Research on Personal Information Protection System of Network Information Platform under the Background of Big Data

XueYijun¹, Zhou Zhide¹²*

¹School of Intellectual Property, Guilin University of Electronic Science and Technology, Guilin 541004, China
²Intellectual Property Research Institute, Xiamen University, Fujian 361005, China

Abstract—The core of an Internet enterprise is the data of the network platform, which usually includes a large amount of personal data and personal information. Big data refers to the massive, high growth rate and diversified information assets that require new processing models to have stronger decision-making power, insight, and process optimization capabilities. It is characterized by a large number, high speed, variety, value, density and authenticity. These ways and legal risks of leaking personal information everywhere on the network information platform. To effectively prevent and completely eliminate the leakage of personal privacy, the government should be taken as the leading factor and rely on all levels of society to deal with this issue from multiple angles.

1. BACKGROUND

In recent years, there have been numerous examples of personal information leaked by the platform. Citizens v. China Eastern Airlines Co., Ltd., Beijing Funa Information Technology Co., Ltd. in privacy disputes and Beijing Baidu.com Inc.’s reputation disputes with a citizen have suffered serious violations of their privacy and reputation rights. It affects people's normal production and life⁴¹. There are also competitions among Internet companies, such as the data dispute between Huawei and Tencent, and the case of Sina.com. It is not hard to find that in these cases, the focus of justice is to obtain another platform through one network platform through its own technology backend. Is this behavior legal when it comes to data on a platform? And who do these data belong to?

2. Analysis of personal information security in the era of big data

In the current big data environment, various things in life and work exist in the form of data, which leads to the gradual expansion of personal privacy from the real space to the data space. With the continuous enhancement of the collection and processing capabilities of big data technology, more and more personal life content has been digitized, recorded and tracked. For the sake of huge economic benefits, people constantly dig and analyze massive amounts of data, which brings huge hidden dangers to personal privacy and information security. The portability and openness of the wireless network make its security management face great difficulties. Wireless data transmission is fragile and unstable, and huge amounts of personal data are too scattered, making it impossible for group organizations to encrypt and protect all data. In this process, data is more likely to be hacked and cracked than wired transmission, so that personal privacy information is lost and leaked. Privacy information security is mainly reflected in two aspects, namely, the individual level and the social level. These two levels are nested and influence each other. Information leakage at the social level will cause harm to individuals to a certain extent. "Personal data” refers to the objective matter records attached to the carrier of the electronic information system, and is the original personal records that have not been processed; and the latter It refers to the useful information of the content with use value formed after the processing of personal data. Because data itself has no meaning, it only becomes information when it has an impact on the behavior of the entity. Data is the form and carrier of information; information is the connotation of data, it is loaded on the data, and has an interpretation of the data. I think that personal information is a legal object with independent protection shown on the data carrier, and the privacy of the data is directly related to the privacy protection of personal information.

A. Digitization characteristics of a large amount of information

Information digitization is a reflection of its natural attributes. In a real environment, data can be used to express people's language behavior and geographic location, making it easier for organizations or others to collect, process, and disseminate relevant information. At the same time, in the big data environment, all personal activities can be displayed in the form of data, such as mobile phone navigation, WeChat video screen, online banking and video call, etc. are displayed in the form of data. These data facilitate the collection, interception, and theft of personal data and other privacy infringements, and bring hidden dangers to privacy

*Corresponding author. Email: 854167177@qq.com
B. The characteristics of massive and mixed data

Due to the popularity of modern mobile smart devices, the frequency of smart devices in life has greatly increased. When people use these communication devices, they will generate huge amounts of data, which are diverse and mixed. The huge and mixed nature of data brings great challenges to data protection, especially in the process of data protection, it is easy to produce vulnerabilities and data leakage of databases and applications, which in turn leads to privacy and security issues.

3. Infringement under Internet big data: commonplace

First, the situation of cyber attacks is getting worse. Nowadays, private data of governments, enterprises or individuals are often obtained on the Internet through various means. Therefore, in the era of big data, data collection and protection have become the focus of competition. From the perspective of privacy, the era of big data has brought the Internet masses into an open and transparent "streaking" era. As we all know, features are the core technology of big data through super collection, storage, timely and accurate data processing capabilities and accurate prediction capabilities. These features have a natural threat to privacy.

On May 25, 2009, Yin searched for "Marine female Yin Mouyan" in the Baidu search engine operated by Baidu. In the search results, a large number of nude photos of the same woman, life photos and individual privacy of the human body were found. Photos of parts. The woman in the photo above was verified by the court, and the court confirmed that it was Yin himself. On the same day, it was found that there was an entry named "Sea Girl" in another column of "Baidu Encyclopedia" on www.baidu.com. Open the entry, and under "Marine Female? Personal Information", you can see "Name: Yin Mou; Gender: Female" and other materials, and there are detailed descriptions of the content of the event in other parts. "Naked". Terms such as "unsightly" describe the content of the photo. As confirmed by Baidu, as of the hearing date of this case, the content of this entry related to this case is still consistent with the content of the printed page provided by Yin Mou. Baidu’s actions clearly violated the citizen’s right to reputation and should bear tort liability. In the end, the court held that Baidu was at fault in the process of providing network services. Baidu did not take reasonable and necessary measures when it knew or should know that network users used its services to spread infringing content, which caused the network users to use their network services to infringe others. The right of reputation shall be liable according to law [4]. When people consume and browse web data, information is leaked quietly. For consumers, they cannot find out at which step their information was leaked. It is difficult to obtain evidence at the source.

In the era of big data, there are endless technologies to enhance the human senses. Sensory enhancement technology enables people to obtain information from the outside of the wall that they had to physically invade private houses in the past. The effect is equivalent to the effect of physical intrusion on the house. Is the legal nature of this behavior equivalent to illegal? What about the search? For example, in the case of Kyllöv. United States, an agent of the United States Department of the Interior suspected Kyllöv[3] Planting cannabis to use a thermal imager to scan the house to detect whether the heat released in the house is suitable for growing cannabis indoors. The case later caused widespread controversy. Another example is that the street view provided by Google is sought after by global netizens for its powerful functions, but at the same time it is also very questioned: someone can accidentally find the figure of a loved one who is no longer in the world through the Google Street View map; some people’s privacy has also been leaked. For example, the embarrassing experience of going out was captured by Google and uploaded to the Internet; some people's random behaviors in their own yards were captured and put on the Internet. A similar case asked Google to compensate 10,000 euros [4].

In short, the challenge of reputation to tort law in the era of big data is mainly concentrated in the following aspects: first, the infringing subject is difficult to determine, the information collection subject is diversified, the use of metadata is diversified, and the privacy of the infringement method makes the The subject is discovered; second, the value of the information makes the setting of tort law take into account multiple interests and is difficult to balance; third, the direct relationship between reputation and personal and corporate information is more elusive, and some information is under certain conditions Can be converted into interests, causing difficulties in legislation.

4. Status of network information protection at home and abroad

A. Multiple standards for Internet regulation in the United States

The Internet originated in the United States and was first spread and used in the United States and other Western countries. For the management of the Internet, the US government has accumulated a relatively complete system and measures. In the construction and management of the Internet, the US government has always played the role of promoter, neither overwhelming nor indifferent. The interests of the network industry, the audience, and countries have been coordinated to a certain degree through mechanisms such as government guidance, legal formulation, technical constraints, and industry self-discipline. The Communication Decency Act (CDA) is part of the 1996 Telecommunications Act of the United States and is one of the earliest efforts by Congress to regulate the Internet [5]. This regulation limits the freedom to disseminate information that is indecent or obviously disgusting, but not obscene. To a certain extent, the right of online reputation has been protected, but its relevant legislative content has been declared unconstitutional by the Federal Supreme Court. Therefore, after the law came into effect, it was questioned by human rights groups such as the American Civil Liberties Union (ACLU). In the case of Reno v. ACLU, The Federal
Supreme Court declared in the final judgment that the Anti-Indecent Communications Act violated the First Amendment to the Constitution\(^6\). Justice Stevens wrote in the summary of the judgment: "As a constitutional tradition, in the absence of evidence to the contrary, We believe that government restrictions on the Internet based on the content of speech will only limit the free exchange of ideas rather than promote it.

Taking into account the characteristics of the Internet compared to traditional media, the Federal Communications Commission (FCC) published in 1997 the "Network and Telecommunication Policy" report emphasized that the management of the Internet should follow the following two points: First, government policy should avoid unnecessary regulation; second, traditional media management norms cannot be fully applied to network management. Therefore, the United States does not have a universally applicable standard for the regulation of online public opinion, but multiple standards. Various interests There is an interest transfer relationship between the subjects. The government encourages the development of the Internet industry, but the Internet industry cannot infringe on the basic rights of the public. The flexibility reflected under the multiple standards makes the US Internet public opinion regulation stronger for the constantly changing reality Adaptability and adaptability\(^7\).

### B. Chinese current legislative model on online personal information

Chinese network information security legal system is imperfect, and laws and regulations are the standards of the network information security rule of law, which can play a role in regulating and protecting the entire network information management. But at present, there are incomplete and unregulated situations in Chinese network information security laws and regulations, which lead to managers failing to have a legal basis in the process of law enforcement, and the ultimate management effect will naturally drop. In addition, the main reasons for this phenomenon include that China does not pay much attention to the construction of the network information security legal system, and the update and development of the entire legal system cannot keep up with the pace of network development.

Network enterprises, service providers and data managers benefit from the huge wealth brought by the data economy, thus forming a big data industry chain. Most of the network applications they develop and operate need to give up personal privacy, and even grant back-end data to third parties. In the tradition of the civil law system, legislators have always included tort law as part of the debt law, but the development of modern social science, the inherent defects of the traditional debt law system, the variety of tort liability, plus The need for democracy and legal system has expanded the scope of rights and interests protected by the tort law, and its functions in the traditional debt law system are not enough to meet the needs of the times. Therefore, it has become a trend to separate the tort law from the debt law system and become an independent legislative model of the civil law system. Article 64 stipulates:"Owners request to provide registration materials of internet users who have committed infringement through the website. If the website operator refuses to provide the information without justifiable reasons, it shall bear corresponding tort liability\(^8\)."

### 5. to strengthen data privacy protection and maintenance and personal privacy information security countermeasures

In the era of web2.0, "Data is the core of the network, not documents or people, and these data are data that can be processed by machine recognition. Therefore, users can obtain information from the network as easily as querying a database without having to master Data organization structure of each website". Although it plays a huge role in the sharing and analysis of network data and the prediction of related industries, and to a certain extent, it has realized the concept of shaping the Internet, integrating open sharing, and creating the prosperity and development of the network, but its use cannot exceed the legal Boundaries, otherwise neutrality will become illegal, and such reptiles will face the risk of criminalization.

#### A. The government should strengthen the construction and supervision of personal privacy information service platforms and storage platforms

At present, there is no personal privacy information service and storage platform in my country that can meet the needs of society and the people. In the era of big data commercialization, personal information has enormous commercial value, and the government should strengthen supervision of personal privacy information services and data storage platforms. The government should also strengthen the supervision and management of personal privacy information service platforms and storage platforms of commercial companies such as Tencent, Alibaba, Baidu, Meituan, Toutiao, and Didi Chuxing. The government should formulate policies and take effective measures to urge the aforementioned companies to strengthen the management and supervision of personnel involved in privacy information operations, strengthen the inspection of network security equipment, and timely upgrade and maintain privacy information protection software.

#### B. Enhance personal privacy protection awareness

In the era of big data, social progress has accelerated through the flow of information, but the unreasonable use of personal privacy has distorted the original meaning of information flow. For users, in the era of big data, every corner of life is full of tentacles of Internet companies. People often like landing websites, traffic trails, search records, consumption preferences, frequent restaurants, receiving addresses, etc. Observed, recorded, and analyzed by thousands of eyes. Protecting personal privacy is a citizen’s right. However, unconsciously our information is tracked, split, traded, and shared. Technology may be neutral, but capital is profit-driven, and it is too fragile to restrict them with morality. In this regard, citizens should increase their awareness of data security and personal privacy protection.

#### C. Legislation regarding the protection of personal data as social public property
Whether it is personal data protection or reasonable protection of corporate data rights, it is necessary to focus on bottom-up cases to promote the formulation and evolution of data protection rules. When personal data information is protected as a public property, the fundamental change of relevant legislative is to shift the regulation of personal data information from the private law system to the public law system. The protection of personal information is the behavior that the state needs to undertake to regulate the use of public goods by the member of the society for national security and public interest. The protection and application of personal data information will not be an obligation between individuals and enterprises based on the protection of private rights. I think that the government should promote the sharing and use of personal data information for the public interest for legislative purposes, rather than directly protecting the private rights of individuals. When treating personal data as a social public object, the legitimacy of its use is no longer based on the efficiency of the "highest price" in the market economy, but on the public interest of improving social welfare. Therefore, the subject of its regulation is a public power organization, and the regulatory measures are public law rather than private law.

ACKNOWLEDGMENT

This research was financially supported by the Innovation Project of Guilin University of Electronic Technology Graduate Education (No.2020YCXS106) and Guilin University of Electronic Science and Technology Internet + Intellectual Property Rights Protection Research Think Tank (Guidian Science [2019] No.3).

REFERENCES