

Legislation of “right to be forgotten” in big data environment — Refer to EU 2012<General Data Protection Regulation>draft

He Zhile^{1a}, Huang Daoli^{2b}, Lei Yunting^{3c}

1 Key Laboratory of the Ministry of Public Security of Information Network Security,
The Third Research Institute of the Ministry of Public Security

2 The Third Research Institute of the Ministry of Public Security

3 The Third Research Institute of the Ministry of Public Security

a hezhile@stars.org.cn, b huangdaoli@stars.org.cn, c leiyunting@stars.org.cn

Keywords: big data; personal information; right to be forgotten; right to erasure

Abstract: In the big data era, for us humans, forgetting have been the norm and remembering the exception. “Right to be forgotten and to erasure” which proposed by Data protection reform of EU got widely attention and controversy. This paper discussed the importance of the “right to be forgotten” for the protection of personal information, researched on the specific content of “Right to be forgotten and to erasure” in EU<General Data Protection Regulation>draft, analyzed the legal status and defects of “right to erasure” in present stage of our country and proposed the legislation of “right to be forgotten”, in order to improve the security of personal information online.

1 background and significance of the right to be forgotten

Technology is not only changing the way of economic growth and human life, but also makes criminals and terrorist activities more efficient. The accumulation of explosive data becomes coveted resource, personal information with high use value and business interests evolved to positions that parties compete for. Digitalization, cheap memories, easy extraction and globalization create a round digital prison, which make personal information nowhere to hide. Traditional personal information protection laws have been insufficient to cope with the complexity of big data environment. So every country responses timely, they adjusted existed laws or enacted new laws to adapt to the development of information technology and increase the security of personal information.

1.1 background

Big Data has brought huge economic benefits and social value; it has become the next frontier domain for innovation, competition and productivity. However, the presence of immature cloud deployment and security vulnerabilities provide a platform for cyber crime and the application of hacking technology, which leads to personal information leak events emerge endlessly domestic and abroad. On December 27, 2011, 40 million accounts information of Tianya(a popular online forum) leaked. In December 2012, GhostShell hacker organization leaked 1.6 million accounts information from NASA, FBI, Interpol, the Federal Reserve, the Pentagon, and other key government agencies and companies. In November 2013, a report which named "20 million open house data" was downloaded crazily by netizens; In December, bank card account data of about 40 million customers of the U.S. giant retail companies Target were stolen.

Big Data has changed the way of search and extract information fundamentally, but led to the exposure of personal information more than that we expected. The right to be forgotten undoubtedly becomes a powerful weapon to cope with a variety of network attacks today when digital memory becomes popular and prevalent. In 2009, members of France put forward legislative motion on the "right to be forgotten". The motion pointed out that users can require the website delete contents related to personal privacy. In order to prevent the abuse of the right of Internet users, it also provides that the request must be issued by a registered letter. [1]In June2012, on the 41st British Parliament meeting for the first time, Columbia Information and Privacy Commissioner Elizabeth Denham proposed: a basic privacy principle is right to be forgotten, so in our law, the organization

retains information only for official purposes according to their needs, and then they would eliminate it. [2]In fact, this is proposed exceptions of the right to be forgotten applied.

In November 2012, EU proposed<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)>Bill (hereinafter referred to as the <Regulations>), which defined the "Right to be forgotten and to erasure". The data subject shall have the right to obtain the right to erasure personal data relating to them and the abstention from further dissemination of such data from the controller, especially when the data subject was a child. Even the bill needed to vote at the European Parliament plenary session to adopt and implement formally, it represents that the right to be forgotten has been regarded as a legal right.

1.2 the importance of the right to be forgotten

In the digital era, perhaps the most fundamental change occurring in humans is that the original balance is reversed between memories and forgetting. Information will be submitted to the digital memories which has become the default state, while forget have become the exception. [3]Twitter, Facebook and other social media and instant communication tools produced data growth exponentially every day. The features of openness and the rapid spread of the Internet make these data can reach anywhere in the world instantly and hard to lose. The long storage time and easy to get can increase the risk of personal information leakage, approximately 74% of the personal information face to the risk of being revealed. However, people's awareness of the protection of personal information is still weak. According to the survey , before joining a social networking site or using an online registration service, users who know these sites may collect and re-use their information account for only 54 %,only 33% of people concern about whether the authority responsible for protecting personal information. Personal information leakage event stake place frequently which prompting people to seek new ways to break the digital cage. Opinion polls show that up to 75 % of European citizens are willing to delete their personal information online. [4]With the time pass and drawbacks of the digital memory appear, there will be more and more people choose to delete their personal information online to avoid harm. Undoubtedly, the right to be forgotten becomes an important legal means for people coping with digital memory.

2 composition and evaluation of the right to be forgotten in<Regulations>

<Regulations>prescribed "right to be forgotten", also known as the "right to erasure", referring to the data subject have the right to require the data controller to permanently delete personal data about the data subject, unless the data retention have legitimate reasons. [5]

2.1 subject of the right to be forgotten

As can be seen from the concept, subject of the right to be forgotten contains rights subject and obligations subject. There is no doubt that rights subject is the data subject, including all person that stored data on the Internet. While obligations subject is controller, refers to business or organization etc which have rights to acquire personal information and conduct the collection and use. Section 4 of<Regulations> explained the data subject and the controller in detail, 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data. This shows data subject and controller's range is very wide, especially data subject, including almost every person who disseminate data via the Internet or other forms. Controller includes individuals, businesses, governments and other organizations getting the data in a variety of ways.

2.2 object of right to be forgotten

Object of right to be forgotten is personal information of data subject, it means any information relating to a data subject. There contains two meanings. First, information should belong to data subject rather than someone else, as defined within the data subject; Second, it should be personal

information, that means data subject should be person rather than the government, business, legal person or any other agency. Thus, the right to be forgotten born primarily to protect the personal information in big data era, it shows the weak position of the individual in the digital memory.1995<Data Protection Directive>of EU explained personal information in detail, "personal information" mean any information relating to an identified or identifiable natural person (data subject), an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

2.3 application conditions and exceptions

Proposed right to be forgotten entirely is to protect personal information, so the applicable condition is also starting from the individual, the only condition is that the data subject chooses their data is forgotten by Internet. However, if the law provisions directly such, it not only lack of executive power and maneuverability, but also easily lead to data subject abuse right to be forgotten and add controller's obligations. Therefore, legislation will generally give specific application conditions. Article 17 of the <Regulations>provisions, the data should be deleted when the purpose of the data collection or processing does not exist, the data subject objects to the processing of personal data pursuant to Article19.In order to prevent possible other case that data should be removed,<Regulations> increases provision, namely 17(1)d, it explicitly stipulated you can delete the data when data processing does not comply with<Regulations>based on other reasons, which provides a basis for deletion which may appear in the future.

17(3)provide four exceptions to the right to be forgotten, including exercise freedom of expression; reasons of public interest in the area of public health; for historical, statistical and scientific research purposes; compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. This means EU legislation gives individuals a broad option, as long as the Internet users want to terminate or prevent their data stored or spread in the network or other areas, they have right to exercise the right to be forgotten to require controllers to delete data but exercising the right not to harm the public interest and relevant obligations in Member states law. However, how should balance between public interests and personal interests in the course of exercise of rights while safeguard the public interest to lead not to exercising the right of be forgotten, how should compensate for the loss of the individual not reflected in the<Regulations>.

2.4 legal liability

<Regulations>provisions administrative punishment in violation of the right to be forgotten, "The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article17."Compared to other countries, right to be forgotten of the reform of the EU data protection contains subject, object, scope, exceptions and penalties, etc., it is more systematic and comprehensive and has merits. But punitive measures of<Regulations>is limited to the administrative level but not related to the penalty, and the provisions are too vague, not separating exceptions from limitations.

3 the current situation and defect of the right to delete in our country

3.1 the current situation of the right to delete

Strictly speaking, currently China has almost no legal raised right to be forgotten or delete directly, but there is provisions of deletion acts of obligations. Deletion as a right mainly reflected in the standard and the advice of the scholars.

3.1.1 law

Referred to delete in the existing laws of China including<Tort Liability Act>and<National People's Congress Standing Committee 's decision on strengthening the protection of network information> (hereinafter referred to as the<Decision>). Article 36(2)in<Tort Liability Act>related to deletion of personal information," Internet users make use of the network services to implement infringement act, infringer has right to notify the network service provider to adopt the necessary measures such as delete, shield, broken links, etc."Although the law just consider deletion as behavior of infringer rather than right, but this is one of the law that few mentioned legal deletion of personal information so far, it can regarded as rudiment of the right to delete in our country.<Decision>was passed in December 2012 which involved the entire life cycle of personal information including collection, use, transfer, destruction. Section 8 provides that "when citizens found disclosure of network information such as personal identity and distribute privacy and other legitimate rights, or subjected to commercial sexual harassment of electronic information, they had right to require Internet service providers to delete information or to take other necessary measures to stop."<Decision>expanded the scope of protected from the network users to the citizen which shows our country increased emphasis on the protection of personal information and had consciousness of the right to delete , it is a big step forward on our legislation.

3.1.2 standard

<Information Security Technology Public and Commercial Services Information Systems Personal Information Protection Guide>implemented in February 2013 defined the concepts and basic principles of personal information. Providing protections in the process of personal information collection, processing, transfer, delete, etc. The last article provisions "When personal information manager go broke or dissolve, if they are unable to continue to complete the promise of personal information processing purpose, they should delete personal information. When you delete personal information that may affect the law enforcement agencies investigate and collect evidence, it should take appropriate measures to store and shield. Compared to the <Tort Liability Act>, the Guide is more comprehensive about the provision of personal information protection and deletes behavior. It not only defines the concept, but also provides application of concrete conditions. But it only limited to delete personal information when the obligations subject disbanded, without the existence of any other circumstances. Compared to application conditions and exceptions of the provisions of EU right to be forgotten there is a big gap.

3.1.3 the advice of scholar

In contrast, the right to delete was more in-depth ruled in<People's Republic of China scholars draft Personal Information Protection Act proposed draft Model Law>which was released in June 2005. It not only defined the concept of deletion, but also detailed the application conditions and exceptions. Deletion apply to two situations: the data subject has right to request to delete personal information when it appears the illegal storage or it is no necessary for information processing subject know the personal information when performing duties. It can avoid to be deleted When appearing four cases as follows: Regulation and contractual provisions cannot delete; delete the information will harm the legitimate interests of information subject; due to storage mode or excessive fees should not suitable delete; according to the nature should not suitable delete.<Draft proposal>should be the most comprehensive on provision of personal information protection in our country, and provides a more systematic deletion behavior. But there is no corresponding penalty, the purpose of use of personal information because of public interest are also not included in exceptional cases. In addition, <Draft proposal>was just the advice of scholar, lacking of force of law and compulsory execution and operational.

3.2legislative defects of the right to delete

As can be seen from the upper, our laws basic did not put forward the right to be forgotten and just proposed to delete behavior of the network service provider, it was lack of systematic and scientific. Broadly speaking, our legislation lack relevant provisions of right to be forgotten, including application conditions, exceptions, the restrictive conditions, in violation of the punishments, etc. Application conditions is to prevent the abuse of rights exist, the main exception

was established in order to balance the relationship between the public and personal interests, and limits the exercise of a right is to remove excessive, has its own peculiarities. Punitive measures are an afterthought relief system which can compensate for the loss of data subject to some extent. It will be lost the original meaning if a kind of right lack penalties, and the penalty is necessary component for creating new right.

China's legislative is unscientific setting for subject of deletion behavior. First, provisioning right subject is the infringed of network users which is not only narrow but also not related to special populations such as children. Second, the scope of obligations subject is one-sided relatively. Big Data era, technology has made great strides and subject is more widely who has the ability to collect and use information, including individuals, corporations, governments or other agencies, but<Tort Liability Act>and<Decision>were only limited it to network services provider. It may make some subjects impunity that collect or use of personal information illegally and causing damage to information subject. We should establish right to be forgotten as soon as quickly, increasing data controller's binding rather than just stay in the standards or academic level.

4 legislation to build of the right to be forgotten in China

4.1 determine legal status of the right to be forgotten

A right gets recognized and implemented to rely mainly on legislation to determine status, but our law does not even clearly put forward the right to be forgotten, which will undoubtedly become barriers of personal information protection in big era. The scale of Population and economy determines the size of China personal information assets crown worldwide; our country should enact laws as soon as possible, so that the protection of personal information can keep up with the development of communications technology and global legislative trend. Since 2003, China began to discuss the Personal Information Protection Act; it has more than ten years but not also really was promulgated and implemented which show sit is difficulty. In our current situation, the real introduction may need a longer time. However, the further development of big data and the persistence of digital memories require us to determine the status of the legal right to be forgotten immediately. Personal information protection of<Decision> is the most comprehensive, so we can revise it and increase the right to be forgotten or raise existed deletion behavior to the right to be forgotten.

4.2 establish the dominant position of the child's rights

The limitation of age and cognitive led to children natural in a vulnerable position in the Internet, children do not have sufficient capacity to understand vulnerability of personal information and the consequences of exposure under the big data environment, so it should be on the special protection. We lack specialized legal like Children's Online Privacy Protection and there is no system of protection of personal information from children which will increase the information risk of children. Therefore, we can alone enact right to be forgotten of children and detailing constitutive requirements of rights to be forgotten of children. When children became the subject of right to be forgotten, the obligations should include not only controllers also guardian. In addition, it should clear obligations of guardian checking the children's personal information online and supervising controllers to delete information.

4.3 specified classification of data

Delete some data would have adverse effects for person or public utilities, such as financial, medical, transportation and etc., so data cannot be removed arbitrarily. In foreign legislation, these are all sensitive data, its collection, treatment and delete should be different from the ordinary personal data. Sensitive data should belong to the exceptions of right to be forgotten because of particularity. Keep sensitive data is in favor of protecting citizens' the property security and traceability of enforcement forensics to stable social order. Our laws do not even have the exact scope of sensitive data, there are also no provisions of classification of personal data which would become puzzle of the right to be forgotten exercised. China legislation should be classified on personal information and divide the categories of information into delete, prohibit the delete and extend the delete, which can restrict digital memories scientifically.

4.4 complete legal liability of the right to be forgotten

Analysis shows that any laws, standards and documents of our country did not mention legal liability that don't cooperate to perform the data subject's the right to be forgotten. The provisions of punishment should not only involve punitive measures of not deleted, but also delineate further responsibility about the consequences of delayed delete. In view of different harmfulness caused by these two kinds of behavior, punishment should be are differentiated. In contrast, not deleted will bring greater negative impact to the data subject, and pure administrative penalties cannot play a very good effect on deterrent and punitive, so criminal penalty should be introduced. Delayed delete should set for the deadline, if beyond the time it shall be treated as deletion, and take criminal penalty. In addition, in order to better protect the right of children, law should stipulate punitive measures when guardians bring children lost because they lazy to perform inspections and oversight obligations.

4.5 establish mechanisms for data storage deadline

Setting life for the data so that the data controller delete data in some future period which is third option balancing relationship between memory and forgetting the, it makes we know the relative value of the data. That is to say data inevitably closely linked with a certain time, and as time goes on, data will lose value and storage significance. Storage deadline is not a new concept and it is generally two years in foreign legislation. But in the digital age, the growth rate of data in future is likely to exceed storage space of computers and control ability of human. Data environments become more complex and growth new data in two years will far exceed deleted data. Technical and legislative of our country are not mature, so the two-year period will increase the risk of personal data revealed and the cost of data control. In summary, the storage period of 18 months can be considered on legislation. It not only protects the personal information to a greater extent, but also set aside time to investigate the case for the executive branches so that maintaining public safety.

5 conclusion

"Prism" incident which has attracted worldwide attention exposed deeply even though the country has the most robust democracy and the informatization of the most powerful in the world, it also use of the advantage in information technology field to collect and steal digital memories of other countries step by step, so legislation to build the right to be forgotten is imminent. On the one hand, the right to be forgotten and to erasure value us to learn and think which was put forward in the EU data reform; On the other hand, legislation should be based on the actual situation of the development of the Internet and big data, and combine with globalization tendency of technology and trade. Enacting the right to be forgotten which is not only adapt to national conditions but also accord with international trends in legislation.

Acknowledgements

This work was financially supported by the Shanghai science and technology commission project (13511504100).

References

- [1]CaiXiongshan. How to be forgotten in the network world –the latest developments of personal data protection in the network environment under EU and the enlightenment to Network planning[J] .Network Law Review.(2012)
- [2]Pierre-Luc Dusseault, M.P.Chair. Privacy and social media in the age of big data[R].Report of the Standing Committee on Access to Information, Privacy and Ethics.April,201341st Parliament, First Session.
- [3] Viktor Mayer-Schonberger. Delete: The Virtue of Forgetting in the Digital Age [M].Princeton University Press.(2009)
- [4] European Commission. Dam Protecftion: Europeans share data online, but privacy concerns remain new survey[EB / OL].(2012)
- [5] Wu Yan."The right to be forgotten" in network Information Age-Taking EU Personal Data Protection Reform as perspective [J]. Library Theory and Practice.(2013)