

Research on legal issues of personal information security protection of college students in the era of big data

—Taking the undergraduate students of China University of Geosciences (Beijing) as an example

Xin Hu, Ruoxi Wang, Fenglin Zhang *

School of Economics and Management, China University of Geosciences, Beijing, 100083

* Corresponding author. Email: zhangfenglin0318@163.com

Abstract. In this paper, we investigate the protection of personal information of college students and find that there is a certain degree of leakage of personal information among college students themselves, colleges and universities, society, and the law, especially college students' lack of awareness of personal information security protection and protection of rights and interests. Therefore, for the healthy development of society, it is necessary to strengthen the protection of college students' personal information, and protecting the security of college students' personal information is an inevitable requirement to safeguard the rights and interests.

Keywords: Personal information security, big data era, legal system, personal information protection.

1. Introduction

The first paragraph of Article 4 of the Personal Information Protection Law clarifies the definition of "personal information". "Personal information" refers to all kinds of information related to an identifiable or identifiable natural person recorded by electronic or other means, excluding Anonymize. Process information. Personal information processing includes the collection, storage, use, processing, transmission, provision, disclosure, etc., of personal information[1].

Before enacting the Civil Code, regulations on personal information were sporadic. The "Personal Information Security Specification" provides more detailed guidance and reference for enterprises to collect, use, share personal information and handle personal information security incidents, but the level of legal effect is low [2].

After the promulgation of the Civil Code, Article 1034, paragraph 1, clearly defines personal information as "all kinds of information that can identify a specific natural person, alone or in combination with other information, recorded electronically or in other ways"[3]. Under the influence of the introduction of civil code legislation and the combination of theoretical theory, "personal information protection" has been written into the personality rights section of the civil code, indicating the recognition of the personality attributes of "personal information protection" at the legislative level [4]. The promulgation of the Personal Information Protection Law on August 20, 2021, means that the protection of personal information rights and interests has entered a new chapter [5]. Improve the legal system for personal information protection, and prevent and punish acts that violate the rights and interests of personal information. The essence of the "Personal Information Protection Law" is the code of conduct for personal information processing activities, and its core is "regulating personal information processing activities". Only by consolidating the link of "regulating personal information processing activities" can we realize personal information rights, promote the rational use of personal information, and conform to the development of the era of big data [6].

2. An overview of college students' personal information security protection

2.1. Classification of personal information in the era of big data

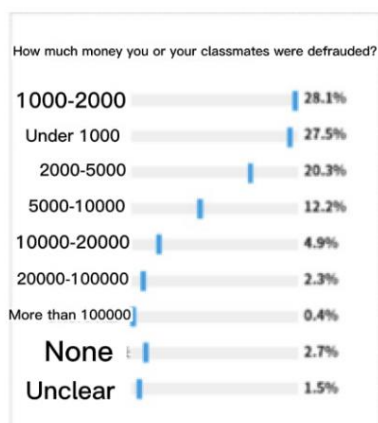
Based on the sensitivity of personal information, it is divided into sensitive personal information and ordinary personal information. Sensitive personal information is personal information that, once leaked or used illegally, may lead to personal discrimination or serious harm to personal and property safety [7]. Whether a specific individual can be directly identified is divided into direct personal information and indirect personal information. Whether or not personal information is disclosed is divided into disclosed personal information and undisclosed personal information.

2.2. The protection of personal information of college students in the era of big data

College students are the frontier groups in modern society. They are progressive in thinking, dare to explore, and are full of innovation. They are the first people to come into contact with emerging things. Therefore, they are also the leading force in the era of big data. However, due to their lack of social experience, they cannot distinguish the information on the Internet very well, and they are easily confused by the virtual information on the Internet. The situation of information leakage is very serious. Relevant data are shown in Fig.1 (a)-(c). From these data, it can be seen that information leakage and Internet fraud are not far away from us. The number of college students who are deceived by information leakage and the Internet every year is huge, seriously damaging college students' health. Economic interests and mental health even affect the normal order of colleges and universities. In the era of big data, today's college students have become a key trap area for personal information protection.

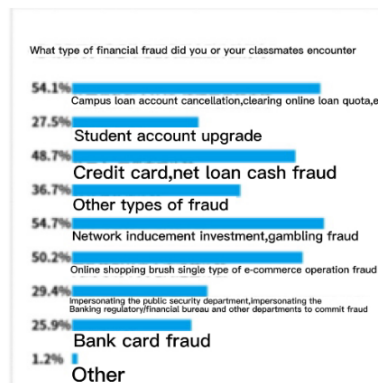


Percentage of college students cheated
(a)



College students were cheated amount distribution

(b)



The scene distribution of financial fraud encountered by college students

(c)

Figure 1. Investigation report on financial anti-fraud of college students

2.3. The harm of personal information leakage of college students

Through investigation and analysis, it will violate the personal privacy rights of college students, violate the economic rights and personal rights and interests of college students, cause psychological panic on campus and destroy the normal teaching order.

3. Necessity and existing problems of personal information protection of college students in the era of big data

3.1. The necessity of personal information protection for college students

As a special group of college students in the new era, the leakage of their personal information not only exists but is very serious. As an emerging generation, college students have a large number but have little experience. They lack self-protection awareness and are not prepared to fill in their personal information, as shown in Fig. 2. Through the survey data, we found that personal information leakage is displayed in Fig. 3, and the specific results are shown in Fig. 4 and Fig. 5.

What are the ways you think your personal information has been leaked?

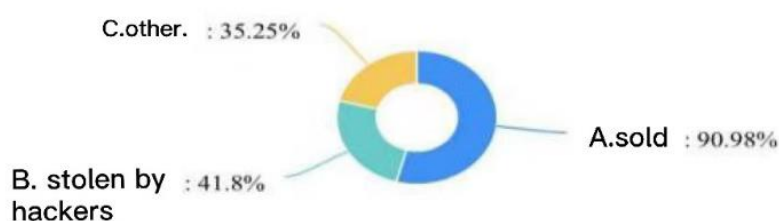


Figure 2. Survey on personal information protection of undergraduate students in china university of geosciences

Do you often receive a series of anonymous calls or text messages containing your personal information?
[Single Choice]

Options	Subtotal	Percentage
A Yes	71	58.2%
B No	51	41.8%
Number of people filled in this question effectively		122

☒ Pie-shaped
 ☐ Ring
 ☒ Columnar
 ☐ Bar

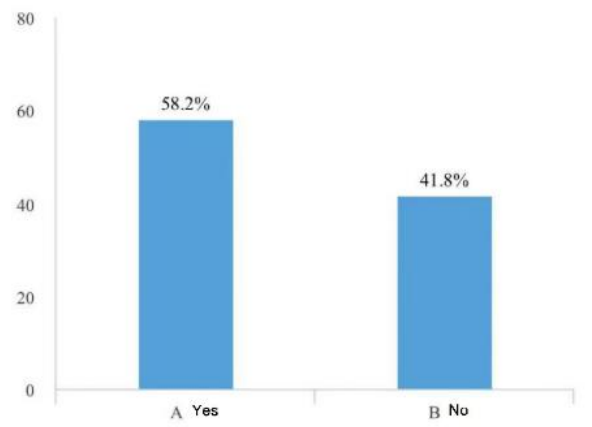


Figure 3. Personal information leakage of undergraduates of china university of geosciences (Beijing)

Have you ever considered that your information will be leaked?
[single choice]

Options	Subtotal	Percentage
A.very worried	77	63.11%
B.not worried	10	8.2%
C.don' t care	35	28.69%
Number of people filled in this question effectively		122

☐ Pie-shaped
 ☐ Ring
 ☒ Columnar
 ☐ Bar

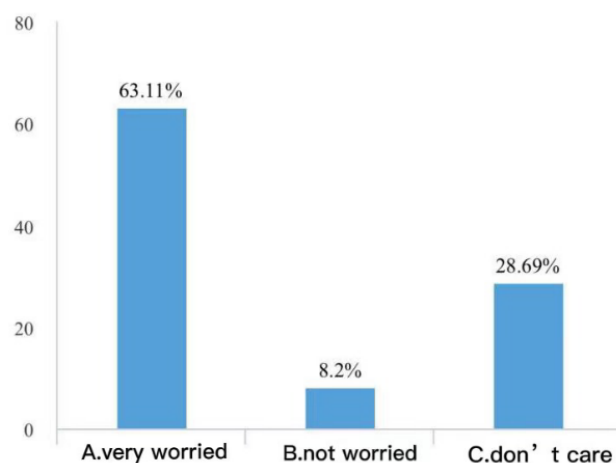


Figure 4. Information leakage of undergraduate students in china university of geosciences (Beijing)

3.2. Problems existing in the protection of personal information of college students at china university of geosciences (Beijing)

3.2.1. College students' personal information security protection and rights protection awareness is not strong

As young people enter society, college students lack experience and discernment, and their relatively shallow understanding of social environment and sophistication has resulted in insufficient protection of personal information. In addition, college students have a long time to receive quality education but a short time to contact social practice. The simple and undefended thinking of being kind to others cannot cope with the diversified social environment, and they are easily deceived by criminals to believe in others. In particular, with the rapid development of the Internet nowadays, college students' daily study and work are inseparable from the virtual network, and there is a risk of information leakage among the various study websites. For example, students are likely to provide their name and phone number to log in to the website in order to inquire about the subject. After illegally obtaining personal information, they will continue to receive calls from training institutions related to the subject inquired in the next few days. In short, due to its own characteristics and the external environment, the protection awareness of college students' personal information cannot avoid omissions. Furthermore, although the public's legal awareness is gradually improving, even college students who have received higher education have little understanding of the specific ways to protect their rights. Many victims choose to give up their rights because they can't do anything.

3.2.2. Lack of education on personal information security in colleges and universities

Schools are one of the primary living environments for students. As the author mentioned in the above necessity, colleges and universities hold a large amount of detailed personal information of students. They have important responsibilities and obligations to secure students' personal information. College students lack personal information security knowledge and have a single way to obtain it. Generally, the education of students in colleges and universities focuses on the ideological and political education of students by student counselors. Before and after the semester, various safety education activities are carried out by class as a unit, such as enrollment education, fire education, and mental health education. There is basically no popularization of safety knowledge education in the face of personal information. There is an urgent need for schools to pay attention to the security of students' personal information and give students a more systematic education on the protection of personal information.

3.2.3. The legal system for personal information security protection is not yet perfect

Personal information protection was not perfect before the promulgation of the two laws. Through previous searches, I found that the legal provisions on personal information are relatively scattered. Citizens who want to defend their rights do not even know which law to start with [8]. Although the "Civil Code of the People's Republic of China" promulgated in 2020 separates privacy rights from personal information, and the "Personal Information Protection Law" was promulgated on August 20, 2021. In China's current personal information security in my country, generally speaking it will take time for the public to understand and apply the new law. Besides, there is no special law enforcement department dedicated to managing personal information security. The reasons mentioned above make it difficult to safeguard the rights of college students after their personal information is violated.

3.2.4. In the era of big data, it is difficult to investigate and deal with crimes related to personal information

In the era of big data, the expansion of the scope of personal information protection and the wide range of leakage channels make it difficult to investigate and deal with crimes related to personal information. Due to the phenomenon that the infringed person is aware of personal information leakage, it is difficult to provide evidence or trace the source of the leakage afterward. In cases related to online personal information infringement, it is often difficult for public security to investigate and obtain evidence. Criminals often use different means in cybercrime, and in order to evade

investigation, they often use mobile Internet access and destroy relevant online evidence after successful fraud. Compared with traditional crimes, online fraud crimes have less risk, spread quickly and quickly, the identity of the infringer and its location is not easy to track and determine compared to other cases, and the infringed is often not an individual but a group. Such cases are usually cross-regional and involve a large scope. Therefore, when public security organs detect such cases, they often have to travel across the country to collect evidence. Establishing the similarity between the infringed individuals often requires a certain time. Moreover, integrating and comparing these situations increase the difficulty of the actual investigation and tracking work.

4. Recommendations for improvement

4.1. National Level

4.1.1. Establish a personal information security supervision department

At present, there are many supervision departments in my country's information industry. The content of supervision overlaps and has some omissions, which increases unnecessary costs and increases the cumbersome supervision work. In order to protect the security of personal information, Canada has established the Office of the Privacy Commissioner at all levels independent of the government and reporting directly to Congress following the provisions of the Privacy Act and the Personal Information Protection and Electronic Documents. my country can also refer to this model, and set up a special personal information security supervision department in the central government and governments at all levels, which is specially responsible for the work related to personal information in the era of big data. The central personal information security department is responsible for the overall planning, coordinating the work of local personal information security departments, and formulating corresponding personal information supervision work rules in accordance with laws and regulations; local personal information security departments at all levels are responsible for personal information security supervision in the region, regularly Report the results of the regional supervision work to the superior, and be deployed and managed by the central personal information security. Such hierarchical management can effectively urge information collectors and users to use personal information within the scope permitted by law, maximize economic and social benefits as much as possible, and effectively protect the security of personal information, including college students.

4.1.2. Strengthen the supervision of information operators

In the era of big data, it is the government's responsibility to strengthen network security management and protect the personal information of college students. On the one hand, the government should pay more attention to the security risks of data usage. Current personal information protection laws focus on users' control over the "collection" of personal information. However, in the new network environment, with the increasing popularity of information collection and the close dependence between information collection and business use, ex-ante control is less important. More importantly, how to prevent misuse of personal information in being used. For example, for big data applications, enterprises can be required to analyze their corresponding security risks and propose related protection measures. In addition, by introducing the "data breach notification" system into legislation more broadly, the protection of personal information will be promoted from focusing on prior informed consent to ex-post security assurance.

On the other hand, government departments should strengthen the supervision of enterprises, and can introduce third-party security assessment agencies for management at appropriate times, strengthen the supervision of the entire process of industrial data processing, and effectively create a safe data use environment for college students.

4.2. Enterprise Level

4.2.1. Establish an effective user personal information protection mechanism

By processing big data, enterprises can more clearly understand customers' consumption habits and consumption needs. By integrating and classifying such information, it is possible to predict where the focus of the company's future development will be. However, the collection and use of information and the protection of information need to go hand in hand to give full play to the value of personal information. Although the "informed consent" system is still effective on many occasions, it is obviously no longer suitable for big data application scenarios. The personal information protection mechanism should be reformed in a more meaningful, enforceable, and personal direction. For example, companies are required to inform users of the benefits and drawbacks of using personal data more concisely and understandably, rather than just providing a lengthy and complex privacy policy. Companies are required to follow the principle of "privacy protection design". In product design, research and development, users' privacy protection requirements are considered in every link such as promotion, use, market exit, etc., to provide users with full life-cycle protection of data.

4.2.2. Inject the concept of personal information security protection into products and services

When designing products and services, information companies should fully consider users' personal information security. At the stage of program design or service planning, the concept of personal information security protection should be injected into it. If a product or service for college students needs to collect personal information as a prerequisite for use, there should be a clear consent framework, and the product's privacy policy should be listed. The privacy policy should be changed from the previous complex and professional, and users should be clearly informed of the reasons for collecting personal information, where the information may go, and the risks it may face. In addition, newer technologies or a more comprehensive anti-vulnerability system should be used in product design, and sufficient simulated attack testing should be conducted before the product is launched to ensure its security. And pay attention to whether customers can accept this method in product sharing and promotion, and also need to provide customers with a mechanism for recommending and rejecting such recommended methods. In this way, the audience, including college students, has the option of withdrawing in time. To a certain extent, it can be used as a protection mechanism to prevent further damage after the personal information of college students is leaked.

4.2.3. Strengthen industry self-discipline and implement an accountability system

Concerning the US policy on personal information security, my country can also establish an effective industry self-discipline model. Information enterprises take the initiative to join the industry self-discipline association, and the association should publicize the importance of complementarity and mutual promotion between the development, utilization and protection of personal information. Security of storage and associations can strengthen accountability for the protection of personal information of companies that benefit from big data applications. Such accountability can be pursued not only through personal information protection laws themselves, but also through contractual mechanisms. Because in the big data application industry chain, more corporate entities will be collecting and processing data, and the market-based transactions of data will be more frequent. It is even more necessary to restrict the data processing behavior of related parties through contracts.

4.3. School Level

4.3.1. Integrate personal information security awareness into the teaching plan

As the area where the daily life of college students is concentrated, if the school has the awareness of integrating the awareness of personal information security into the teaching plan, it can promote the protection of college students' personal information to a certain extent. First, the school can incorporate outstanding individuals or groups engaged in information technology research and information-related legal research into the school's education team to provide a certain number of teachers for college students' information protection education. Secondly, schools can set up elective

courses. Teachers can systematically explain the development and protection of personal information to students through a semester of class hours, and analyze specific cases. Thirdly, the school can also regularly invite professionals inside and outside the school to hold personal information security lectures to expand the acceptance of students to learn personal information security knowledge. Finally, holding a personal information security rights protection case reproduction moot court competition can also allow students to acquire knowledge related to personal information security in preparing for the competition. These measures can enable college students to understand and learn about personal information security.

4.3.2. Strengthen the information management system

As the main body that holds the most personal information of college students, colleges and universities still need to improve the protection of students' personal information. When the school needs to count all kinds of big data, the students' personal information can be anonymized to enhance the confidentiality of the information. When the information is released to the public, it can also protect the students' personal privacy. For those who manage students' personal information, more checks should be made on their identities to confirm the safety of the administrators, and at the same time, the importance of student information should be made clear and increased. The information management system of colleges and universities should also be supervised from time to time, updated in time, and filled in time when loopholes are found, so as to prevent criminals from invading and stealing information, and provide a strong guarantee for the security of students' personal information.

4.4. College Student Level

4.4.1. Stay vigilant and avoid personal information leakage from details

College students should start small, always be alert to the need to provide self-information, and try to avoid leakage of their personal information as much as possible. For example, for businesses or entities that require personal information, they should carefully confirm the use and purpose of the other party before providing information; Keep personal information properly, especially information carriers such as bank cards and mobile phones; Fill in personal information carefully, ID number, Do not disclose payment account numbers, mobile phone numbers, etc. at will; Develop a good habit of regularly changing passwords, and must set separate passwords for important accounts (such as common email addresses, online payment, chat accounts, etc.) Wi-Fi, do not click on unknown links in text messages and scan unknown QR codes, do not believe in so-called refunds, judicial assistance investigations, product refunds, point exchanges, and tax refunds for winning prizes. At the same time, we should also pay more attention to the security protection measures of college students' personal information in the society and keep abreast of the current methods of stealing personal information and the relevant knowledge of preventing information leakage.

4.4.2. Establish awareness of rights protection

College students should establish awareness of rights protection. By knowing how to protect themselves and bravely defending their due rights, they prevent infringement incidents and reduce the loss of interests caused by infringement. College students should actively study and clarify laws and regulations related to personal information protection on weekdays, pay attention to social-related events, and pay attention to rights protection departments and rights protection methods. In addition, college students can participate in more personal information security lectures held by schools, society, and the government. If students have teaching conditions, they can also choose to listen to related courses. As young people in the new era, you must know how to protect your own interests after personal information is violated, and promptly and bravely protect your rights by assisting school teachers and legal means, so as to know the law, understand the law, and obey the law.

5. Conclusion

In this paper, we investigate the protection of personal information of college students and find that there is a certain degree of leakage of personal information among college students themselves, colleges, society, law and other aspects, especially college students' lack of awareness of personal information security protection and protection of rights and interests, which is likely to cause adverse social effects. Therefore, we college students themselves should be more vigilant, avoid the leakage of personal information from the details, and establish awareness of rights protection to avoid the tragedy caused by the leakage of personal information. Similarly, schools should also strengthen legal publicity, raise students' awareness of protecting personal information, and work with teachers and students to prevent illegal acts.

References

- [1] W. Q. Qing, "Personal Information Protection Law" and "Civil Code" personal information protection system problems and improvement, *Legal Expo*, 2022, 02: 16 - 18.
- [2] X. Hong, the protection of personal information rights and interests in my country has entered a new chapter, *Confidentiality Work*, 2021, 11: 25 - 27.
- [3] W. C. Hui, Analysis of the ten core points of the "Personal Information Protection Law", *China Telecom*, 2022, 01: 54 - 60.
- [4] D. X. Dong, Reflection and remodeling of personal information rights: On the applicable premise and legal basis of personal information protection, *Chinese and Foreign Law*, 2020, 32 (2): 339 - 356.
- [5] X. Hong, the protection of personal information rights and interests in my country has entered a new chapter, *Confidentiality Work*, 2021, 11: 25 - 27.
- [6] W. C. Hui, Analysis of the ten core points of the "Personal Information Protection Law", *China Telecom Industry*, 2022, 01: 54 - 60.
- [7] H. Fang, C. Ying. Enlightenment and reference of foreign personal information protection legislation to my country, *Northern Finance*, 2021, 11: 63 - 65.