ISSN: 2688-8653

Legal Protection of Children's Personal Information in the Internet Age

Liangqian Gu, Yanhong Lin, Wei An

Anhui University of Finance and Economics, Bengbu 233000, China.

Abstract

With the development of science and technology, people have ushered in the era of big data with information resource as the core, and the protection of personal information of children in our country is faced with the difficulty of coordination and timeliness at both the theoretical and practical levels. Therefore, strengthening the protection of personal information is urgent. The core of the children's personal information legal governance system is the "guardian consent mechanism", and the "alternative decision" mode of the guardianship theory of civil law is the underlying logic of its rule design, which needs to be further improved in practice. The guardian consent mechanism of the "alternative decision" model should be further refined from the aspects of identity rules, guardian consent rules, withdrawal consent rules, etc., so as to crack the realistic dilemma of children's personal information protection.

Keywords

Children, Personal Information, Guardian Consent, Alternative Decision.

1. Determination of legal concepts related to the protection of children and their information

1.1. Definition of the subject of children's rights and interests

From the existing regulations, there is no unified age limit standard for minors' information protection in China. When it comes to information protection of groups other than adults, there are many subject names used in the academic world, the most commonly used are: minors, juveniles, children. The concept of "minors" is clear, referring to the group of people under the age of 18.

There are some translation factors in its wide use. For example, "juvenile" has both juvenile and juvenile meanings. However, most scholars in our country translate "juvenile" into "juvenile" in foreign judicial systems. Provisions on the Trial of Juvenile Criminal Cases stipulate that those who are under the age of 18 at the time of committing a crime can be applied to juvenile courts under certain conditions. Therefore, in summary, it can be clarified that a juvenile refers to a natural person who has reached the age of 12 but not 18.

The term "child" appears many times in various laws and regulations, such as "guaranteeing school-age children and adolescents to go to school" stipulated in Article 19 of the Education Law; Article 49 of the Constitution provides that " The child is protected by the State ", etc. In 1989, the Supreme People's Court's reply to the question of how to divide the age limit of infants and toddlers in human trafficking cases (Law (Research) Fu (1989) No. 5, July 7, 1989) gave the definition of "children", that is, "infants, infants, and children should be classified as infants under one year old, and children over one year old and under six years old. And children over six and under fourteen years old." Another landmark achievement of the "Children's Personal Information Network protection Provisions" defines "children" as minors under the age of 14, the division may be combined with the actual situation of children's physical and mental development, under China's compulsory education system, 14 years old may graduate from

ISSN: 2688-8653

junior high school, that is, complete the basic nine-year compulsory education, its knowledge reserve and psychological cognition gradually mature.

Considering the laws and facts, minors under the age of 14 and under the age of 18 are mentally mature, and regulating their online behaviors according to the "alternative decision" model will not be conducive to exercising their autonomy. In order to take into account the information rights and interests of the parties concerned and the autonomy to determine their personal information, this paper holds that the "Regulations" define the subject of protection as minors under the age of 14, namely "children". It shows that the legislator has fully considered the demands and current situation of the development of China's industry. The needs of industrial development and rights protection have achieved dual legislative purposes, and should be the main body of personal information protection.

1.2. Definition of the scope of protection of children's personal information

The essence of children's personal information is an important carrier of children's rights and interests. Because of the emergence of the Internet, the boundary between children's private sphere and public sphere is gradually blurred, and a middle zone is generated, that is, the boundary of "private sphere" in Germany's "domain theory". The core feature of information that needs to be protected is "identifiability", which includes two parts: identity identification and feature identification, that is, "who" and "what kind of person" the subject is. Take a software account registration process as an example, the platform requires users to use real identity information to register an account, provide mobile phone number, email address and other information to ensure normal use of the service. In the application permission list, there are rights to determine the number and ID of the local device, take photos and record videos, record audio, read calendar, read contacts, access approximate location information and other sensitive privacy information of the user. Some contents of these sensitive privacy rights are authorized to use the application software after the user clicks "agree" during the registration process. After the user logs in, the default is used and is disclosed ID account, city location information, etc., in the attention column "people you may be interested in" push "address book friends", in the personal information column "Add friends" column, there is a list of mobile phone contacts using the software.

According to the Personal Information Protection Law, the personal information of children under the age of 14 is sensitive information. The information collected in the above platform can reflect the family residence, school, activity track, etc., and there are private Spaces, private information and private activities that guardians do not want others to know. If such information is not effectively managed, it may disturb children's peace of life and even pose risks to children's physical and mental health, and can be regarded as private information. It is worth noting that although the software platform adopts a laissez-faire attitude towards child user registration, the software platform adopts a label association mechanism to set thousands of labels for personal characteristics identification of the user's portrait, gender, browsing content, duration, etc., which can generally accurately identify the age of the user. That is, the software platform does not need to clearly indicate when children register, and children's personal information can be identified through big data algorithms. There are illegal situations in which users are allowed to collect their personal information while knowing that they are children.

1.3. Challenges faced by children in the digital age

The development of the Internet has brought profound changes to human social norms of behavior. While providing speed and convenience to human life, the Internet has a large number of security risks, and its virtual, indirect and hidden nature contains and breeds criminal incentives. On the one hand, if people with criminal tendencies take the initiative to collect or be pushed to children's account information, children's personal information may be

ISSN: 2688-8653

secretly collected, over-used or illegally used by such people, and converted into other criminal tools or objects, which will directly cause harm to children's safety, including but not limited to personal injury. On the other hand, if inappropriate content is pushed to children, they will be highly susceptible to bad induction due to their young age, shallow experience, weak ability to distinguish right from wrong, inability to maintain physical and mental balance, strong curiosity and other reasons. If the first risk is driven by seeking economic benefits and there is a risk of adverse effects on child users, then the second risk is more socially harmful and may directly lead to criminal acts against children.

The guardian and the network operator are the subjects to meet the challenge. In the protection of children's personal information, both parties have obligations and responsibilities, but there is an imbalance in their ability and an asymmetry in information mastery. In order to provide correct guidance to children in the process of surfing the Internet, guardians really need to continuously improve their awareness of network security, enhance their ability to identify risks, and even learn certain professional knowledge. However, it is undeniable that if the online platform cannot effectively fulfill the obligation of informing consent strictly in accordance with the law, even if the guardian has a sense of security and understands the importance of information security, it can only stay at the subjective cognition level and cannot be implemented in various forms of network application environments and specific scenarios, and can not actively identify the specific risk points affecting the information security of children users. And can not effectively guide children's online behavior.

2. Comparative analysis of legal protection of children's personal information

2.1. American children's personal information protection regulations and judicial practices

The Internet originated in the United States. As one of the countries with the most developed Internet technology, the United States has traditionally attached great importance to the protection of personal information in its laws. As for the legislation on the protection of children's personal information, the United States has adopted the same legislative model, that is, it has systematically stipulated the relevant systems for the protection of children's personal information, and specially formulated the code on the protection of children's personal information. The US federal government and various states have passed laws to protect the personal information of minors (including children and adolescents), including the following key laws:

The Children's Online Privacy Protection Act (COPPA): This law was passed on October 21, 1998, went into effect on April 21, 2000, and is limited to children under the age of 13. This is a federal law on the privacy protection of Internet users, which was introduced into the Internet age in the United States, and its purpose is to make it difficult for commercial websites to collect private information directly from children without parents' knowledge and consent. COPPA requires websites and online service providers (OSPs) to obtain the explicit consent of biological parents or guardians before collecting, using and disclosing children's personal information, and has established strict data protection measures to ensure the safety of children's information.

Student Privacy Protection Act (PPRA): This law was enacted in 1974 to protect students' right to privacy. It requires schools and other organizations to obtain the consent of a parent or guardian when collecting, using, and disclosing personal information about students. The law also sets out rights to access, verify and correct student information.

Security and Privacy Act (COPPA): The Security and Privacy Act (FISMA) was enacted in 2002 to ensure the effective management of information technology and information resources by

ISSN: 2688-8653

the federal government. The Act requires the federal government to develop security measures to protect information systems and data, and to monitor and report on any security breaches or data breaches.

In addition to these federal laws, different states have enacted their own children's personal information protection laws that aim to "prohibit the collection of certain data" or "require states and school districts to strengthen their oversight facilities and procedures." California, for example, has passed the California Consumer Privacy Act (CCPA), which requires companies to provide access to and deletion of consumer data they collect, including children's personal information.

In judicial practice, children's personal information protection laws have been effectively enforced. For example, in 2019, Google reached a $570 million settlement with the Federal Trade Commission (FTC) for alleged violations of COPPA regulations. That same year, third-party app maker "TikTok" was also fined $5.5 million for violating COPPA regulations. These cases show that government agencies will strictly enforce the relevant laws, and law enforcement agencies will also continue to work to ensure that children's personal information is properly protected.

2.2. Eu regulation on the protection of children's Personal Information and judicial practice

The EU has a number of regulations to protect children's personal information, including:

General Data Protection Regulation (GDPR): GDPR came into force on 25 May 2018 and is a regulation that applies to companies and organisations that structure data within and outside the EU. The GDPR requires account law businesses to obtain the consent of a parent or guardian before collecting personal information from children under the age of 16.

EUROP (EU Rules for Online Privacy Protection) sets the standard for children's privacy online. EUROP requires platforms to obtain the consent of the parent or guardian of a child under the age of 13 when collecting and using personal information about a child.

In practice, some of the most recent EU court cases relating to children's data privacy have been about banning the use of a Facebook "like" button in public places. This case is about a German education-related website that has some of Facebook's "like" buttons. The German court's decision requires the agency to delete data on anyone, including children, and not disclose it to the recipients of the information without the explicit consent of their parents or guardians.

In addition, the GDPR is widely used in everyday practice. The regulation is constantly implemented and updated regularly by the supervisory authorities in various countries, ensuring that the protection of personal information for European children is fully guaranteed.

3. Innovative suggestions on legal protection system of children's personal information in China

3.1. Innovation of personal information identification mechanism

For the first time, the EU GDPR has incorporated a personal data authentication mechanism into legal norms. According to the "Certification and Certification Standards Guidelines" designated by the EU Data Protection Council, certification mechanism refers to "third-party certification of data processing procedures", as a commercial appearance, proving that information providers have met certain standards in the protection of personal information, including compliance standards, risk control standards and technical standards. Applying the certification mechanism in the field of minors' personal information protection can effectively reduce the cost of trust and improve transaction efficiency. Referring to the countries of the civil law system, France and Germany have adopted the public right certification model, with

ISSN: 2688-8653

the national agency in information protection as the certification body. For example, in France, the "National Commission for Information and Freedom" makes certification rules, has the right to evaluate and is responsible for granting certification. Certification is equivalent to a recognition and honor, bringing goodwill, social recognition, public sector awards and other incentives for enterprises, so as to stimulate the motivation of enterprises to protect personal information. At present, the industry involving minors' personal information has greater compliance pressure, and the ambiguity of legal rules and the unpredictability of law enforcement have become the pain points of market players. The information protection certification mechanism has a new way to form a higher standard through the practice of enterprises, so as to mobilize the subjective initiative of enterprises and contribute a large number of feasible and operational examples. These examples can become an important reference for the design of legal rules after the practice test.

3.2. The guardian consent mechanism has been improved

At present, China's Internet enterprises refer to the "Personal Information security Code", generally provide two documents in the user registration process service agreement and privacy policy. However, the description of the content of the document is often more complicated, and it is difficult for adults to read, let alone children; At the same time, the consent method of the file is often to actively check the consent, otherwise you can not register or use the service. Although privacy policies generally include the protection of minors and require children and guardians to read together and obtain the consent of the guardian, in practice operators generally do not take the initiative to judge whether the service object has obtained the consent of the guardian in advance, and it is difficult to detect the behavior of information collection under technical conditions. As a result, children's personal information is likely to be widely collected without the knowledge of the guardian. China's "Regulations on the Protection of Children's Personal Information Online" has added the provision of guardian's express consent. The three core links of the guardian's consent mechanism are obtaining in advance, fully informing and clearly agreeing. Around these three links, combined with the social needs of industrial development and the protection of minors, the system rules are reasonably designed.

In the prior acquisition process, the user undertakes the specific obligation to obtain consent, and if the right holder cannot effectively implement the act, no legal effect can occur. The current privacy policy and general authorization practice can not extend the protection of minors' information, can not be used as the main obligation to obtain the consent of the guardian, but can only be used as the standard for enterprises to regulate their own behavior and auxiliary reference for fulfilling the compliance obligation. Because if it is confirmed that this kind of "going through the motions" can produce a defense effect, it will create loopholes for information companies to avoid legal supervision, resulting in an imbalance of interests.In the process of full notification, information processors are required to fully disclose important matters related to the rights and interests of the parties, including the content, scope, use, method, rights and remedies of the parties to be collected and processed, as well as the importance of personal information protection, consumer education, etc., to ensure the right to know and the right to remedy of minors and their guardians. To avoid damage to rights and interests and adverse competition caused by information asymmetry.In the process of explicit consent, information processors must rely on the identification mechanism to accurately identify minors and fulfill the obligation of full notification. At the same time, requests to collect and process personal information are issued to the guardian and the minor, and the guardian gives express consent, so that there is no ambiguity and can be verified.

ISSN: 2688-8653

3.3. The withdrawal of consent mechanism innovation

The physical and mental development of minors is in the process of constant shaping and improvement, and their ideas and ideas are in an unstable state.

Due to their unique behavioral characteristics and emotional fluctuations and even impulsivity, minors are more vulnerable to harm on the Internet. After the minors authorize the processing of information, when they reach a certain age and realize that the authorization may violate their privacy and affect their reputation, they should have the right to ask the operator to delete the relevant information, that is, to realize the right to withdraw consent and the right to delete. In July 2020, China's "Shenzhen Special Economic Zone Data Regulations (Draft for Comments)" stipulated the "withdrawal of consent rules", natural persons can withdraw consent at any time, after the withdrawal of consent, data collection and processing should promptly and effectively delete the stored relevant data. China's "Children's Personal Information Network Protection Regulations" set up the "right to delete", in addition to the collection and processing of matters beyond the power, when the guardian with takes the consent, minors or guardians terminate the use of products and services, network operators should promptly and effectively delete minors' personal information. Considering the characteristics of minors' physical and mental development, such a system design is particularly important in the field of minors' protection, which directly determines that the life cycle of specific information can be "self-determination" by citizens, and avoids the collection and processing of minors' personal information from beginning to end. Therefore, in the legislation on the integration of minors' personal information, the rules of withdrawal of consent and the right to delete should be set up uniformly.

Acknowledgements

Anhui University of Finance and Economics Undergraduate Research Innovation Fund project support (project approval number: XSKY22217). We appreciate the support of Anhui University of Finance and Economics.

References

[1] CAI Yibo, Wu Tao. Dilemma of Minors' Personal information protection and institutional Response: from the perspective of improving guardian consent mechanism of "alternative decision" [J]. Chinese Youth Social Sciences, 21,40(02): 126 -133.

[2] Han Kailun. A Study on the Application of Guardian Consent Rules for Minors' Information Protection [D]. Henan University. 2323.

[3] Zhang J H, Yin H. Legal protection of Minors' Personal Information in the Digital Age.Juvenile Delinquency,2021(02): 97-106.

[4] Sun Yiwu. Whether the protection of Children's Personal Information is a false proposition or a real problem--Comments on the Regulations on the Protection of Children's Personal Information Online [J]. Juvenile Crime,2020(02): 90-97.

[5] Lin Lin.Judicial Approach to Children's Personal Information Network protection--from the perspective of public interest litigation [J]. Journal of Applicable Law, 2022(04): 108 -116.

[6] Huang Xudong, Yang Fei. Legal Protection of Minors' Online Privacy Rights [J].Contemporary Youth Research, 2009(04): 31-38.

[7] Meng Xiaoli. Protection of Minors' information Rights and interests in the Digital Age: a dimension of protection based on parental informed consent [J]. Journal of anhui agricultural university (social science edition), 2022, 31 (5): 89-98.

[8] CAI Yibo, Wu Tao. Research on Juvenile Information Protection under Interest Measurement and Scenario practice [J]. Juvenile Delinquency, 2021(04): 152-160.