Proceedings of the 4th International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.30414

Analysis of the New Framework for the Trustworthy Personal Information Protection System—From the Perspective of the "Internet ID Project"

Hongyu Tang

School of Public Affairs, University of Science and Technology of China, Hefei, China
sa24216005@mail.ustc.edu.cn

Abstract. The construction of trustworthy network identity is a common pursuit of various technological powers in the world, which is specifically manifested as the "Internet ID Project" in China. With the official introduction of the "Public Service Management Measures of National Network Identity Authentication (Draft)", a series of specific regulations that still need to be elaborated. ID accounts and online ID certificates have caused certain misunderstandings among the public, leading to panic. This article provides a detailed explanation of the legal basis of the "Internet ID Project" and a detailed interpretation of the draft, specifically analyzing the current heated controversies surrounding the "Internet ID Project". It is concluded that the "Internet ID Project" does not have the so-called difficulty to implement supervision, pseudo voluntary principles, and information disclosure risks, but rather may have issues such as whether the Internet ID belongs to personal information. In terms of value judgement, the implementation of the "Internet ID Project" has more pros than cons, and should be strictly implemented in accordance with the prescribed framework in the future. The "Internet ID Project" is not only an important measure to develop rule of law in the Internet but also an effective attempt to ensure national security from the safety of citizens.

Keywords: Internet ID Project, Internet trustworthy identity system, personal information protection, rule of law in the internet

1. Introduction

The Third Plenary Session of the 20th Central Committee of the Communist Party of China emphasized that "improving the comprehensive internet governance system" is a key task in advancing Chinese-style modernization. Entering the digital age, everyone increasingly feels the profound transformative impact of information (in the form of data) on education, work, and daily life, and clearly recognizes that human development in the future is inseparable from such information—forming an interdependent and mutually promoting relationship. As personal information directly related to citizens, it is the "vanguard" that requires protection. The state is fully aware of the public's demand for personal information protection and has formulated a series of relevant laws and regulations starting with the Cybersecurity Law of the People's Republic of China

DOI: 10.54254/2753-7048/2025.30414

(hereinafter referred to as the Cybersecurity Law). In August 2021, the Personal Information Protection Law of the People's Republic of China (hereinafter referred to as the Personal Information Protection Law) was formally adopted by the Standing Committee of the National People's Congress, explicitly defining the concepts, methods, and approaches to personal information protection in law and providing an authoritative guiding direction for subsequent work. Article 62, Paragraph 4 of the Personal Information Protection Law clearly stipulates "promoting the construction of a social service system for personal information protection". Currently, the Ministry of Public Security, the Cyberspace Administration of China, and other authorities have drafted and released the Measures for the Administration of Public Services for National Network Identity Authentication (Draft for Comments) (hereinafter referred to as the Measures), which proposes that "a nationally unified public service platform for network identity authentication shall provide public services for national network identity authentication. Natural persons may obtain a network identity symbol (Internet ID) corresponding to their identity information but excluding explicit identity information through this service, and subsequently use the Internet ID to obtain an identity authentication credential (online ID certificate) in cyberspace"[It should be noted here that a series of constructs regarding network identity symbols (network IDs) and network identity authentication credentials (network certificates) in the "Administrative Measures for National Public Services of Network Identity Authentication (Draft for Soliciting Opinions)" are hereinafter collectively referred to as the "Network ID Project". Network certificates represent the application scenarios and methods of network IDs, so the term "network ID" is selected here as the main term for this project], thereby achieving the protection of personal information. However, for this yet-to-be-implemented trustworthy personal information protection system, it is necessary to first clarify its legal basis and structural logic, then analyze potential controversial focuses. This will help the public form a correct understanding of the "Internet ID Project", avoid unnecessary panic, and put forward feasible suggestions for further improving the Measures.

2. The significance of the "Internet ID Project"

Since it is impossible to change the basic model of platforms requesting user information, the solution lies in regulating the information obtained by platforms—hiding "explicit" content directly related to personal information. The state has launched a trustworthy personal information protection system, where individuals receive corresponding credentials from the state after completing authentication, giving birth to the "Internet ID Project". Seizing this opportunity, China also attempts to optimize the platform operation mechanism of "blindly requesting information from individuals" and reduce the possibility and feasibility of criminals infringing on Chinese citizens' personal information in the name of platforms.

The "Internet ID Project" is a transformative initiative in the field of personal information protection, embodying significant significance at both substantive and formal levels. Substantively, the actual operation of the Measures will completely change the content of personal user information that internet platforms can collect—shifting from information that was previously individually identifiable to a string of identity symbols similar to "pseudonyms". Obtaining only these identity symbols makes individual identification impossible, representing a "usable yet invisible" form. This blocks the possibility of collecting personal information and greatly reduces the risk of direct leakage of personal information. Formally, the "Internet ID Project" constitutes a "negation of negation" of the use of personal information in cyberspace. In the past, there was a focus on the accuracy and irreplaceability of individual identification; through repeated questioning and revision of this focus, the project critically redesigns the way personal information is used in cyberspace.

DOI: 10.54254/2753-7048/2025.30414

This process can be abstracted as continuous deliberation between "How (to improve personal identification methods)" and "Why (to conduct personal identification)", ultimately changing "What"—i.e., the nature of personal identification itself.

3. The legal basis of the "Internet ID Project" and the structural logic in the measures

The Party Central Committee and the State Council have always attached great importance to the construction of a network trustworthy system. As early as 2006, the General Office of the State Council forwarded the Notice of the National Coordination Group for Network and Information Security on Several Opinions on Promoting the Construction of a Network Trust System, which emphasized regulating and strengthening electronic authentication work. The "Internet ID Project" is an extension of this electronic authentication work. Currently, some scholars claim that the "Internet ID Project" lacks a legal basis and even carries constitutional risks, but such claims are unfounded. The "Internet ID Project" is a legally compliant initiative designed in accordance with national strategies.

3.1. The legal basis of the "Internet ID Project"

3.1.1. Cybersecurity law

Article 24 of the Cybersecurity Law explicitly stipulates that "the state implements a trusted network identity strategy, supports the research and development of safe and convenient electronic identity authentication technologies, and promotes the mutual recognition of different electronic identity authentications". This law elevates the construction of a trusted network identity to a strategic level, clearly supporting the research and development of safe and convenient electronic identity authentication technologies and the mutual recognition of different electronic identity authentications. It aims to promote the formulation and implementation of technical schemes and plans for trusted network identities, create a safer and more trustworthy network environment, and vigorously promote the popularization, application, and development of the internet [1]. It lays down the principled provisions for the construction of the trusted network identity strategy [2].

3.1.2. Data security law

Article 18 of the Data Security Law of the People's Republic of China (hereinafter referred to as the Data Security Law) stipulates that "the state promotes the development of services such as data security testing, evaluation, and certification, and supports professional institutions to carry out such services in accordance with the law". This provides a theoretical basis for government departments to provide services related to the network trustworthy identity system. The state supports relevant departments, industry organizations, enterprises, educational and scientific research institutions, and professional institutions to cooperate in areas such as data security risk assessment, prevention, and disposal [3]. It is important to note that these non-governmental entities play a collaborative rather than leading role in data security and other fields—meaning that government departments remain the main drivers for promoting the construction and application of the network trustworthy identity system.

DOI: 10.54254/2753-7048/2025.30414

3.1.3. Personal information protection law

Article 62, Paragraph 3 of the Personal Information Protection Law stipulates that the national cyberspace administration department shall coordinate with relevant departments to support the research, development, and promotion of safe and convenient electronic identity authentication technologies, and promote the construction of public services for network identity authentication. This defines the nature, content, and scope of network trustworthy identity services provided by government departments. Building on the relevant provisions of the Cybersecurity Law, this article requires the national cyberspace administration department to play a coordinating role, support the research, development, and promotion of safe and convenient electronic identity authentication technologies, and advance the construction of public services for network identity authentication—providing support for strengthening personal information protection and the development and application of information technologies [4].

Thus, it is clear that with trusted network identity as the thread, the Cybersecurity Law lays down principled provisions for strategic construction; the Data Security Law supports professional institutions in providing services; and the Personal Information Protection Law designates state departments as professional service providers to carry out trusted personal information work in cyberspace. These laws continuously refine, detail, and clarify the work of trusted network identity, with no subsequent law exceeding the scope prescribed by the previous ones. As the latest implementation of the trusted network identity strategy at the current stage, the "Internet ID Project"—which involves state departments such as the Ministry of Public Security and the Cyberspace Administration of China issuing Internet IDs and online ID certificates—naturally has a solid legal basis.

3.2. The structural logic of the Measures

While the "Internet ID Project" has an impeccable legal basis at the upper-level legal level, any legal inconsistencies would stem from the Measures itself exceeding the scope of statutory provisions. Therefore, it is necessary to analyze the structural logic and content of the Measures.

According to legal interpretation methodologies, the legal text is the object of interpretation in form, while understanding the content of legal provisions is the substantively meaningful object of interpretation [5]. The Measures consists of 16 articles, which can be classified based on their content: definitional provisions (Articles 1, 2, 3, 15, 16), provisions on the application and registration of Internet IDs and online ID certificates (Articles 4, 5, 6), provisions on the handling of Internet IDs and online ID certificates by internet platforms (Articles 7 to 13), and penalty provisions (Article 14).

3.2.1. Definitional provisions

Article 1 of the Measures clarifies the legal basis and purpose of formulating the measures; Article 2 defines public services, Internet IDs, online ID certificates, and other related terms; Article 3 specifies the supervisory and administrative responsibilities for public services; Article 15 defines legally valid identity documents; and Article 16 stipulates the effective date of the Measures. Among the definitional provisions, the most prone to ambiguity is the relationship between Internet IDs and personal information. The Measures explicitly defines an Internet ID as "a network identity symbol composed of letters and numbers, corresponding to a natural person’s identity information but excluding explicit identity information". The Personal Information Protection Law defines personal

DOI: 10.54254/2753-7048/2025.30414

information as "various information recorded electronically or in other forms related to an identified or identifiable natural person, excluding information that has been anonymized". Given this, can an Internet ID— as a form of anonymized information related to a natural person—still be protected by the Personal Information Protection Law? The answer is yes. Reversing the logic, although an Internet ID anonymizes personal information, individuals can still be identified through the Internet ID. In other words, an Internet ID is essentially another "ID card" issued by the state and does not eliminate the nature of individual identification. Therefore, it still falls within the scope of personal information as defined by the Personal Information Protection Law.

3.2.2. Provisions on the application and registration of internet IDs and online ID certificates

Article 4 of the Measures specifies the basic conditions for natural persons (including minors) to apply for an Internet ID; Article 5 regulates the use of Internet IDs by natural persons (including minors); and Article 6 stipulates the principle of voluntary promotion of Internet IDs and online ID certificates. It is important to note that the internet is not a "forbidden zone" for minors. As a form of ID-like credential, Internet IDs should be applied for by minors under the guardianship of adults, allowing them to access cyberspace—a necessary space for future development.

3.2.3. Provisions on the handling of internet IDs and online ID certificates by internet platforms

Article 7 of the Measures requires internet platforms to safeguard the relevant rights and obligations of citizens using Internet IDs; Article 8 stipulates the principle of minimization for internet platforms in collecting citizens' information; Article 9 defines the scope and methods for internet platforms to process citizens' information (including Internet IDs); Article 10 specifies the obligation of notification of the public service platform; Article 11 allows the public service platform to take "emergency risk avoidance" actions while requiring subsequent notification; Article 12 outlines the direction for the future development and improvement of the public service platform; and Article 13 regulates the management of passwords. The principle of minimization in the handling of Internet IDs and online ID certificates by internet platforms is consistent with the provision in Article 6 of the Personal Information Protection Law that requires "adopting methods that have the least impact on personal rights and interests".

3.2.4. Penalty provisions

Article 14 of the Measures stipulates the penalties for violating the measures. Both internet platforms and public service platforms must not exceed the scope of conduct prescribed in the Measures in verifying and processing users' personal information. Those who constitute a crime shall be held criminally responsible.

A step-by-step analysis of the provisions reveals no violations of upper-level laws, thus refuting the claim that the "Internet ID Project" lacks a legal basis. However, remaining controversies surrounding the project still require verification and leave room for improvement, which will be elaborated on in the next section.

4. Controversial focuses and analysis of the "Internet ID Project"

During the public comment period of the Measures, there were many controversial topics. Some scholars questioned and expressed concerns about its voluntary principle, the risk of personal

DOI: 10.54254/2753-7048/2025.30414

information leakage, and even the involvement of public power. With in-depth understanding of the "Internet ID Project" and official explanations, many unfounded controversial points have become unsustainable and faded from the spotlight. However, the issues of who bears the regulatory responsibility for the "Internet ID Project", the implementation of the voluntary principle, and the assessment of information leakage risks remain key focuses for the subsequent implementation of the project and require detailed analysis.

4.1. Where does the regulatory responsibility lie

Article 2 of the Measures mentions that the state will build a public service platform for Internet IDs and online ID certificates to provide services such as application, issuance, and identity verification for natural persons. But who will formulate the Internet IDs and online ID certificates? Is it the Ministry of Public Security and the Cyberspace Administration of China, which are responsible for overall coordination, or other scientific research departments entrusted by them? The former will face the dilemma of "self-supervision", while the latter will encounter ambiguity regarding the supervised entity. Both scenarios raise the same questions: Who is the supervised entity? Who is the supervisory authority? Article 60 of the Personal Information Protection Law stipulates that "the national cyberspace administration department shall be responsible for coordinating the work of personal information protection and relevant supervisory and administrative work". Following this logic, the national cyberspace administration department should assume the regulatory responsibility for the "Internet ID Project". In other words, the national cyberspace administration department shall supervise the Ministry of Public Security and the Cyberspace Administration of China in the implementation of the "Internet ID Project".

4.2. True voluntariness or "disguised coercion"

The Measures explicitly states that the application and use of Internet IDs and online ID certificates shall follow the principle of voluntariness. However, when the number of users reaches a certain scale, an "inertial effect" will gradually emerge, which may seriously infringe on the relevant rights and interests of natural persons who do not use Internet IDs or online ID certificates. This is also a substantive manifestation of the "digital divide". How to ensure that the voluntary principle does not degenerate into a form of "disguised coercion" in practice? The only way is to ensure that natural persons who do not apply for Internet IDs or online ID certificates are not "neglected" or "discriminated against" when receiving internet services, and that they receive equal services as those using Internet IDs or online ID certificates. The voluntary principle of the "Internet ID Project" does not depend on the literal provisions in the Measures but on the actual operation during implementation.

4.3. Is the risk of information leakage reduced

In essence, the "Internet ID Project" involves hiding existing personal information to generate new information. If improperly handled during this process, major mistakes similar to those in South Korea's implementation of the national real-name identity strategy may occur. Previously, South Korea forced the implementation of an internet real-name system to combat cyber violence and crimes without adequate consideration for citizens' privacy protection, resulting in the leakage of identity information of more than 70% of the country's citizens. Ultimately, the internet real-name system failed [6]. The failure in South Korea was due to focusing solely on practical needs while

DOI: 10.54254/2753-7048/2025.30414

neglecting technical support, leading to the ineffective protection of a large amount of citizens' personal data despite the existence of regulatory provisions. In legal discussions, we do not involve the maturity of technology but focus on the risk of information leakage during the implementation of the trusted network identity strategy. In fact, the term "trusted" in trusted network identity already includes the concept of security, as trustworthiness requires compliance with principled provisions such as the principles of scientific practicality, clear boundaries, and dynamic updates—all of which ensure that network data security requirements are met at the strategic level. A trusted network identity possesses excellent security performance, capable of resisting various acts such as identity theft and cyber fraud, and is an important means to address a series of network security issues [7]. Therefore, the risk of information leakage only exists at the specific operational stage, and the ability to ensure information security during the implementation of the trusted network identity system is beyond the control of the strategy itself. From the perspective of China's trusted personal information protection and the trusted network system strategy, the risk of information leakage is almost negligible.

Through analysis, it can be concluded that the controversies surrounding the "Internet ID Project" mainly stem from misunderstandings and narrow interpretations of the project. In fact, many major global network powers are competing to build trusted network identities (with different names but the same essence). For example, the European Union has formulated a new plan to expand the pan-European digital identity framework; the United States has adopted the National Strategy for Trusted Identities in Cyberspace;

The United Kingdom is developing an easy-to-use and universal digital identity; Australia is committed to establishing a national digital identity authentication, management, and operation mechanism; Singapore is fully promoting a national digital identity authentication system; and India is implementing the "Aadhaar" unique identification program [8]. In China, it is referred to as the "Internet + Trusted Identity Authentication Platform" (CTID Platform for short), which provides three core functions: real identity verification, online ID certificate issuance and management, and online ID certificate authentication [9]. The trusted network identity strategy is also a manifestation of national sovereignty, as national sovereignty includes the power to manage citizens' identities [10].

5. The important significance of the "Internet ID Project" for the rule of law in the internet

While the state-led construction of a trusted network identity represented by the "Internet ID Project" makes tremendous contributions to the cause of personal information protection, it is bound to have a new impact on existing laws. The proposal and update of any concept will have a more or less profound impact on the law, and the law evolves and develops through such continuous impacts. However, there are too many branch laws to enumerate, so this paper focuses on criminal law and civil law, while also discussing the promoting role of the "Internet ID Project" in the future cause of the rule of law.

5.1. Criminal law perspective

The impact of the "Internet ID Project" on China's current criminal law mainly manifests in three aspects: first, crimes endangering national security, mainly involving the dissemination of harmful, negative, and false information using false identity information; second, crimes of infringing on personal information, mainly including acts such as tampering with, destroying, leaking, illegally

DOI: 10.54254/2753-7048/2025.30414

obtaining, and illegally using personal information; third, cyber fraud crimes, mainly involving defrauding money by impersonating others' identity information.

5.1.1. Eliminating false identities

Law plays an important role in the perspective of national security, which is not only required by the rule of law but also determined by the core concept of national security. Taking advantage of the anonymity of false identities, criminals can freely speak and spread harmful information in cyberspace. The core of the "Internet ID Project" lies in the state's management of citizens' identities. Under certain conditions related to case handling and potential criminal activities, national authorities can retrieve relevant information, eliminating the anonymity of false identities. At the same time, even if criminals refuse to apply for an Internet ID or online ID certificate, law enforcement agencies can analyze the group of non-users, which also improves investigation efficiency and enables the rapid identification of criminal suspects.

5.1.2. Combating the illegal use of personal information

Article 253-1 of the Criminal Law of the People's Republic of China stipulates the crime of infringing on citizens' personal information. An Internet ID is a network identity symbol corresponding to an individual's identity information but excluding explicit identity information, and it is difficult to identify an individual solely based on this symbol. In this case, can an Internet ID be regarded as personal information? From a teleological perspective, an Internet ID is derived from personal information and reflects a citizen's identity, so it should naturally be considered personal information. From a consequentialist perspective, an Internet ID is different from relatively anonymized data in public cyberspace—such anonymized data can still be used to locate personal information through in-depth mathematical analysis, leading to information leakage [11]. The special nature of an Internet ID means that even if illegally used, it will not cause harm to the actual personal information. Therefore, it should not be regarded as personal information under the crime of infringing on citizens' personal information. However, both perspectives indicate that criminals cannot cause harm to personal information other than the Internet ID even if they infringe on the Internet ID, nor can they easily use the Internet ID for infringement. Moreover, such acts are easy to trace. It can be predicted that the implementation of the Internet ID will significantly reduce the number of crimes involving personal information.

5.1.3. Curbing fraud through identity impersonation

In the internet era, fraud in cyberspace is more common than in the real world. At the same time, most cyber fraud originates from identity impersonation. However, the separation of real personal identity information and Internet ID information makes it more difficult for fraud to succeed. For example, in the process of fund transfer, the Internet ID completely anonymizes the recipient, so normal individuals will be more inclined to confirm the identity of the recipient, making it likely that the fraudulent intent will be exposed and preventing the success of cyber fraud.

DOI: 10.54254/2753-7048/2025.30414

5.2. Civil law perspective

5.2.1. Contributing to personal information protection

The innovative role of the "Internet ID Project" in civil law mainly lies in the field of personal information protection. In the digital age, how to protect personal information? Article 1034 of the Civil Code of the People's Republic of China stipulates that natural persons' personal information is protected by law. However, mere legal provisions and remedies cannot fully ensure the protection of personal information—at best, they are relatively sound remedial measures. The "Internet ID Project" constructs a trusted network identity system, which effectively compensates for the lag of the law but also brings new controversial risks, namely the distinction between Internet IDs and personal information discussed earlier. Undeniably, the emergence of the Internet ID has made a significant contribution to the cause of personal information protection.

5.2.2. Better distinguishing between the right to privacy and personal information

There is significant academic controversy between the concepts of the right to privacy and personal information. Some scholars have argued that there are no essential differences between the two rights in terms of nature, scope, characteristics, and purpose [12]. Others believe that the legislative spirit and protection models of the right to privacy and personal information are different, leading to inconsistencies in liability principles, illegality determination, and damage assessment standards [13]. Additionally, some scholars argue that the content contained in the right to privacy and personal information is inconsistent based on the different purposes and consequences of infringement [14]. The "Internet ID Project" is generated based on the reprocessing of personal information. Using reverse thinking, it can be inferred that content not required for generating the Internet ID is not personal information but may fall within the scope of privacy.

5.2.3. Further safeguarding users' right to know about personal information

In the field of civil law, personal information protection mainly adopts the "informed-consent system". "Informed" means that personal information processors and managers must fully inform personal information holders and explain the process of processing their personal information. "Consent" means that personal information holders can voluntarily decide whether to consent based on their ability to make true and voluntary expressions of will. Article 9 of the Measures stipulates three requirements and two scenarios for the public service platform in processing personal information. The three requirements are the consent requirement, the confidentiality requirement, and the deletion requirement—i.e., "when providing public services to natural persons, the platform shall perform the obligation of notification in accordance with the law and obtain their consent", "without the separate consent of the natural person, the public service platform shall not arbitrarily process or provide relevant data and information to third parties", and "the public service platform shall promptly delete users' personal information in accordance with legal and administrative provisions or user requests". The two scenarios are that separate consent from the holder is required when processing sensitive personal information, and written consent from the holder is required when stipulated by laws and regulations. Article 10 of the Measures details the matters subject to the obligation of notification. The Measures not only elaborates on the right to know about personal information from the perspective of personal information processors but also emphasizes that "personal information" here refers to the Internet ID. As a regenerated code, the Internet ID is more

DOI: 10.54254/2753-7048/2025.30414

conducive to the implementation of the right to know and will not cause issues related to the right to know in the use of actual personal information.

5.3. Future perspective of the rule of law in the internet

5.3.1. The integration of mature technology and law has become an international trend

Over the past 10 years, the United States has basically achieved the strategic goals of the National Strategy for Trusted Identities in Cyberspace (NSTIC), establishing a user-centric identity ecosystem, improving the privacy protection environment, and enhancing the convenience of online transactions and the security of sensitive information [15]. Although China started late in the construction of a trusted network identity, its purpose is not the same as that of the United States. As explained in the official interpretation of Internet IDs and online ID certificates, one of the roles of the public service for national network identity authentication is to improve the level of network integrity and optimize the business environment. Another important role is to reduce costs and increase efficiency for enterprises, enabling them to focus more on improving product and service quality and user experience, and promoting the sustainable and healthy development of the internet industry and the digital economy [16]. While technology provides clearer conceptual definitions for the law, it will inevitably lead to the emergence of new rights, responsibilities, and challenges in the law. The two promote each other and develop continuously.

5.3.2. Paving the way for state intervention in specific legal protection fields

A major feature of the "Internet ID Project" is that the state, on behalf of relevant institutions and departments, acts as the builder of the public service platform for Internet IDs and online ID certificates. Both the traditional legal philosophical trend of "citizens as the state" and the academic recognition that "the legislative purpose of the current legal system centered on private interests is inconsistent with the original intention of personal information protection and difficult to safeguard public security and national security" [17] indicate that the legal protection of personal information not only supports citizens' autonomy in exercising their rights but also safeguards public security and even national security. When the legal interest of a protected object rises to the level of national security, the state should fulfill its obligation corresponding to citizens' transfer of certain rights—specifically, taking the initiative to assume the responsibility of building a security protection system.

5.3.3. Expanding the scope of citizens' personal rights in the internet

If the trusted network identity is officially implemented, citizens will obtain new legal rights. With the advancement of technology, the continuous development of "Internet +", and the deepening of " data element ×", new rights related to the internet and data assets will inevitably emerge, and citizens' existing rights in the internet will continue to expand in scope and extension. For example, regarding personal data, there is a parallel and comprehensive protection approach between personal information as a private law interest and data as a public law interest [18]. In the future, individuals may have the right to decide the use of certain personal data similar to the Internet ID, which will represent a further expansion of the scope of citizens' personal rights.

DOI: 10.54254/2753-7048/2025.30414

6. Conclusion

The "Internet ID Project" is undoubtedly a "bold innovation" for China's internet rule of law and has a certain impact on the existing legal system, such as criminal law and civil law. Given the public's panic caused by misunderstandings of the Measures (Draft for Comments), the authorities need to provide further explanations to help the public understand that the trusted network identity system is a necessary and feasible means of personal information protection, not an act of prying into or interfering with citizens' privacy through the convenience of public power. The birth of the Internet ID hides the actual personal information, allowing citizens to enter cyberspace with a more free, open, and assured identity. In this process, the state assumes three roles—designer, manager, and operator—forming a "trinity" to more effectively safeguard the normal exercise and reasonable use of citizens' private rights. At the same time, the future official implementation of the Measures means that China's technical means are constantly catching up with those of major global technological powers, gradually narrowing the technical gap. In this process, the focus is not on the mandatory application of technical means but on the protection of citizens' personal rights, reflecting China's firm determination to advance Chinese-style modernization and its theoretical belief in implementing people's mastery of the country.

References

[1] Yang, H. Q. (Ed.). (2016). An interpretation of the Cybersecurity Law of the People's Republic of China. China Democracy and Legal System Press, p. 80.
[2] Zheng, X. D. (2018). Promoting the construction of a trusted network system under the condition of big data intellectualization. The People's Congress of China, (11), 49.
[3] Long, W. Q. (Ed.). (2021). An interpretation of the Data Security Law of the People's Republic of China. China Legal Publishing House, p. 62.
[4] Yang, H. Q. (Ed.). (2022). An interpretation of the Personal Information Protection Law of the People's Republic of China. Law Press China, p. 156.
[5] Wei, Z. X. (2017). Legal interpretation: Exploring the normative meaning in the tension between object and goal. Journal of Nantong University (Social Sciences Edition), 33(01), 41-48.
[6] Song, X. R., & Zhang, M. (2018). Research on technical issues of trusted network identity authentication. Cyberspace Security, 9(03), 69-77.
[7] Peng, X. B. (2019). The importance of constructing a research center for network identity security technology. Journal of Information Security Research, 5(10), 913-917.
[8] Yu, R. (2022). The construction of digital identity in various countries and the development path of trusted digital identity in China. Journal of Information Security Research, 8(09), 858-862.
[9] Yang, L., Guo, W., & Sun, Y. L. (2020). The construction and application of the "Internet + trusted identity authentication platform". Police Technology, (03), 11-14.
[10] Guo, Q. (2022). Research on issues related to the construction of a trusted network identity system. Journal of Information Security Research, 8(09), 871-878.
[11] Yu, R., Deng, C., Zhao, Y., et al. (2024). Current situation, problems and countermeasures of identity management in the digital society. Strategic Study of CAE, 26(03), 207-216.
[12] Peng, D. (2023). Re-discussing the right to privacy in Chinese law and its relationship with personal information rights and interests. China Law Review, (01), 161-178.
[13] Cai, Y. B., & Guo, F. Q. (2022). Conjunctive protection under the distinction between privacy and personal information. Academic Exchange, (12), 105-118.
[14] Zhang, H. (2022). Re-distinguishing the functional orientation of information privacy and personal information. Social Sciences in Beijing, (01), 98-108.
[15] Li, X. Y., & Guo, Q. (2020). The latest progress of the U.S. national strategy for trusted identity in cyberspace. Journal of Information Security Research, 6(07), 575-581.
[16] Xinhua Daily Telegraph. (2024, August 26). Six key questions about the hot topics of online ID and online certificate (p. 002).

DOI: 10.54254/2753-7048/2025.30414

[17] Chang, Y. H. (2023). The impact effect of personal information on public security and risk response. Journal of Intelligence, 42(05), 184-191.
[18] Zeng, C. (2022). On the hierarchical protection model of personal information and data. Studies on the Socialism with Chinese Characteristics, (Z1), 131-142.