Paradigm Academic Press
Law and Economy
ISSN 2788-7049
FEB. 2025 VOL.4, NO.2

Risks and Countermeasures of Personal Information Processing in Minors' Network Socialization

Huiyi Zhu[1]

[1] East China University of Political Science and Law, Shanghai, China

Correspondence: Huiyi Zhu, East China University of Political Science and Law, Shanghai, China.

doi:10.56397/LE.2025.02.08

Abstract

Minors experience network cognition, network imitation and network interaction in the algorithmic society. The invisible hand of algorithm is inseparable from every network action. When minors encounter algorithmic recommendation services on social media, their personal information is abused by the algorithm. The existing regulations for the protection of personal information based on algorithms have some problems, such as rigid age division of notification and consent mechanism and one-time notification and consent. In this regard, it is necessary to re-establish the risk assessment system for minors' personal information, improve the operability of consent notification and emphasize dynamic notification, balance the rights and interests of minors' personal information and the freedom of expression on the Internet, and build an algorithmic society for minors to communicate and trust.

Keywords: minors, algorithm recommendation, personal information, consent notification

1. The Presentation of the Problem

"Socialization" is the process in which natural persons grow into social people. It is the process in which children and adolescents learn social knowledge and skills norms, consciously abide by social order and values, interact with others and groups, and develop into social people. [1]The development of Internet technology enables minors to grow up in the network society. Various network products such as smart phones, smart watches and tablet computers have become the main channels for young people to obtain information and understand the world, including experiencing electronic games, online classes and online socializing through the Internet. However, network socialization is also a double-edged sword. In order to increase the time spent on the Internet and obtain more information on the Internet, minors bypass the anti-addiction system by buying second-hand accounts or using adult accounts. [2]In addition to the Internet addiction caused by electronic care, the reasons for the increased frequency of minors' Internet contact and increased risk also include passive exposure of minors' information, typically personal information disclosure caused by online sharing of children, and the subsequent use of minors' personal information by algorithmic platforms.

As "network natives", minors are different from those who grow up in the media environment of radio and television. The network platform builds a more complex information environment with the support of algorithm technology, which also has a new impact on the socialization of minors. The algorithm becomes the main body of communication, and the combination of data-driven and computational support realizes "intelligent

[1] China Education Information Network, (2020). The Law on the Protection of minors helps the socialization and development of minors. https://web.ict.edu.cn/news/jrgz/jydt/n20201028_74071.shtml, 10-28.

[2] China Education News Network, (2023). How can "adolescent mode" effectively prevent addiction? http://www.jyb.cn/rmtzgjyb/202304/t20230422_2111031516.html, 04-22.

communication". From a technical point of view, minors who use the Internet cannot do without the information transmission logic of the algorithm recommendation mechanism. As a decision-making AI, the technical path of algorithm recommendation technology is to classify data and label it to distinguish different categories of data for targeted recommendation. The operation of this mechanism relies on the collection and utilization of minors' network use data to achieve the dissemination mode of "information search". In contrast, generative AI tends to summarize existing data and use deep learning techniques to create imitative and stitched content. Both information push technology and deep synthesis technology have illegal risks for minors' data input, data processing and data output. Take a civil public interest lawsuit as an example, Yuhang District People's Procuratorate of Hangzhou City, Zhejiang Province against a Beijing company for infringing on children's personal information rights and interests, the case is mainly involved in two behaviors: one is to use algorithms to push short videos containing children's personal information without consent; The second is the collection and storage of children's personal information without significant and clear notice and consent. Both are manifestations of the platform's use of algorithms to process minors' personal information in violation of regulations.

China's research on the protection of minors' personal information mainly focuses on the following aspects. First, define the scope of minors' personal information. China has set the age of 14 as the limit for the protection of minors' personal information, and determined that the personal information of minors under the age of 14 is sensitive personal information and can be strictly protected. [1]In this regard, some scholars questioned the rationality of the limit, arguing that the protection of the personal information of minors over the age of 14 was ignored, resulting in the narrow scope of the legislation. [2]Some scholars also believe that the age limit may over-protect minors under the age of 14 who are mature and capable of handling personal information. [3]Second, reflection on the operability of the guardian consent system. China's law stipulates that personal information processors should obtain the consent of guardians when processing the personal information of minors. [4]Due to the lack of implementation of relevant legislation on age verification of minors, the system of guardian consent is low in operability, which may lead to minors posing as guardians, or guardians have the problem of "consent fatigue" due to formatted notification texts, thus affecting the guardian's right to know and consent. [5]Third, the discussion on relief and prevention of minors' personal information rights. Scholars believe that based on the existing legislation and relevant norms of personal information protection in China, there is no clear legal reference and no effective legal guidance for the infringement of minors' personal information rights in the Internet application scenario. [6]In the context of unclear legislation, some scholars believe that trial experience can be summarized from judicial practice to improve platform regulation. [7]From the perspective of judicial prosecution, some scholars put forward the connection between network protection and judicial protection, and supervise the violation of minors' personal information through "digital supervision". [8]In order to protect children's information from excessive recording or use, some scholars proposed that China should establish the right of children's information to be forgotten, which can be exercised by the guardian of the child, and should be exercised by the child himself after he grows up to be a minor or an adult. [9]The existing research on the protection of minors' personal information mainly focuses on the protection of minors' personal information rights and interests, while emphasizing the protection of minors' online rights and interests, and the joint efforts

[1] Article 28 of the Personal Information Protection Act.

[2] Anqi, (2023). Protection of Minors' Personal Information: Theoretical Clarification and Rule remodeling. *Chinese Youth Social Sciences*, *42*(02), 132-140.

[3] Liu Yonghong, Deng Haixia, (2024). Realistic dilemma and path optimization of Minors' Personal information protection. *Journal of Chengdu University (Social Science Edition)*, (04), 115-128.

[4] Article 9 of the Children's Personal Information Network Regulations, Article 72 of the Minors Protection Act, and Article 31 of the Personal Information Protection Act.

[5] Liu Yonghong, Deng Haixia, (2024). Realistic dilemma and path optimization of Minors' Personal information protection. *Journal of Chengdu University (Social Science Edition)*, (04), 115-128.

[6] Wang Yongqi, (2024). The dilemma and countermeasures of minors' personal information rights protection in the digital age. *Journal of Shanxi Datong University (Social Science Edition)*, *38*(06), 17-22.

[7] Wang Hui, ZHANG Xiao, (2024). Judicial Regulation on the Processing of Minors' Personal Information by Algorithm Platform. *Journal of Shandong Judge Training College*, *40*(04), 26-42.

[8] Lei Xiaozheng, Yan Shuyue, (2024). The connection Problem and Countermeasures of Minors' Network Protection and "Digital Prosecution". *Journal of Hunan University of Science and Technology (Social Science Edition)*, *27*(01), 117-127.

[9] Jiang Jinliang, Li Li, (2022). Children who do not need to be recorded: the proof and content of children's right to be forgotten. *Preschool education research*, (05), 69-78.

of platforms and society. This paper analyzes the risks of algorithmic processing of minors' personal information from the perspective of algorithmic intervention in minors' online use. For the realization of the transparency of the algorithm, the focus is on the processing behavior of the personal information of the minors, pointing out the challenges faced by the protection of the personal information of the algorithm, and the improvement plan is proposed based on the legislation and practice of our country.

2. The Online Personal Information of Minors Is Faced with Algorithmic Risks

With the younger age of minors using the Internet, more and more minors experience the socialization process through online media. There is no denying that the algorithm deprives parents of their rights as guardians to take care of minors. [1]However, it should be noted that in more cases, parents take the initiative to give the responsibility of monitoring minors to the algorithm, that is, the so-called "electronic care", so that mobile phones become minors' childhood toys, resulting in minors' cognition being affected by the algorithm, increasing the possibility of minors being violated by the algorithm. Network media make use of the basic right of minors' media use, especially the characteristic of strong randomness in the exercise of minors' media use right, from the two aspects of "discourse" and "technology", to control and alienate minors' media use right. [2]With minors' personal information as the carrier, the penetration of algorithmic power encountered by minors mainly includes the following aspects: the algorithm becomes the network teacher, the formation of the network unconscious imitation and the algorithm constructs the network communication logic.

2.1 The Algorithm Becomes the Network Teacher

In a networked society, algorithms become teachers outside of the school and parents, feeding students new information. Some parents and schools take the initiative to provide minors with mobile phones, tablets and other learning tools; Some guardians are forced to provide minors with mobile phones to achieve remote contact because they work outside the home, so that minors can obtain Internet tools. In the process of forming their self-awareness, minors lack judgment about the information provided by algorithm technology and are easily influenced by online views. Different from the education of minors by parents and teachers, after minors use the Internet, the order of information transmission they receive will be determined by the algorithm model. This kind of algorithm model has certain positive significance. The algorithm model of the platform has embedded three sample libraries, such as the pornographic model, the abusive model and the vulgar model, according to which the text analysis of the network content is carried out, and the value of the information is defined by the algorithm to distinguish whether the information should be pushed. The "algorithm teacher" establishes the criteria for selecting information for minors, and can remove information harmful to minors' physical and mental health.

However, the ability of algorithms to rank information can also give priority to the dissemination of ideas and services that are in line with their own values or interests. On the one hand, the information that minors receive on the network comes from the push of the algorithm to the labeled individuals, which wraps them in the content that they identify with and are interested in, and loses their independent thinking of society. On the other hand, the algorithm's excessive collection of minors' browsing technology will also have an impact on minors' mental health. Some minors said in the interview that they felt monitored by the short video platform and their freedom of action was restricted by the outside world, resulting in irritability and resistance. [3]Article 24 of the Personal Information Protection Law stipulates that individuals have the right to refuse to allow personal information processors to make decisions only through automated decision-making. In response, many platforms have introduced the "one-click shutdown" option, but the "one-click shutdown" is not able to achieve the expected regulatory effect or does not meet the legal problems to be solved.[4]

2.2 The Algorithm Forms the Network Unconscious Imitation

Imitation is an important part of the socialization process of minors, and it will lead to the imitation of network culture in the context of network socialization. The online imitation behaviors of minors include singing along to online popular songs, learning online language and shooting online short videos, etc. In 2022, the song *Lone Brave* became popular among minors. A teacher found that students were exposed to the song through an online

[1] Lin Huanmin, (2023). Normative Response to algorithmic "Guardianship" of Minors. *Contemporary Jurisprudence*, *37*(03), 106-116.

[2] Zhu Qinghe, Shi Xiaorui, (2024). Minors' Use of Internet media and protection of Personal Information: A Case Study No. 141. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)*, *36*(01), 25-34.

[3] Wang Huanni, Liu Haiqun. (2023). Algorithm recommendation in short video platform infringes on teenagers' data rights. *Science and Technology Communication*, *15*(04), 112-115.

[4] Lin Jia, Luo Huanxin. (2024). Toward Personalized recommendation of trust Algorithm: Legal Reflection on "One-click close". *Friends of the editor*, (03), 79-88.

video, saying that the spirit of the swordsman who kills the virus with a sword in the video inspired the students. [1]The love of a song reflects the inner emotional needs of minors, and the high intensity and wide range of singing cannot be without the influence of algorithm technology. The algorithm gathers all kinds of people with common characteristics through the way of "labeling", expressing their own opinions in cyberspace and forming cultural groups.

"The technical empowerment of algorithms has undoubtedly greatly enhanced the media access rights and initiative of users, enabling users to pass on their opinions and opinions. However, research has shown that most users do not understand how personalization algorithms work." [2]Not only minors, but also some parents do not understand the operation of the algorithm recommendation mechanism, and lack the ability to protect minors' personal information. The algorithm controls and processes information independently, and is in a state of technical unconsciousness. The platform uses the form of "information flow organ" to increase users' usage time and attract users' attention. People interact with the environment transformed and reconstructed by technology unconsciously, and the popularity of various network activities does not leave the commercial or political interests behind the algorithm. If the public wants to continue to own the information services of the platform, it must acquiesce to the acquisition of personal data by commercial capital, and it must continue to digitally produce it. [3]For example, in 2018, algorithms caused the large-scale dissemination of children's cult videos. Producers packaged cartoon characters familiar to children as bloody violence or soft pornography into video platforms. Combined with the platform's algorithm recommendation technology, children's existing viewing records and data will be pushed to more similar videos. [4]The popularity of online copycat challenges has also resulted in the death of minors. In 2022, two girls in the United States accidentally hanged themselves to death by challenging the "Blackout challenge" on TikTok's international version. [5]According to the parents, they had watched a lot of blackout challenge videos on TikTok before their deaths. Apart from the negligence of the guardians, the tragedy could not have happened without the large-scale spread of the online challenge caused by algorithms.

2.3 The Algorithm Builds the Network Communication Logic

Speaking on the network platform needs to face both network users and platform algorithms. The former is the audience of the content, and the latter gathers the public's attention on the topic of minors through the hotspot push mechanism. Minors' personal information faces passive exposure and active disclosure in the process of online communication, both of which will lead to the risk of abuse of minors' personal information.

On the one hand, some guardians take the initiative to create social accounts to share minors' daily lives and expose minors' information to the Internet. Such "online child sharing" not only exposes minors' portraits and voices, but also may expose their school and home address. Since such photos and short videos will exist on online platforms for a long time, this information may also affect children's self-evaluation in the form of memory in the future. [6]The above interaction also easily makes minors the objects of commercial consumption. Guardians make them into Internet celebrities by shooting short videos of minors' daily life. Excessive commercial consumption of minors will distort their view of money. Although the state has clearly cracked down on the behavior of "making profit by Internet celebrity children", in the media practice of "video survival", the mass media contact landscape is mainly characterized by the image of information behavior. [7]It is very common to record the growth of minors on video and upload it to the Internet.

---

[1] Beijing Youth Daily, (2022). How did "Lone Warrior" become a national children's song from the Internet?. https://news.cctv.com/2022/07/07/ARTIDJzAmsNzy2CtklWFpYVm220707.shtml, 2020-07-07.

[2] Yu Guoming, Yang Yingying and Yan Qiaomei, (2018). Algorithms as Power: The Power Revolution of algorithmic paradigms in Journalism. *Friends of the Editor*, (05), 5-12.

[3] Pang Jinyou, Sun Yuxun, (2024). Subject alienation and democratic dilemma of algorithm propagation in digital age. *Learning and Exploration*, (12), 45-54+176.

[4] Qianjiang Evening News, (2018). Media comments on the flow of children's cult films into China: Highlighting the algorithm recommendation black hole. https://www.thepaper.cn/newsDetail_forward_1963098, 2018-01-23.

[5] IFeng Technology, (2022). Two girls in the United States have been indicted for participating in a short video challenge that accidentally killed TikTok Overseas. https://ishare.ifeng.com/c/s/v004QRYdMhM9u2OP5ZET0SSzZ33ha2wbCCzpfnREYHNctxQ__?from=ucms_web, 2022-07-07.

[6] Jiang Jinliang, Li Li, (2022). Children who do not need to be recorded: the proof and content of children's right to be forgotten. *Preschool education research*, (05), 69-78.

[7] Li Jing, Yuan Yongtao, (2023). From "Media Representation" to "Video Survival": the Information effect and order logic of short video media practice. *A collection of Dongyue papers*, *44*(12), 43-52+191.

On the other hand, in addition to browsing information online, minors also take the initiative to post information and interact with other users' comments in the online community. According to the policies of the major platforms, the age limit of user registration is different for different platforms. In 2018, Weibo ruled that minors who are less than the 14th anniversary of their microblog could not register. In contrast, those who are less than 18 years old can register on the Douyin platform, but will go directly into the teen mode, with functional access restrictions to protect the safety of minors' online activities. Although the entry threshold is different, minors can still enter the platform and interact with online users through other means, such as borrowing adult accounts. In the case of Liu Xuezhou, for example, a minor actively posted a video on the Internet and publicized the process of searching for his family, which caused many netizens to ridicule or accuse him, and finally chose to commit suicide. In addition to the personalized recommendation mechanism, the algorithm mechanism also includes the collective hot spot algorithm, which forms the platform "hot search" by calculating the collective focus of Internet users and attracts the collective attention of the public. [1]The more people pay attention to the event, the more likely it is to be recommended by hot spots. The algorithm has brought countless netizens' attention and comments to the incident, which also magnifies the external pressure the protagonist needs to face. When countless netizens poured their criticism into microblog private messages and real-time hot search entries, it brought great psychological burden to minors.

3. The Regulations for the Protection of Minors' Online Personal Information Are Insufficient

The online activities of minors are easily influenced by algorithms and even misled. The above algorithms all involve the processing of minors' personal information. On the one hand, algorithm recommendation is essentially a kind of personal information processing behavior, the operation of the algorithm cannot be separated from the collection and utilization of personal information, and the illegal collection of personal information is one of the manifestations of algorithm abuse. On the other hand, the online activities of minors include not only the content pushed by the algorithm, but also the video containing their personal information being pushed. The Law on the Protection of Minors implemented in June 2021 establishes a chapter on "network protection", Article 18 of the Regulations on the Management of Internet Algorithm Recommendation Services stipulates the obligation of minors protection of algorithm recommendation services, and the Regulations on the Management of Internet pop-up information Push Services implemented in September 2022 stipulate that "algorithms shall not be used to draw portraits of minor users, to push information that may affect their physical and mental health". The Regulations on Cybersecurity Protection for Minors, which came into effect on Jan 1, 2024, further optimized the prevention mechanism for minors' information leakage by proposing a verification system for minors' real identity information, an emergency response mechanism for personal information security incidents, and a compliance audit system for personal information protection. [2]The above laws and regulations have made a positive response to the protection of minors' personal information, reflecting China's attention to the protection of minors' personal information, but the above legislation is mostly framed and principled provisions, and it is difficult to timely protect the problem of infringing minors' personal information in practice.

3.1 There Is a Contradiction Between the Transparency of the Algorithm and the Need for the Protection of Minors

In view of the "technical black box" generated by automatic decision-making of algorithms, the main countermeasures are to publicize algorithms and improve the transparency of algorithms. Accountability makes transparency a key goal, and transparency is seen as the basis for accountability. Algorithmic transparency not only has instrumental value, including the proof value of providing evidence of violations and the improvement value of enhancing the efficiency of algorithms, but also has the intrinsic value of guaranteeing human freedom and dignity. The algorithm transparency can promote the communication of algorithms and realize the self-improvement of human beings in the algorithm society. [3]However, algorithmic openness may further expose minors' privacy and personal information. Some scholars have pointed out that algorithmic transparency is not enough to protect minors, because algorithmic transparency is equivalent to disclosing information such as algorithmic code and data, which will expose minors' secrets and privacy. [4]In addition, algorithmic transparency also faces the conflict between algorithmic transparency and commercial protection. Article 9 (4) of the

[1] Zhou Baohua, (2022). Algorithm, Visibility and Attention Allocation: The Historical transformation of public opinion Foundation logic in the Age of Intelligence. *Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition)*, *43*(01), 143-152.

[2] Wang Lei, Kong Xiaoting, (2024). Risks and governance Paths of Minors Using the Internet. *Procurator*, (20), 30-31.

[3] An Jincheng, (2023). Algorithmic transparent Hierarchy theory. *Legal Research*, *45*(02), 52-66.

[4] Li Dejia, Li Rang, (2022). Reflection and Breakthrough: A regulatory approach to prevent algorithms from infringing on minors. *Research on prevention of juvenile delinquency*, (04), 69-76.

Anti-Unfair Competition Law includes technical information that satisfies confidentiality, confidentiality and practicality into the category of trade secrets, which is the direct source of algorithmic recognition as trade secrets. [1]From the perspective of user cognition, disclosure of algorithms is not equivalent to increasing users' understanding of algorithms, and may not be able to completely resolve users' doubts.

Article 16 of China's "Internet Information Service Algorithm Recommendation Management Regulations" clarifies the "algorithm transparency obligation", requiring the platform to inform users and publicize, so as to protect the user's right to know. [2]To realize algorithm transparency, it is not only necessary to publicize and explain the algorithm, but also to ensure the transparency of information processing. By disclosing the algorithm, the strangeness and distrust of the algorithm can be reduced, and it is convenient for the user to decide whether to accept the information service using the algorithm recommendation technology. For the online protection of minors, it is not only necessary to rely on accountability after the fact, but also to emphasize transparency and prevention in the process of information flow, and play the role of algorithmic transparency in the process of handling minors' personal information from the level of regulation.

3.2 The Age Division of the Consent Mechanism for Minors Is Rigid

After the completion of the algorithm model, the use of algorithm technology needs to establish the basis of obtaining user personal data, which is divided into two stages of notification and consent. As far as the notification rules are concerned, Article 17 (1) of the Personal Information Protection Law stipulates the obligation of the personal information processor to notify. The Regulations on Online Protection of Children's Personal Information stipulate provisions such as fully informing collection and processing rules, obtaining explicit authorization and consent from children's guardians, and identifying the guardianship relationship and the validity of the guardian's authorization and consent, but only for the protection of the personal information of minors under the age of 14. In general, Article 72 of the Law on the Protection of Minors stipulates that "information processors shall follow the principles of legality, legitimacy and necessity when processing minors' personal information through the Internet." The above law does not have special provisions on the processing of minors' personal information between the ages of 14 and 18.

As far as consent rules are concerned, Article 31 of the Personal Information Protection Law requires the consent of minors' parents or guardians for the processing of minors' personal information less than 14 years old, which is the guardian consent rule. Article 24, paragraph 2, provides for the right of refusal in the application of algorithms against personalized recommendation algorithms. However, Article 31 only provides for the guardian's consent system for minors under the age of 14, which is equivalent to the default that minors between the ages of 14 and 18 have the ability to consent to or refuse the algorithm's processing of personal information, which not only reduces the authorization burden of information processors, but also can be regarded as "empowering" minors. Some scholars have proposed that one of the disputes facing the legal protection of children's personal information in the era of big data lies in "empowerment and protection". The provision of empowerment is based on the fact that children are constantly growing and developing, and their understanding and maturity will gradually improve with age. Therefore, they need to be endowed with the right of self-decision-making and participation, such as the right to freely express their thoughts and make speeches close to adults. [3]The question is how to empower and protect at the same time. The consent rule itself requires users to fully understand the content and make decisions based on their true will, so as to protect individuals' right to know and make decisions. In reality, minors between the ages of 14 and 18 do not necessarily have sufficient social experience and knowledge accumulation to understand the privacy policy and give consent or refusal. Even if minors can understand, their expressions are most likely coerced by the functions of the platform and only have formal effects, because minors are most likely to realize that if they refuse to agree to the privacy terms, they will not be able to obtain corresponding services, so they can only choose to agree to all the contents of the terms.

On the basis of protecting minors' right of information self-determination, the guardian consent rule endows the guardian with the right to control instead. [4]However, the system itself also has challenges to the concept of "empowerment and protection". On the one hand, there may be conflicts between minors and guardians as

[1] Chen Fengrun, (2022). The Legal Dilemma and Resolution Path of algorithm Regulation. *Learning and Practice*, (12), 38-47.

[2] Zhao Jing-Wu, (2021). From process control to result accountability: the difference between algorithm transparency obligation and algorithm accountability mechanism. *Peking University Law Review*, *22*(02), 18-31.

[3] Milda Macenaite, (2017). From Universal Towards Child-specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, *19*(5), 765-779.

[4] Sun Yueyuan, (2023). Review and improvement of guardian consent Rules in the protection of minors' personal information. *Journal of South China Normal University (Social Sciences)*, (01), 149-164+208.

network natives. Minors under the age of 14 have been exposed to digital technology for a long time, and their awareness of autonomy has increased, which may lead to the failure of the guardian consent system. On the other hand, the guardian arbitrarily discloses the portrait and voice of a minor on the Internet, a move that may go against the true will of the minor's heart. Under the guardian consent mechanism, it is necessary to consider how to adhere to the principle of "maximizing minors' interests" on the basis of strictly protecting the personal information of minors under the age of 14. On the basis of the effective of the guardian consent system, there is also a lack of discussion on its standard setting, that is, to what extent it can be regarded as obtaining the consent of the guardian, asking the guardian to do the maximum possible or within a reasonable range. Due to the operability and credibility of obtaining guardian's consent is not high, China's "Information security technology in the implementation of the Guide to inform and consent in the processing of Personal information" mentioned SMS and email verification methods, but may produce minors using the guardian's mobile phone or mailbox to send verification information vulnerabilities. Therefore, it is also necessary to refine the consent mechanism of minors' guardians for personal information processing, including how minors between the ages of 14 and 18 can obtain reasonable prompts to clearly inform them of the risks of algorithm application, and the standard scope of guardian consent.

3.3 A One-Time Notification of Consent Leads to Abuse of Personal Information by the Platform

Article 28 of the EU's Digital Services Act (DSA), which came into force in August 2023, states that online platform providers may not display advertisements to service recipients via portraits on their interfaces if they are reasonably certain that the recipient of the service is a minor. As a result, users under the age of 18 in the EU will be forced to turn off all AD recommendation content, and users over 18 will be able to voluntarily choose whether to turn off AD recommendation. For the prohibition of algorithmic portrait regulations and calls, China's legislation is not "one-size-fits-all" ban, choose to outline the use of algorithms to push content to minors, including "may cause minors to imitate unsafe behavior and violate social morality behavior, induce minors' bad habits and other information that may affect minors' physical and mental health, as well as inducing minors to indulge in the Internet" and other content. And many software developers targeting minors ignore regulations on their protection. In the cases mentioned above, the software developers collected, processed and exploited the information of children without the explicit notification and consent of the guardians. Driven by commercial interests, the platform will obtain as much basic information of users as possible and feed it to the algorithm, resulting in the extensive collection and utilization of users' personal information by the platform. At the same time, the platform can also promote videos containing minors' personal information to users who are interested in minors.

The information processing behavior of different platforms reflects different technical characteristics, including the steps of information collection, analysis and distribution. Among them, the personal information of minors aged 14 and below is considered sensitive personal information as stipulated in the Personal Information Protection Law, and the processing rules include that the information collection behavior should have a specific purpose, the collection behavior should be sufficient, and the collection behavior should be strictly protected. The problem is that the platform usually uses a one-time authorization to apply the "informed consent" rule when consenting to minors' use of the web page or software to obtain minors' personal information. In the face of the use of personal information involved in the subsequent use process, it is assumed that the previous authorization can cover the subsequent use behavior, so that the "informed consent" rule is often static. Article 24 of the Regulations on the Protection of Minors Online stipulates that online product and service providers are not allowed to conduct commercial marketing to minors through automated decision-making. However, the information that minors browse, like, pay attention to and comment on the Internet, after subsequent processing, may also become an automated decision-making behavior that is not conducive to minors' physical and mental health. How to realize the confirmation and notification of the collection behavior is the necessary meaning of the platform to prevent the infringement of minors' personal information.

4. The Scenario-Based Improvement of Minors' Online Personal Information Protection

The minds of minors are not mature, and they do not have sufficient ability to recognize the network information they come into contact with. At the same time, the damage caused by the network information is hidden. Therefore, it is necessary to prevent and protect them. In view of the infringement brought by algorithms on minors, the principle of "protecting the best interests of minors" should be adhered to. It is not only necessary to establish pre-algorithm recommendation supervision for minors, but also to protect the right of self-determination of minors in accessing the Internet.

4.1 Scenario-Based Information: Establish a Risk Assessment System for Minors' Personal Information

The limitation of algorithmic transparency is that it is difficult to solve problems such as algorithmic black box and dynamic change by simply requiring algorithmic transparency, while risk prevention emphasizes prevention in advance and minimizes risks by identifying, evaluating and controlling risks. In the processing of minors'

personal information, the idea of risk prevention can be expressed as the classification of risk levels for minors' personal information. Whether it is minors' information as sensitive information or ordinary minors' personal information, it is necessary to judge according to the scene where the information is located. For example, in educational applications, the collection of students' learning data may be low-medium risk, but if these data are used in commercial advertising, the risk level will rise significantly. Therefore, the evaluation system needs to be dynamically adjusted, graded according to the changing purposes and scenarios for which the information is used.

The UK Age-Appropriate Code sets out 15 standards for the design of child-appropriate online services, including data protection impact assessment requirements. The regulation stresses that agencies should conduct risk assessments based on children's age abilities and developmental needs, follow the principles of necessity and proportionality, identify potential risks and take corresponding measures to reduce them. In order to ensure the safe and compliant use of children's data, China can refer to the concept of data classification and classification protection in the Cybersecurity Law and the Data Security Law for minors' personal information, based on the importance of minors' personal information in different scenarios and the impact on their physical and mental health.

4.2 Scenario-Based Subject: Improve the Operability of the Consent Mechanism

Minors growing up in the Internet era have more opportunities to access new things. It is not only necessary to strictly protect minors, but also to provide them with opportunities to exercise their right to information self-determination, emphasizing their practical judgment ability on the basis of age division. For minors over the age of 14, the law acquiesces that they can consciously process personal information, which can be understood as helping minors transition to the Internet society and achieve a balance between "empowerment and protection". Guardians should help assess whether they are mature enough to make their own decisions and avoid inappropriate exposure of minors' personal information. The degree of maturity of a minor may be judged on the basis of his or her intellectual or mental state under the civil law. For minors under the age of 14, under the mechanism of guardian consent, in order to ensure the survival of minors in the algorithmic society, it is necessary to improve their algorithmic cognition and awareness of rights. In addition to the algorithm recommendation tips provided by the platform, it is necessary for parents to inform minors in a timely manner about the role and consequences of opening algorithm recommendation, and fully protect minors' right to know and right to refuse. In the face of conflicting opinions between minors and guardians, the rules of guardian consent should not be blindly followed, and the conscious autonomy of minors under the age of 14 should also be given due consideration. This consideration is not to require the double consent system of minors and guardians, which is more difficult to implement, but to recognize the civil legal acts of minors over 8 years old and under 14 years old in accordance with their age and intelligence, in addition to those under 8 years old who have no capacity for civil conduct.[1]

In order to further refine the guardian consent system, the guardian can take the initiative to provide identity proof, rather than using a passive response such as SMS or email to verify. It should be noted that the implementation standard of the "guardian's consent" system should be based on reasonable ability certification, rather than the maximum possible consent from the guardian. With reference to the EU's General Data Protection Regulation (GDPR), processors of personal data should be required to verify whether the consent was given by the child's guardian using "state of the art" and "reasonable efforts". For minors over the age of 14, although the law does not require parental consent to turn on the algorithm recommendation mechanism, the platform can directly include it in the first youth mode protection, and then set a pop-up window for minors to choose whether to turn on the algorithm recommendation, and the "turned on algorithm recommendation" logo on the personal homepage.

4.3 Scenario-Based Process: Dynamic Consent Notification Should Be Emphasized to Realize the Platform Protection Obligation

In order to improve the transparency of platform information processing in the process of communication and realize platform protection obligations, the implementation of platform dynamic consent should be emphasized. First of all, the first step to implement the informed consent rule requires the platform to optimize the expression of the informed consent rule. For minors under the age of 14, the law requires platforms to set up special children's personal information protection rules and user agreements. [2]The content of the Children's Privacy Policy needs to be specialized, which is different from the content of the general version of the privacy policy.

[1] Li Yongjun, Zhang Lanlan, (2022). The Dual function of minors' information consent ability and its legal realization. *Nanjing Social Sciences*, (04), 87-96.

[2] Article 8 of the Regulations on the Protection of Children's Personal Information Online.

Minors over the age of 14 shall sign the same user agreement as adult users, and the Platform shall avoid the use of obscure technical terms, or the addition of logos, notes, etc., to increase the comprehensibility of the terms.

Secondly, "when to inform", "what to inform" and "how to agree" should be determined according to specific scenarios. Platform notification is the main source of users' knowledge about how the platform handles their personal information. If users are unable to grasp the way and process of processing their personal information, they cannot determine whether their personal information is at risk. Article 34 of the Regulations on the Online Protection of Minors stipulates that personal information processors should provide minors or their guardians with ways and means to access the types and quantities of minors' personal information. Therefore, it is necessary to improve the "informed consent" rule with a dynamic information disclosure mechanism, so that minors and their guardians can know the type and use of personal information they obtain in a timely manner. In case the behavior of minors actively releasing personal information on the network causes public opinion, the platform should prompt the user in time. To obtain consent from the platform, it needs to be clear that the platform's initial consent does not mean that the subsequent processing of minors' information is entirely legal. On the one hand, the consent itself may be invalid, especially if the minors use the guardian account fraudulently, the consent is not authentic. On the other hand, the platform may illegally process the personal information of minors, resulting in the invalidation of consent. According to Article 5, paragraph 7, of the Regulations on the Administration of Internet popup Information Push Services, existing laws and regulations do not prohibit all Internet service providers from using digital portrait algorithms for minors, but only Internet popup information push service providers. Therefore, if the Internet pop-up window information push service provider uses the information obtained by the minors to paint a portrait of the user and achieve personalized information push, it violates the legal provisions.

Therefore, for the algorithm recommendation that cannot be absolutely disabled, the platform needs to ensure the good implementation of the "informed consent" rule. When fulfilling the obligation of "informing" and "publicizing", the platform should reduce the content of algorithm concept and operation principle that the public cannot understand, and focus on letting the public understand the relationship between the acceptance of algorithm technology and user rights. For minor users, the algorithm recommendation service should be turned off by default, and the impact of the algorithm recommendation service should be informed, and the way to turn on and off the algorithm recommendation service should be provided for minors, so as to protect the algorithmic right to know and choose of minor users. In order to ensure that the platform actively performs the above obligations, the public needs to supervise the platform in a timely manner.

References

An Jincheng, (2023). Algorithmic transparent Hierarchy theory. *Legal Research*, *45*(02), 52-66.

Anqi, (2023). Protection of Minors' Personal Information: Theoretical Clarification and Rule remodeling. *Chinese Youth Social Sciences*, *42*(02), 132-140.

Chen Fengrun, (2022). The Legal Dilemma and Resolution Path of algorithm Regulation. *Learning and Practice*, (12), 38-47.

Jiang Jinliang, Li Li, (2022). Children who do not need to be recorded: the proof and content of children's right to be forgotten. *Preschool education research*, (05), 69-78.

Lei Xiaozheng, Yan Shuyue, (2024). The connection Problem and Countermeasures of Minors' Network Protection and "Digital Prosecution". *Journal of Hunan University of Science and Technology (Social Science Edition)*, *27*(01), 117-127.

Li Dejia, Li Rang, (2022). Reflection and Breakthrough: A regulatory approach to prevent algorithms from infringing on minors. *Research on prevention of juvenile delinquency*, (04), 69-76.

Li Jing, Yuan Yongtao, (2023). From "Media Representation" to "Video Survival": the Information effect and order logic of short video media practice. *A collection of Dongyue papers*, *44*(12), 43-52+191.

Li Yongjun, Zhang Lanlan, (2022). The Dual function of minors' information consent ability and its legal realization. *Nanjing Social Sciences*, (04), 87-96.

Lin Huanmin, (2023). Normative Response to algorithmic "Guardianship" of Minors. *Contemporary Jurisprudence*, *37*(03), 106-116.

Lin Jia, Luo Huanxin. (2024). Toward Personalized recommendation of trust Algorithm: Legal Reflection on "One-click close". *Friends of the editor*, (03), 79-88.

Liu Yonghong, Deng Haixia, (2024). Realistic dilemma and path optimization of Minors' Personal information protection. *Journal of Chengdu University (Social Science Edition)*, (04), 115-128.

Liu Yonghong, Deng Haixia, (2024). Realistic dilemma and path optimization of Minors' Personal information

protection. *Journal of Chengdu University (Social Science Edition)*, (04), 115-128.

Milda Macenaite, (2017). From Universal Towards Child-specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society*, *19*(5), 765-779.

Pang Jinyou, Sun Yuxun, (2024). Subject alienation and democratic dilemma of algorithm propagation in digital age. *Learning and Exploration*, (12), 45-54+176.

Sun Yueyuan, (2023). Review and improvement of guardian consent Rules in the protection of minors' personal information. *Journal of South China Normal University (Social Sciences)*, (01), 149-164+208.

Wang Huanni, Liu Haiqun. (2023). Algorithm recommendation in short video platform infringes on teenagers' data rights. *Science and Technology Communication*, *15*(04), 112-115.

Wang Hui, ZHANG Xiao, (2024). Judicial Regulation on the Processing of Minors' Personal Information by Algorithm Platform. *Journal of Shandong Judge Training College*, *40*(04), 26-42.

Wang Lei, Kong Xiaoting, (2024). Risks and governance Paths of Minors Using the Internet. *Procurator*, (20), 30-31.

Wang Yongqi, (2024). The dilemma and countermeasures of minors' personal information rights protection in the digital age. *Journal of Shanxi Datong University (Social Science Edition)*, *38*(06), 17-22.

Yu Guoming, Yang Yingying and Yan Qiaomei, (2018). Algorithms as Power: The Power Revolution of algorithmic paradigms in Journalism. *Friends of the Editor*, (05), 5-12.

Zhao Jing-Wu, (2021). From process control to result accountability: the difference between algorithm transparency obligation and algorithm accountability mechanism. *Peking University Law Review*, *22*(02), 18-31.

Zhou Baohua, (2022). Algorithm, Visibility and Attention Allocation: The Historical transformation of public opinion Foundation logic in the Age of Intelligence. *Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition)*, *43*(01), 143-152.

Zhu Qinghe, Shi Xiaorui, (2024). Minors' Use of Internet media and protection of Personal Information: A Case Study No. 141. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)*, *36*(01), 25-34.