ISSN 2616-7433 Vol. 6, Issue 7: 1-5, DOI: 10.25236/FSST.2024.060701

Network Information Security Risks and Maintenance in the Construction of Digital Courts

Long Jiaqin[1,a,*]

[1]*School of Law, China Jiliang University, Hangzhou, China*
[a]*823396828@qq.com*
[*]*Corresponding author*

Abstract: *In 2023, the "Overall Layout Plan for the Construction of Digital China" issued by the Central Committee of the Communist Party of China and the State Council pointed out that "the construction of digital China is an important engine for promoting Chinese-style modernization in the digital era", and the construction of digital courts is the positive response and implementation of the construction of digital China in the judicial field. The construction of digital courts relies on the two major elements of digital information and digital technology to optimize the allocation of judicial resources and improve judicial efficiency. The digital court takes the network platform as the basic carrier, and the platform integration and paperless transformation are the two highlights of the construction of the digital court, but at the same time, the online judicial data and the cloudification of judicial behavior have also triggered the network information security risks in all aspects of the online judiciary. In response to network information security risks in the construction of digital courts, such as information leakage and illegal intrusion, case-handling offices, litigation participants, and outsourcing managers who participate in platform-based integration and paperless applications can be used to enhance relevant entities' awareness of information security protection and information security protection capabilities through multiple legal and technical means, and complete a network information security construction system that "combines internal leakage prevention and external intrusion prevention".*

Keywords: *digital court construction; information leakage; trespassing; Network information security maintenance*

1. Overview of the Construction of Digital Courts

The report of the 20th National Congress of the Communist Party of China emphasized the importance of accelerating the construction of a cyber power and a digital China. In recent years, the Supreme People's Court of China has actively responded to the needs of the rule of law in the digital era, and comprehensively promoted the construction of digital courts with online handling of all services and online synchronization of all links. Shanghai and Zhejiang have taken the lead in deploying and promoting the construction of digital courts and the construction of global digital courts in the country, further driving the construction of digital courts to radiate across the country. At present, the people's courts across the country are stepping up the construction of digital courts, and strive to achieve that by the end of 24, more than 3,500 courts across the country will be able to handle cases on the "one network", so as to promote the further improvement of the quality and efficiency of litigation services and trial work.

The digital court provides the people with a new type of judicial service that is intensively integrated and integrated online. On the one hand, the "People's Court Online Service" platform covering the four levels of courts has been developed and used, including online services for all aspects of the judiciary and the whole process, such as case filing, court hearings, service, and enforcement, so that ordinary people can handle actual litigation affairs in the whole process and around the clock. On the other hand, an online pluralistic dispute resolution system that breaks down information barriers at the departmental, regional and hierarchical levels has been constructed, including people's mediation, industry professional mediation, administrative mediation, judicial mediation and other dispute resolution forces have settled in the platform to provide menu-based, intensive and one-stop online dispute resolution services for the people.

The digital court provides a new working model for judicial workers that is efficient, convenient, and online collaborative. The first is to implement the whole process of online case handling based on

ISSN 2616-7433 Vol. 6, Issue 7: 1-5, DOI: 10.25236/FSST.2024.060701

electronic files. Since 2016, the Supreme People's Court has comprehensively promoted the simultaneous generation and in-depth application of people's courts' electronic files with cases, and guided courts at all levels to produce electronic files along with cases. Judicial workers carry out various tasks such as reading the case file, collegiate deliberation, adjudication, and enforcement on the basis of electronic files, increasing the efficiency of judicial work and facilitating the connection of judicial work. The second is to build a multi-service online collaboration system based on information sharing. With the support of the online platform and online system, various departments within the court, the court and the public security and other external units have realized data sharing and business collaboration, and built an overall intelligent governance, efficient and collaborative work model.

2. Highlights of the Construction of Digital Courts

The ultimate goal of digital court construction is digital empowerment, and the two major prerequisites and foundations to achieve this purpose are platform integration and paperless transformation, which are also the outstanding achievements and highlights of the current digital court construction.

2.1. Platform-based integration

The construction of digital courts adheres to the integration of platforms as the basis for digital applications, accelerates the creation of an integrated case-handling office platform that is connected up and down and horizontally, and opens up data channels for all court service matters, all handling processes, and all case-handling elements. The construction of the digital platform base is the primary task of the construction of the digital court, and the integration of the platform runs through the entire process of the construction of the digital court. The first is to integrate the original online platforms and business systems in the judicial system, and build a unified national integrated court case-handling office platform. If online platforms and business systems are not integrated, they may cause problems such as application duplication, system fragmentation, and data incompatibility, hindering data sharing and departmental collaboration, and affecting the efficiency of judicial work and litigation services. The second is to optimize the existing platform to meet the new development needs under the construction of digital courts. Expand the data capacity and types of existing platforms, and provide guarantees for the judicial digital platform to continuously gather various data resources and integrate multi-source and polymorphic judicial big data. The third is to build a new platform-based application to meet the increasing practical needs of judicial intelligent services under the construction of digital courts. With the continuous advancement of the construction of digital courts, courts around the country continue to develop new digital applications according to actual needs, providing more diversified, smarter and more comprehensive services for judicial workers and the people.

2.2. Paperless Transformation

Relying on the integrated case-handling office platform, the construction of digital courts has comprehensively implemented paperless reform in case filing, trial, enforcement, archiving and other links, forming a full-process paperless case-handling mechanism[1], and realizing the full-process "online litigation" case-handling model. First, judicial workers have handled cases paperlessly, realizing the transformation of the traditional mode of handling cases based on paper files to a new model of handling cases based on electronic files. The relevant materials, handling process and results of dispute cases are recorded in the online system through the platform, which is convenient for judicial workers to find, store, handle and hand over, and is also conducive to the formation of supervision of judicial workers, promoting judicial openness and transparency, and ensuring judicial fairness. Second, the subject of the dispute participates in the case online. Dispute subjects may submit case materials online through the platform, and participate in judicial activities such as mediation and trial online. Online participation breaks the time and space limitations in the traditional litigation mode, and the parties can participate in litigation activities at different times, in different places, and not synchronously, effectively solving the litigation inconvenience caused by "time difference" and "difficulty in different places", so that the temperature of justice for the people can reach the hearts of the people and the speed of judicial justice can be accelerated.

ISSN 2616-7433 Vol. 6, Issue 7: 1-5, DOI: 10.25236/FSST.2024.060701

3. Network Information Security Risks in the Construction of Digital Courts

The construction of digital courts is based on "paperless" and "platform", that is, offline work is transformed into online, and the whole process and stages of litigation are networked and visualized, which is important for judicial staff and litigation participation While people bring great convenience, it also raises the risk of network information security in judicial activities, especially the risk of information leakage and illegal intrusion.

3.1. Information Leakage

There is a risk of leakage in the collection, storage, utilization, and disclosure of judicial data. First, in the course of office and case handling, judicial workers leak judicial information due to improper operation or management. Whether it is an Internet court, a shared court, a mobile micro-court, or an online dispute multi-mediation platform, various digital applications and intelligent systems that have emerged in the wave of digital court reform are all in the online environment, and judicial personnel may be leaked in the process of collecting and processing judicial cases in the online environment. For example, improper use of communication apps at work, even the transmission of files, and the improper access of mobile devices to the intranet are all causes of judicial data leakage. In addition, judicial personnel are still deficient in the application of digital technology, and when online systems encounter external cyber attacks, they may not be properly handled or defended in a timely manner, which will also increase the risk of information leakage. Second, the outsourcing management party illegally processes and leaks judicial information driven by profits. Due to the lack of digital technology talents within the courts and the lack of professionalism of the court's big data technology, courts at all levels across the country are relying on outsourcing technology companies to provide intelligent data and information services to varying degrees in the process of building smart courts and developing online litigation, and all kinds of digital platforms are basically outsourced by the courts to third-party companies for construction and management. Although this public-private partnership model in judicial technology innovation is necessary for the digital reform of the courts at this stage, it should be noted that companies are profit-making and profit-driven, and third-party platform companies and their staff are likely to illegally operate personal information or other data during technical processing[2], thus increasing the risk of third parties leaking or illegally processing online judicial information.

3.2. Unlawful Trespass

Materials stored in the form of data on the court's digital applications or systems are in a state of being easy to attack and difficult to defend[3]—they are easily intercepted, tampered with, or invaded by viruses during static storage or dynamic transmission, causing network information security risks. In the construction of digital courts, the network system is roughly divided into three network domains: intranet, extranet, and private network, and such a complex application network environment is vulnerable to attacks and damage by hidden, sudden, and easily ignored hacker viruses. The main function of the private network is to maintain the information communication of various units, and it is easy to be attacked by the terminal system in the process of transmission and communication; As a public service layer, the extranet is open to the public and is vulnerable to data crawling attacks by crawler software. Although the content of the core data layer is relatively tightly protected, it is also easy to be transmitted and spread by mobile devices such as USB flash drives. In the process of switching to online litigation, all kinds of information that should have been submitted and recorded by offline entities are now operated online, and this information involves the personal information and privacy of litigation participants, and illegal external intrusion has caused judicial data leakage, which greatly harms the rights and interests of personal information and privacy. In addition to personal information and privacy, some of the information on the court's digital applications or systems also involves trade secrets and state secrets, and if such information is illegally crawled, stored, analyzed, and predicted, it will even cause great hidden dangers to national security[4]. With the continuous advancement of the construction of digital courts, the relevant network protection system is also constantly improving, but the risk of illegal intrusion of the system still exists, and the attack of related viruses should not be underestimated.

4. Network Information Security Maintenance in the Construction of Digital Courts

The network information security problems faced by digital courts are mainly concentrated in platform-based integration and paperless application scenarios, and the above-mentioned scenarios

ISSN 2616-7433 Vol. 6, Issue 7: 1-5, DOI: 10.25236/FSST.2024.060701

mainly involve the three parties of the case-handling office, litigation participants, and outsourcing managers.

4.1. Internal Release Leakage

In terms of internal leakage prevention, it is a primary task to improve the awareness of network information security and the ability to protect network information security among case-handling offices, outsourcing managers, and litigation participants[5]. The maintenance of network information security in the digital construction of courts is not only the responsibility of the court's informatization department, but also the full participation of case-handling offices, outsourcing managers, and litigation participants. Whether it is the case-handling office, the outsourcing manager, or the litigation participants themselves, they should strengthen their awareness of network information security protection and improve their ability to protect network information security.

First, the courts, as the leaders of judicial digitalization, should put forward overall requirements or provide relevant guidance to the cybersecurity awareness of the tripartite personnel. Courts shall conduct publicity and education on network information security awareness for case-handling offices, such as prohibiting arbitrary switching between internal and external networks, and inviting professional and technical personnel to conduct relevant skills training for judicial workers, emphasizing the cultivation of judicial compound talents; The ability to protect network information security should be taken into consideration when selecting technical cooperation third parties, and the third-party technology cooperation companies should be required to conduct network information security protection training for their employees on a regular basis; Methods such as prompt interfaces, oral education, and case publicity shall be used to raise litigation participants' security awareness during the use of court digital applications, and to convey basic cybersecurity experiences, such as prohibiting the download and use of pirated application software, and prohibiting arbitrarily clicking on unknown SMS links. Second, the third party of technical cooperation or the outsourcing manager should implement network information security awareness training for internal employees, requiring them to have the ability to detect network insecurity factors and identify sources of danger at any time, such as screening the authenticity of information sources, phishing websites, etc., and supervise the personnel involved in the construction or operation and maintenance of the court's digital platform, requiring them to base themselves on the goal of information processing when managing information, and must not arbitrarily change the original data they control and the processed result information, and ensure the accuracy and completeness of the data. Third, litigation participants should improve their own security awareness, enhance their ability to prevent and distinguish illegal information crawling and other behaviors, and at the same time take the initiative to supervise the behavior of bankruptcy network information security, and promptly give feedback to the relevant responsible institutions.

4.2. External Defense against Intrusion

In terms of external intrusion, two major measures can be taken: legal and technical. Clarify the limits on the collection and use of information in the digital court system from the legal level, and set up corresponding punishment mechanisms for illegal information crawling and other behaviors. Both the Civil Code and the Personal Information Protection Law stipulate that the collection and use of personal information shall follow the principle of necessity limitation, and require that personal information processors must strictly limit the collection and use of personal information to the scope and limits necessary for the target. On the one hand, this provides a basis for the requirements for the limit of information collected by the digital court, and delineates the scope of information that needs to be collected within the "scope and limit necessary for the performance of statutory duties", so as to avoid the excessive collection of information by the digital court and the damage to the rights and interests of the information subject. On the other hand, it can effectively prevent internal and external illegal information crawling behaviors by screening out abnormal behaviors of excessive collection and use of information. In addition, it is necessary to clarify the legal responsibility for information leakage and the punishment mechanism for information intrusion. For example, the Data Security Law stipulates that data processors shall strengthen risk monitoring, conduct regular risk assessments, promptly address data security issues, and fulfill corresponding reporting obligations when carrying out data activities. The tort liability of network users and network service providers stipulated in the Civil Code also provides a basis for the application of legal liability for information intrusion in the process of building digital courts. Of course, in addition to civil liability, the construction of digital courts is a public and government act, and the corresponding administrative liability and even criminal liability should be pursued for illegal acts

ISSN 2616-7433 Vol. 6, Issue 7: 1-5, DOI: 10.25236/FSST.2024.060701

such as information intrusion, so as to achieve the effect of deterrence and punishment after the event for illegal information intruders.

From a technical level, measures such as anonymization, data encryption, and setting retention periods can be taken. The use of digital technology by the court and its trustee platform to perform data security protection duties is crucial to the construction of a digital court information security protection system[6]. When the court collects information through digital applications, it may use data desensitization technology to anonymize personal information, delete or blur symbols that can directly identify a natural person, so as to block the inevitable connection between personal information and a specific natural person[7]; At the same time, encryption algorithms are used to convert personal information into ciphertext, and only authorized users can decrypt and access the data. When maintaining information in digital applications, the case-handling office entity and the outsourced management party rely on computer technology to promptly install and maintain secure systems and applications, and fix known security vulnerabilities; Adopt a data backup and recovery mechanism, regularly back up personal information, and establish a reliable data recovery mechanism to prevent data loss or tampering.

5. Conclusions

The construction of digital courts relies on online platforms and online systems to provide more efficient, intelligent and accurate judicial services, better meet the people's needs for fairness and justice, and promote the high-quality development of judicial work and the development of Chinese-style modernization. The information involved in the judicial system is not only related to citizens' personal privacy and personal information rights and interests, but also related to corporate trade secrets and even national security, and digital courts in the online environment are facing great cyber information security risks. The construction of digital courts must make the maintenance of network information security a top priority, improve laws and regulations, optimize the application of technology, weave a tight information security protection network, and strictly abide by the red line of network information security.

Acknowledgements

Science and technology plan project of Zhejiang Provincial Department of Education "Research on the Reform of ‘Zhejiang Regional Digital Court’ " (Y202249411)

References

[1] Li Zhanguo. Designing and Realizing Comprehensive Digital Court[J]. Peking University Law Journal, 2022, 34(01): 5-24.
[2] Hou Meng. The Impact of Internet Technology on the Judiciary: A Case Study of Hangzhou Internet Court[J]. Journal of Law Application, 2018(01): 52-57.
[3] Chen Yuefeng. Cooperative Governance of Critical Information Infrastructure Protection[J]. Chinese Journal of Law, 2018, 40(06): 175-193.
[4] Liu Youhua, Zhu Lei. The Risks and Prevention of Online Live Broadcast of Court Trial in the Big Data Era[J]. Law Science Magazine, 2020, 41(12): 18-31.
[5] Deng Heng, Yang Xue. Research on Information and Data Security in Online Trial[J]. China Journal of Applied Jurisprudence, 2021(01): 20-34.
[6] Zhang Suhua, Wang Nian. Data Security Issues and Legal Regulation in Online Litigation[J]. Science Technology and Law Chinese-English Version, 2022(04): 46-53.
[7] Liu Yanhong. Research on Rules for Compliance Processing of Personal Information in Smart Court Applications [J]. Legal Forum, 2022, 37(06): 38-50.