Proceedings of the 2nd International Conference on Social Psychology and Humanity Studies
DOI: 10.54254/2753-7048/39/20240612

Research and Analysis on the Current Implementation of Real-Name System in Cyberspace

Zhang Yousheng[1,a,*]

[1]*Zhuhai University of Science and Technology, No. 8 Anji East Road, Sanzao Town, Jinwan District, Zhuhai City, Guangdong Province, China*
a. zhangyousheng0411@163.com
**corresponding author*

Abstract: With the advent of the digital age, human society has inevitably entered a trend of digitization. Within this context, the fundamental unit of social operation—citizens—is also inevitably becoming digitized. Citizen identity authentication and management are essential prerequisites for the orderly operation of a digital society and represent a significant challenge that digital governments need to address. There exists a close relationship between digital citizens and the current implementation of the real-name system in cyberspace. In the future, this system will not only help enhance the sense of identity for citizens in the digital realm but will also aid digital governments in better fulfilling their responsibilities to maintain order within the digital society. This research is rooted in the present and aims to analyze the current status of the real-name system in cyberspace, identify existing issues and challenges, and propose corresponding strategies and solutions.

Keywords: Digitization, Real-Name System in Cyberspace, Digital Government, Citizens

1. Introduction

As humanity progresses towards the digital era, the basic constituent unit of society—citizens—is inevitably being digitized. In the future, digital citizens will efficiently exercise their responsibilities, rights, and obligations in the digital society through authenticated digital identities. The authentication of digital citizens' identities is an important task that future digital governments must undertake, contributing significantly to maintaining order within the digital society.

The current cyberspace serves as a digital and virtual embodiment of information exchange. In the future, the digital society will further digitize the real world and interconnect all entities. Challenges and information faced by the future electronic society and government will become increasingly complex. The internet serves as a crucial platform for accessing information, exchanging opinions, and expressing viewpoints. However, it has encountered numerous issues such as cyberbullying, information theft, online scams, and a large number of fake users. To address these issues, the call for a real-name system in cyberspace has grown louder. Some countries and regions have already started implementing this system, using authentication to trace and confirm user identities, thereby enhancing governance efficiency and ensuring cyber safety.

DOI: 10.54254/2753-7048/39/20240612

2. Concept and Features of the Real-Name System in Cyberspace

2.1. Advantages and Significance of the Real-Name System in Cyberspace

2.1.1. Maintaining a Favorable Atmosphere on Online Platforms

Cyber language violence often occurs on internet blogs and forums. In recent years, with the advancement of internet technology, interactive social media platforms such as microblogs and video websites have become hotspots for cyber language violence. [1] Implementing a real-name system can promote the construction of a social integrity system, making individuals more mindful of their conduct. On platforms like social media, users are required to use their real names when posting content, leading to increased awareness of their behaviors. This aids in reducing the spread of negative information and curbing malicious activities by netizens.

2.1.2. Facilitating Government Digital Management

Real-name authentication assists governmental bodies and other institutions in managing and supervising cyberspace. When cyber incidents or criminal activities occur, real-name authentication makes it easier for relevant departments to track and identify responsible individuals, thereby maintaining societal stability and security. Moreover, for both relevant enterprises and governments, the real-name system in cyberspace can weed out a large number of fake users and online mercenaries, reducing the monitoring and governance costs for platforms or even governments. This not only alleviates the burden of daily operations but also helps curb illegal activities such as fraudulent transactions, manipulation of public opinion, and server attacks.

2.1.3. Enhancing Credibility of Online Information

The implementation of the real-name system in cyberspace prompts users to consider the appropriateness of their behavior and the credibility of their content when posting or disseminating information. This approach aids in curbing the spread of online rumors, anti-intellectual speech, and online scams. Furthermore, it could even be considered to link the credibility index in cyberspace with personal credit, tying internet credibility to individual creditworthiness.

2.1.4. Augmenting Affability in Online Interactions

In business or social settings, real-name authentication allows individuals to more easily verify each other's identities, backgrounds, and even interests, fostering trust and cooperative relationships. It also facilitates a sense of familiarity among netizens in social interactions, enabling them to recognize that they are communicating with living individuals rather than just interacting with a cold screen. This aspect contributes to furthering the healthy development of digital platform culture.

3. Current Status of the Real-Name System in Cyberspace

3.1. Development and Present State of China's Real-Name System in Cyberspace

In the early stages, China primarily implemented backend real-name systems through forums and other social platforms, requiring users to provide genuine personal information when registering accounts. While this approach to some extent safeguarded users' rights, it did not completely eliminate the spread of false information and instances of cyber violence.

From 2011 onwards, the government mandated frontend real-name systems for social platforms like Weibo, necessitating users to use real names and identity information when posting. This policy

DOI: 10.54254/2753-7048/39/20240612

significantly improved the information quality in cyberspace and streamlined the government's supervision and management of cyberspace.

In recent years, most incidents of online violence have been associated with a lack of effective regulation among internet service providers [2]. The dissemination process in traditional media is rigorous and controllable, allowing for timely corrections upon identifying errors, thereby reducing the harm caused by dissemination. However, the dissemination in new media platforms like Weibo is a raw and unrefined process, allowing netizens to freely repost and share [3]. The implementation of the real-name system in cyberspace, as an effective management tool, has gradually become a focal point of public attention. Its prominence continues to rise as people's aversion to online violence and desire for a well-regulated cyberspace grow stronger.

China has enacted three regulations mandating the real-name system, aiming to expand its usage across more platforms. Challenges such as inaccurate user information and disruptions in network supervision exist within this system [4]. Overall, while the real-name system has elevated information quality and the civility of netizens, concerted efforts are still required from all parties to address these challenges.

3.2. Implementation Status of the Real-Name System in Foreign Countries

3.2.1. South Korea

In South Korea, the real-name system in cyberspace is known as "personal confirmation," adhering to the principle of "backend real-name, frontend voluntary." During user registration and login, individuals must use genuine names and identification numbers for identity verification, yet they can opt to use pseudonyms when posting messages.

The foundation of managing South Korea's real-name system in cyberspace involves establishing internet supervisory bodies and creating coordinated governance mechanisms, employing a tiered management system to address potential issues. Daily management of the real-name system is supported by relevant legal frameworks aimed at safeguarding citizen privacy and fostering healthy online development, with sentencing guidelines for cybercrimes. However, on August 23, 2012, the South Korean Constitutional Court ruled the real-name system unconstitutional. It was deemed ineffective in reducing malicious speech and illegal information while increasing the risks of personal information leakage and illegal exploitation. Additionally, it hindered foreigners without South Korean IDs from registering and accessing South Korean websites [5]. Other countries manage the internet through private self-discipline without implementing a real-name system, achieving the goal of controlling illegal information through alternative means like IP tracking, criminal penalties, and compensation measures.

3.2.2. European Union

In August 2014, the European Union officially implemented the "Regulation on Electronic Signatures and Electronic Identity Cards," equating eIDs with physical identity cards legally. This regulation aimed to promote the adoption and use of electronic signatures, ensuring the authenticity and reliability of electronic identities. It removed legal barriers surrounding electronic signatures, fostering the development of e-commerce and the digital economy, while enhancing the authenticity and credibility of electronic identities, holding significant implications for network security and societal credit systems.

However, some individuals believe the promotion of eIDs could pose risks of privacy breaches due to the centralized storage of personal identity information in electronic databases. Additionally, using eIDs might present challenges for certain demographics such as older individuals, those with lower literacy levels, and those unfamiliar with internet technology.

DOI: 10.54254/2753-7048/39/20240612

To address these concerns, the government and relevant departments have taken measures to improve and refine the system. These measures include establishing and enforcing legislation to enhance eID privacy protection, guaranteeing citizens' personal privacy through clear legal frameworks [6]. Moreover, tailored training and awareness programs for e-signature and eID usage have been conducted to cater to various user groups, offering options to use both traditional physical identity cards and electronic signatures to meet diverse needs.

After years of practice and application, electronic signatures and eIDs in the European Union have become integral components of people's daily lives and work. This regulation not only propelled the widespread use of electronic signatures but also heightened public awareness and emphasis on network security.

3.3. Current Challenges Faced by the Real-Name System

3.3.1. Incomplete Relevant Institutional Systems

The foundation for stable operation lies in legal frameworks and practical, feasible systems. However, China's most significant issues in related domains revolve around incomplete system designs, unreasonable allocation of responsibilities, and the absence of effective legal recourse pathways. Failure to assign specific responsibilities to concrete entities makes it challenging to carry out effective actions in actual execution, supervision, and governance. Additionally, concepts surrounding the real-name system remain unclear, legal frameworks supporting the real-name system in social networks are inadequate, and sentencing guidelines for cybercrimes remain ambiguous, leading to legal gaps and gray areas in its implementation.

3.3.2. Information Leakage and Privacy Protection Issues

During the implementation of the real-name system in cyberspace, ensuring the security of user information and protecting privacy rights poses a significant challenge. Personal authentic information stored in platforms' databases poses irreversible public event risks if leaked. South Korea previously experienced incidents of massive personal information leaks due to hacker attacks. The potential misuse or leakage of information could adversely impact users' personal privacy and lives.

3.3.3. Data Divide and Platform Barriers

The implementation of the real-name system should establish a cross-platform authentication mechanism and technical support to ensure that once a user registers on one platform, they can swiftly log in and authenticate across other platforms. However, current commercial platforms, forums, and even different government platforms each maintain their authentication systems. This inconvenience in daily use for netizens creates fragmentation for individuals across different platforms. This impedes the seamless engagement of netizens in the online community, posing hindrances and increasing operational burdens on various administrative entities.

3.3.4. Inconsistent and Inaccurate Identity Authentication Standards

The essence of the real-name system lies in ensuring the identity verification of individuals. However, current identity authentication under the internet's real-name system faces challenges. Firstly, the verification process lacks standardization, and authentication content and methods vary across platforms, resulting in reduced accuracy in authentication. Secondly, these vulnerabilities might enable malicious actors to impersonate others for nefarious activities. There's a risk of identity theft for AI facial swapping, spoofing, doxing, and engaging in online fraud.

DOI: 10.54254/2753-7048/39/20240612

4. Strategies and Recommendations to Address the Issues

4.1. Refinement of Legal Frameworks and Related Concepts

The significance of legal frameworks in society is self-evident. The implementation of the real-name system and operation of digital citizen identity authentication hinge on clearly defining legal frameworks and related concepts. This not only concerns citizens' fundamental rights but also forms a vital cornerstone in ensuring future order and stability in the digital society.

Both South Korea and the European Union introduce amendments promptly to address shortcomings in the real-name system, ensuring that legal systems can resolve issues arising from new technological applications. In the forthcoming digital era, the complexities of interconnectivity will exacerbate. Social concepts will undoubtedly be influenced by electronic information technology. Therefore, continuous updates and advancements in defining legal frameworks and related concepts are crucial to adeptly address new governance challenges in the digital age.

Moreover, with the evolution of the era, citizen consciousness will deepen, requiring careful consideration of citizens' rights to freedom of speech, privacy, and human rights. Laws themselves constitute an extensive system. Only through interconnectedness can their maximum efficacy be realized. Thus, clear delineation of various illegal activities in the network and explicit sentencing divisions are necessary to enable the digital government to operate lawfully, based on the law and in administrative affairs.

4.2. Enhancement of Citizen Social Awareness

Citizens are both recipients of digital government services and participants in digital life. In the internet environment, many perceive the web merely as a platform for information retrieval, entertainment, and social interaction, often overlooking its societal implications. Netizens might engage in behaviors online, such as verbal abuse, attacking others, or disseminating false information, without recognizing the legal responsibilities behind these actions. The repercussions of online actions can affect the real world and may constitute infringements on others' rights [7].

Therefore, elevating the social awareness of citizens or netizens regarding the digital society and the real-name system is paramount. The internet originates from the real world, and citizens need to recognize that the digital society or internet is a tangible social space, not exempt from laws. Referring to legislative instances in countries like the United Kingdom and Germany, their internet management relies on civilian self-discipline. Digital citizens must respect laws and others in the same way as in the physical world.

Only when citizens comprehensively understand the importance of mutual respect and law compliance and intertwine it with the digital era to form a new consciousness of digital citizenship, can the initial intent of maintaining digital citizen identity authentication and management, i.e., upholding societal order in the digital age, be sustained in perpetuity.

4.3. Establishing a Unified System or Platform

A significant highlight of information technology is its disruption of temporal and spatial boundaries, introducing unprecedented efficiency and convenience. If various platforms or government levels lack uniform standards, hindering information flow, the full advantage and unique allure of electronic information technology cannot be realized. For the real-name system and future digital citizen identity authentication and management, it's imperative to establish a unified and interconnected system. This facilitates citizens' smooth passage across various online domains.

A unified and interconnected system would allow digital citizens to comprehend each other more comprehensively, further enhancing the mutual trust of the entire digital society and network. This

DOI: 10.54254/2753-7048/39/20240612

benefits not only citizens but also reduces operational and maintenance costs for platforms and digital governments. Genuine cross-domain big data analysis would lead to more efficient and personalized resource allocation in the digital society.

A unified large system or platform aids in monitoring illegal activities comprehensively, swiftly detecting and addressing criminal behaviors, and upholding social safety and stability. However, the contradiction between information regulation and privacy rights, as well as commercial confidentiality, requires enhanced legal regulations.

4.4. Strengthening Collaboration among Diverse Entities

Citizens, platforms, governments, and nations are indispensable elements in operation. In the digital society of interconnectivity, the interrelationships between systems or elements are becoming increasingly tight-knit, deepening their mutual dependence.

Citizens form the foundational force of societal operations, establishing close connections with various elements through participating in digital social activities, work, learning, and life. Platforms act as the link, providing citizens with convenient, efficient, and intelligent services while offering comprehensive and precise data support and service assurance to enterprises and governments.

Governments, as providers of digital social management and public services, also need close collaboration with citizens, platforms, and the nation. Through interaction with citizens and enterprises, digital governments can better understand citizens' needs and demands to enhance digital citizen management systems and improve governance and service levels.

Thus, only by strengthening diverse entity collaboration can the implementation of digital citizen identity management be more effective, societal order be maintained, and the development of the digital society be propelled at a faster pace.

5. Conclusion

The real-name system holds positive significance in maintaining a favorable online platform atmosphere, ensuring information authenticity and credibility, and enhancing warmth and trust in online interactions. Its implementation helps standardize online behavior, reduce false information and irresponsible speech, fostering a healthy, harmonious, and safe online environment. Moreover, it promotes trust and interaction among users, elevating the overall quality and social benefits of online platforms.

However, the real-name system encounters issues such as incomplete institutional frameworks, lack of legal protection and regulatory mechanisms, severe information leakage and privacy protection concerns, limitations in promoting due to data gaps and platform barriers, and inconsistent and inaccurate identity authentication standards. Solutions encompass refining legal frameworks and related concepts, elevating citizen social awareness, establishing a unified system or platform, enhancing diverse entity collaboration, and advancing related technologies.

The current online community has achieved digitized and virtualized information exchange, while the future digital society will realize a higher degree of digitization and interconnectivity than existing online platforms. While envisioning the future of the digital society is inspiring, grounding ourselves in the present issues is crucial. Addressing present problems is pivotal to inaugurating the digital era step by step. If current issues in the online network remain unresolved and inadequately discerned, humanity will face even more uncertainty upon truly entering the electronic society.

References

[1] *Mao Xiangying. Psychological Mechanism Analysis of Cyberbullying Behavior[J]. Journal of Suzhou Education Institute, 2018, (04).*

DOI: 10.54254/2753-7048/39/20240612

[2] *Han Xiaozhen. Research on Legal Regulation of Cyber Violence in the New Media Era[D]. Hebei University of Economics and Business, 2020.*
[3] *Li Shanmin. The Rise and Fall of South Korea's Network Real-Name System and Its Enlightenment for China[D]. Soochow University, 2014.*
[4] *Yuan Wendong. Research on Legal Regulation of Personal Information Infringement by Network Service Providers[D]. Hebei University, 2020.*
[5] *Bian Quanchao. Research on the Legal Protection of Freedom of Speech on the Internet in China[D]. Harbin Engineering University, 2018.*
[6] *Zhao Yanan. Analysis of Legal Issues Exempting Information Disclosure in Chinese Universities[D]. Xiangtan University, 2016.*
[7] *Deng Weihui. National Obligations to Safeguard Freedom of Expression on the Internet[J]. Journal of Gansu Political Science and Law Institute, 2015, (01):123-132.*