The Predicament and Way Out for Realizing Lawyers' Defense Rights in the Era of Big Data: A Perspective on the Prosecution-Defense Relationship

Yuzhen Guo[1]

[1]School of Law, China University of Political Science and Law, Beijing, China.

Email: howcaniseeyou@163.com

Abstract: In the big data era, lawyers' defense rights face many challenges. As a key part of the judicial system, the criminal defense system is crucial for protecting the rights of the accused and ensuring procedural justice. However, in practice, lawyers' defense rights are often not well - protected. While technological progress has provided new support for the judiciary, it has also further compressed the defense space. Traditional problems like difficulties in accessing files, investigating, and cross - examining have taken on new forms in the big data era.

From the perspective of prosecution-defense relationship, this paper analyzes the impact of emerging technologies such as big data and artificial intelligence on the judicial field. It also explores the challenges to lawyers' defense rights in the big data era and proposes solutions. These include improving lawyers' investigation and evidence - collection rights, access - to - files rights, standardizing algorithmic applications, and increasing judicial data transparency. The aim is to ensure lawyers' defense rights and achieve equality between prosecution and defense.

Keywords: big data; defense rights; prosecution-defense relationship

Introduction

In recent years, riding on the waves of China's judicial reform, China's criminal defense system has advanced significantly, as seen in the improvement of the duty solicitor system and the pilot - testing and promotion of the criminal defense full - coverage initiative. But as these systems evolve, it's crucial to address the gaps between theory and practice. Lawyers are pivotal in implementing these systems and are indispensable in the defense mechanism. China's "Criminal Procedure Law" and "Lawyers Law" have codified lawyers' defense rights, such as meeting with clients, accessing files, and collecting evidence.

However, in practice, there are frequent incidents where lawyers' defense rights are not well - safeguarded. Defense lawyers often struggle to exercise their rights when meeting with parties, accessing files, and collecting evidence. These issues have given rise to the traditional "three difficulties" problems, which have become the main challenges for criminal defense lawyers during the defense process. [1]As a result, in the ideal equilateral triangle relationship structure of prosecution, defense, and adjudication, the defense and prosecution have shown a trend of one side rising as the other declines. Lawyers often find themselves in a passive and isolated position when facing public prosecution organs. The equal structure of the equilateral triangle has become a mirage and a symbolic representation, leading to practical distortions. This has also sparked widespread academic and social discussions on the issue of effective defense.

Technological progress has provided new technical support for criminal justice. The development of big data and artificial intelligence has brought new opportunities for the informatization of judicial organs. Lawyers, too, have used big data and artificial intelligence to improve their work, building case - law databases and intelligent auxiliary working platforms. Yet, as traditional criminal defense fields collide with emerging technologies, friction is inevitable. Since the 21st century, machine learning and big data have led a new wave of legal technology. [2]Against the backdrop of unaddressed prosecution - defense imbalance, judicial big data and legal artificial intelligence, backed by state public power and supported by fiscal and policy resources, have an inherent pro - public - power nature. Lawyers, however, lack the ability to allocate such resources. Public prosecution organs, as the prosecuting party, bolstered by technological means, have further compressed the defense space. On the one hand, lawyers can't join national - organ - based case - handling auxiliary systems, and the prosecution's monopoly on case - file information makes it harder for lawyers to access files.Algorithmic opacity in judicial systems creates a "black box effect," embedding biases that disproportionately disadvantage defendants and undermine procedural fairness.[3]Big data technology acts as a double-edged sword, enhancing judicial efficiency while exacerbating systemic inequalities, particularly in contexts where public authorities monopolize data resources and widen the prosecution-defense capability gap.[4] On the other hand, data - based information and strengthened data associativity make big data widen the prosecution - defense capability gap, both in data collection and analysis.[5] In summary, given the existing defense - rights dilemmas and lawyers' inherent weaknesses, we need to answer whether legal - technology use will aggravate prosecution - defense inequality and how to safeguard lawyers' defense rights

[1] Han, X. (2023). Where Lies the Path to Safeguarding Lawyers' Defense Rights?*China Reform*, 2023(5), 71–74.
[2] Wei, B. (2024). The Transformation of Legal Technology: From Computerization to Digitization and Intelligentization.*Jurists Review*, 2024(3), 16–29.
[3] O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, New York: Crown.
[4] Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think, Boston: Houghton Mifflin Harcourt.
[5] Pei, W. (2018). The Conflict Between Personal Information Big Data and Criminal Due Process and Its Reconciliation.*Chinese Journal of Law*, 2018(2), 42–61.

1. The theoretical basis

1.1 The requirement of the principle of equality between prosecution and defense

Before 1979, China's legal framework for prosecution, defense, and their relationship was nearly non - existent, except for general provisions on defendants' defense rights in the Constitution and the Organic Law of the People's Courts. The first Criminal Procedure Law in 1979 detailed defense rights in a separate chapter and clarified the rights of defenders and lawyers. Subsequent regulations, such as the Interim Regulations on Lawyers, gradually provided a legal basis for prosecution - defense relations. It is necessary to issue that The principle of "equality of arms" in criminal proceedings requires not only formal legal parity but also substantive access to resources, ensuring both prosecution and defense can effectively advocate their positions.[6]However, influenced by traditional concepts and an imperfect system, these relations remained seriously unbalanced.

The 1996 amendment to the Criminal Procedure Law strengthened the protection of the accused's rights, established legal aid, expanded lawyers' defense rights, and introduced an adversarial litigation model to promote equality between prosecution and defense. The Law on Lawyers, enacted in the same year, reduced the administrative nature of lawyers' roles, marking the beginning of a confrontation - dominated stage of prosecution - defense relations. This led to the "old three difficulties" problem, where communication and cooperation were lacking. The 2012 amendment further refined these relations towards rational confrontation. Despite the key role of the prosecution - defense confrontation mechanism in modern criminal litigation, it has also led to problems such as large - scale judicial resource consumption and reduced litigation efficiency. Faced with increasing numbers of criminal cases and tight judicial resources, scholars have advocated transforming prosecution - defense relations into a model combining confrontation and cooperation. This requires defense lawyers to actively perform their duties and the prosecution to adhere to its objective obligations and safeguard lawyers' litigation rights.[7]

Whether it involves prosecution - defense confrontation or cooperation, it must be based on equality between prosecution and defense. Otherwise, confrontation may turn into suppression, and cooperation may become exploitation. In modern criminal litigation, the principle of equality between prosecution and defense is one of the core concepts for ensuring judicial fairness. It requires both sides to have equal legal status, reciprocal litigation rights and obligations, and equal strength to ensure a balanced and cooperative relationship. This principle should apply not only in the trial stage but also throughout pre - trial procedures such as investigation and review for prosecution. The full exercise of lawyers' rights to meet with clients, access files, and collect evidence affects the protection of the accused's legitimate rights and the effectiveness of the defense.

The realization of this principle depends on the "equal arming" and "equal protection" of both sides. Equal arming means providing both sides with equal legal tools to ensure they can fully exercise their rights in litigation. Equal protection requires

---

6 Dworkin, R. (1986). Law’s Empire, Cambridge: Harvard University Press.
7 Zhang, B. (2020). On the manifestations, impacts, and corrective paths of the formalization of interactions between prosecution and defense. *Journal of Henan University (Social Science Edition)*, 2020(5), 70–75.

judges to remain objective and neutral, offering the same level of protection to both sides and giving equal attention and evaluation to the opinions and evidence provided by each. The theoretical basis of this principle includes the requirements of the criminal litigation structure, the theory of checks and balances, and the requirement of human rights protection.

In the adversarial criminal litigation system, the separation of prosecution, defense, and adjudication functions forms an equilateral triangle structure, which is essential for procedural justice. The equality between prosecution and defense reflects the theory of checks and balances in criminal litigation, preventing either side's power expansion and ensuring effective confrontation. It also aligns with human rights protection requirements, as the defendant's exercise of defense rights can effectively restrain and supervise the state's prosecutorial power, ensuring rational power exercise and the purposefulness of criminal litigation. Only on the basis of equality between prosecution and defense can both sides maintain a balance of power in confrontation and achieve mutually beneficial cooperation, jointly promoting the realization of fairness and efficiency in criminal litigation.

1.2 Requirements for building a legal profession community

The legal profession is a social organism. American legal scholar Roscoe Pound defined it as a group pursuing learned arts as a common calling in the spirit of public service.[8]Nowadays, with legal and commercial self - interest on the rise, some legal professionals lose ethical standards. Conflicts arise among judges, prosecutors, and lawyers, and the legal service market is in chaos. To solve these problems, it's vital to re - establish legal professionals' common faith in law and shared pursuit of social order and justice. This is key for the legal profession to fulfill its rule - of - law mission.If legal professionals work outside the common legal dispute - resolution system, using their own methods, languages, and logics, mistrust and blaming will emerge.[9]To build a legal profession community, it's necessary to both seek common ground and respect differences. On one hand, legal professionals share a common foundation: legal education, language, thinking, and courtroom practice. They all bear the responsibility of upholding social fairness, justice, and the accurate implementation of the law. On the other hand, each legal role has a unique positioning, with specific rights, obligations, values, and ethical standards. Every legal professional must fulfill relevant laws and adhere to ethical requirements.

In criminal proceedings, lawyers and procuratorates have natural conflicts due to their different duties. Lawyers defend suspects and defendants to protect their rights and ensure judicial fairness. Procuratorates, as the state's representatives, prosecute to protect public interests and ensure the law is correctly implemented. Despite these differences, both aim for social justice and should cooperate on an equal basis.To build a positive relationship between them and reduce conflicts, their equal status must be ensured. This paves the way for a legal profession community. Take the 1996 Criminal Procedure Law revision, which shifted court trials from an inquisitorial to an adversarial system. But defense lawyers didn't gain equal litigation status with prosecutors. Judges often dismissed their defense opinions with "not accepted".

---

[8] Pound, R. (1953). The Lawyer from Antiquity to Modern Times, St. Paul: West Publishing Co.
[9] Ge, H. Y. (2016). One Step Away: The Chinese Legal Profession Facing the Community. *Law Science*, 2016(5), 3–12.

Scholar Liu Sida calls this detachment from the public's daily life a "symbolic process".[10]

To prevent the building of a legal profession community from being just empty talk and only a "symbolic" idea, we must ensure positive interaction between lawyers and procuratorates in criminal proceedings. Only fully protecting lawyers' practice rights and respecting their status can gradually form the initial outline of this community.

2. The predicament in realizing lawyers' defense rights

2.1 Difficulty in collecting evidence

Article 43 of China's Criminal Procedure Law permits defense lawyers to collect case-related materials from witnesses and other entities or individuals with their consent, and to apply to the procuratorate or court to gather evidence or summon witnesses. However, in the face of the informatization and data-driven transformation of criminal proceedings, the right of lawyers to investigate and collect evidence is confronted with numerous challenges. On the one hand, the electronic and data-based case files enhance the efficiency of prosecution, but the accused and their lawyers struggle to access the case-handling auxiliary systems of public security, procuratorate, and court, and thus have difficulty in obtaining electronic data from these systems. At the same time, the construction of multi-departmental information-sharing systems involving administrative and judicial organs has broadened the channels for the prosecution to collect information, but the defense has difficulty in benefiting from these systems. [11]For instance, the procuratorate can extract relevant data, build digital models, and use big-data analysis to uncover case leads from bank accounts, financial records, and property or vehicle registration information.

Article 54 of China's Criminal Procedure Law stipulates that the People's Court, People's Procuratorate, and public security organs have the authority to collect evidence from relevant entities and individuals. Confidentiality is required for evidence involving state secrets, trade secrets, and personal privacy. Article 42(1) of the Cybersecurity Law prohibits network operators from disclosing, tampering with, or destroying personal information without the consent of the individuals from whom the information was collected, except when the information has been irreversibly anonymized. Article 14 of the Government Information Disclosure Regulation specifies that government information classified as state secrets, prohibited from disclosure by law or administrative regulations, or whose release could endanger national, public, economic, or social security, shall not be disclosed. When data crucial to proving the accused's innocence or minor guilt falls under these non-disclosure provisions, lawyers are unable to access it.

On the other hand, big data analysis can integrate fragmented data into a comprehensive dataset. Even if a lawyer only seeks part of the information during evidence collection, they may be denied access if these fragments can be used to derive sensitive data related to national security, trade secrets, or personal privacy

---

[10] Liu, S. D. (2008). *The Lost City-State: The Transformation of the Legal Profession in Contemporary China* (pp. 4-6), Beijing: Peking University Press.
[11] *Jia, Y. (2023). On Digital Procuratorial Work.China Legal Science, 2023(1), 5–24.*

through big data techniques. This significantly hinders lawyers' investigation rights.[12]

Moreover, with the growing emphasis on personal privacy, lawyers may be refused access to any fragmented data that could be linked to personal privacy during investigations, based on privacy protection grounds.

In contrast, Articles 13 of the 2016 Provisions of the Supreme People's Court, Supreme People's Procuratorate, and Ministry of Public Security on Several Issues Concerning the Collection, Extraction, and Review of Electronic Data in Handling Criminal Cases and Article 41 of the 2019 Ministry of Public Security Rules on Electronic Data Investigation in Criminal Cases stipulate that data holders, network service providers, and relevant departments must assist and cooperate with investigative authorities in collecting electronic data. In this context of judicial promotion of data sharing, public authorities can easily obtain data from third parties. However, defense lawyers lack communication channels and data - access mechanisms, making data acquisition subject to the data controller's willingness. Thus, there is a vast disparity in evidence - collection capabilities between public authorities and defense lawyers.

Furthermore, due to the rapid evolution of electronic data storage methods and technologies, defense lawyers specializing in law may encounter technical challenges. They often lack professional evidence - collection skills and equipment. For complex data, without hiring experts to preserve and replicate evidence, the evidence obtained may be deemed invalid by the court, or even be destroyed, which can affect case - fact determination and may lead to criminal liability. This exacerbates the difficulties lawyers face in evidence collection.

In summary, defense lawyers, especially when conducting their own investigations, face two main barriers in the evidence - collection process: technical barriers and barriers in obtaining assistance from third - party platforms. Hindered by these internal and external factors, they struggle to obtain evidence proving the accused's innocence or minor guilt.

2.2 Difficulty in accessing case files

Under traditional conditions, case - file materials in criminal cases exist in tangible forms such as text and images. With the widespread use of big data and other information technologies, the objects of case - file review have become intangible and numerous. This has impacted the traditional case - file review system and brought serious challenges to the scope and difficulty of lawyers' case - file review rights.

Article 40 of China's Criminal Procedure Law stipulates that defense lawyers may review,copy, and reproduce case - file materials from the time the People's Procuratorate begins reviewing the case for prosecution. Other defenders may also do so with the permission of the People's Court or People's Procuratorate. Traditional case - file review was limited to tangible evidence and related materials disclosed to the defense. However, in the era of big data and artificial intelligence, judicial informatization uses modern technologies such as electronic case files, online platforms, and databases. The materials judicial organs use in case trials no longer only include traditional case - file contents. The traditional scope of case - file review

[12] Li, X. M. (2020). Risks and Countermeasures of Big Data and Artificial Intelligence Intervening in Criminal Proceedings: From the Perspective of Equality Between Prosecution and Defense. *The South China Sea Law Journal*, 2020(3), 66–68.

is relatively narrow and cannot cover modern information carriers like electronic case files. In practice, there are also issues of one - sided evidence collection and deliberate concealment of innocence - related evidence. Due to the closed nature of the investigation stage, some key information derived from big data analysis is only regarded as case - solving clues and is not documented or reflected in case materials, making it inaccessible to defense lawyers. Additionally, whether the data related to big data - assisted investigation in the investigation stage constitutes a state secret and how to ensure data security during case - file review for the defense are issues not yet regulated by existing laws. Thus, in addition to the old problems of unclear case - file review scope and locations, lawyers now also face new problems such as a narrow scope of review and increased difficulty in accessing case files.

Currently, as criminal case numbers and data volumes surge, defense lawyers face two main challenges. On one hand, the massive data acts like an information ocean, making it tough for the defense to pinpoint key evidence favorable to the accused. They often get lost in the complexity, struggling to effectively mine and analyze data that's truly useful for defense. On the other hand, judicial authorities may dump large amounts of unfiltered, untargeted data on the defense. Given the prosecution's technical edge, there's a rising risk of them leveraging this to create a litigation advantage. This boosts the defense's workload and the difficulty of reviewing case files. Lawyers then spend excessive time and effort sifting through data, often without obtaining truly valuable information, which in turn affects the quality and efficiency of defense work.

2.3 Difficulty in effective cross - examination

Against the backdrop of big data and AI in criminal justice, the information gap between prosecution and defense during cross - examination is amplified by algorithms. This compresses the defense's cross - examination and defense space. Also, the lack of algorithmic cross - examination mechanisms and the use of sentencing - assistance systems worsen inequality in the cross - examination process.Automated judicial tools lacking transparency violate due process by denying defendants meaningful opportunities to challenge algorithmic decisions.[13]

On one hand, algorithmic opacity restricts the space for cross - examination and defense. In China's criminal justice practice, smart prosecution - assistance systems are established on big data and run via algorithms. [14]Algorithms play a key role in big data and AI. Under different algorithms, the same dataset can generate varying results. Yet algorithms are often opaque, creating an "algorithmic black box". While the input and output are visible, the processing in - between is partially or fully hidden.[15]Thus, when cross - examining algorithm - based evidence, lawyers can only address procedural legality. Algorithmic systems in justice must adhere to transparency, explainability, and human oversight principles to prevent technology from overriding defense rights.[16]Substantive examination of authenticity and relevance often becomes

[13] Citron, D. K., & Pasquale, F. (2014). The Scored Society: Due Process for Automated Predictions. Washington Law Review, 89(1), 1–33.

[14] Bian, J. L. (2022). Advancing Digital Judicial Construction Based on the Requirements of Digital *Justice.Journal of Beijing University of Aeronautics and Astronautics Social Sciences Edition*, 2022(2), p. 24.

[15] Zhang, J. H. (2025). Research on Algorithmic Black Box: A Perspective from Cognitive Science. *Studies in Science of Science*, 2025(1), 1–14.

[16] European Commission for the Efficiency of Justice (CEPEJ). (2018). Ethical Charter on the Use of Artificial Intelligence in Judicial Systems. Council of Europe. Retrieved from https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

superficial due to opacity. Even if some algorithmic models are interpretable, they may be shielded as trade or state secrets.

Currently, judicial organs can't develop smart systems on their own. They usually collaborate with enterprises via social bidding. The algorithms in these systems are core corporate competencies and trade secrets. However, there's a cognitive divide over algorithms' nature. Balancing defendants' cross - examination rights and trade secret protection requires judicial discretion.A typical case is State v. Loomis in the US. The court deemed COMPAS a commercial secret and used its risk assessment in sentencing without infringing the defendant's due process rights.[17] In China, this might be seen as violating defense rights.

On the other hand, in the field of criminal justice, the application of big data and artificial intelligence is mainly focused on the big - data-driven trial assistance and decision - support systems. The most typical application modules are case - law recommendation, sentencing assistance, and deviation early warning. These modules are widely used in the whole process of criminal trial decision - making. But in practice, the big - data intelligent assistance system may change its function and reduce the discretionary space for judges, thus weakening the defense - counsel's influence on the judge's judgment and reducing the effectiveness of defense work. It is hard enough for defense counsel to influence the judge's opinion. When the defense counsel's opinion and the algorithmic results are contradictory, it is even more difficult to achieve this goal. In this sense, this situation indirectly worsens the inequality between prosecution and defense in the cross - examination and courtroom debate.

3. The realization path of lawyers' defense rights

3.1 Improving lawyers' rights to investigation and evidence collection

3.1.1 Clarifying the cooperation obligations of network operators

Article 43 of China's Criminal Procedure Law permits defense lawyers to gather case - related materials from witnesses and other entities or individuals with their consent, and to apply to the procuratorate or court to collect evidence or summon witnesses. When conducting their own investigations, lawyers need third - party consent. In today's big data era, where information and digital technologies are deeply integrated, evidence is mostly in the form of data. However, in practice, network operators and other entities often refuse to assist lawyers in evidence collection, citing commercial secrets or personal privacy concerns.

To safeguard lawyers' evidence - collection rights, it's necessary to use legal means to clarify the scope of electronic evidence collection and delineate the boundaries between personal information protection and criminal investigation. A tiered and categorized approach can be adopted to differentiate data types and prevent conflicts between network operators' confidentiality obligations and their duty to assist. Specifically, network operators should promptly provide lawyers with information not involving personal, commercial, or national security secrets. For information that may involve personal privacy or trade secrets, network operators must state their reasons and provide relevant proof. Lawyers can only access such data with the information

[17] *Zhu, T. Z. (2018).* Uncertainty Risks of AI-Assisted Criminal Adjudication and Their Prevention: Enlightenment from the Wisconsin v. Loomis Case.*Zhejiang Social Sciences, *2018*(6), 76–85.*

owner's consent, or by applying to the court or procuratorate for evidence collection. If the data solely involves the accused's personal information or the commercial secrets of their controlled organization, lawyers' confidentiality obligations to their clients can exempt them from certain restrictions. Network operators cannot simply refuse to assist on personal or commercial secrecy grounds but must cooperate with lawyers. This aligns with China's legislative intent to protect personal and commercial secrets. For other data types, only authorized authorities have the power to collect evidence.

Besides, it is essential to clarify the legal responsibilities of network operators who obstruct lawyers' legitimate evidence - collection activities. If it is proven after the fact that a network operator or other entity has maliciously impeded a defense lawyer's evidence collection and refused to provide evidence critical to the case, the responsible parties should be held accountable through measures such as fines.

To address the technical challenges faced by defense lawyers during evidence collection, a two - pronged approach can be adopted. Firstly, professional technical tools can be integrated into the legal practice workflow. Law firms and bar associations should provide timely training to enhance lawyers' technical skills, enabling them to legally and effectively collect and manage electronic evidence related to the case. Secondly, dedicated electronic storage devices can be provided to ensure the proper preservation of data and prevent data loss due to improper evidence - collection procedures, thereby guaranteeing the smooth conduct of evidence collection and the integrity of the data.

3.1.2 Ensuring the implementation of lawyers' applications for evidence collection

When self - investigation is blocked, lawyers can apply for evidence collection. Compared with self - investigation, this option is often more feasible and has a higher likelihood of success. On the one hand, the backing of public authorities makes the relevant parties more cooperative and lends legitimacy to the evidence - collection process. However, this also means that the discretion over evidence collection is handed over to public authorities. If there is collusion between the judiciary and the prosecution to deliberately obstruct lawyers' evidence collection through various excuses and delays, lawyers' rights to evidence collection still cannot be guaranteed.

In cases where evidence is obviously favorable to the accused, the prosecution may resort to backroom operations, leading to an unequal relationship between lawyers and the prosecution. Therefore, the system of lawyers' application for evidence collection should be strengthened, and the discretion of courts and procuratorates should be reasonably restricted. Specifically, courts and procuratorates should generally agree to lawyers' applications and only reject them in exceptional circumstances. When rejecting an application, they should provide written reasons in the relevant decision for the defense lawyer's reference. This does not diminish the power of courts and procuratorates nor inappropriately expand lawyers' rights. Instead, it adds a written explanation obligation for courts and procuratorates, enhancing the rigidity of lawyers' applications for evidence collection, preventing unfounded rejections, and reducing conflicts and disputes between lawyers and procuratorates.

At the same time, lawyers must meet certain formal and substantive requirements when applying for evidence collection. The evidence to be investigated should be clearly defined, not overly broad, to allow the prosecution to make a judgment. In the context of big data, if a lawyer applies to collect electronic evidence, they should also explain the facts to be proven by such evidence and whether it involves personal information, trade secrets, or state secrets. This can alleviate the prosecution's review burden and improve efficiency.

Finally, a relief mechanism for lawyers should be established. If a lawyer's application for evidence collection is rejected, they should have the right to apply for a review to the same - level or higher - level judicial authorities. The assistance obligations of bar associations and judicial administrative organs should also be clarified. When a lawyer cannot legally conduct an investigation and collect evidence, the bar association and judicial administrative organs should communicate with courts and procuratorates to safeguard the lawyer's legal rights.

3.2 Refining lawyers' rights to access case files

3.2.1 Expand the scope of lawyers' access to case files

Databases of public security, procuratorates, courts, and other administrative agencies (e.g., financial, ecological) primarily serve the public interest and are highly public. Generally, they should be open. However, in criminal proceedings, massive data growth inevitably includes large amounts of personal and national security information. Thus, while ensuring lawyers fulfill their defense duties, we need to balance multiple interests.

In the traditional scope of case - file review, integrating new big - data - era information into the objects of lawyers' case - file review requires caution and clear boundaries and conditions. A general principle for lawyers' case - file review can be established: data that may influence judges' discretion, prove the accused's innocence or minor guilt, or record other procedural matters should, in principle, be disclosed to lawyers. If such data involves personal privacy, certain confidentiality conditions should be imposed on lawyers' access. Lawyers' case - file review should be subject to certain restrictions, but not prohibitions. These restrictions must comply with the principle of proportionality and should not disrupt main investigation activities.

As public security, procuratorate, and court data - sharing mechanisms mature, lawyers, as key legal - profession - community members, should be included. Dedicated lawyer data - access channels can be set up to offer one - stop data - sharing services. For instance, systems can be configured to automatically push case - related data and case - flow info from handling agencies to these channels. This way, upon accepting a case, lawyers can directly track case progress and access databases used by public - power organs.

On February 5, 2021, the Supreme People's Procuratorate released typical cases of procuratorates protecting lawyers' practice rights. In one case, a city's investigative body added a function to its "Integrated Application System for Law Enforcement and Case Handling." Once defense - lawyer information is entered, the system automatically informs the lawyer via text of the suspect's compulsory measures, detention location, and case transfer during the investigation phase, effectively upholding the lawyer's right to know.

Procuratorates can follow this example by creating a dedicated case - file review section in their internal systems for lawyers. Lawyers using this section must strictly keep case - related information confidential. Those violating this obligation should be promptly reported to the bar association and judicial authorities for punishment.

3.2.2 Assisting lawyers in identifying effective information

As mentioned earlier, on the one hand, there is a phenomenon of "document dumping" in the process of judicial organs providing case files to the defense, which means that a large amount of unsorted and untargeted data is provided to the defense. Given the inherent gap in data - processing capabilities between the prosecution and the defense, the risk of the prosecution leveraging its technical superiority to suppress the defense in litigation also increases. On the other hand, as the prosecution, especially prosecutors, bear the "objective duty" of going beyond the prosecutorial stance to fulfill their legal responsibilities in an objective and fair manner, they are obliged to conduct searches to identify information favorable to the accused. However, given the current surge in case numbers, even if procuratorates are assigned this duty, it is hard to ensure effective implementation in practice.

An effective solution is to involve lawyers in the process of analyzing and organizing data alongside the technical staff of procuratorates, with the latter being responsible for supervision and providing channels for this collaboration. After the relevant procedures are completed, all parties involved should sign to confirm that the prosecution has fulfilled its duty to assist.

Furthermore,lawyer’s participation also supervises the prosecution, preventing improper omissions and processing of information. This avoids judicial risks from relying solely on the prosecution's moral self - restraint. It ensures that big data analysis is used not only to collect information unfavorable to the accused but also to find information favorable to them, such as proving their innocence or minor guilt. This guarantees the impartiality and comprehensiveness of judicial procedures.

3.3 Regulating the application of algorithms in criminal proceedings

In the field of criminal justice, the rise of big data technology and the integration of artificial intelligence into criminal litigation reforms have significantly enhanced the efficiency of judicial proceedings. This advancement has actively alleviated the contradiction between the growing number of cases and the limited judicial resources. However, algorithms, which are the core of these technologies, pose risks due to their opacity and potential for bias. These issues may jeopardize the application of artificial intelligence in criminal trials and sentencing prediction. Therefore, regulating the application of algorithms in criminal proceedings is imperative.

Firstly, to ensure algorithmic transparency, the Supreme People's Court issued the "Opinion on Regulating and Strengthening the Judicial Application of Artificial Intelligence" in December 2022. It outlines five basic principles, including the "principle of transparency and trustworthiness." This requires all aspects of AI systems used in the judicial process to be open to review, assessment, and filing by relevant parties in an interpretable, testable, and verifiable manner.

Based on this, algorithms should be disclosed to defendants and their defense lawyers, and when necessary, to the public. This ensures procedural justice and upholds the procuratorate's authority and credibility. Given that public authorities often collaborate with commercial entities when adopting IT, it is essential to selectively disclose algorithms to balance the interests of all parties. Private companies developing these systems often treat algorithm design and training data as trade secrets with very limited disclosure.

Specifically, algorithms directly impacting defendants, such as those used for evidence and sentencing, must be fully disclosed to defendants and their lawyers. The prosecution should proactively share relevant algorithmic information and cannot refuse to disclose it when requested. In return, recipients of algorithmic information must undertake to use it exclusively for the relevant litigation and comply with confidentiality obligations.

Secondly, to guarantee the reliability of algorithms, first and foremost, it is essential to establish stringent admission criteria. These criteria should focus on evaluating and testing algorithms across various dimensions, including transparency, interpretability, and reliability. Any algorithm that fails to meet these standards must be barred from being utilized within the realm of criminal proceedings.

Subsequently, it is crucial to define specific technical requirements for algorithms that are to be employed in the domain of criminal proceedings. Given that algorithms operate on the foundation of data and construct models through the analysis and learning of vast amounts of data, the management and utilization of data emerge as critical factors. Beyond merely excluding algorithms that do not conform to the set standards, it is imperative to implement rigorous admission criteria for data that is to be used within the sphere of criminal proceedings. This proactive measure ensures the reliability of algorithms right from the inception.

Finally, it is imperative to define the auxiliary nature of algorithms, reducing their influence on judges' convictions and reserving space for lawyers' defense and cross - examination. As mentioned earlier, when intelligent technologies provide seemingly irrefutable arguments and reasoning, judges may fall into a state of "cognitive stinginess." This indirectly weakens the defense counsel's ability to sway the judge's conviction and diminishes the effectiveness of the defense. During the algorithm - assisted judicial adjudication process, particularly in the application of sentencing - assistance systems, algorithms should not possess mandatory features. Judges should be allotted the discretion to determine whether and to what extent they utilize algorithmic recommendations. They should also be required to provide detailed explanations in their judgments. Otherwise, should judges rely on algorithmic outcomes to achieve consistent sentencing, the defense may, over time, become a mere formality. Eventually, cold digital logic, rather than human reasoning and emotion, would influence the defendant's fate, which is contrary to the principles of criminal proceedings.

4. Conclusion

Lawyers are an essential component of the effective functioning of the defense system. The digitization of justice demands a paradigm shift in legal ethics, prioritizing equitable access to technology while safeguarding against its potential to entrench systemic inequities.[18]The right to defense is a crucial element in countering and preventing wrongful investigations and prosecutions. The development and protection of this right are vital measures for ensuring the objectivity and fairness of prosecutorial actions. In the era of big data, reforms in the criminal justice field present new challenges to the exercise of lawyers' defense rights. The double - edged

[18] Hildebrandt, M. (2016). Law as Information in the Era of Data-Driven Agency. *The Modern Law Review*, 79(1), 1–30.

sword effect of technology is becoming increasingly evident in legal practice. While technology offers the potential to enhance judicial efficiency and achieve justice, it has also, to a certain extent, intensified the inequality between the prosecution and defense.

The digital and technological divides within the prosecution - defense relationship are gradually emerging. Instead of bridging the gap between public authorities and the accused, as well as defense lawyers, new technologies represented by big data and artificial intelligence have caused a polarizing Matthew effect. This has made the prosecution - defense relationship move further away from the ideal of equal confrontation and cooperation.

This paper attempts to strengthen institutional and technical regulation to create more favorable conditions for the effective exercise of defense rights by lawyers. The goal is to promote the development of criminal justice in a more just and efficient direction. This will help ensure that every judicial case can achieve true fairness and justice with the assistance of big data. However, we are fully aware that safeguarding the right to defense and building an equal prosecution - defense relationship are long - term propositions. Finding a middle - way balance amid the intense collision of old and new elements remains a topic for future in - depth exploration.