Advances in Social Science, Education and Humanities Research, volume 571
Proceedings of the 2021 5th International Seminar on Education, Management and Social Sciences (ISEMSS 2021)

The Impact of Big Data on People and Data Security Issues

Xiaomeng Li[1,a]

[1]*School of international education, Henan University of Technology, Zhengzhou city, Henan province, China, 450001*
[a*]*Corresponding author. Email: shilishuang@cas-harbour.org*

ABSTRACT
The era of big data is accompanied by scientific and technological progress and social development. Its emergence also brings great convenience to people's life and social production. However, there are also many data privacy security issues based on it. Privacy leakage will lead to all kinds of inconvenience in life, such as telephone or Internet harassment, and more serious is the loss of property. This paper focuses on in the era of big data, how people will be affected and how they should protect their privacy security in the face of the constantly emerging data privacy leakage problems, and gives suggestions by comparing the mainstream methods and problems to deal with data leakage at present. On the premise of legislation, the government should strengthen publicity so that raise the public's attention to privacy security, and at the same time cooperate with enterprises and platforms to establish an effective monitoring platform.

Keywords: *Big data, Personal privacy, Data security, Media platforms.*

1. INTRODUCTION

Along with the social development and progress of science and technology, the human life is more and more inseparable from the network. Mobile computers increasingly dominate the lives of people. People need to use network to deal with a lot of things every day, to accept information from others, and also publish their own information. Compared to the paper media era, now the generation of information and communication has become very quickly. All kinds of social media have gradually become the main platform for people to obtain information and express their opinions. The uses of Facebook already reach to a third of the world's population [1], and Weibo has 230 million daily active users. In such a high-intensity network life, our information is received and analyzed by the network big data every day, and then the algorithm will use this information to recommend things that it thinks people are interested in, and even divide people with different personalities, which have both positive and negative influences on people's life. Under the premise that the network holds a large amount of our private information, now people cannot ignore the problem about the security of network privacy. Nowadays, there are various kinds of crimes caused by privacy leakage. This paper aims to discuss the impact of network big data on people's lives and data security issues based on people's dependence on network social media.

2. BIG DATA ERA

With the progress of science and technology, big data has become the mainstream at present. It is not only large in scale, but also presents diversified modes. Big data refers to the integration of a large amount of information resources on the network, and then targeted investigations on these resources, stores and processes them, so as to obtain the corresponding valuable information and data [2]. The current big data technologies include data collection, data storage, data cleaning, data mining and data model, etc [3]. Acquisition, analysis and statistics of data information with the help of the information age and the ability to identify valuable information have become the main characteristics of the development of the big data era [4].

3. THE IMPACT OF BIG DATA ON PEOPLE

So far, network data calculus has become an inseparable part of our lives, and they also inevitably affect people's lives, whether it is ordinary entertainment

life or medical science and technology or other aspects. People can find their presence in everywhere. For example, shopping software calculates users' preferences from their browsing history and the user information, suggests items that the algorithm thinks they will be interested in wherever people can see them, increasing the time people spend browsing the web and the likelihood that they will buy more goods. An automated stream of "guess what you're interested" videos next to what people are watching may also cause people to unwittingly spend more time watching more videos. That's how the web makes money by using big data to attract clicks.

Network data are just like the goods on the shelves of a supermarket. The supermarket in real life may only be able to load limited goods to meet the needs of customers with speculation, but the network is large enough to master nearly unlimited data, and can provide one-to-one VIP services for each "customer" to meet all of their needs. However, unlike the real supermarkets, customers are not only buyers of these products, they are also providers of data products. Each "customer" participated in this "supermarket" also provides its own privacy for online algorithms to calculate, then use the data to quickly calculate your interests and even potential other possibilities, such as political ideas, religious beliefs or character.

Cambridge Analytica worked with the Donald Trump campaign to use data from millions of Facebook users to target them with ads and campaign materials during the campaign [5].

This example not only shows how Cambridge Analytica makes use of big data to analyze the personality of users, so as to push targeted information to achieve the desired goal, but also shows a phenomenon that people's data not only serve themselves, but also become other people's goods to serve and fulfill their needs and goals, finally even influence the decisions of these people who provide the data.

4. THE PROBLEM OF PRIVACY LEAKAGE

According to the "2020 Annual Observation Report on Privacy of China's Internet Mobile Apps". At the end of 2020, in the more than 500,000 apps in China, 66.48% of them violated the rules of "collecting personal information when users clearly disagree with it", and 61% of these apps violated the rules of "collect personal information without obtaining users' consent", 47.86% of these applications have the situation that "the frequency of collecting personal information exceeds the actual needs of business functions". All these will cause users' personal privacy to be stolen or even trafficked without knowing it and used by others. However, when the platform collects a lot of user information, the data security of the platform cannot be guaranteed. By the end of 2020, 104 vulnerability scans were carried out on more than 3.3 million applications in China, of which 82.72% had vulnerability risk. In the case of multiple levels of vulnerability in the same application, the "high risk" level accounted for 81.07% [10].

There are also different reasons for privacy leakage. Firstly, the public is not aware enough of privacy protection, so they easily fill in their own information on various websites and applications, and they easily trust the "staff" to tell others their personal information. There are many reasons for this situation, including poor publicity and the fact that many applications compulsively collect information about users before they can use their functions.

Secondly, hacking is much better than it used to be. In the first half of 2018, a total of 7,748 information system security vulnerabilities were collected and sorted by the National Information Security Vulnerability Sharing Platform, an increase of 16.5% compared with 6,653 in the same period of 2017 [9].

Thirdly, even now there are specialized information collection companies, specialized in collecting users' privacy information for sale to telemarketing teams or scam teams to make money.

The platform's overruling regulations, and the ignorance of users, and there are a number of vulnerabilities in data security, these series of operations eventually lead to the data leakage problem becomes increasingly serious. In July 2016, information leakage of AIDS patients occurred in China. As of July 22, a total of 498 patients from 127 regions of 31 provinces and regions in China had received fraudulent phone calls. In this case, their names, diseases and other information had been leaked [6].

5. COPING WITH PRIVACY LEAKS

Due to the concealment and other characteristics of Internet crimes, it is more difficult to maintain network information security, which also makes the network information security is facing a more and more severe situation. Therefore, it is necessary to establish a complete technical means and management system in order to better deal with the malicious use of network information by criminals [7].

At present, most of countries mainly take legislative intervention to deal with privacy leakage. For example, the European Union adopted the *Convention on the Protection of Individuals in Automatic Processing of Personal Information* as early as 1981, highlighting the protection of privacy rights in Europe. This was followed by the *General Data Protection Regulations,*

which ensured that personal data were accurate, updated, corrected and deleted, prevented illegal processing of data, and emphasized timely reporting to regulators. *The Personal Information Protection Law* of Japan promulgated in 2003 also emphasizes that the purpose of using data should be within a reasonable scope, preventing leakage and damage of data, emphasizing timely reporting of accidents and the study of effective measures to prevent such incidents. China has also passed the *Regulations on the Protection of Telecommunications and Internet Users' Personal Information* and the *Guidelines on the Protection of Personal Information in Information Security Technology Public and Commercial Service Information Systems*, and other laws stipulating against improper use, damage or tampering of data, so as to ensure that personal privacy data are legally collected.

The United States also legislates to ensure data security.In addition, they mainly adopt the mode of industry self-discipline. That is to say, on the basis of the broad framework set by the Basic Law, organizations or industries in different fields should formulate norms for the protection of personal privacy, and require enterprises in the same field to self-regulate and jointly abide by industry regulations, so as to promote and protect personal privacy information [8].

Although these regulations and modes have certain effects on information leakage containment, there are still some gaps between the theoretical implementation and the practical effect. For example, the European Union's unified legislation is restricted by most of small and medium-sized enterprises, and the restriction on cross-border Internet enterprises is limited [8]. It is no unified self-discipline standard for the mode of industry self-discipline in the United States, and the implementation is difficult in the face of the actual leakage situation [8].

6. PRIVACY PROTECTION METHOD

6.1. Establish a regulatory platform and system

Although there are many laws and regulations to deal with privacy leakage, the problem of privacy leakage of enterprise platforms is still mainly dependent on enterprises' self-consciousness. But in the situation of enterprises pursuing more profit maximization, most of the rules are also difficult to implement. Faced with such a situation, the government can cooperate with social media platform and enterprises to establish a third-party regulatory agency to conduct independent supervision and management of data. In this way, not only the data of various platforms can be monitored, but also the phenomenon of concealment or mutual concealment between the government and enterprises can be prevented due to interest conflicts in the self-supervision of enterprises. At the same time, the regulator can also regularly publish the data supervision to the public, punish the company platforms that violate the laws and regulations, and promote the implementation of relevant laws. But at the same time, people should also pay attention to the improvement of the regulatory system.

6.2. Strengthening the publicity.

With the progress of science and technology and the popularization of the Internet, the number of Internet users has increased significantly. As of June 30, 2020, the number of Chinese Internet users has reached 904 million [8], among which the number of young and old people has increased significantly. These people are often not vigilant enough in the face of data privacy leakage, or even unable to detect it. For one thing, they cannot avoid privacy leakage, when they meet the possible Internet fraud after privacy leakage. For another they do not know how to deal with it. For this group of people, governments should be strengthened publicity, through television, radio and even community speeches and other ways to strengthen people's awareness of privacy protection, focus on all kinds of situations where the privacy may leak, improve their ability to distinguish. At the same time, the publicity should also emphasize how to use the law to protect oneself and recover the property cheated in the face of privacy leakage and network fraud.

6.3. Improving user participation in the network platform

Part of the reasons for users' privacy leakage is that they are strange to the network and do not know which behaviors can be avoided and which operations can protect their privacy. Therefore, the platform should be more open, improve users' participation in various media platforms, and supervise their own information and data from being leaked. For example, social platforms or applications to open part of the background data to users, so that users can intuitively see their own data, which are at risk of leakage. On this basis, these measures let people decide what can be filled in, and which data cannot be used, and also set reminders to avoid risky behavior.

7. CONCLUSION

Under the premise that the development of big data is irreversible and people's personal privacy is becoming more and more commercialized, data security has become the most important thing and must be solved. At present, the maintenance of data security requires not only the efforts of citizens themselves, but also the efforts of the government to improve legislation and platform supervision. Only when data security is

maintained, can the role of big data be better played and contribute to social development.

REFERENCES

[1] B.C. Sacha. The ‘Silicon Six’ spread propaganda. It’s time to regulate social media sites. The Washington Post. 2019.

[2] Z. Tao, R.F. Li. Computer network information security and protective measures under the background of big data[J].Information and Computers (Theory Edition), 2020, 32(18):202-204.

[3] P.Q. Tang, X.J. Dai. Application analysis of computer network security technology based on big data era. Network security technology and application, 2021(06):52-53.

[4] H.Y. Chen. Computer information security and privacy protection strategy under the background of big data. Network security technology and application, 2017(11):8.

[5] G. Hannes, K. Mikael. The Data That Turned the World Upside Down. 2017. https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win

[6] G.L. Ma, X. OuYang,, L. Li, G.W. Chen. Discussion on the subsequent impact of information leakage of a suspected AIDS patient in Xiamen City. Journal of Practical Medical Technology, 2021, 28(05):630-631.

[7] W.Y. Wang, Y.F. Wang. Reflection on network information security problems and countermeasures. Application of network security technology, 2021(06):164-165.

[8] H. Zhang. Research and enlightenment on the protection mode of citizens' personal information in the era of big data. Network security technology and application, 2021(06):59-61.

[9] J.Y. Wang. Research on the Privacy Protection of College Students in the "Internet +" Era. Technological innovation and productivity, 2020(09):86-88+91.

[10] 2020 Annual Observation Report on Privacy of China's Internet Mobile Apps https://m.sohu.com/a/446622858_255316?ivk_sa=1024320u