Mr. Ren hopes to make use of his own good reputation in the industry to attract customers and students. Nevertheless, his personal qualification is important for the public that customers and students have the right to know and use it as a basis for reasonable judgments. In other words, such information is newsworthy. Thus, it appeared that the interest in being forgotten is not legitimate and necessary for protection. Thereby Mr. Ren's so-called "right to be forgotten" cannot be granted.

Regarding Baidu's liability, since the "related suggestion" service provided by Baidu is objective, neutral, and dynamically updated in time, Baidu is not at fault or conducts illegal behaviors. At the same time, if the ISPs fail to fulfill its "notice and takedown" obligation or cease infringement behaviors, it shall be liable for its own infringement or the enlarged part of the damage caused by infringement of other third parties. However, the premise of an intermediary's tort liability is the infringement by the intermediary itself or other third parties is established. In light of the fact that the right of name, the right to reputation, and the so-called "right to be forgotten" in the general personality right claimed by Mr. Ren have all been rejected, Baidu was not liable even it failed to fulfill the "notice and takedown"

obligation.

On the above basis, the court dismissed all complaints lodged by Mr. Ren against Baidu.

2.2. Trial at second instance

The Court of the second instance upheld the judgment made by the Court in the first instance. In particular, concerning the claim of the right to be forgotten, the Court confirmed the general personality right approach adopted in the lower Court. The Court held that the right to be forgotten belongs to a kind of personality interests. Thus, in order to obtain protection, additional arguments of the legitimacy and necessity of protection are required, which Mr. Ren failed to achieve. Therefore, the judgment of the first instance is upheld.

3. Comment

3.1. The legal basis of the “Right to Be Forgotten” in china: Comment on the general personality right approach

The existing Chinese law does not provide for an explicit written “right to be forgotten.” Although it still hangs in doubt about whether to recognize the right to be forgotten in China, there is less dispute to believe that the right to be forgotten contains personality interests. Therefore, the courts conducted trials from the perspective of the protection of personality rights. Under the current legal system, it is reasonable to protect the right to be forgotten under the approach but also has limitations.

3.1.1. The approach is reasonable

Article 2 of Tort liability law stipulates the protection of civil legitimate interests[189], which combined with the general provision of Article 6 concerning tort liability[190], constitutes the legal basis for protection to some civil interests that have emerged with the development of society and are not yet covered statutory personality rights.

In judicial practice, the recognition of general personality right can be tracked back to Article 1 of the "interpretation of the Supreme People's Court on several issues concerning the determination of liability for mental damage compensation in civil infringement" in 2001,[191] wherein the "personality dignity" and "personal freedom" stipulated in the first paragraph and the "other personality interests" stipulated in the second paragraph can be regarded as playing a role of general

[189] Article 2 of Tort liability law: Those who infringe upon civil rights and interests shall be subject to the tort liability according to the law , wherein the "Civil rights and interest" used in the law shall include the right to life, the right to health, the right to body, the right to name, the right to reputation, the right to honor, right of portrait, right to privacy, martial autonomy, guardianship, ownership, usufruct (用益物权) security interest（担保物权），copyright, patent right, exclusive right to use a trademark, right to discovery（发现权 ）equities (股权)，right of succession(继承权) and other personality and property rights and interests.

[190] Article 6 of tort liability: One who is at fault for infringement upon a civil right or interest of another person shall be subject to the tort liability.

[191] Article 1 of "interpretation of the Supreme People's Court on several issues concerning the determination of liability for mental damage compensation in civil infringements": individuals can file a claim for requesting compensation of mental damage to the people's court, if any of the following personality rights has been unlawfully violated:

(1) The right to life, right to health, right to body;

(2) Right of name, right of portrait, right to reputation, right to honor;

(3) Personality dignity, personal freedom.

Wherein in cases of infringing on privacy or other personality interests that violate public interests or social morality, the victim files a claim for compensation of mental damage to the people's court on the grounds of infringement, the people's court shall accept in accordance with the law.

personality rights. Given that the litigation model in China adopts a formalism of cause of action, any litigation must find a corresponding cause of action to determine the object and scope of the litigation.[192] Thus in 2011, the Supreme People's Court promulgated "the regulation of cause of actions in civil cases", wherein item 9 of the cause of actions involving "Personality rights dispute" specifics a "general personality rights dispute" as a miscellaneous cause of actions, in addition to the causes of actions corresponding to the other eight typed personality rights. This stipulation provides comprehensive protection for legitimate personality interests that have not been included in typed personality rights. And gradually, since a right to personal information has not been established yet, in judicial practices, many cases of personality rights and interests related to personal information are invoked under the category of "the general personality personal rights dispute".

Moreover, after the case of Renjiayu vs Baidu, Article 109 of the "General Principle of Civil Law" enacted in 2017 was regarded as a clause of "general personality rights"[193], which provides protection of personal freedom and personal dignity enshrined in Article 37 and Article 38 of the Constitution.[194] In addition, in

[192] The cause of action is the summary of the nature of legal relationship involved in the lawsuit adopted by People's Court.

[193] 尹志强. 论人格权一般保护之民法实现——兼评《中华人民共和国民法总则》第 109 条[J]. 新疆社会科学,2017(04):100-108+160.

[194] Article 109 of the General Provision of Civil Law: The personal freedom and dignity of a natural individual shall be protected by law.

Article 37 of the Constitution of the People's Republic of China: Freedom of the person of citizens of the People's Republic of China is inviolable. No citizen may be arrested except with the approval or by decision of a people's procuratorate or by decision of a people's court, and arrests must be made by a public security organ. Unlawful detention or deprivation or restriction of citizens' freedom of the person by other means is prohibited, and unlawful search of the person of citizens is prohibited.

the civil code adopted in 2020, Article 990 (1) provides an enumerated definition of personality rights and a pocket clause in the second paragraph, including natural persons' "other personality rights and interest based on personal freedom and dignity" in the scope of protection. Thus, it provides a normative basis and space for the protection of various personality interests that may emerge in the future.[195] It is noted that there is no distinction between the "general personality rights", "other personality interests," and "legitimate interests" mentioned in the article, which merely reflects differences between the legislative and judicial language.

Thus, the General personality right can be understood as a general provision for abstract protection of personality interests, which enshrine the personality dignity, freedom, and equality.[196] It is a comprehensive and flexible right.[197] In this sense, the general personality right implies a value of self-determination of personality and the right to exclude others from interfering with the free-development of their personality, which is consistent with the purpose pursued by the right to be forgotten.

Article 38 of the Constitution of the People's Republic of China: The personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited.

[195] Article 990 of Civil Code: Personality rights are the rights enjoyed by civil subjects which includes right of life, right of body, right of health, right of name, right of portrait, right to reputation, right of honor, right to privacy and so on.

In addition to the personality rights stipulated in the first paragraph, natural individuals enjoy other personality rights and interests based on personal freedom and dignity.

[196] 尹田.论一般人格权[J].法律科学.西北政法学院学报,2002(04):11-18.

[197] In Geman, the general personality right is regarded as a kind of framework right (Rahmenrecht in German). Although the academic circle still argues whether Article 109 create an independent right or legitimate interests (das rechtsgut). See:刘召成.民法一般人格权的创设技术与规范构造[J].法学,2019(10):34-48.

3.1.2. Limitation of the approach

The superiority of the general personality right lies in its inclusiveness, which has a wide space for interpretation. Therefore, it can provide legal protection of the new emerging personality interests that may arise along with the social or technological developments. The design of general personality rights guarantees the openness of the personality rights law. However, it is also precisely due to the flexible interpretation embedded with the essence of the general personality right, the content and boundaries of the right are uncertain.

Therefore, when asserting protection on the basis of general personality right under tort liability law, the illegality of the behavior needs to be actively proved through value judgment based on a case-by-case analysis, instead of presuming the illegality by default like other typed personality rights.[198] Because the interests are not stipulated by law lacks publicity of clear constitutive elements, individuals cannot know whether a specific behavior will harm others' interest in advance. Therefore, if legal interest protection is too broad, it will hinder people's freedom of behavior.[199] Therefore, it is necessary to conduct additional arguments when requesting judicial protection for non-statutory legitimate interests. In other words, it is up to the court to determine the scope and extent of protection of the personality interests at issue base on facts of specific cases.

At present, there is no mature view on the standards of judicial confirmation of

[198] 方新军.一项权利如何成为可能?--以隐私权的演进为中心[J].法学评论,2017,35(06):109-118.

[199] 王利明、易军，中国民法学的学术前沿问题，载《中国社会科学学术前沿（2006-2007）》社会科学文献出版社 2007 年版，第 314-315 页

civil legitimate interest. The determination mainly relies on the discretion of the judge.[200] The past judicial practice shows great uncertainty in the cases of generality personality rights.[201] In fact, Renjiayu's case also exposes the shortcomings of the approach. Although the standards of the "legitimacy of interest" and "the necessity of the protection" proposed in this case provide certain guidelines in judging the right to be forgotten within the existing civil law framework, it is relatively abstract and vague and is not specifically tailored to the context of the right to be forgotten or data protection. Especially, the judge's reasoning has ignored the value enshrining in the right to be forgotten and confused the structure of the right.

First, the judgment is slightly biased for ignoring Mr Ren's interest in informational self-determination. The plaintiff's request is based on the concern that related suggestions may mislead other internet users into thinking that he is still working at "Taoshi Company". In this perspective, the interest behind the request is to protect Mr Ren's online persona and information self-determination, which can justify its legitimacy.

Second, In the judgment of Renjiayu's case, the court denied the necessity for protection based on the public's right to know. Instead, it should be regarded as an exemption of the right to be forgotten.[202] The court should first confirm the

[200] When exercising the discretion, a judge can protect the interests by adopting the Application of analogy, or following the basic principles of civil law, such as the principle of public order and good social custom（公序良俗）, or making a decision with reference to custom or trading practice. See: 李建华, 王国柱. 论民事权益——民法保护对象的立法和司法双重确认[J]. 法学杂志, 2011, 32(01):第 30 页.

[201] 沈建峰. 论我国司法实践中的一般人格权制度 以司法机关公布的案例为考察重点[J]. 法律适用, 2009(08):23-28.

[202] 余煜刚. 司法视域下“被遗忘权”的逻辑推演与论证建构——以我国首例“被遗忘权”案的分析为切入点[J]. 北方法学, 2018, 12(02):34-44.

personality interest in the right to be forgotten is necessary for protection, then weigh the interest against the public right to know when there is a conflict. Thus, the logic of the argument is flawed since the court failed to confirm the necessity to protect the interests enshrined in the right to be forgotten.

Thus, due to the vagueness of the general personality rights for protecting the abstract interest of personality equality, dignity and freedom, it requires judges to do some interpretative and creative works to make the relationship between the general personality interests and the right to be forgotten more concrete and logical, so as to highlight the independent attribute of the right to be forgotten in the big data era.

Also, in the absence of explicit legal provisions and judicial interpretations by the Supreme People's Court, it would be reluctant for judges to support the plaintiff's claims due to concerns about the generalization of emerging new rights and other risks. In today's rapidly changing society, novel right assertions keep emerging. Judicial adjudication, as the last line of defense for the generalization of rights, is encouraged to solve the various emerging rights or interests of citizens based on the existing legal framework, which results in a relatively conservative attitude to new rights.

In the author's view, relative to the abstract interest of personality equality, dignity, and freedom, the right to be forgotten has its special value, that is, the informational self-determination of personal information. Thus, rather than treating the general personal right as an attribute of the right to be forgotten, it is more appropriate to regard it as the theoretical basis or source of the right.

3.2. Worthy of Forgetting?

In the case, the court rejected Mr. Ren's interest in being forgotten from the perspective of the relevancy of information and the public's right to know.

3.2.1. Data quality and the effect of time

Concerning the Data quality of the information, first of all, it was indeed true at the time when the information was published. The information about Mr. Ren's work experience was released through media promotion, voluntarily made by Mr. Ren himself while working for Taoshi Company.

Then the question is whether the passage of time has made it lose its original truthless? According to the logic contained in the right to be forgotten, the content of data stored online remains the same, but the reality is constantly changing. Thus, the accuracy of the data may decrease over time. After a period of time, it is necessary to re-evaluate the data's accuracy and correct the inaccuracy in time or delete and replace it with updated data. If inaccurate data remains on the internet, it will form a wrong image or even cause other harm or damage to the data subject. As Mr. Ren claimed, the related suggestions that appeared in the search box may mislead other internet users into thinking he still works at "Taoshi Company." Therefore, in the name of preserving his online reputation and avoiding unnecessary misunderstandings, the information should be forgotten.

Admittedly, since the suggested search words after inputting the plaintiff's name provide a little bit of context, they will assume that Mr. Ren is somehow related to the company when internet users see the suggested search words. Some of them may

keep such an impression without further dipping further information. In this sense, the suggested search words may have a slight tendency to mislead Internet users that the plaintiff still has a relationship with the company. However, in the big picture, Mr. Ren is still working in the related industry, and it has been only one year since he ended his cooperation with Taoshi. It even cannot be counted as outdated news. Thus, the information is considered to be relevant.

3.2.2. Ren Jiayu's role in society and the right to know

In this case, the court considered the conflict of interests between the plaintiff's interest in "forgotten" with the reputation of the company, as well as the potential students and partners' right to know. First, Mr. Ren is not an ordinary person as the plaintiff in the Google Spain case, but a public figure who has a certain influence in the education industry and has a degree of media exposure. Therefore, his privacy interest should be appropriately derogated. On the other hand, the information at issue is involved with his work experience, which has great public interests, coupled with its relevance and timeliness. Therefore, in balancing the conflicting interests, the public interests outweigh Mr. Ren's personality interest.

3.3. Baidu's liability: Safe card of "Technology Neutrality"

In the case, Baidu's liability lies in whether the search engine service provider has made artificial interventions and whether the business model of "related search" infringes Mr. Ren's "right to be forgotten". The court found that the business model of the "related suggestion" search service is objective, neutral, and dynamically

updated in time. Thus, Baidu is not at fault or conducts wrongful behaviors, and thereby was not held liable.

In fact, this is not the first time that Baidu has been sued for its related search function. As early as 2009, in the case of Jinde Pipe Industry v Baidu case[203], the plaintiff Jinde Pipe Industry company found that when inputting search terms such as “Jinde” “Jinde Pipe” “Jinde Pipe Industry Company Recruitment”, the “Related search” sections show “Jinde Liar” “Jinde Company Recruitment shady deal” and other similar suggestions, which seriously affected the reputation of Jinde Pipe Industry company. The court of the Second instance (Beijing No.1 intermediate people’s court) stated that because the related search terms were automatically generated, they only reflected the objective situation of the search terms used by internet users during a specific period in the past, and it aims at providing a reference for the current users. Thus, it is neutral and does not contain any substantive judgment. In this case, although the related search terms at issue did appear to have a certain negative implication, they were not essentially negative words subjectively controlled or created by Baidu, which means that Baidu has no substantial control over the formation of these search terms. Therefore, there is no subjective intention of Baidu to damage the company’s reputation. In addition, the related search function is justified for its purpose of providing searching references to facilitate internet users. Thus, Baidu should not be held responsible.

[203] 参见北京市第一中级人民法院（2009）一中民终字第 17680 号

From the two cases, we can see that the current judicial practices in china are relatively consistent on whether the search engine should take tort liability for its search results. Because the search results are automatically generated by the algorithm, and the algorithm has not been subjected to human intervention, the search engine provider does not have “subjective faults”. It should not be held responsible. The defense of “Technology Neutrality” has become a “safe card” for search engines to be exempted from responsibility in china.

Compared with judgment in the Google Spain case, the logic of the two decisions is quite different. The CJEU rebutted Google’s defense of no awareness from a perspective of data protection, reasoning that the processing of search engines could have far-reaching effects on individuals’ interests because of the core position in information dissemination. Thus, in contrast with Google Spain judgment, which set the preponderant value of the individual's private interest over search engines' economic interest as a general rule, the Chinese court has undoubtedly given more protection to commercial freedom. As a leading high-tech enterprise in China, Baidu has a substantial leading effect on the upgrading and development of the Internet industry. In fact, Judge Chen, the judge of the first instance, talked about the concern of social impact if the right is confirmed in judicial practice. Judge Chen concerned that once the judge confirms the right to be forgotten, it is equivalent to declare that other citizens can control any information related to them on the internet. Search

Engines like "Baidu" will bear a substantial burden for review and deletion, which may raise more problems than it actually solves.[204]

3.4. Judicial attitude to the right to be forgotten

From the analysis of the judgment both in the first instance and the second instance, the denial of legitimacy and necessity for protection is based on the specific fact in the case rather than denying the legitimacy and necessity for the protection of the right itself. Therefore, the rejection of Renjiayu's claim does not mean the complete denial of the value of the right to be forgotten, but rather shows a prudent attitude to the exotic concept.

Thus, the court did not directly address the conception of the right to be forgotten, nor did it place the right to be forgotten in the context of the right to privacy or EU's informational self-determination to discuss its legitimacy, but considered the effect of removing search results from a perspective of general personality right. In this way, the court avoids the question of whether the right to be forgotten has the value of being introduced in china and leaves more space for the academic discussion on the right to be forgotten. In fact, in the process of the second instance, there is a suggestion of reasoning based on the general tort liability approach. However, since it is difficult to prove Baidu's fault and causal relationship between the search keywords and damage of Mr. Ren, a reasoning based on the general tort liability will directly reject Mr. Ren's claim and completely avoid the discussion of the right to be

[204] 《结案状元“ 陈昶屹：敬畏法律，判案越多越如履薄冰》 http://news.sina.com.cn/c/nd/2017-10-20/doc-ifymzzpv7200597.shtml，最后访问时间：2020 年 10 月 14 日

forgotten.[205] Thus, the court gave up such a kind of reasoning and adopted a cautious but non-explicit attitude of rejection based on the specific fact present in the court.

[205] 丁宇翔.被遗忘权的中国情境及司法展开——从国内首例“被遗忘权案”切入[J].法治研究,2018(04):27-39.

Chapter 7 Reflection on the localization of the right to be forgotten in china

1. Basic attitude

1.1. Necessity: Fulfill the contemporary needs

The right to be forgotten is a new right assertion that has emerged with the advancement of technology. The birth of the right to be forgotten is a byproduct of the Internet's permanent storage and search engines' power searchability. With the potential risks to the personal dignity and personal liberty posed by the searchable, permanent Internet, the issue of the right to be forgotten becomes prominent.

1.1.1. The need to maintain digital personality

Dignity in the perspective of personal information protection is expressed as the right to be informed of the collection, storage, use of other's personal information and maintain the digital personality is consistent with the actual personality of the data subject. With the ubiquitous collection of personal information, individuals gradually become so-called "transparent people." After the personal information is disclosed, anyone has the possibility to access and further process the personal information. However, the added value of processes may be possible to change the content of the information that has been disclosed. Big data analysis may deviate from reality and result in wrong or misleading outcomes, especially analysis based on outdated or de-contextualized data. Since the public information online

constitutes the individual's digital personality in society, therefore, this improper processing may cause the social image of the individual to be distorted, which will further affect their right to participate in social life and personality development. Therefore, in order to accurately reflect oneself, an individual should have the right to request a correction, deletion of distorted or false information, so as to maintain the person's social image and meet the expectations of the individuals.

1.1.2. The need for the free development of personality

Although in principle, a person with full civil capacity is responsible for his action. However, no one is perfect, and everyone makes mistakes. What matters is we can learn from our mistakes and grow into a better person through the process. Therefore, an ideal tolerant society should give people who have corrected their mistakes a second opportunity to start again and protect them from haunted by the past. The forgiveness value underlying the right to be forgotten is helpful in forming a respectful, harmonious, and tolerant society.

Due to the perfect memory of the Internet, any trivial or foolish misdemeanor that is no longer or never be the subject of public debate and no prevailing public interest could be dug out after many years and result in an unsuccessful background survey for job seeking or load application. In addition, any misdemeanor has the risk of being overly magnified under the Internet with the effort of netizens. By concealing personal information that you don't want to be known by others, such as negative or embarrassing information, individuals can protect themselves from excessive criticism and ridicule and effectively avoid cyber violence, which is

conducive to the free development of personality and continue to conduct good interpersonal interactions.

As reflected in Renjiayu's case, people's demand to maintain an online reputation on the Internet increases. In the absence of the right to be forgotten, in reality, there are already many institutions or individuals which provide online reputation management service to help data subjects maintaining their image on the Internet[206]. By deleting, blocking, or even hiring people to leave positive comments on the Internet to help data subject to get rid of negative impact. However, such kind of business is still in a gray area of the law. The introduction of the right to be forgotten can provide people with a legitimate way to control online negative information about them, so as to pursue a healthy development of the data subject offline.

1.1.3. The need to manage online content

One objection to the right to be forgotten is the potential threat to internet archives. It is concerned that the future of online content will share the same destiny as the lost library of Alexandria if the internet archive got impeded. However, to achieve the purpose of cultural preservation, it is necessary to monitor the way how knowledge and culture are managed. Since the study on the persistence of the content on webs has shown that the internet more like a poorly organized warehouse, as opposed to an organized library. The internet itself is very lazy to categorize

[206] 郭小安,雷闪闪.“数据被遗忘权”实施困境与我国的应对策略[J].理论探索,2016(06):108-114

information as irrelevant or not[207]. Thus, the introduction of the right to be forgotten can satisfy the need for online information management through multiple parties' effort, filtering information with a low value on the web, so as to benefit the purpose of personality protection or cultural preservation at the same time.

1.1.4. Public interest in published information does not always outweigh an individual's privacy interest

During the information life cycle, the relationship between individuals' privacy interest and the public interest is always in a dynamic comparison. They are not absolutely superior to each other in the flux of time. Although the relationship between the value of information and time is still understudied, it cannot deny the possibility that the information has a disproportionately negative impact on the subject, or even his or her family but has no wider public interest as time passes. The right to be forgotten is justified in giving an individual a second chance to weigh the public interest with privacy interests in published personal information, which is beyond the scope of traditional privacy protection.

1.2. Obstacles of the localization of the right to be forgotten in china

Although people's privacy awareness has awakened after entering the information

[207] Korenhof, Paulan, et al. "Timing the Right to be Forgotten: A study into "time" as a factor in deciding about retention or erasure of data." *Reforming European data protection law*. Springer, Dordrecht, 2015. 171-201.

age, the value of freedom and efficiency should not be overlooked.

1.2.1. The inherent Obstacle: impact on openness of public opinion

In China, the function of traditional media playing in the public sphere is inherently insufficient. Social networks have successfully assisted the traditional media forming many major agendas that affect public life, penetrating all aspects of shaping the public sphere. Thus, social media provides the public with a platform for actively discussing numerous personalized, entertaining, and social issues.[208] Professor Weiguang Wu believed that one of China's major tasks is to use the media, especially the new media, to strengthen ties among members of society, shorten the gaps between different regions or groups, and finally enhance the consensus of the whole society. While in order to achieve this goal, it is necessary to strengthen the dissemination and organizational capacity of the media.[209]

Viewing from the realization of freedom of expression in China, the constitutional judicialization has not yet been fully achieved. Without truly "constitutional review",[210] Nor has a specific constitutional court that performs a function of interpreting the Constitution. In addition, the courts cannot directly invoke the Constitution in their judgment as the basis for their decisions. Thus, the

[208] 路鹃.个人信息自决权在中国社交网络语境下的再阐释——以情境脉络完整性为视角[J].现代传播(中国传媒大学学报),2019,41(11):74-80.

[209] 吴伟光.从隐私利益的产生和本质来理解中国隐私权制度的特殊性[J].当代法学,2017,31(04):50-63

[210] Although in 2018, under the deployment of the Communist Party of China (CPC) for "Deepening the reform of the party and State Institutions," the renamed "Constitution and Law Committee of the National People's Congress (NPC)" is responsible for the "constitutional review" at the legislative level. However, this is substantially different from the "constitutional review" in the judicial context.

freedom of expression, as a constitutional right, cannot get fully protected. As discussed in Chapter 3, it is difficult to have clear and easily operable standards in determining which information is worth forgetting. Either the principle of proportionality or the balancing framework provided by data protection authorities still leaves a great degree of discretion to the party that needs to decide. In this perspective, any abuse of the right to be forgotten may further compress the space of expression in the public sphere, turning the right to be forgotten into "a tool for information censorship."[211] Therefore, the transplantation of the right to be forgotten needs to be careful and require to pay attention to the institutional environment at the macro level.

1.2.2. The external obstacle: challenges in implementation

Besides the enforcement dilemma discussed in Chapter 4, due to china's national circumstance, there are extra obstacles in enforcing the right to be forgotten in china.

1.2.2.1. Contradiction with the development of information industry

It is said that the data is the new oil of the digital economy. In the era of big data, consumers generate massive data while enjoying services. Then these data enter a new round of productive circles, providing new productive factors for the digital economy. As far as an enterprise is concerned, it is impossible for enterprises provide

[211] 张浩."被遗忘"能否成为一项法律权利?——兼与杨立新、韩煦教授商榷[J].广西社会科学,2016(07):101-105

individuals with various customized services in the absence of effective data.

Viewing from the European practice, the right to be forgotten, while stimulating the imagination of informational autonomy, is not a right without cost. As the leading area to implement the systematic internet regulation, along with the most stringent personal data protection, the internet economic development in the European Union and the personal information protection do not seem to go hand in hand.[212] In the 2019 Internet Trends Report released by Mary Meeker, the "Internet Queen", among the top 20 of the Global Internet Market Capitalization leaders, 14 enterprises are from the United States, and the others include five Chinese companies and a Japanese Company. There is no Internet Company on the European continent.[213] In contrast, the U.S. has occupied the dominance of international trade through the internet industry. Bypassing the Communications Decency Act (CDA), internet industries are exempted from or restricted to intermediary liability. The loose regulation on the network industry has guaranteed a broad space for economic development. Thus, Judge Changqi Chen, who participated in the first instance of the Renjiayu vs. Baidu case, pinpoints the emergence of the right to be forgotten is the result of competition between the E.U. and the United Stated for information sovereignty. The purpose behind the E.U.'s right to be forgotten is to contain the control power over personal data hold by the U.S. tech-giant.[214]

Currently, the Chinese information/internet service industries have huge room

[212] 刘泽刚.欧盟个人数据保护的"后隐私权"变革[J].华东政法大学学报,2018,21(04):54-64.
[213] Mary Meeker's 2019 Internet Trends report is available at: https://techcrunch.com/2019/06/11/internet-trends-report-2019/
[214] 陈昶屹. "被遗忘权"背后的法律博弈[N]. 北京日报, 2014-05-21

for development and market potential. The informational industries have become the core driving force for the development of today's society. Thus, it is suggested to give a relatively loose policy and legal environment to boost the development of the emerging industry, instead of imposing a heavy burden on enterprises, especially to small and middle-sized enterprises (SMEs). The excessive protection of personal information will weaken the foundation and vitality of the technological innovation of enterprises in the information age. Tencent Research Institute, a social science research institution under Tencent, which is china's largest internet company, has published several reports expressing an attitude of caution or even opposition to the introduction of the right to be forgotten in China.[215] They believed that the right to be forgotten is an invalid burden. For individuals, the right is invalid since it is almost impossible to delete information on the internet. For enterprises, it is a heavy burden. The deletion of information in the internet age is often scattered among multiple systems. Once a user's information needs to be completely deleted, it is a complicated and expensive operation.[216]

1.2.2.2. Potential litigation will occupy judicial resources

The realization of rights requires support from the State. Almost every right carries a corresponding government obligation. Only when the public authorities mobilize public resources to punish non-compliance with the right, can the right be taken seriously.

[215] 杨乐，曹建峰，"从中国"被遗忘权"第一案谈网络治理路径的选择"，https://www.tisi.org/4631
[216] Ibid

As far as the right to be forgotten is concerned, once it is established in China, there will be countless “Mr. Ren” initiating litigation against Baidu or other search engines, which may squeeze the limited judicial resources and put pressure on the courts. China is currently undergoing a period of social transformation, and the public’s awareness of the exercise of rights has increased, which represents a huge challenge to scarce litigation resources. Therefore, when considering to establish new types of rights, we should not only consider the protection of individual rights, but also take into account the rational allocation of judicial resource, and find ways to maximize the use of judicial resource based on the historical and cultural traditions and national realities.[217] The current prominent problem in China today is information security problems caused by illegal leakage of personal information. It is worth weighing whether the judicial resource should be allocated to protect the interest in the right to be forgotten, which is at an advanced stage of personal information protection.

1.3. Summary

Legislative confirmation of an emerging right assertion is not achieved overnight. According to professor Yongqin Su, personality rights are very subjective, and it must be a right that is formed in society through a long process of mutual subjective discussion.[218]

[217] 曹全来.国情与司法模式构造的规律性研究——以司法供求关系为中心[J].法律适用,2014(05):50-55.
[218] 江平.民法的回顾与展望[J].比较法研究,2006(02):1-21.

As a country with the largest number of internet users in the world, many problems faced by western countries in the process of digitization also exist in China, such as human flesh searching, cyber violence, hate speech, information leakage, and malicious marketing. Thus, from a normative perspective, we argue that the right to be forgotten is necessary. On the other side, based on the national situation of china, the implementation of the right to be forgotten would face lots of hurdles. Introducing the European right to be forgotten in a rush may adversely affect the openness and integrity of public opinions, the development of internet enterprise, and the limited judicial resource in China. Thus, we need to consider the issue in a more prudent stance.

Moreover, In the legalization of emerging new rights, Chinese scholar QinTing Wang suggested that a distinctive Chinese path is gradually taking shape, which is a gradual approach to legislation based on "judicial lawmaking. "The "gradual legislative approach" takes the remedy of individual cases as the first step. The second step is the normative formulation by judicial interpretation. At last, the third step is the generalization construction of legal provisions.[219] Thus, currently, the protection of the right to be forgotten could be focused on the first step: strengthening the judicial relief in individual cases and exploring a rational argumentation model of the right to be forgotten. Ideally, when the legal attribute and protection standard of the right to be forgotten are clear in the future, it could become a right independently.

[219] 王庆廷.新兴权利渐进入法的路径探析[J].法商研究,2018,35(01):30-41.

2. Insights from the European's right to be forgotten

Although it is not ripe for China to introduce the right to be forgotten, as an attempt to solve the problem of "forgetting" in the digital world, the EU's right to be forgotten is undoubtedly having referential significance. In the following, we draw some insights from the European's right.

2.1. Reflection of the informational self-determination: control

Informational self-determination empowers individuals' control over their personal information. The theory of the informational-determination itself is relatively vague, which leads to the ambiguity of its application. In the perspective of implementation, it may cause both insufficient or overly protection of personal information.

First, following the theory of informational self-determination may cause insufficient protection of personal information. In an era of big data, individuals suffered from a consent dilemma both internally and externally. Internally, due to the high complexity of personal information issues and the high volume of privacy policy online, consent made based on fully understand is no longer realistic. Externally, with the development of technology, even if the data subject has never disclosed any sensitive information, the big data algorithm can guess and identify a specific individual by integrating non-sensitive information, even disparate in

different databases, or deduce sensitive information based on known information,[220] such as a prediction of a teenager's pregnancy based on her vitamin purchases.[221] That makes it is difficult for users to accurately predict the impact of their personal information while clicking "Agree".

Thus, due to the current online privacy policy issues, the control based on the current "inform and consent" mechanism is more than an ideal declaration and lacks substantive effects in a realistic context. Therefore, the right to be forgotten in Europe helps to compensate the shortcomings of the "inform-and-consent" model by giving the data subject a right to withdraw their consent in cases where processing is based solely on users' consent, especially in the context of social media.

On the other hand, following the theory of informational self-determination may cause over-protection of personal information. A broad interpretation of informational self-determination may lead to the effect of an "information island". The highest level of the value based on informational self-determination will be the individual's control over their personal information.[222] Following the theory of informational self-determination, the collection, use, or dissemination of personal information is prohibited in principle, unless obtaining consent from the information subject or having a legitimate interest containing in the information processing or

[220] Barocas, Solon, and Helen Nissenbaum. "Big data's end run around procedural privacy protections." *Communications of the ACM* 57.11 (2014): 31-33. Communications of the ACM **57**(11): 31-33.

[221] "*How Companies Learn Your Secrets*", CHARLES DUHIGG, Feb 16, 2012. The New York Times Magazine, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[222] 杨芳.德国一般人格权中的隐私保护——信息自由原则下对"自决"观念的限制[J].东方法学,2016(06):104-116.

legal grounds. Furthermore, the purpose of the collection must be specific and clear, and the subsequent information processing of personal information is bounded by the original purpose. Any information processing beyond the purpose is deemed to violate the right to informational self-determination. In daily communication, such a statement is obviously absurd. Especially when it refers to a person's negative information, the data subject often does not agree to any use or publication of such information. It will inevitably disrupt communication freedom and lead to prevalent personal information infringement in daily life. Thus, excessive data protection may make any processing of personal data becomes an extremely sensitive legal issue.[223] Secondly, it cannot be ignored that, with the benefit of the information society, more people are willing to give up a certain degree of privacy protection in order to make their lives more convenient.[224]

The internet benefits the whole society due to its interconnectedness of massive amounts of data and free sharing. An over-powerful right to dispose and determine personal information will cause the originally linked, and intertwined information/data chain and net returned to sporadic data fragments[225]. From this point of view, it is not conducive to the development of the information industry. Therefore, in order to prevent this phenomenon, the right to be forgotten must be constructed with extremely cautious, setting a precise boundary to prevent over-

[223] Veil, W. (2018). "The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law." Neue Zeitschrift für Verwaltungsrecht 10(2018): 686-696

[224] 谢远扬.《民法典人格权编(草案)》中"个人信息自决"的规范建构及其反思[J].现代法学, 2019, 41(06):P140

[225] 王婧琳. 论被遗忘的权利[D].山东大学, 2019.

protection of personal information.

The EU's right to be forgotten is established in data protection and embodies data subjects' right to information self-determination. As a positive right, the data subject can proactively challenge the retention of data that is publicly available online to the data controller and request deletion, regardless of whether it is sensitive information or whether it will cause damage in social evaluation of the data subject. Thus, it shows a high level of protection of personal information. The right may operate well in Europe with support from well-developed personal data protection legislation and ample judicial practice. It would not be the case in China. We don't need to set such a high standard for personal information protection in order to be in line with the world.

2.2. Reflection to the protection of published information: flexible balancing mechanism

In essence, the right to be forgotten is a deletion regime of public information. Traditionally, information that has been made public has lost its privacy interest, thus cannot be withdrawn into the private sphere. The innovation of the right to be forgotten has made it possible to withdraw public information back to the private sphere under specific grounds.

The birth of the internet has blurred the division of the public and private spheres in traditional privacy protection. In addition, China’s excessive attachment to the notion that privacy protection only covers information where is no public interest also makes it difficult to obtain remedies for privacy protection. As some

scholars suggested, in the protection of privacy, the involvement of public interest and the scope of the disclosure should not be considered on an "all or nothing" approach, but should be further assessed in terms of degree.[226]

Concerning the protection of published information in china, although it is not possible to establish a right to be forgotten system like Europe, where the dignity of human is paramount, it is considerable to learn from its balancing framework.[227] For example, in balancing the conflict between private interest and freedom of expression, a sound consideration can be made by taking into account factors including the data subject's role in public life, the nature of information, source of information, and time. We can adjust the weight of each factor based on china's privacy culture so as to harmonize with china's legal system. In this way, we can increase the openness of the privacy protection mechanism in China in order to adapt to the development of information technology. Considering the burden to search engines and potential judicial cost of the implementation of the right to be forgotten, the scope of the right to be forgotten should be strictly limited. In the author's opinion, drawing on the theory of contextual integrity, the scope of relief should be limited to information that is distorted from its original context and has a substantial negative impact on the information subject.

2.3. Reflection of Obligations of search engines

The right to be forgotten has correctly pointed out the independent value of

[226] 叶名怡. 真实叙事的边界 隐私侵权抗辩论纲[J]. 中外法学, 2014, 26(04): 第 957 页,
[227] 蔡培如. 被遗忘权制度的反思与再建构[J]. 清华法学, 2019, 13(05): 第 181 页

search engines in the dissemination of information. The search engine is not merely a tool for providing a catalog-style index, but an independent entity involved in the speech space that holds private power and has its substantive judgment.

As the judge noted in the Google Spain case, search engines play a pivotal role in information dissemination, which in turn shapes the public sphere of a democratic society. The emergence of the Internet has had the effect of decentralization, where information no longer needs to be disseminated through one or a few key media. Thus, it fundamentally changes the way information is acquired, distributed, recorded, and interpreted. In contrast, the individuals' ability to absorb information is not growing at the same pace. The sheer volume of information makes the attention of information recipients a scarce resource. The shortage of attention highlights the importance of organizing, classifying, and filtering information. The search engine that has mastered the key position of information dissemination undoubtedly stands in the central position of information dissemination[228]. Uta Kohl compares the search engine to "light bulbs" in cyberspace. Without light, we would not perceive the physical world we live in. Following in the same vein, without search engines, we cannot see the online world where we are surfing in.[229] Put exaggeratedly, the information provided to us by search engines has shaped our knowledge structure to a particular thing or issue to a certain extent. Moreover, search engines further blur the boundaries between online and offline, thus affecting the way we see the chunks of reality. In the context of data protection, in a world of "you are what Google says

[228] 赵鹏.搜索引擎对信息传播的影响及其法律规制[J].比较法研究,2018(04):188-200.

[229] Kohl, Uta. "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)." *International Journal of Law and Information Technology* 21.2 (2013): 187-234.

you are", Google's activities commonly affect the online identity of data subjects.

Corresponding to the public nature of search engines is the fact that only a few companies monopolize the industry. Thus, competition in the free market cannot provide effective constraints. Either the collection of online information or the update of search algorithms all require a lot of investments in infrastructure. Thus tech-giants have a greater advantage over small startups. The advantage will further be strengthened by the high reliance on internet users. The active inputs of internet users will, in turn, promote the improvement of search services, thereby further enhancing the dominant position of those tech-giants.[230] The dominant position grants those tech-grants a kind of private power, which is not authorized by law, but is obtained by its technology and resource to have the ability to carry out one's wills even if they encounter opposition in social relations[231]. If private power is left without regulation, there is a risk of abuse.

In addition to such a "private power", it is worth noting the nature of search engines is still profit-oriented. When search engines such as Google changed how information is delivered through a complex set of algorithms, including paid listing and related search suggestions, such algorithms are not totally neutral. Some extent of economic interests is involved. Therefore, it seems unfair to exempt liability based on technology neutrality while ignoring privacy or data protection.

On the other side, it is also clear that the current burden of search engines under the GDPR is too heavy, and it requires search engines to conduct a complex

[230] 赵鹏.搜索引擎对信息传播的影响及其法律规制[J].比较法研究,2018(04):188-200.
[231] 周辉.技术、平台与信息:网络空间中私权力的崛起[J].网络信息法学研究,2017(02):68-99+215-216.

balancing test of conflicting values, which is even not a simple task for a judge. Search engines, as online platforms, are obviously difficult to handle such a large scale of balancing work independently. At the same time, in the implementation of the EU's right to be forgotten, the process lacks external participation and constraints, and there is a large margin of discretion in its judgment, which implies the possibility of arbitrariness when faced with a large scale of deletion applications.[232] Thus, the legitimacy of the EU's right needs to be reinforced from the procedure. Multiparty participation or appropriate judicial intervention is necessary and justified.

2.4. Specific implementation method

2.4.1. Principle of proportionality

In the implementation, conflicts between the right to be forgotten, and related rights and interests should be reconciled through a case-by-case analysis. In this perspective, we can learn from the method of balancing tests in Europe, judged by combining the abstract principle of proportionality and concrete analysis with specific criteria.

2.4.2. Differentiation should be made on the data subjects

In order to balance the privacy of individuals with the public interest, the right to be forgotten can be appropriately restricted or enhanced according to different data subjects.

[232] 刘泽刚.过度互联时代被遗忘权保护与自由的代价[J].当代法学,2019,33(01，第 97 页

2.4.2.1. Natural person and legal entities

The right to be forgotten should only be available to natural persons. Legal entities and other organizations are inanimate. Thus, trade secrets or information owned by them are impersonal and should be regarded as the content of property rights, which can be protected by invoking intellectual property laws or unfair competition law when they are infringed.

2.4.2.2. Public figures and ordinary citizens

In the context of the right to be forgotten, whether the public figure has the right to be forgotten is a controversial issue. On the one hand, some scholars believe that public figures should be treated differently because their information is highly related to the public interest[233]. Assuming public figures are given the same level of protection as ordinary people, whenever unfavorable or negative news appears on the internet, public figures could immediately exercise the right to be forgotten, which will cause significant harm to the public's interest in accessing information. Thus, the public figure's right to be forgotten should be derogated. On the other hand, the concept of "public figure" in china is not officially recognized in law. First, the criteria for identifying public figures are unclear. And based on the particular time-oriented character of the right to be forgotten, it is necessary to consider the possibility of role reversal between public figures and ordinary. Second, the

[233] 杨立新,韩煦.被遗忘权的中国本土化及法律适用[J].法律适用,2015(02):第 31 页.

derogation of public figures' privacy interest goes against the Chinese traditional culture of "为尊 /长者讳" which means that it's best to say less about the shame, negligence, or shortcoming of the honorable, the wise, and the elderly people.[234]

In the author's opinion, rather than dwelling on the concept of "public figures", it is more efficient to determine, based on the value of the information and the purpose of the information to be disclosed. Thus, public figures' private matter, which is totally unrelated to the political and public interest of society, should also be protected.

2.4.2.3. Special treatment of minors and victims

Due to the particularity of minors, in constructing the right to be forgotten system, we should strengthen the protection of minors. As for children, their personalities are still in the processing of shaping and undergoing rapid changes. Compared with adults, they are more likely to do things on the internet that they will regret later because of their youthful exuberance. Thus, society should give much more understanding and opportunities to the minors.

In addition, victims should be given special treatment in the context of the right to be forgotten. For example, if pictures or videos of a young girl being abused are uploaded on the internet. Due to the ability of the internet to bring up information constantly, the girl would be suffered as being constantly reminded of such miserable memory. In such a case, for protecting the mental and physical well-being, public

[234] 苏力.隐私侵权的法理思考——从李辉质疑文怀沙的事件切入[J].清华法学,2019,13(02):第127 页

interest should give its way to the young girl's privacy interest.

2.4.3. Coordinate Alternative manners other than erasure

It is also suggested to coordinate the specific manner in which the right to be forgotten has been exercised. Deletion is not the only option for the effect of the right to be forgotten. Because a complete deletion of information has a great impact on freedom of speech and the right to know, sometimes deletion is not the best practice. Delisting, flagging[235], reordering ranking result[236], updating or correction, restricting access can also be taken as alternative ways to achieve an effect of forgotten to some extent. In this sense, the right to be forgotten can turn into a right to erasure, but also a right to anonymization, a right to reorder ranking in the context of search engines, a right to delist electronic links, or a right to restrict further dissemination, tailored according to different data controllers

3. Restore the virtue of forgetting beyond the law

3.1. Market

In constructing China’s system for protection of the interests in being forgotten, the value of freedom and efficiency should not be overlooked. The free flow and use of personal information can be achieved by strengthening the cooperation between data controllers and data subjects on the premise of promoting industry self-regulation.

[235] Cook, Hannah L. "Flagging the Middle Ground of the Right to Be Forgotten: Combatting Old News with Search Engine Flags." *Vand. J. Ent. & Tech. L.* 20 (2017): 1.

[236] Cooper E. Following in the European Union's Footsteps: Why the United States Should Adopt Its Own Right to Be Forgotten Law for Crime Victims[J]. J. Marshall J. Info. Tech. & Privacy L., 2015, 32: 185.

For example, it is suggested to allow the industry to promulgate self-regulatory norms based on its own circumstances and establish information retention periods according to different types of data.

3.2. Technology

For the problems caused by technology, it is an option to resort to the technical level to find solutions. When processing personal information, the industry should consider the impact of data retention and the disclosure on the individuals and set the appropriate expiry date according to their processing purpose. By implementing technical measures, digital storage devices can automatically delete information that has reached or exceeded the expired date. At the same time, by introducing the "user privacy preference" mechanism, it allows users to change the storage period on the software according to the actual situation flexibly.[237]

3.3. Culture

The right should not encourage some internet users, especially young generations, to be reckless with their speech and abandon a conservative attitude towards the internet with the mind that they can always delete what they write anyway. In the meanwhile, search engines and other internet companies, as data controllers, would be burdened with heavy deletion work. Therefore, the state and society should take various measures to improve citizens' quality of their internet behaviors. Schools can

[237] 郭小安,雷闪闪."数据被遗忘权"实施困境与我国的应对策略[J].理论探索,2016(06):108-114.

educate young people about the importance of protecting their privacy and the danger of recklessly disclosing personal information, while guiding them to develop healthy online behaviors.

Conclusion

Originating from the value of human dignity and informational self-determination, the right to be forgotten has been officially recognized as a statutory right by written in the EU General Data Protection Regulation (GDPR) along with the right to erasure. In fact, the right to be forgotten is a similar but not identical right to the right to erasure.

In the legislative process, the right has undergone an expansion both in the scope of the application and the subject of the obligation. The scope of the right to be forgotten has been expanded from withdrawal information posed by data subjects themselves to personal information that has been lawfully processed by a third party. And the subject of obligation was also expanded to search engines due to their decisive role in the dissemination. Generally, the right to be forgotten can be broadly regarded as a right to request deletion or restriction of the processing of personal data in the online environment. The added value of the right to be forgotten is that it provides data subjects more informational autonomy to re-exam subsequent data processing in facing the eternity effect of the internet.

The practice of the right to be forgotten in Europe shows that although the right to be forgotten has conflicts with freedom of speech, the public's right to know and freedom of commerce, it can be balanced by adopting the principle of proportionality and specific balancing criteria. But at the same time, by examining the compliance of Internet giants after the establishment of the right to be forgotten, it can be seen that although the right to be forgotten can be legitimate after repeatedly argument at

a theoretical level, it still poses a considerable challenge to freedom of expression and the operative burden when being put into practice. The effectiveness of the right to be forgotten has yet to be tested and refined over time.

Looking at the current status of private and personal information protection in China, China and Europe have a different privacy culture. Under the influence of collectivism and Confucius culture, both the cultural foundation and legal tradition of privacy protection in China are relatively weak. The future privacy system still tends to focus on promoting the exchange and communication of social information. On the other side, the protection of the personal information protection system has been established, but is still in the fundamental stage. Although the recent initiatives show a trend to enhance the protection of published information, it still has a distance from the protection level afforded by the right to be forgotten. The right to be forgotten is slightly ahead of the legislative processes in china.

In the judicial practice of the right to be forgotten: Renjiayu vs Baidu case, the judge opened up a path to protect the right to be forgotten through the general personality right. Although the rejection of Renjiayu's claim does not mean the complete denial of the value of the right to be forgotten, it shows a prudent attitude to the exotic concept, and also leaves more room for the discussion of the right to be forgotten in the academic circles.

Concerning the localization of the right to be forgotten, although the demands of being forgotten has existed in Chinese society, introducing the European's right in a rush may adversely affect the openness and integrity of the public opinions, the development of internet enterprise, and the limited judicial resource in China. Thus,

it is more appropriate to assume a prudent stance toward the new right that is still evolving. The introduction of the right to be forgotten should not be rushed.

References

Abril, P. S. and J. D. Lipton (2014). "The Right To Be Forgotten: Who Decides What the World Forgets." Ky. LJ 103: 363.

Abril, P. S. and E. P. Moreno (2016). "Lux In Arcana: Decoding the Right to Be Forgotten in Digital Archives." Laws 5: 1.

Ambrose, M. L. (2012). "It's about time: privacy, information life cycles, and the right to be forgotten." Stan. Tech. L. Rev. 16: 369.

Ambrose, M. L. (2014). "Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception." Telecommunications Policy 38(8-9): 800-811.

Ambrose, M. L. and J. Ausloos (2013). "The right to be forgotten across the pond." Journal of Information Policy 3: 1-23.

Ambrose, M. L., et al. (2012). "Seeking digital redemption: The future of forgiveness in the Internet age." Santa Clara Computer & High Tech. LJ 29: 99.

Ausloos, J. (2020). The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection, Oxford University Press.

Barocas, S. and H. Nissenbaum (2014). "Big data's end run around procedural privacy protections." Communications of the ACM 57(11): 31-33.

Bertram, T., et al. (2019). Five Years of the Right to be Forgotten. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.

Bernal, P.A., 'A Right to Delete?', European Journal of Law and Technology, Vol. 2, No.2, 2011

Chiou, W.-T. (2020). Limits and Prospects of the Right to Be Forgotten in Taiwan. The Right To Be Forgotten, Springer: 311-318.

Cook, H. L. (2017). "Flagging the Middle Ground of the Right to Be Forgotten: Combatting Old News with Search Engine Flags." Vand. J. Ent. & Tech. L. 20: 1.

Cooper, E. (2015). "Following in the European Union's Footsteps: Why the United States Should Adopt Its Own Right to Be Forgotten Law for Crime Victims." J. Marshall J. Info. Tech. & Privacy L. 32: 185.

Corcione, E. (2019). "The Right to Be Forgotten, between Web Archives and Search Engines: Further Steps at the European Court of Human Rights." Eur. Data Prot. L. Rev. 5: 262.

de Mars, S. and P. O'Callaghan (2016). "Privacy and search engines: forgetting or contextualizing?" Journal of Law and Society 43(2): 257-284.

De Terwangne, C. (2012). Internet privacy and the right to be forgotten/right to oblivion. VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet,[monografía online], IDP, Revista de Internet, Derecho y Política, UOC.

De Terwangne, C. (2014). The right to be forgotten and informational autonomy in the digital environment. The ethics of memory in a digital age, Springer: 82-101.

Druschel, P., et al. (2013). The right to be forgotten-between expectations and practice. I Congreso sobre retos sociales y jurídicos para los menores y jóvenes del siglo XXI.

Forde, A. (2015). "Implications of the Right to be Forgotten." Tul. J. Tech. & Intell. Prop. 18: 83.

Fuster, G. G. and R. Gellert (2012). "The fundamental right of data protection in the European Union: In search of an uncharted right." International Review of Law, Computers & Technology 26(1): 73-82.

Garstka, K. and D. Erdos (2017). Hiding in Plain Sight? The'Right to Be Forgotten'and Search Engines in the Context of International Data Protection Frameworks. The'Right to Be Forgotten'and Search Engines in the Context of International Data Protection Frameworks (October 1, 2017). Published in final form in the Report of the 2017 Internet Governance Forum (IGF) Dynamic Coalition on Platform Responsibility, University of Cambridge Faculty of Law Research Paper.

Henry, M. (2001). International privacy, publicity and personality laws, Butterworths.

Hoffman, D., et al. (2015). "The right to obscurity: How we can implement the google spain decision." NCJL & Tech. 17: 437.

Jacques, S. and F. Hempel (2020). The Right to Be Forgotten in the UK: A Fragile Balance? The Right To Be Forgotten, Springer: 195-222.

Jones, M. L. (2012). "You are what Google says you are: The right to be forgotten and information stewardship." International Review of Information Ethics 17.

Karas, S. (2002). "Privacy, identity, databases." Am. UL Rev. 52: 393.

Kaye, J. (2012). "The tension between data sharing and the protection of privacy in genomics research." Annual review of genomics and human genetics 13: 415-431.

Keller, D. (2018). "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation." Berkeley Tech. LJ 33: 287.

Kohl, U. (2013). "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)." International Journal of Law and Information Technology 21(2): 187-234.

Koops, B.-J. (2011). "Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice." SCRIPTed 8: 229.

Korenhof, P., et al. (2015). Timing the right to be forgotten: a study into “time” as a factor in deciding about retention or erasure of data. Reforming European data protection law, Springer: 171-201.

Kulk, S. and F. Z. Borgesius (2015). "Freedom of expression and right to be forgotten cases in the Netherlands after Google Spain." Eur. Data Prot. L. Rev. 1: 113.

Lee, E. (2015). "Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten." UCDL Rev. 49: 1017.

Lynskey, O. (2014). "Deconstructing data protection: The added-value of a right to data protection in the EU legal order." Int'l & Comp. LQ 63: 569.

Mantelero, A. (2013). "The EU Proposal for a General Data Protection Regulation and the roots of the ‘right to be forgotten’." Computer Law & Security Review 29(3): 229-235.

Mayer-Schönberger, V. (2011). Delete: The virtue of forgetting in the digital age, Princeton University Press

McNealy, J. E. (2012). "The emerging conflict between newsworthiness and the right to be forgotten." N. Ky. L. Rev. 39: 119.

Murphy, J. G. (1998). Forgiveness in counseling: A philosophical perspective. Character, Liberty, and Law, Springer: 223-238.

Nissenbaum, H. (2004). "Privacy as contextual integrity." Wash. L. Rev. 79: 119.

Parry, O. and N. S. Mauthner (2004). "Whose data are they anyway? Practical, legal and ethical issues in archiving qualitative research data." sociology 38(1): 139-152.

Post, R. C. (1989). "The social foundations of privacy: Community and self in the common law tort." Calif. L. Rev. 77: 957.

Post, R. C. (2017). "Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere." Duke LJ 67: 981.

Singh, A. P. and R. Setia (2018). "Right to Be Forgotten-Recognition, Legislation and Acceptance in International and Domestic Domain." Nirma ULJ 8: 3

Singleton, S. (2015). "Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD." Ga. J. Int'l & Comp. L. 44: 1

Slane, A. (2018). "Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow." Osgoode Hall LJ 55: 349.

Solove, D. J. (2003). "The virtues of knowing less: Justifying privacy protections against disclosure." Duke LJ 53: 967.

Tamò, A. and D. George (2014). "Oblivion, erasure and forgetting in the digital age." J. Intell. Prop. Info. Tech. & Elec. Com. L. 5: 71.

Tranberg, C. B. (2011). "Proportionality and data protection in the case law of the

European Court of Justice." International Data Privacy Law 1(4): 239-248

Tzanou, M. (2013). "Data protection as a fundamental right next to privacy?‘Reconstructing’a not so new right." International Data Privacy Law 3(2): 88-99.

Veil, W. (2018). "The GDPR: The Emperor’s New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law." Neue Zeitschrift für Verwaltungsrecht 10(2018): 686-696.

Voss, W. G. and C. Castets-Renard (2015). "Proposal for an International Taxonomy on the Various Forms of the Right to Be Forgotten: A Study on the Convergence of Norms." Colo. Tech. LJ 14: 281.

Whitman, C. B. (1985). "Privacy in Confucian and Taoist thought."

Whitman, J. Q. (2003). "The two western cultures of privacy: Dignity versus liberty." Yale LJ 113: 1151.

Xanthoulis, N. (2013). "The right to oblivion in the information age: A human-rights based approach." US-China L. Rev. 10: 84.

Zufall, F. (2019). "Challenging the EU's Right to Be Forgotten: Society's Right to Know in Japan." Eur. Data Prot. L. Rev. 5: 17.

Chinese Literatures

刘学涛, 李月, 大数据时代被遗忘权本土化的考量——兼以与个人信息删除权的比较为视角[J].科技与法律,2020(02):78-88.

谢远扬,《民法典人格权编(草案)》中“个人信息自决”的规范建构及其反思[J].现代法学,2019,41(06):133-148.

路　鹃, 个人信息自决权在中国社交网络语境下的再阐释——以情境脉络完整性为视角[J].现代传播(中国传媒大学学报),2019,41(11):74-80.

刘召成, 民法一般人格权的创设技术与规范构造[J].法学,2019(10):34-48.

蔡培如, 被遗忘权制度的反思与再建构[J].清华法学,2019,13(05):168-185.

王利明, 生活安宁权:一种特殊的隐私权[J].中州学刊,2019(07):46-55.

王婧琳, 论被遗忘的权利[D].山东大学,2019.

李立丰, 本土化语境下的“被遗忘权”:个人信息权的程序性建构[J].武汉大学学报(哲学社会科学版),2019,72(03):145-155.

苏　力, 隐私侵权的法理思考——从李辉质疑文怀沙的事件切入[J].清华法学,2019,13(02):109-128.

刘泽刚, 过度互联时代被遗忘权保护与自由的代价[J].当代法学,2019,33(01):91-100.

郑志峰, 人工智能时代的隐私保护[J].法律科学(西北政法大学学报),2019,37(02):51-60.

叶名怡, 论个人信息权的基本范畴[J].清华法学,2018,12(05):143-158.

赵　鹏, 搜索引擎对信息传播的影响及其法律规制[J].比较法研究,2018(04):188-200.

刘泽刚, 欧盟个人数据保护的“后隐私权”变革[J].华东政法大学学报,2018,21(04):54-64.

丁宇翔, 被遗忘权的中国情境及司法展开——从国内首例“被遗忘权案”切入[J].法治研究,2018(04):27-39.

余煜刚, 司法视域下“被遗忘权”的逻辑推演与论证建构——以我国首例“被遗忘权”案的分析为切入点[J].北方法学,2018,12(02):34-44.

刘文杰, 被遗忘权:传统元素、新语境与利益衡量[J].法学研究,2018,40(02):24-41.

满洪杰, 被遗忘权的解析与构建:作为网络时代信息价值纠偏机制的研究[J].法制与社会发展,2018,24(02):199-217.

王庆廷, 新兴权利渐进入法的路径探析[J].法商研究,2018,35(01):30-41.

方新军, 一项权利如何成为可能?--以隐私权的演进为中心[J].法学评论,2017,35(06):109-118.

吴伟光, 从隐私利益的产生和本质来理解中国隐私权制度的特殊性[J].社会科学文摘,2017(09):80-82.

杨　芳, 个人信息保护法保护客体之辨——兼论个人信息保护法和民法适用上之关系[J].比较法研究,2017(05):74-86.

周　冲, 个人信息保护:中国与欧盟删除权异同论[J].新闻记者,2017(08):71-79.

尹志强, 论人格权一般保护之民法实现——兼评《中华人民共和国民法总则》第 109 条[J].新疆社会科学,2017(04):100-108+160.

何雪莲, 隐私的辩证:被遗忘还是被观望?[J].南京社会科学,2017(07):120-127.

叶金强,《民法总则》“民事权利章”的得与失[J].中外法学,2017,29(03):645-655.

张里安,韩旭至,“被遗忘权”:大数据时代下的新问题[J].河北法学,2017,35(03):35-51.

徐　明, 大数据时代的隐私危机及其侵权法应对[J].中国法学,2017(01):130-149.

陈昶屹, 现有法律体系下“被遗忘权”案件的审理思路及保护路径——从我国“被遗忘权”第一案说起[J].法律适用(司法案例),2017(02):41-46.

张建文, 被遗忘权的场域思考及与隐私权、个人信息权的关系[J].重庆邮电大学学报(社会科学版),2017,29(01):24-30.

韩旭至, 搜索引擎对侵扰性自动提示内容的责任——兼评北京市第一中级人民法院(2015)一中民终字第09558号民事判决[J].私法研究,2016,20(02):249-270.

万　方, 终将被遗忘的权利——我国引入被遗忘权的思考[J].法学评论,2016,34(06):155-162.

杨　芳, 德国一般人格权中的隐私保护——信息自由原则下对“自决”观念的限制[J].东方法学,2016(06):104-116.

郭小安,雷闪闪, “数据被遗忘权”实施困境与我国的应对策略[J].理论探索,2016(06):108-114.

张　浩, “被遗忘”能否成为一项法律权利?——兼与杨立新、韩煦教授商榷[J].广西社会科学,2016(07):101-105.

李承亮, 个人信息保护的界限——以在线评价平台为例[J].武汉大学学报(哲学社会科学版),2016,69(04):109-120.

李　倩, 被遗忘权在我国人格权中的定位与适用[J].重庆邮电大学学报(社会科学版),2016,28(03):44-50.

郑晓剑, 比例原则在民法上的适用及展开[J].中国法学,2016(02):143-165.

张立翘,被遗忘权制度框架及引入中国的可行性[J]. 互联网金融与法律,2015.

张新宝, 从隐私到个人信息:利益再衡量的理论与制度安排[J].中国法学,2015(03):38-59.

谢远扬, 信息论视角下个人信息的价值——兼对隐私权保护模式的检讨[J].清华法学,2015,9(03):94-110.

杨立新,韩煦, 被遗忘权的中国本土化及法律适用[J].法律适用,2015(02):24-34.

杨临萍,姚辉,姜强.《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》的理解与适用[J].法律适用,2014(12):22-28.

叶名怡, 真实叙事的边界　隐私侵权抗辩论纲[J].中外法学,2014,26(04):956-977.

曹全来, 国情与司法模式构造的规律性研究——以司法供求关系为中心[J].法律适用,2014(05):50-55.

张礼洪, 隐私权的中国命运——司法判例和法律文化的分析[J].法学论坛,2014,29(01):11-19.

刘　晗, 隐私权、言论自由与中国网民文化:人肉搜索的规制困境[J].中外法学,2011,23(04):870-879.

李建华,王国柱, 论民事权益——民法保护对象的立法和司法双重确认[J].法学杂志,2011,32(01):27-30.

沈建峰, 论我国司法实践中的一般人格权制度　以司法机关公布的案例为考察重点[J].法律适用,2009(08):23-28.

白　奚, “仁者人也”——“人的发现”与古代东方人道主义[J].哲学动态,2009(03):77-79.

王利明，易军，中国民法学的学术前沿问题，载《中国社会科学学术前沿（2006-2007）》社会科学文献出版社 2007 年版

江　平, 民法的回顾与展望[J].比较法研究,2006(02):1-21.

张新宝，隐私权的法律保护(第 2 版)，群众出版社 2004 年版

尹　田, 论一般人格权[J].法律科学.西北政法学院学报,2002(04):11-18.

Korean Abstract (요약문)

인터넷상에서의 수많은 개인정보의 장기간 노출과 보유, 또 빅데이터 시대에 회사와 개인들이 데이터에 열광하면서 새로운 프라이버시 위기가 찾아오고 있다. 유럽 연합은 인터넷의 영원한 기억에 대한 법적 대응으로 '잊혀질 권리'를 내세웠고, 개인에게 특정 상황에서 자신의 정보를 인터넷에서 삭제하도록 권한을 부여함으로써 이번 프라이버시 위기를 해결할 수 있도록 했다. 이러한 권리에 대해 중국의 법 제도는 어떤 태도를 취해야 하는가? 유럽을 따라야 하는가, 아니면 이 문제에 대해 좀 더 신중한 입장을 유지해야 하는가?

잊혀질 권리는 유럽에서 새롭게 생겨난 권리이다. 잊혀질 권리를 구축하고 정착 시키려는 EU 의 시도를 연구함으로써 이 새로운 권리에 대해 명확한 시각에서 이해해 볼 수 있다. 따라서 본 논문은 EU 의 개인정보보호규정(GDPR)의 입법 및 잊혀질 권리 실행에 대해 면밀하게 탐구함으로써 '잊혀질 권리'의 함의를 정의하고, 법의 가치 충돌 및 현실적 집행 딜레마에 대한 분석을 시도하였다. 또한 이를 바탕으로 본 논문은 중국의 실정에 맞추어 잊혀질 권리의 중국에서의 도입 가능 여부를 검토하였다.

본 논문은 총 7 장으로 이루어져 있다.

제 1 장에서는 잊혀질 권리의 원리에 대해 탐구하고, 유럽에서의 잊혀질 권리의 탄생과 발전 기반에 대해 살펴보았다.

제 2 장에서는 역사 분석을 통해 EU 의 잊혀질 권리 관련 입법 과정을 살펴보고, 잊혀질 권리의 기본 가치를 규명하였다.

제 3 장에서는 잊혀질 권리의 가치의 갈등에 대해 다루고, 어떠한 데이터가 잊혀질 만 한지에 대해 탐구하였다.

제 4 장에서는 잊혀질 권리의 실행 딜레마, 특히 검색엔진의 역할과 데이터 통제자로서의 의무에 대해 논하였다.

제 5 장에서는 중국에 주안점을 두어, 중국의 프라이버시와 데이터 보호법의 틀을 개략적으로 서술하였다. 또한 EU 의 잊혀질 권리와의 비교를 통해 입법 동향에 잊혀질 권리가 내재되어 있는지 평가하였다.

제 6 장에서는 중국의 '잊혀질 권리 제 1 사건'으로 불리는 '런지아위 바이두 고소 사건'에 대해 분석하였다. 판결문 해석을 통해 중국 현행법의 잊혀질 권리 보호 경로와 거부 사유, 그리고 판결 배후의 법관 고려 사항과 태도 등을 살펴볼 수 있었다.

마지막으로 제 7 장에서는 중국의 잊혀질 권리 도입의 필요성과 현실적인 장벽 등의 관점에서 중국의 잊혀질 권리 도입의 실행 가능성을 분석하였다.