Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33279

The "Digital Divide" in Criminal Defense and Its Bridging

Yuheng Zheng

School of Foreign Languages, Zhongnan University of Economics and Law, Wuhan, China
1273917368@qq.com

Abstract. The integration of digital technology into the judiciary, while enhancing the efficiency and quality of case handling, also exacerbates the inequality between the prosecution and defense in terms of information access, technical capabilities, and procedural participation in the digitalization of the judiciary, giving rise to the "digital divide" in the field of criminal defense. It is manifested as the technical resource gap, the digital competence and literacy gap, and the procedural participation gap. Overall, the emergence of the "digital divide" is mainly due to the imbalance in the allocation of judicial information, the differences in the quality and ability of defense lawyers, and the structural disadvantage of defense parties in terms of procedures. To address this, efforts should be made to alleviate the imbalance in the prosecutorial relationship, enhance the substantive level of defense participation, and ensure fairness and justice in criminal justice by improving digital evidence rules and information disclosure mechanisms, perfecting the support system for lawyers' digital capabilities, and reconstructing procedural guarantee mechanisms in the context of judicial digitalization.

Keywords: Criminal defense, Digital divide, Data dumping, Procedural justice

1. Introduction

In recent years, the widespread application of digital technologies has greatly enhanced the efficiency of investigation and justice. However, the gap in access to digital materials and application technology between the prosecution and the defense has further exacerbated the information asymmetry in criminal proceedings, giving rise to the "digital divide" in the field of criminal defense. In the case of Shi's cyber theft, the prosecution confirmed that the defendant had committed the crime through technical means such as in-depth analysis of logs, underlying data and network connection traces, and convicted and sentenced him [1]. The application of digital technology has significantly enhanced the efficiency of case investigation and the accuracy of conviction. However, in this highly technological and data-intensive case-handling model, the prosecution has a significant technological advantage, while the defense often has to respond passively. This reflects the growing "digital divide" in the field of criminal defense, which is typically characterized by the prosecution taking the lead in fact-finding and data processing of evidence by leveraging its technological superiority, while the defense is at a disadvantage. If left unchecked for a long time, it will exacerbate the existing power asymmetry between prosecution and defense and undermine the defense right. Although the academic community has paid attention to

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.33279

the changes brought about by the integration of digital technology into criminal proceedings and has conducted research from the perspectives of electronic evidence rules and technological governance, exploring the application and rule restrictions of artificial intelligence in criminal proceedings, systematic research on the "digital divide" in the context of criminal proceedings is still insufficient and lacks an overall analysis [2]. It is necessary to further deepen and integrate on the basis of existing research.

Therefore, starting from practice, this paper analyzes the types, causes and countermeasures of the "digital divide" in criminal defense, aiming to provide references for alleviating the information asymmetry between the prosecution and the defense, bridging the "digital divide" in criminal defense, enhancing the substantive degree of defense participation, promoting the balance of power between the prosecution and the defense, in order to promote fairness and justice in the judiciary and safeguard human rights.

2. Definition and type analysis of the digital divide in criminal defense

2.1. Definition of the "digital divide" in criminal defense

In the 1990s, with the increasingly widespread use of the Internet, the digital divide became a general label or metaphor used to describe the gap in people's adoption and use of information dissemination technologies, especially the Internet [3]. In the context of criminal proceedings, the "digital divide" refers to the imbalance between the prosecution and the defense in terms of their rights status, resource allocation, technical understanding ability, and procedural participation rights in the process of handling evidence. This imbalance directly affects the operation of criminal defense and the exercise of the right to defense. In criminal proceedings characterized by the tripartite structure of prosecution, defense, and trial, the purpose of criminal defense is not merely to overthrow or weaken the alleged grounds. Facing an independent adjudicator, the ultimate destination of criminal defense is to persuade the adjudicator to accept or accommodate one's own defense opinion in the adjudicator's conclusion [4]. According to the provisions of the Criminal Procedure Law, lawyers can only access the case file after the case enters the review and prosecution stage, which leads to the natural lag of the defense and reduces the space for lawyers' participation. At the same time, although digital evidence has been widely used, the existing procedures are not well-regulated in terms of relevance, completeness and legality, which causes the emergence of the "digital divide" between the prosecution and the defense.

2.2. Types and characteristics of the "digital divide" in the criminal field

In criminal practice, the "digital divide" is manifested in the following three types.

First, the technological resource divide. The main feature of the technology resource gap is the high concentration of technology resources. The technical resource gap refers to the situation in criminal defense where public security and judicial authorities generally have more complete technical, talent and tool support, which can easily achieve deep data mining and automatic analysis to discover information favorable to the charges, while defense lawyers often have to rely on limited copy evidence and public information.

Second, digital literacy gap. The digital literacy gap is characterized by an imbalance in the ability to process technical evidence. The digital literacy gap is mainly manifested in criminal defense lawyers, who, due to reasons such as income status, the cycle of defense work, personal information literacy and professional competence, have difficulty handling highly technical

DOI: 10.54254/2753-7048/2026.33279

evidence on their own and can only turn to third-party institutions or commercial software. The asymmetry of technical knowledge ultimately leads to the defense's poor cross-examination results and the difficulty in effectively questioning the prosecution's technical proof, resulting in the emergence of the digital competence literacy gap.

Third, procedural participation gap. The main feature of the procedural participation gap is the limited participation of defenders. The procedural participation gap is characterized by procedural constraints that defense attorneys receive in the process of evidence formation and review. Despite the statutory provisions in Article 38 of the Criminal Procedure Law that define lawyers' litigation rights during the investigation stage, the practical enforcement of these rights, particularly the collection of evidence, faces significant hurdles. Whether it is meeting criminal suspects or seeking the cooperation of witnesses, it requires the assistance of courts and procuratorates. When confronted with highly technical evidence, defense lawyers often find it difficult to pose substantive challenges. In practice, there can also be cases where the prosecution uses "data dumping" to shorten the defense's preparation time. If the prosecution submits it in a concentrated manner without sorting, it will make it difficult for both the defense and the adjudicator to complete the effective review within the limited time.

2.3. The natural lag of the defense in the "digital divide"

In judicial practice, the "digital divide" is manifested in the following aspects:

First, asymmetry in the right to know all evidence. Defense attorneys often only have access to copies of the data provided by the prosecution and collated analysis results, and are constrained by the insufficient publication of judgments and the non-disclosure of judicial data, unable to verify the completeness and legality of the evidence from the source. Incomplete access to information directly weakens lawyers' ability to distill judgments, and the information barriers created further exacerbate the defense dilemma of lawyers and the imbalance of power in the prosecutorial relationship.

Second, the defense's pledge rights are weakened. Unlike traditional physical or documentary evidence, the probative value of technical evidence, such as electronic data, depends heavily on how it is obtained and the tools used. Current judicial review lacks clear standards, often focusing on authenticity while neglecting legality, relevance, and the evidence formation process. Moreover, elements like server logs and algorithmic logic exceed the scope of traditional legal training.

Third, limitations in the Effectiveness of Cross-Examination by the Defense. Under the influence of digitization in judicial practice, barriers such as technological and resource disparities exacerbate the power imbalance between the prosecution and the defense, further marginalizing the position of criminal defense attorneys. Simultaneously, due to technological reliance, some judges have developed a cognitive bias encapsulated by the notion that "if it is scientific, it must be infallible" [5]. when evaluating big data evidence. This fallacy leads to an erroneous perception of technology as possessing absolute neutrality, prompting a preference for technical standards over legal criteria. Consequently, there is an uncritical acceptance of professional judgments provided by technology controllers, which may restrict the efficacy of cross-examination and ultimately compromise judicial outcomes.

3. The real predicament of criminal defense in the context of the "digital divide"

The extensive application of information technology in criminal justice has profoundly changed the way criminal proceedings operate. While digital technology has improved the efficiency of case handling, it has also disrupted the original balance between the prosecution and the defense.

DOI: 10.54254/2753-7048/2026.33279

Criminal defense faces a series of practical predicaments in the context of the "digital divide" due to insufficient protection of the defense in institutional design and practical operation, mainly manifested as insufficient acquisition of case information by the defense and unequal defense preparation, insufficient digital literacy of the defense and serious external dependence on information processing technology, as well as limited procedural participation and structural weakness of the defense.

3.1. Inadequate access to case information by the defense and unequal defense preparation

In the context of the digitization of criminal justice, the scope of evidence materials involved in criminal defense has long gone beyond traditional forms and expanded to aspects such as information data processing. Under the "data gap", the first predicament of criminal defense is manifested as lawyers' inadequate access to case information and the imbalance in defense preparation with the prosecution.

Article 37 of the Criminal Procedure Law stipulates that the duties of defenders are to present materials and opinions favorable to the suspect based on the law and facts, and to safeguard their litigation rights and other legitimate interests. To assist defenders in fulfilling this duty, the law grants defense attorneys the right to collect evidence and to review case files. But in practice, defense attorneys are generally at a disadvantage in obtaining case information. First of all, in terms of evidence collection, since Article 40 of the Constitutional provisions strictly limit the authority to inspect communications to public security and procuratorial organs, and only in pursuit of legitimate state security or criminal justice objectives. This limits defense attorneys' access to electronic data. In the future, when it comes to obtaining evidence of electronic data, defense attorneys may have to rely on applying to relevant authorities to do it on their behalf, subject to the time of application and the certification of judicial authorities. In addition, with the development of judicial digitalization, criminal defense lawyers have also been restricted in the exercise of their right to access case files. For example, in 2019, the Supreme People's Procuratorate's "Rules of Criminal Procedure of the People's Procuratorate" listed "involving state secrets or business secrets" as one of the circumstances where access to case files is not permitted. The defense's right to review case files is subject to multiple restrictions at the institutional level, including state secrets, business secrets and personal privacy.

On the other hand, in criminal proceedings, the numerous data places higher demands on the technology of digital review. In this case, the prosecution has more technical talent and more complete technical capabilities, while the defense often lacks the corresponding tools to assist. Within the limited defense time, defense attorneys have to complete the analysis of complex information. This creates an imbalance in preparation between the prosecution and the defense.

3.2. There is a serious imbalance in the information technology capabilities between the prosecution and the defense

In the context of the "digital divide", there is a huge gap between the prosecution and the defense in terms of technological cognition, the ability to use technological tools, and the ability to integrate resources. In smart justice, the prosecution, relying on public power institutions, can smoothly cross the digital technology threshold by setting up specialized agencies, recruiting professional talents, and adopting "outsourcing of judicial auxiliary functions" to obtain technical support from technology enterprises.With more abundant resources, more complete technical capabilities, and more comprehensive talent reserves, the prosecution can handle relevant data efficiently throughout

DOI: 10.54254/2753-7048/2026.33279

the pre-trial phases, encompassing investigation and prosecutorial review. For example, in Shi's theft case, the prosecution used forensic software to track the IP of the victimized company and the traces of illegal recharges, providing precise data for the accusation and giving it a clear advantage in the progress of the case.

In contrast, the defense was clearly lacking in technical capabilities. First of all, in terms of innate ability development, defense lawyers often lack professional technical background, and when confronted with technical evidence such as cyberattack logs, encrypted data, or algorithmic analysis reports, they generally lack the corresponding knowledge and ability to contend with fully staffed public authorities. Secondly, in terms of tool assistance, compared with the prosecution backed by the national network database, when dealing with massive amounts of data, the defense often has limited tools and resources available and can only rely on general software and third-party institutions, or handle it through traditional manual methods. At the same time, since the current rule construction for electronic data evidence is mainly from the perspective of identifying guilt, especially in the context where big data is closely related to judicial proof, there are no clear norms or guidelines on how to identify evidence in favor of the defense in the vast amount of data and from which angles the prosecution's electronic data evidence can be effectively cross-examined, making it difficult for the defense to identify evidence of innocence [6].Let alone cross-examination of electronic evidence. In such cases, it is difficult for the defense to present a valid cross-examination of highly technical evidence.

3.3. Structural weakness limits the defense's procedural participation

Under the "digital divide", the defense is subject to multiple constraints in the criminal defense of digital criminal cases, resulting in the defense being structurally vulnerable in the investigation, review and prosecution, and trial stages.

First, during the investigation stage of the case, because the defense is unable to participate in the investigation of the case by state organs, it is usually impossible to simultaneously participate in the acquisition and analysis of relevant data. The formation and collection of evidence are dominated by the prosecution, making it difficult for the defense to obtain raw data and limiting the possibility of objecting to technical evidence. In some cases, if the public security, procuratorial and judicial organs present a large amount of relevant data during the trial and shorten the time for defense lawyers to prepare for the trial, it will also leave them struggling to deal with it and weaken the effect of cross-examination. Secondly, during the trial stage, the defense has limited opportunities to cross-examine technical evidence. Because the defense has difficulty obtaining the original data related to the case and is unable to question the authenticity of technical evidence, technical evidence becomes an unshakable "black box". At the same time, due to the prosecution's incomplete disclosure of judgments and technical reports, the defense has limited opportunities to cross-examine underlying data, log analysis, and algorithmic logic, especially for artificial intelligence evidence, whose "machine generation" and "unexplicability of conclusions" have made traditional cross-examination methods almost ineffective [7]. The defense was unable to directly challenge the logic of the algorithm as it would question human experts, nor could it touch upon core reliability issues such as data bias and model flaws. This state further compresses the defense's procedural involvement space, putting it at a structural disadvantage throughout the criminal proceedings.

DOI: 10.54254/2753-7048/2026.33279

4. Analysis of the causes of the digital divide in criminal defense

The emergence of the "digital divide" in criminal defense is not caused by a single factor, but is the result of the interwoven effects of multiple factors such as institutional design, subject capacity and procedural structure. In order to ensure fairness and justice in criminal proceedings through judicial digitalization, it is necessary to analyze the causes of the "digital divide" in criminal proceedings from the institutional, subject and procedural levels.

4.1. Institutional level: imbalance in the allocation of judicial information

The formation of the "digital divide" in criminal defense is closely related to the imbalance in the allocation of judicial information. From the perspective of judicial practice, the current form of judicial digitalization is still aimed at improving the efficiency of prosecution by judicial organs and the capacity of social governance, with insufficient attention paid to the participation rights of defenders.

Firstly, when criminal judicial authorities independently promote the integrated construction of big data through administrative decision-making, they will inevitably collect a large amount of data oriented towards the needs of performing their duties, neglecting the effective sharing of data resources [8]. Whether it is big data or artificial intelligence technology, the purpose of incorporating it into judicial cases is to improve the efficiency of case handling and the ability to control cases of state organs. Defense lawyers' participation in these technologies is limited. This institutional arrangement has led to a high concentration of control and interpretation of case information on the prosecution, intensifying the data barrier between the prosecution and the defense, and is one of the major causes of the "digital divide".

Secondly, the current system's regulation of judicial information disclosure is relatively lagging behind, presenting a pattern where the rules lag behind the practical demands, which restricts the operation of the criminal defense system [9]. Although Article 40 of the Criminal Procedure Law ensures defenders' right to access case files, it mainly targets traditional forms of evidence and the scope is too narrow to fulfill the needs. At the same time, defenders often can only obtain the results of technical processing during the trial stage and have difficulty obtaining the relevant original data. In such cases, the defense's access to judicial information is heavily dependent on the prosecution's proactive disclosure.

In addition, there are structural differences in the resources invested by the prosecution and the defense in the allocation of judicial information. As the state promotes the construction of smart justice, various technical resources and professional talents are continuously being invested in public authorities. Defense lawyers, on the other hand, mainly rely on third parties such as software and law firms for technical support, lacking stable institutional guarantees and having a gap with the digital capabilities of the prosecution.

Therefore, from an institutional perspective, the "digital divide" in criminal defense is not accidental but an inevitable result of the long-term bias of judicial information allocation towards the prosecution.

4.2. Subject level: differences in the quality and competence of defense lawyers

The formation of the "digital divide" in criminal defense is also related to the differences in digital literacy and professional competence among defense lawyers.

DOI: 10.54254/2753-7048/2026.33279

First of all, judicial digitalization places higher demands on defense lawyers. Defense lawyers need not only traditional legal interpretation and argumentation skills, but also an understanding of digital technology. However, the existing legal professional training system is still centered on traditional substantive and procedural legal knowledge, with insufficient cultivation of digital capabilities. This leaves some defense attorneys at a loss in the face of technical evidence.

Secondly, there is also a significant disparity in digital capabilities within the group of defense attorneys. In judicial practice, the relevant data is often numerous and diverse, requiring specialized tools and technical teams to handle. Large law firms can fill the technical gaps by introducing technical teams or external technicians. But for ordinary defense attorneys, there is a widespread lack of such tools and team support, making the inability to handle data a norm.

It also needs to be emphasized that the differences in subject capabilities are not merely individual issues but are closely related to the lack of institutional support. In the absence of systematic training and institutional support, the improvement of individual capabilities is difficult to make up for the huge gap in institutions.

4.3. Procedural level: defense at a structural disadvantage

From the perspective of procedural structure, the pattern of criminal proceedings itself presents a basic pattern where the prosecution takes the lead and the defense responds passively. Among the prosecution, defense and trial in criminal proceedings, the prosecution and the trial both represent the state, while the defense is an individual; The defense, as an individual, has an "inherent deficiency" compared to the prosecution, which represents the state, in the prosecutorial relationship [10]. The involvement of digital technology has, to some extent, strengthened this feature.

First, the initiation of criminal proceedings begins with state organs. In both traditional and digital contexts, the discovery of case leads, the collection of evidence, and the initial construction of case facts are all led by the prosecution. This allows the prosecution to integrate information and form case judgments earlier, and the defense can only intervene after the facts of the case have basically taken shape, putting it at a procedural disadvantage from the very beginning.

Secondly, the procedural weakness further amplifies its disadvantage in digital technology by restricting the defense's participation. The defense lawyer's own limited right to participate in the investigation is limited, and a large amount of processing activities in digital case handling take place before the trial, and the difficulty in obtaining raw data makes it difficult for the defense to intervene in a timely manner. At the same time, in judicial practice, in many cases, lawyers need the help of government agencies to obtain the assistance of witnesses. Such procedural rules have restricted defenders' right to defend in the process of judicial digitalization.

From the perspective of procedural justice, the fairness of the process should not only be reflected in the outcome, but also in the sufficiency and equality of the participation of all parties. When the "inherent disadvantage" of the defense in terms of procedure is magnified in the process of judicial digitalization, the "digital divide" in criminal defense emerges.

5. Ways to bridge the digital divide in criminal defense

In the context where digital technology is deeply embedded in the operation of criminal justice, the "digital divide" in criminal defense is no longer merely a technical issue, but an important topic related to the protection of the right to defense, the realization of procedural justice and the credibility of the judiciary. Therefore, in order to bridge the "digital divide" in criminal defense, efforts must be made in terms of systems, subjects and procedures.

DOI: 10.54254/2753-7048/2026.33279

5.1. Improve the relevant rules for safeguarding the right to defense

The first way to bridge the "digital divide" in criminal defense is to improve relevant laws and regulations and strengthen the participation rights of lawyers. The right to participate is guaranteed through institutional rules, and lawyers' right to defend is better exerted.

First, it is necessary to clarify the right of defense lawyers to be informed of digital case information. In the current litigation system, defense lawyers' access to case files is mainly centered around traditional case files, with insufficient attention paid to digital evidence. To guarantee the right of lawyers to be informed, it is necessary to refine the necessary information in digital case handling through legislation or judicial interpretation to provide rule guidance for the exercise of the right to defense. Therefore, the right to data access can be introduced, granting the defendant access to the data that the prosecution holds about the defendant personally. A lawyer, as an agent, can exercise this right on behalf of the defendant, including both favorable and unfavorable parts to the suspect, to prevent key case information from being excluded from the exercise of the right of defense. In order to control the risks of algorithms and regulate the use of information technology in criminal proceedings, rules for the cross-participation of algorithms should be established and improved. For database algorithm comparisons based on massive data, it is advisable to adopt evidence methods such as presentation in court and cross-examination by the defense, and for big data analysis based on algorithm models, it is advisable to adopt methods such as special examination assistance to provide examination opinions and cross-examination in court [11]. This ensures the reliability of the technical algorithms used by the investigation authorities. At the same time, a substantive confrontation and review mechanism for technical evidence, especially artificial intelligence evidence, must be established, and the collection and review of artificial intelligence evidence should be incorporated into the rules[2] of "technical due process".

Secondly, the obligation of state organs to assist should be strengthened. In criminal proceedings, the defense needs to be respected by state organs if it wants to exercise its right to defense smoothly. Given that the prosecution has more complete litigation resources, in order to make up for the imbalance, the state authorities should undertake more obligations of assistance. If the defense lacks the corresponding technical equipment, the prosecution can provide the corresponding technical guidance and equipment support. In the opening procedure, the obligation of the prosecution to assist in identifying valid data should also be strengthened to prevent the prosecution from using "digital dumping" to shorten the trial preparation time. The prosecution can add key evidence labels to help the defense locate core evidence, thereby avoiding information overload, getting sufficient preparation time, and preventing "data dumping" from weakening the right to defense.

5.2. Improve the digital skills training mechanism for criminal defense lawyers

While improving the system and rules, bridging the "digital divide" in criminal defense also requires enhancing the digital capabilities and digital literacy of defense lawyers at the subject level, so that technology empowers rather than becomes an obstacleto defense. The exercise of the right to defense requires both institutional safeguards and individual lawyers' adaptation to judicial digitalization.

On the one hand, the development of digital capabilities should be incorporated into the professional training system for criminal defense lawyers. In the digital wave, defense lawyers will inevitably come into contact with and use various digital technologies in the course of participating in litigation. Lawyers should first be guided to break the conventional mindset and understand the impact of digital technology on the criminal justice litigation system [12]. Through the reform of the

DOI: 10.54254/2753-7048/2026.33279

lawyer training system, information technology fundamentals and other contents can be incorporated into the training system to help defense lawyers enhance their overall understanding of the digital case-handling model. But it should also be clear that the transformation of criminal defense models in the digital age should maintain the subjectiveposition of professional judgment of defense lawyers while adhering to the basic position of "person-main-auxiliary". Courses should be set up to warn of the risks of technology application and educate lawyers that when using technology tools, they must adhere to professional ethics and ensure that technology operates within the legal framework

On the other hand, state organs should develop forward-looking plans. It is necessary to reverse the current situation where defense lawyers rely on third parties to handle technical outcomes and change the imbalance between prosecution and defense. Bring in the support of state power and have the government take the lead in researching the construction of a big data platform for the legal profession. Bridge the digital competence gap for defense lawyers by providing public training resources through industry associations or judicial administrative authorities.

5.3. Reconstructing procedural safeguards in the context of intelligent justice

Bridging the "digital divide" in criminal defense requires a reconfiguration of procedural safeguards in the context of intelligent justice. Traditional procedural rules are difficult to respond to the power risks brought about by judicial digitalization, exacerbating the imbalance of power between the prosecution and the defense.

On the one hand, the early participation mechanism of the defense in the judicial process should be strengthened. In trial confrontations, many factual judgments are actually formed before the trial, especially with the development of judicial digitalization, digital technology has further moved forward the nodes of factual construction and evidence screening. Therefore, it is necessary to expand the space for defense lawyers to participate in the early stages of the case through procedural design to ensure the sufficiency and equality of litigation participation.

On the other hand, the constraints in digital procedures should be improved. There should be a clear and actionable path when lawyers raise objections to the results of technical treatments. By clarifying procedural rules such as application review and re-evaluation, the impact of possible algorithmic bias can be reduced, digital procedures can be prevented from becoming an unquestionable "black box", and the right of defense lawyers to cross-examine can be guaranteed.

6. Conclusion

With the widespread application of digital technology, the power structure of criminal proceedings is undergoing profound changes. While digital technology enhances judicial efficiency, it may also exacerbate the imbalance between the prosecution and the defense in terms of information access, technical literacy and procedural participation due to imperfect institutional design and arrangement. In light of the specific circumstances in judicial practice, it can be found that the formation of the "digital divide" is mainly manifested as insufficient access to case information, restricted rights to defense, and potential crises facing procedural justice. The reasons for its formation are the long-term bias of judicial information towards the prosecution, the differences in the digital capabilities of defense themes, and the further reinforcement of the bias of criminal proceedings themselves towards the prosecution in the digital context. Ultimately, digital technology should be a tool for promoting justice. The direction of digitalization of criminal justice should enable a positive interaction between technological progress and the protection of the right to defense and procedural

DOI: 10.54254/2753-7048/2026.33279

justice. Only in this way can a harmonious unity of criminal proceedings and the value of justice be achieved. In the future, with the deep coupling of information technology and criminal justice, more challenges will arise. Only by advancing technology and rights simultaneously can digital criminal justice enhance governance efficiency while ensuring the realization of procedural justice.

References

[1] Supreme People's Procuratorate. (2025) Typical Cases of Criminal Prosecution Technical Evidence Review Supported by Prosecutorial Technical Support. Retrieved from: https://www.spp.gov.cn/xwfbh/wsfbt/202509/t20250918_706818.shtml#2
[2] Xie, D. (2025) A Typological Analysis and Rule Construction of Artificial Intelligence Evidence. Study & Exploration, 3.
[3] Jin, J. (2003) A Conceptual Analysis of the Digital Divide. Journalism & Communication Research, 1, 75-79, 95.
[4] Zhang, Y. (2025) The Practical Dilemmas and Institutional Responses of Lawyer Defense from the Perspective of Digital Criminal Justice. Master's Thesis, Yantai University.
[5] Li, Z. (2025) Research on the Dilemmas and Countermeasures of Effective Defense for Lawyers under the Background of Big Data [in Chinese]. Master's Thesis, Hunan Institute of Science and Technology.
[6] Pei, W. (2020) On Digital Criminal Defense: From the Perspective of Effective Defense. Research on the Modernization of the Rule of Law, 4, 124-142.
[7] Ma, G. (2023) Dual Risks in the Application of Artificial Intelligence Evidence and Their Regulation. Journal of Dalian University of Technology (Social Sciences), 4, 86-93.
[8] Qi, C. (2025) Practical Issues and Mechanism Construction of Integrated Big Data in Criminal Justice. Legal Forum, 4, 150-161.
[9] Zheng, Xi (2025) Challenges and Responses of the Criminal Defense System in the Digital Era. China Law Review, 5, 141-154.
[10] Han, D. (2023) Research on the Relationship among Prosecution, Defense and Trial under the Leniency System for Guilty Pleas and Punishments. PhD Dissertation, East China University of Political Science and Law.
[11] Lin, X. (2021) A Preliminary Study on the Application of Big Data Evidence in Criminal Justice. Legal Forum, 3, 27-36.
[12] Chen, W. and Han, Y. (2025) On the Digital Transformation of Criminal Defense. Digital Rule of Law, 6, 1-16.