Research Inventy: International Journal of Engineering And Science
Vol.14, Issue 1 (January 2024), PP 114-120
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Research on privacy protection issues and strategies for college students in the era of big data

Pingshui Wang[1], Qinjuan Ma[2]
[1] *School of Management Science and Engineering, Anhui University of Finance & Economics, Bengbu 233030, China*
[2] *School of Business Administration, Anhui University of Finance & Economics, Bengbu 233030, China*
Corresponding Author: Qinjuan Ma

Abstract: *With the advent of the big data era, the widespread application of big data technology has brought enormous convenience and opportunities to human social life. However, there is also a risk of personal privacy leakage. Especially for college students, their activities on the internet are frequent and diverse, making them more susceptible to privacy breaches. While big data brings great convenience to the learning and life of college students, it also highlights serious security and privacy issues. The paper systematically analyzes the current situation and existing problems of personal information security and privacy for college students in the era of big data, analyzes the reasons, and proposes specific countermeasures from the perspectives of technical means, institutional mechanisms, education management, laws and regulations, in order to create a safe, healthy, and harmonious network ecological environment, reduce the risk of privacy leakage for college students, and better promote the development of the big data era.*

Keywords: *Big data era; College students; Privacy protection; Problems and countermeasures.*

Date of Submission: 15-01-2024 Date of acceptance: 28-01-2024

I. Introduction

The era of big data refers to the era of rapid growth of data volume, diversified data types and fast data processing speed.In this era, people can obtain a large amount of data through various means, and analyze and mine these data to obtain valuable information.With the rapid development and widespread popularity of the Internet and mobile intelligent terminals, as well as the continuous promotion and continuous construction of digital country, smart city and smart campus, it marks that human society has entered the era of big data. All kinds of network applications emerge in an endless stream, and college students have become the main body of network applications. All kinds of data of college students are collected into the corresponding system by network operators, such as personal information, health data, consumption data, behavior data, social data and so on. In addition, the relevant laws and regulations and constraint mechanisms of all kinds of Internet applications are not perfect, and these data may be illegally abused by the collector, leading to privacy disclosure, mental distress and even property loss for college students [1].

With the arrival of the era of big data, the wide application of big data technology provides more services and convenience for human society, such as personalized recommendation, intelligent search and so on. However, it is also accompanied by the risk of personal privacy disclosure, especially for college students, who have frequent and diversified activities on the Internet, so they are more likely to become the object of privacy disclosure. In the era of big data, the problem of college students' privacy protection has become an urgent practical problem to be solved, and it is also a hot issue that the industry and academia pay attention to.

In the era of big data, protecting the privacy of college students is an important task. Only by protecting the privacy of college students can we better promote the development of the era of big data and ensure that personal rights and interests are fully respected.This paper briefly introduces the basic concepts of privacy and privacy protection, systematically analyzes the current situation of college students' personal information security and privacy in the era of big data and the existing privacy disclosure problems, analyzes the root causes, and puts forward specific countermeasures from the aspects of college students' privacy protection technology, privacy protection system and mechanism, privacy protection education, privacy protection awareness and privacy protection laws and regulations, in order to create a safe, healthy and harmonious network ecological environment, reduce the risk of college students' privacy disclosure, and improve their sense of security and happiness in network applications.

1 Research Status of College Students' Privacy Protection in the Age of Big Data

In the age of big data, college students' privacy protection is faced with many challenges.On the one hand, college students often disclose their personal information, such as name, age, gender, phone number, etc. when using the Internet; on the other hand, some criminals will also use technical means to steal college students' personal information, so as to conduct fraud, harassment and other behaviors [6]. In addition, some universities also have problems such as poor management and inadequate supervision, coupled with the lack of college students' awareness of privacy protection, and the lack of privacy protection laws and regulations, which further increase the risk of college students' privacy disclosure.The following is an introduction to the privacy protection problems faced by college students in the age of big data, and an analysis of the root causes of their existence, so as to formulate countermeasures for college students' privacy protection.

1.1 Problems of College Students' Privacy Protection in the Age of Big Data

The following is an analysis of the privacy protection problems faced by college students in the age of big data from three aspects: privacy disclosure on social networks, data collection on educational platforms, and abuse of privacy rights in third-party applications.

(1) Privacy disclosure on social networks

College students' social network activities are becoming increasingly frequent, and the information, photos and other personal privacy released by college students on social networks may be obtained and abused by unauthorized third parties. These information may affect the reputation and personal image of college students, and even lead to identity theft, property loss and other adverse consequences.

(2) Data collection on educational platforms

College students use educational platforms for learning and communication, but these platforms may collect a large number of personal learning records and information.These data may be used for commercial purposes, such as personalized advertising push, and students' right to independent choice may be infringed.

(3) Abuse of privacy rights in third-party applications

College students often use third-party applications, which may require access to users' private data such as address book and location information.However, some applications abuse their rights and sell data to advertisers or other stakeholders, increasing the risk of personal privacy disclosure.

1.2 Causes of college students' privacy disclosure in the era of big data

In view of the privacy protection problems faced by college students in the era of big data, the causes of college students' privacy disclosure are analyzed from three aspects: data disclosure and abuse, lack of informed consent, data association and personalized recommendation.

(1) Data disclosure and abuse

In the era of big data, a large amount of personal data is collected and stored, including students' personal information, learning records, social media activities, etc.However, these data may be hacked or leaked, resulting in the infringement of students' privacy. In addition, if these data are abused, it may cause potential harm or unfair treatment to students.

(2) Lack of informed consent

In the era of big data, the collection and use of many personal data have not been clearly informed consent.When using various applications, social media or online education platforms, students may not be aware of how their data are used and shared.The lack of informed consent makes it difficult for students to control the use of personal data, thus increasing their privacy leakage risk.

(3) Data association and personalized recommendation

Big data technology can carry out data association and personalized recommendation by analyzing students' behavior and interest.Although this provides students with better services and resources, it will also have an impact on their privacy.Especially in the process of personalized recommendation, students' behavior and preferences may be further analyzed, thus exposing more personal information.

1.3 Status quo of college students' privacy protection education in the era of big data

In view of the problem of privacy leakage of college students in the era of big data, the current situation of college students' privacy protection education is briefly analyzed, so as to formulate relevant measures to strengthen college students' privacy protection education and improve their privacy protection awareness and skills.

(1) Lack of systematicness and pertinence At present, most colleges and universities lack systematic and targeted education in privacy protection, often only as an elective course or lecture, without forming a complete education system for privacy protection.

(2) Single education content
The existing education content of privacy protection mainly focuses on network security, personal information protection, etc., for other forms of privacy protection, such as mental health, interpersonal relationship and other aspects of education is less.
(3) Traditional education methods
At present, most colleges and universities still use the traditional teaching methods, lack of interaction and practicality, difficult to arouse students' interest and participation.
(4) Insufficient education resources
Many colleges and universities have serious insufficient resources in privacy protection education, including textbooks, teachers, facilities, etc., which has caused some difficulties in the development of privacy protection education.
(5) The impact of social environment
In the current social environment, some college students have insufficient understanding of the importance of privacy protection, thinking that privacy disclosure is a trivial matter, thus paying little attention to privacy protection.
(6) The lack of laws and regulations
Although China has issued some laws and regulations on privacy protection, in the specific implementation process, due to the lack of specific operation guidelines and implementation rules, the privacy rights and interests of college students cannot be effectively protected.

II. Countermeasures for College Students' Privacy Protection in the Era of Big Data

The problem of college students' privacy disclosure in the era of big data is becoming increasingly prominent. In order to protect the privacy security of college students, a series of countermeasures need to be taken.First of all, college students should improve their awareness of self-protection and not leak personal information at will;secondly, universities should strengthen information security management, establish and improve the information security system and technical support system;finally, the government and society should also strengthen the protection and management of personal information, and formulate relevant laws, regulations and standards.

2.1 Commonly used privacy protection technologies

College students, education platforms and third-party application developers should strengthen the application of security technology means, including data encryption, permission control and the development of user privacy protection functions, through technical means to prevent unauthorized access to and abuse of personal privacy.The commonly used privacy protection technologies in the era of big data mainly include data encryption technology, anonymization technology and access control technology, which are briefly introduced below.

2.1.1 Encryption technology

Encryption technology is one of the most commonly used technologies in the field of information security, with the advantages of high security factor and low difficulty in implementation.Through encryption technology, the user's important information can be converted into another form that cannot be intuitively understood and identified.Encryption technology contains two basic elements: encryption algorithm and encryption key. Encryption algorithm is the process of combining the original information (plaintext) with the encryption key to generate information (ciphertext) that cannot be intuitively understood and identified.Decryption algorithm is the process of combining the ciphertext with the decryption key to restore the plaintext.Only users who know the decryption algorithm and the decryption key can restore the plaintext.According to whether the encryption key and the decryption key are the same, encryption technology can be divided into symmetric encryption and asymmetric cryptography.Symmetric encryption refers to the use of the same key for encryption and decryption. Common symmetric encryption algorithms include DES (Data Encryption Standard), 3DES (Triple Data Encryption Algorithm), AES (Advanced Encryption Standard) and so on. Symmetric encryption has the advantages of simplicity, convenience and difficulty in decryption.Asymmetric encryption uses different encryption keys and decryption keys. Representative asymmetric encryption algorithms include RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm) and so on.The encryption keys and decryption keys of symmetric encryption need to be kept secret, while the encryption keys of asymmetric encryption are public.In addition, homomorphic encryption algorithms are also commonly used. When calculated on the ciphertext, they can ensure that the calculation results have the same properties as those calculated on the plaintext.Common homomorphic encryption algorithms include Paillier, LWE (Learning With Error) and so on.

2.1.2 Anonymization technology

Anonymization technology is one of the most commonly used technologies in the field of data security release. It has the advantages of strong data availability and easy implementation. Anonymous technology can transform the important information of users into a more fuzzy form, so that it can not be directly identified.Commonly used anonymization technologies include: k-anonymity, l-diversity, t-proximity, etc.These technologies are processed by data processing, so that the processed data can not directly identify the individual information in the original data, so as to protect individual privacy.

Commonly used implementation methods of anonymization technology include generalization (Generalization) and suppression (Suppression), etc. This technology is different from general data distortion, disturbance and randomization methods, which can maintain the authenticity and consistency of data before and after release, so as to facilitate data statistical analysis.

(1) Generalization

The basic idea of generalization is to replace the original attribute value with a more general value [3].Usually, generalization can be divided into two types: domain generalization and value generalization.

Domain generalization refers to the generalization of a given attribute domain into a general domain.For example, the original domain Z0={ 02138, 02139, 02141, 02142} of attribute ZIP is generalized into Z1={ 0213*,0214*} in order to express a larger range in semantics,.The domain generalization hierarchy formed by continuous multiple generalization is called the domain generalization layer, denoted as DGHA.

Value generalization refers to the direct generalization of each value in the original attribute domain into the unique value in the general domain. The value generalization relationship also determines the existence of the value generalization layer, denoted as VGHA.

(2) Suppression

Suppression refers to replacing the original attribute value with the most general value.For example, the "maximum value" at the top level of the value generalization layer VGHZ0 is the result of the suppression operation of each value of the attribute.In the process of -anonymization, if some records cannot meet the requirements of -anonymization, suppression operation is generally adopted. The record with the corresponding attribute value that is suppressed is either deleted from the data table, or the corresponding attribute value is filled with a number of "*" to maintain the relevant statistical characteristics.

2.1.3 Access control technology

Access control technology is one of the most important strategies for network data security governance, mainly used to prevent unauthorized users from illegally accessing network resources. Commonly used access control technologies include access control, access authority control, and access attribute control. They are mainly used to verify whether the user's identity is real and grant the user the appropriate level of access authority according to the context information such as device, location, and role, through authentication and authorization technologies.

(1) Access Control

Access control is the first gateway to access network resources. It can control which users can access network resources and when and where (IP address) they can access them. It is generally achieved through three basic steps: user identity identification, user password verification, and default limit check of user accounts.

(2) Access Authority Control

Access authority control is used to control which users or devices can access network resources and the types of operations they can perform.This control is an important part of network security and is usually implemented through firewalls, routers, and other security devices.Access control can be divided into physical access control and logical access control.

(3) Access Attribute Control Access attribute control is an attribute-based access control method, which decides to allow or reject the operation requested by the subject to the object according to the assigned attributes of the subject, the assigned attributes of the object, the environmental conditions and the policies related to these attributes and conditions.In this mechanism, attributes are the characteristics of the subject, the object or the environmental conditions, which are usually defined in the form of "name-value" pairs. Good, reliable and timely updated attribute data are crucial for making appropriate and reasonable access decisions.Therefore, the attributes provided by access control functions or attribute providers need to be verified by some kind of mechanism to ensure the accuracy of the attributes, and also need to define and describe a set of principles and standards to determine those attributes that can be used for access decisions.

These technologies can effectively protect the privacy of personal information of college students, but it is worth noting that these technologies are not omnipotent, but can only play a certain role in protection. Therefore, when using various network services, college students also need to be vigilant and enhance their awareness of personal information privacy protection.

2.2 Establish and improve the system and mechanism of college students' privacy protection.

School is the direct management unit of students, and various applications of the school are collecting and storing students' personal information. It has an inescapable responsibility for the privacy protection of students' personal information. Schools can protect the privacy of college students' personal information from the following aspects:

(1) formulate student personal information protection policies

Schools should formulate detailed student personal information protection policies, clarify the provisions of student personal information collection, use, storage, protection, etc., and inform students of the content and purpose of these provisions.

(2) strengthen technical support

Schools should strengthen technical support, adopt safe and reliable technical means to protect students' personal information from being leaked, tampered with or destroyed.

(3) establish management system

Schools should establish a sound student personal information management system, clarify the responsibilities and obligations of various departments and personnel, especially for the acts of ignoring students' personal information security and endangering students' privacy disclosure, strengthen the management and maintenance of students' personal information, and create a clean campus ecology.

(4) strengthen security awareness education

School management departments at all levels, especially the student management department, should strengthen the education of students' security awareness, improve students' emphasis on personal information protection, and make students develop good information security habits.

2.3 Strengthen privacy protection awareness education of college students

Privacy awareness education is very important for college students. According to the results of the questionnaire survey on the awareness of privacy protection of college students, we find that college students have a strong awareness of personal information protection, but there are still some shortcomings in the actual action, and the awareness of privacy disclosure rights is relatively weak. Therefore, schools can adopt a variety of methods to educate college students on privacy protection awareness.

(1) Respect for privacy and fully understand the right to privacy of college students

In the higher education environment, college students' right to privacy is a basic and important right. Colleges and universities should attach great importance to and fully understand the right to privacy of college students when conducting comprehensive education management. This means that schools should understand that the right to privacy is a fundamental human right for every student, and that it embodies respect and freedom for people under the law. Therefore, any violation of students' privacy may violate the law and lead to serious consequences.

(2) To harness technology and deeply understand its ethical risks

Universities need to have a deep understanding and mastery of technology, especially those that may have privacy implications. This includes the management and use of students' personal information, such as academic data, health status, etc. Before using such data, schools should ensure that explicit consent has been obtained from students and that full use should be made on a well-planned basis.

(3) Run the school according to law, and exercise the power of education management according to law and compliance

Colleges and universities should govern themselves according to law, that is, conduct education management according to existing laws and regulations. This includes the protection of students' privacy rights and the appropriate and lawful use of students' personal information in educational activities.

(4) Avoid minefields and be alert to infringements in sensitive areas

Universities need to be alert to minefields and avoid infringement in sensitive areas. For example, schools should not release test scores or other private information from students without their consent.

In addition to the above mentioned points, in view of the protection of college students' right to privacy existing in modern university management, some experts have put forward suggestions such as changing the concept of teaching management, improving the legal awareness of education administrators, and improving the privacy protection system of college students. In addition, universities should also clarify the relationship between the protection of students' privacy rights and university management rights, especially in the context of the era of big data.

In general, universities have multiple responsibilities and challenges in respecting and protecting the privacy of college students. This requires comprehensive consideration and systematic response from multiple levels such as law, technology and education management.

2.4 Develop good personal information privacy protection habits

In the era of big data, college students face greater risks of privacy disclosure. Students' names, phone numbers, home addresses, school records and other private information may be collected, shared, mined and used by personal information collection platforms, social networks, e-commerce platforms, etc., and some undesirable third-party institutions may even use this information to carry out illegal activities. Therefore, college students should develop a good habit of protecting personal information privacy, and do not disclose their personal information at will.

(1) Disclosure of personal information should be treated with caution

When registering for a website or using an app, try to avoid filling out your actual name and information in your profile, except for the necessary real name authentication. In addition, in the process of using the Internet, you should not disclose personal information at will, such as when Posting personal information and photos on social media, you should pay attention to privacy Settings to avoid being obtained by strangers.

(2) Changing passwords regularly and strengthening passwords is also an effective means to protect personal information

In order to ensure the security of personal accounts, college students need to change their passwords regularly and set strong passwords, including a combination of upper and lower case letters, numbers and symbols, and a password length of at least 8 characters. At the same time, avoid using the same password or too simple password to prevent the password from being cracked.

(3) Pay attention to the use of public WiFi is essential to protect personal information

Because public WiFi is often not password protected, it is an easier target for hackers to steal personal information. In addition, when shopping online, you should choose regular channels for shopping, do not believe in unknown links and QR codes, be alert to phishing websites, and prevent personal information from being leaked; When downloading software, pay attention to whether the download source is reliable to avoid downloading malicious software.

In general, college students should be aware of the importance of personal information and have the responsibility to protect their personal information. At the same time, society and schools also have the responsibility to provide an environment for learning, knowing, using and abiding by the law, and guide them to cherish and protect personal privacy information.

2.5 Improve privacy protection laws and regulations for college students

From the legal level, the government should strengthen the construction of laws and regulations on the protection of personal information, improve relevant laws and regulations, and clearly specify the scope and responsibility of personal privacy protection. At the same time, a regulatory body will be established to supervise and punish violations of privacy protection regulations, strengthen the crackdown on illegal acts, and effectively safeguard the privacy rights and interests of college students.

The state has promulgated the Cybersecurity Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China and other laws and regulations to protect the security of citizens' personal information, which clearly stipulates that the personal information of natural persons is protected by law, and no organization or individual may infringe upon the rights and interests of natural persons' personal information. The Act not only provides for general rules on the processing of personal information, but also specifically provides for sensitive personal information and the processing of personal information by state agencies. In addition to the above laws and regulations, a regulation on Network Security Management of colleges and Universities issued by the Ministry of Education details the obligations of schools to protect privacy, security measures and other responsibilities. Therefore, in order to protect the rights and interests of college students' personal information, regulate the processing activities of personal information, and promote the rational use of personal information, the university, as the subject of student management, should abide by relevant laws and regulations and management regulations, strengthen the protection of students' personal information, and shall not disclose, tamper with or destroy students' personal information.

In addition, college students should also understand their rights and obligations and learn to protect their personal information through legal means. If you find that personal information has been leaked or abused, you can complain to the relevant departments or seek legal assistance.

III. Conclusion

In the era of big data, college students have become the hardest hit area of privacy leakage. Countermeasures such as strengthening education and awareness, improving privacy protection laws and regulations, and strengthening the application of privacy protection technology can effectively reduce the risk of privacy leakage of college students. This paper analyzes the current situation and existing problems of college students' privacy protection in the era of big data, and puts forward countermeasures from the aspects of privacy protection technology, privacy protection system and mechanism, privacy protection education, privacy protection awareness and privacy protection laws and regulations, hoping that contemporary college students can improve their privacy protection awareness and reduce the risk of privacy disclosure while enjoying the convenience brought by big data. In the future, we can look forward to the introduction of more perfect laws, regulations and technical security systems, and also need the efforts and actions of college students to jointly safeguard their privacy rights and interests.

Conflict of Interest

There is no conflict to disclose.

Acknowledgment

We thank the anonymous reviewers and editors for their very constructive comments. This work was supported by the scientific research project of Anhui University of Finance & Economics under Grant ACKYC23070.

Reference

[1]. HL Wang. Research on data privacy protection strategies for college students [D]. Master Dissertation, Beijing University of Posts and Telecommunications, 2021.

[2]. PS Wang, JD Wang. Review of anonymous privacy protection technology [J]. Small and Micro Computer Systems, 2011,32(2):248-252.

[3]. PS Wang. Research on anonymized privacy protection technology based on clustering [D]. Doctoral Dissertation of Nanjing University of Aeronautics and Astronautics, 2013.

[4]. PS Wang, QJ Ma. Research on Personalized Privacy Protection Technology of Mobile Social Network in Big Data Environment [M]. Economic Management Press, 2022.10.

[5]. B Yang. Investigation and Analysis of college students' online privacy Protection Behavior in the Era of Big Data [J]. Heilongjiang Education (Theory and Practice), 2020,(5):25-26.

[6]. W Bai, ZY Li, XH He. Research on Personal privacy protection of college students' mobile social networks [J]. Value Engineering, 2018,(27):215-216.